# Exponential sums, hypergeometric sheaves, and monodromy groups

Nicholas M. Katz and Pham Huu Tiep

Department of Mathematics, Princeton University, Princeton, NJ 08544
*E-mail address*: nmk@math.princeton.edu

Department of Mathematics, Rutgers University, Piscataway, NJ 08854
*E-mail address*: tiep@math.rutgers.edu

2010 *Mathematics Subject Classification.* 11T23, 20C15, 20D06, 20C33, 20G40, 22E46

*Key words and phrases.* Local systems, Hypergeometric sheaves, Exponential sums, Monodromy groups, Finite simple groups, Weil representations

# Contents

# Introduction

The study of *exponential sums* over finite fields goes back to Gauss. The importance of estimating them goes back at least to Kloosterman's 1926 paper [**Kl**]. In the one-variable case, it was understood by Hasse and Davenport in 1934 [**HD**] that the good estimate would result from the proof of the Riemann Hypothesis for curves over finite fields. That proof was supplied by Weil in 1945 [**Weil1**]. See also Weil's 1948 paper [**Weil2**], whose Math Review was written by Kloosterman. The following year, Weil explained [**Weil3**] what should be true for projective smooth varieties of any dimension over finite fields, in what came to be known as the Weil Conjectures. The next big advance came with Grothendieck's invention, and the development by his school, of $\ell$-adic cohomology and its sheaf theoretic setting, cf. [**SGA4**, 7.2]. This setting allowed Deligne to prove the Riemann Hypothesis part of the Weil Conjectures in the general case, cf. [**De1**, 1.6]. Deligne then vastly generalized his result to the setting of *$\ell$-adic sheaves* in [**De2**, 3.3.1], and used this generalization to prove the Sato–Tate Conjecture for elliptic curves over function fields, cf. [**De2**, 3.5.7]. To do this, Deligne brings to bear the *arithmetic and geometric monodromy groups* attached to a lisse sheaf which is "pure of weight zero", and shows that determining these groups is precisely what leads to equidistribution theorems in the function field case.

At this point, let us clarify the notion of "pure of integer weight $w$" for a lisse $\overline{\mathbb{Q}_\ell}$ sheaf $\mathcal{F}$ on a smooth, geometrically connected $X/\mathbb{F}_q$. The requirement is that for **every** field embedding $\iota : \overline{\mathbb{Q}_\ell} \subset \mathbb{C}$, the following condition holds: for every finite extension $L/\mathbb{F}_q$, and every point $x \in X(L)$, the eigenvalues of $\mathsf{Frob}_{x,L}$ on $\mathcal{F}$ all have, via $\iota$, complex absolute value $(\#L)^{w/2}$. Note that if an element $\alpha \in \overline{\mathbb{Q}_\ell}$ has $|\iota(\alpha)|_{\mathbb{C}}$ independent of $\iota$, then $\alpha$ is an algebraic number, all of whose conjugates (as algebraic numbers) have the same complex absolute value as each other.

Another key output of the $\ell$-adic theory is the ability to interpret a parametrized family of exponential sums as the Frobenius traces of an $\ell$-adic sheaf on the parameter space, and to control the open set on which this sheaf is a *local system*. Moreover, the results of Weil and Deligne will ensure that this local system, after a partial Tate twist, is pure of weight zero. One then obtains equidistribution results for the family of exponential sums in question, as soon as one computes the arithmetic and geometric monodromy groups of the local system in question.

The families of exponential sums we will deal with in this book will typically have parameter space either the affine line $\mathbb{A}^1$ or the multiplicative group $\mathbb{G}_m := \mathbb{A}^1 \smallsetminus \{0\}$ over a finite field $k$, of characteristic $p > 0$. Their incarnating sheaves will be $\ell$-adic local systems on the parameter space, for any choice we like of a prime $\ell \neq p$.

Given a prime $p$, it was conjectured by Abhyankar [**Abh**] and proven by Raynaud [**Ray**] (see also [**Pop**]) that any finite group $G$ which is generated by its Sylow $p$-subgroups occurs as a quotient of the fundamental group of the affine line $\mathbb{A}^1/\overline{\mathbb{F}_p}$. The analogous result for the multiplicative group $\mathbb{G}_m$, also conjectured by Abhyankar and proven by Harbater [**Har**], is that any finite group $G$ which, modulo the subgroup $\mathbf{O}^{p'}(G)$ generated by its Sylow $p$-subgroups, is cyclic, occurs as a quotient of the fundamental group of $\mathbb{G}_m/\overline{\mathbb{F}_p}$. In the ideal world, given such a finite group $G$, and a complex representation $V$ of $G$, we would be able, for any prime $\ell \neq p$, to choose an embedding of $\mathbb{C}$ into $\overline{\mathbb{Q}_\ell}$, and to write down an explicit $\overline{\mathbb{Q}_\ell}$-local system on either $\mathbb{A}^1/\overline{\mathbb{F}_p}$ or on $\mathbb{G}_m/\overline{\mathbb{F}_p}$ whose geometric monodromy group is $G$, in the given representation.

Needless to say, we do not live in the ideal world. On $\mathbb{G}_m/\overline{\mathbb{F}_p}$, the simplest local systems are the *hypergeometric sheaves*. They are simplest in the sense that among irreducible local systems of rank $> 1$, they are characterized by having their $H^1_c$ of minimum possible dimension, namely one, cf. [**Ka-ESDE**, 8.5.3]. So it is natural to investigate their monodromy groups. A key step in this investigation is to show that monodromy groups of a wide class of hypergeometric sheaves $\mathcal{H}$ satisfy the group-theoretic *condition* (**S**+), cf. Theorem 5.2.9 for the precise statement. [Condition (**S**+) is a slight strengthening of condition ($S$) introduced in [**GT3**], and roughly speaking, corresponds to Aschbacher's class $\mathcal{S}$ of maximal subgroups of classical groups [**Asch**].] When (**S**+) holds, it imposes strong restrictions on the pair $(G_{\mathrm{geom}}, \mathcal{H})$. If $G_{\mathrm{geom}}$ is infinite, then the identity component $G^\circ_{\mathrm{geom}}$ of $G_{\mathrm{geom}}$ is a simple algebraic group, still acting irreducibly. If $G := G_{\mathrm{geom}}$ is finite, then either $G$ is *almost quasisimple* (that is, $S \lhd G/\mathbf{Z}(G) \leq \mathrm{Aut}(S)$ for some non-abelian simple group $S$), or $G$ is an "*extraspecial normalizer*", in particular, the dimension of the representation is a prime power $r^n$ and there is an extraspecial $r$-group $E$ in $G$ of order $r^{1+2n}$ acting irreducibly.

The converse question of which (complex or modular) representations of almost quasisimple groups satisfies condition (**S**) is of great importance to the Aschbacher–Scott program of classifying maximal subgroups of finite classical groups, and ultimately to primitive permutation group theory. We refer the reader to [**T**] for a detailed account of this problem. The complex representations of almost quasisimple groups that can arise in the hypergeometric context have been classified in [**KT5**], see §3.1; for these representations condition (**S**+) is established in Theorem 3.1.6. We also note that the full extraspecial normalizers in $\mathrm{GL}_{r^n}(\mathbb{C})$, respectively in $\mathrm{Sp}_{r^n}(\mathbb{C})$ or $\mathrm{O}_{r^n}(\mathbb{C})$, satisfy (**S**); see [**KlL**, Proposition 7.6.2] for the result in the more general situation of $\ell$-modular representations with $\ell \neq r$.

In studying local systems and their monodromy groups, there are two kinds of natural questions which arise. The first is this: given a simple (in the sense of simple to remember) local system, determine its monodromy group.

One of the main themes of this book, along the lines of the first kind of question, is to investigate what are arguably the simplest one-parameter families $\mathcal{F}(A, B, \chi)$ of exponential sums, those of the form

$$t \mapsto -\sum_x \psi(x^A + tx^B)\chi(x), \tag{0.0.0.1}$$

for given prime to $p$ integers $A > B > 0$ with $\gcd(A, B) = 1$, a fixed additive character $\psi$, and a given multiplicative character $\chi$? It turns out that these families are Kummer pullbacks of hypergeometric sheaves, cf. Theorem 10.1.1. This relation allows us, in §§10.2, 10.3, to completely determine their monodromy groups. In turn, building on these one-parameter results, in Chapter 11 we complete the classification of all multi-parameter families

$\mathcal{F}(A, B_1, \ldots, B_r, \chi)$ of exponential sums

$$(0.0.0.2) \qquad (t_1, t_2, \ldots, t_r) \mapsto -\sum_x \psi(x^A + t_1 x^{B_1} + \ldots + t_r x^{B_r})\chi(x)$$

that admit finite monodromy, and the determination of the corresponding geometric monodromy groups $G_{\rm geom}$.

The second kind of natural question is this: given a finite group $G$ together with a faithful irreducible representation $V$ satisfying (**S**+), construct a simple (again, in the sense of simple to remember) local system whose monodromy is $(G, V)$, if such a local system exists. This second question, when $G$ is almost quasisimple, has already been the subject of a number of papers by the authors, some jointly with Antonio Rojas-León, cf. the Bibliography. Investigation of the other (**S**+) case, when $G$ is an extraspecial normalizer, is a second main theme of this book.

Let us now turn to a more detailed description of the contents of this book. We work with geometrically irreducible hypergeometric sheaves $\mathcal{H}$ on $\mathbb{G}_m$, i.e., those that are lisse on $\mathbb{G}_m$ and whose $G_{\rm geom}$ acts irreducibly. At the possible expense of interchanging 0 and $\infty$ on $\mathbb{G}_m$ by inversion, we may and will assume $\mathcal{H}$ is of type $(D, m)$ with $D > m$. One knows [**Ka-ESDE**, 8.4.11] that if $G_{\rm geom}$ is finite, then a generator of local monodromy at 0 is an element of $G_{\rm geom}$ which has all distinct eigenvalues in the given representation (a *simple spectrum element*). In general, such a generator has *regular spectrum*, in the sense of Definition 1.1.5.

Our first main result, Theorem 2.4.4, shows that if such a sheaf $\mathcal{H}$ in characteristic $p$ has wild part of dimension $1 \leq w < (p-1)/2$, then its geometric monodromy group $G_{\rm geom}$ is either infinite, or finite but imprimitive (unless $\mathcal{H}$ has rank 2 and $p = 5$). This result can be viewed as a hypergeometric version of the celebrated result [**FT**] of Feit and Thompson on linear groups of degree $< (p-1)/2$.

Building on [**KT5**, Theorem 7.4], our Theorem 3.1.10 shows that if $D \geq 11$ and $\mathcal{H}$ has a finite geometric monodromy group $G_{\rm geom}$ which is almost quasisimple of Lie type in some characteristic $r$, then the characteristic of $\mathcal{H}$ must necessarily be $r$, aside from three exceptions for $D = 12$ and $D = 14$. A similar result for hypergeometric sheaves with $G_{\rm geom}$ an extraspecial normalizer was established in [**KT5**, Theorem 9.19].

Our next result, Theorem 3.3.4, extending prior work of Howe [**HS**, Theorem 4.6.3], gives a full classification of representations of (not necessarily connected) simple algebraic groups that admit elements with regular spectrum.

The next main result, Theorem 5.2.9, vastly generalizing earlier related results in [**KT5**], shows that any geometrically irreducible hypergeometric sheaf of type $(D, m)$ with $D > m$ satisfies (**S**+), as long as it is primitive and has rank $\neq 4, 8, 9$.

In Chapter 6, we determine, in Theorem 6.2.14, the possible identity component $G^\circ_{\rm geom}$ of $G_{\rm geom}$ for a hypergeometric sheaf $\mathcal{H}$ of type $(D, m)$ with $D > m$ satisfying (**S**+) whose $G_{\rm geom}$ is infinite. Recall from [**GT3**, Proposition 2.8] that (**S**+) (which by Theorem 5.2.9 is automatic so long as $D \neq 4, 8, 9$ and $\mathcal{H}$ is primitive) implies that $G^0_{\rm geom}$ is a simple algebraic group acting irreducibly. In [**Ka-ESDE**, 7.2.7], it is proved that in *sufficiently large* (depending on $w := D - m$) characteristic $p$, the only such possibilities for the given representation of $G^0_{\rm geom}$ are either one of the classical groups $\mathrm{SL}_D$, $\mathrm{SO}_D$, or $\mathrm{Sp}_D$ for even $D$, in the standard $D$-dimensional representation or its dual, or $G_2$ in its 7-dimensional representation, or $\mathrm{SL}_3$

in its 8-dimensional adjoint representation, or $\mathrm{Spin}_7$ in its 8-dimensional spin representation. Removing the constraint on size of the characteristic $p$, Theorem 6.2.14, shows that, aside from a few possible low-rank exotic exceptions in characteristic $p = 2, 3$, these are the only possibilities.

Chapter 7 is devoted to the study of the extraspecial normalizer case in odd characteristic, with Theorem 7.3.5 as the principal result. Perhaps not surprisingly, the study of the extraspecial normalizer case in characteristic $p = 2$ is hugely more complicated, and takes up Chapters 8 and 9. Among other results, in parallel with the approach of [**KT7**], we are able to realize in Theorem 9.1.11 the extraspecial normalizers $2^{1+2nf}_{+} \cdot \Omega^{+}_{2n}(2^f)$ as geometric monodromy groups of hypergeometric sheaves, whereas type $-$ extraspecial normalizers $2^{1+2nf}_{-} \cdot \Omega^{-}_{2n}(2^f)$ are realized in Theorem 8.5.5 following the approach of [**KT6**]. Furthermore, a novel use of Witt vectors allows us to produce, for the first time, explicit local systems with geometric monodromy groups of shape $(4 * 2^{1+2nf}_{-}) \cdot \mathrm{Sp}_{2n}(2^f)$, see Theorem 9.3.9.

Chapter 10 is devoted to computing the monodromy groups of the one-parameter families $\mathcal{F}(A, B, \chi)$ in (0.0.0.1). The main results are Theorems 10.2.4 and 10.2.7 (for exponents $A > B = 1$), and Theorems 10.3.13, 10.3.14, and 10.3.21 (for exponents $A > B > 1$). In particular, the list of $(A, \chi)$ for which the local system $\mathcal{F}(A, 1, \chi)$ in (0.0.0.1) has finite monodromy, previously conjectured in [**KT1**] and [**R-L**], is proved to be complete. We also show (see Lemmas 10.3.15, 10.3.16,10.3.17, and 10.3.18) that the exotic possibilities for $p = 2, 3$ in Theorem 6.2.14 do not occur in the context of the one-parameter systems $\mathcal{F}(A, B, \chi)$. Multi-parameter analogues of these results for the families $\mathcal{F}(A, B_1, \dots, A_r, \chi)$ in (0.0.0.2) are obtained in Chapter 11.

Chapter 12 is devoted to treating some of the very few cases of families with *non-monomal* perturbing terms where we can say anything at all. This is very much an area in which much remains to be done. The proofs of the main results in this chapter, Theorems 12.2.3 and 12.3.6, once again highlight the importance of the moment $M_{2,2}$ in the study of the $G_{\mathrm{geom}}$ of local systems. In addition, Theorems 12.5.4, 12.5.5, 12.5.11, and 12.5.12 determine geometric monodromy groups for some special classes of two-parameter local systems with non-monomial coefficients. This theme will be further explored in the forthcoming paper [**KT8**].

The appendices consist of two Magma programs.

A word about notation. Throughout the book, we use $\mathcal{F}$ for a local system which is pure of some integer weight, and we use $\mathcal{G}$ to denote a suitable constant field twist of $\mathcal{F}$ which is pure of weight zero. The two are geometrically isomorphic, so have the same geometric monodromy group $G_{\mathrm{geom}}$, but their arithmetic monodromy groups $G_{\mathrm{arith},\mathcal{F}}$ and $G_{\mathrm{arith},\mathcal{G}}$ may differ. [They will coincide if $\mathcal{F}$ is itself pure of weight zero and we take $\mathcal{G} := \mathcal{F}$.] When $\mathcal{F}$ has nonzero weight, the group $G_{\mathrm{arith},\mathcal{F}}$ is never finite, indeed never has a semisimple identity component, simply because its determinant is pure of nonzero weight. It is only $G_{\mathrm{arith},\mathcal{G}}$ which can ever be finite.

CHAPTER 1

# The basic (S−), (S), and (S+) settings

## 1.1. Conditions (S−), (S), and (S+) for local systems

We work over an algebraically closed field $\mathbb{C}$ of characteristic zero, which we will take to be $\overline{\mathbb{Q}_\ell}$ for some prime $\ell$ in the rest of this book. Given a nonzero finite-dimensional $\mathbb{C}$-vector space $V$ and a Zariski closed subgroup $G \leq \mathrm{GL}(V)$, recall from [**GT3**, 2.1] that $G$ (or more precisely the pair $(G, V)$) is said *to satisfy condition* (**S**) if each of the following four conditions is satisfied.

(i) The $G$-module $V$ is irreducible.
(ii) The $G$-module $V$ is primitive.
(iii) The $G$-module $V$ is tensor indecomposable.
(iv) The $G$-module $V$ is not tensor induced.

We also say that $G$, or the pair $(G, V)$, *satisfies condition* (**S**−), if it fulfills (i), (ii), and (iii).

We have the following two elementary but useful lemmas.

Lemma 1.1.1. *Suppose that $H \leq G \leq \mathrm{GL}(V)$ and $G, H$ are both Zariski closed. If $(H, V)$ satisfies* (**S**) *(respectively satisfies* (**S**−)*), then $(G, V)$ satisfies* (**S**) *(respectively satisfies* (**S**−)*).*

Proof. Immediate from the definitions. □

Lemma 1.1.2. *Suppose that $G \leq \mathrm{GL}(V)$ is Zariski closed, irreducible and primitive, and that $\dim(V)$ is a prime number. Then $(G, V)$ satisfies* (**S**).

Proof. Indeed, conditions (iii) and (iv) are automatic. □

Lemma 1.1.3. [**KT5**, Lemma 1.1] *Suppose $1 \neq G \leq \mathrm{GL}(V)$ is a Zariski closed, irreducible subgroup. Then the following statements holds.*

(i) *If $G$ satisfies* (**S**), $\dim(V) > 1$, *and $\mathbf{Z}(G)$ is finite, then we have three possibilities:*
  (a) *The identity component $G^\circ$ is a simple algebraic group, i.e. $G^\circ$ has no nontrivial connected normal Zariski closed subgroups, and $V|_{G^\circ}$ is irreducible.*
  (b) *$G$ is finite, and almost quasisimple, i.e. there is a finite non-abelian simple group $S$ such that $S \lhd G/\mathbf{Z}(G) < \mathrm{Aut}(S)$.*
  (c) *$G$ is finite and it is an "extraspecial normalizer" (in characteristic $r$), that is, $\dim(V) = r^n$ for a prime $r$, and $G$ contains a normal $r$-subgroup $R = \mathbf{Z}(R)E$, where $E$ is an extraspecial $r$-group $E$ of order $r^{1+2n}$ acting irreducibly on $V$, and either $R = E$ or $\mathbf{Z}(R) \cong C_4$.*

(ii) $\mathbf{Z}(G)$ *is finite if and only if* $\det(G)$ *is finite.*

Definition 1.1.4. A pair $(G, V)$ is said *to satisfy the condition* (**S**+), if it satisfies (**S**) and, in addition, $|\mathbf{Z}(G)|$ is finite (equivalently, $\det(G)$ is finite). More generally, if $\Gamma$ is any group given with a finite-dimensional representation $\Phi : \Gamma \to \mathrm{GL}(V)$, then we say $(\Gamma, V)$ *satisfies* (**S**+), if $(\Phi(\Gamma), V)$ satisfies the three conditions of (**S**) and, in addition, $\det(\Phi(\Gamma))$ is finite.

DEFINITION 1.1.5. Given a group $G$, an element $g \in G$ and a a finite dimensional representation $\Phi : G \to \mathrm{GL}(V)$ over $\mathbb{C}$, we say that

(a) $g$ has *simple spectrum* on $V$, or $g$ is an ssp-*element on* $V$, if $\Phi(g)$ is diagonalizable and has pairwise distinct eigenvalues on $V$;
(b) $g$ has *almost simple spectrum* on $V$, or $g$ is an asp-*element on* $V$, if $\Phi(g)$ is diagonalizable and has at least $\dim(V) - 1$ pairwise distinct eigenvalues on $V$;
(c) $g$ is an m2sp-*element on* $V$, if $\Phi(g)$ is diagonalizable and each of its eigenvalues on $V$ has multiplicity $\leq 2$;
(d) $g$ has *regular spectrum* on $V$, if for any $\lambda \in \mathbb{C}$, $\dim \mathrm{Ker}(\Phi(g) - \lambda \cdot \mathrm{Id}) \leq 1$, equivalently, $\Phi(g)$ has at most one Jordan block with eigenvalue $\lambda$ for any $\lambda \in \mathbb{C}$; and
(e) $g$ has *almost regular spectrum* on $V$, if $V$ decomposes as the sum $V_0 \oplus V_1$ of $\Phi(g)$-invariant subspaces, $\dim V_0 \leq 1$, and $g$ has regular spectrum on $V_1$.

In a perhaps unfortunate terminology due to Sylvester [**Syl1**], an element $g \in \mathrm{GL}(V)$ with regular spectrum is also called "non-derogatory". Such an element is regular in the sense that its centralizer in $\mathrm{GL}(V)$ has smallest possible dimension, and this is the reason behind our term "regular spectrum".

The relevance of Definition 1.1.5 to the study of monodromy groups of hypergeometric sheaves is explained in Proposition 2.4.3 (below). Let us also recall two elementary results.

LEMMA 1.1.6. [**GT3**, Lemma 2.5] *Given a Zariski closed subgroup $G \subset \mathrm{GL}(V)$ and a Zariski closed normal subgroup $H \lhd G$, suppose that $(G, V)$ satisfies* (**S**−). *Then either $H \leq \mathbf{Z}(G)$ or $V|_H$ is irreducible.*

LEMMA 1.1.7. [**KT5**, Lemma 1.6] *Let $\Gamma$ be a group, $\mathbb{C}$ an algebraically closed field of characteristic zero, $n \in \mathbb{Z}_{\geq 1}$, $\Phi : \Gamma \to \mathrm{GL}_n(\mathbb{C}) = \mathrm{GL}(V)$ a representation of $\Gamma$, and $G \leq \mathrm{GL}(V)$ the Zariski closure of $\Phi(\Gamma)$. Then $(\Gamma, V)$ satisfies* (**S**+) *if and only if $(G, V)$ satisfies* (**S**+). *This equivalence holds separately for each of the four conditions defining* (**S**+).

To prove an analogue of Lemma 1.1.3 for groups satisfying (**S**−), first we need the following result on $p$-groups:

LEMMA 1.1.8. *Let $p$ be a prime and let $P$ be a finite $p$-group. Suppose that every characteristic abelian subgroup of $P$ is cyclic, and also central if $p = 2$. Then $P = E * C$ is a central product of subgroups $E$ and $C$, where $E = 1$ or $E$ is an extraspecial $p$-group, and $C = \mathbf{Z}(P)$ is cyclic.*

PROOF. By Hall's theorem, see e.g. [**Gor**], we have that $P = E * X$ is a central product, where $E = 1$ or $E$ is an extraspecial $p$-group, and either $X$ is cyclic, or $p = 2$ and $X$ is either a dihedral group

$$D_{2^m} = \langle x, y \mid x^{2^{m-1}} = y^2 = 1, yxy^{-1} = x^{-1} \rangle,$$

a generalized quaternion group

$$Q_{2^m} = \langle x, y \mid x^{2^{m-2}} = y^2, y^4 = 1, yxy^{-1} = x^{-1} \rangle,$$

or a semi-dihedral group

$$SD_{2^m} = \langle x, y \mid x^{2^{m-1}} = y^2 = 1, yxy^{-1} = x^{-1+2^{m-2}} \rangle,$$

of order $2^m \geq 16$. In either case, $\mathbf{Z}(P) = \mathbf{Z}(E) * \mathbf{Z}(X)$ is characteristic abelian in $P$, hence cyclic by assumption, and $\mathbf{Z}(E)$ has order 1 or $p$. Hence we are done if $p > 2$ or if $p = 2$ but $X$ is cyclic (taking $C := X$).

Assume now that $p = 2$, but $X$ is non-cyclic. In the above notation, $\mathbf{Z}(X) = \langle x^{2^{m-2}} \rangle \cong C_2$, hence $\mathbf{Z}(P) = \mathbf{Z}(X) \geq \mathbf{Z}(E)$. Note that $P/\mathbf{Z}(P) = E/\mathbf{Z}(E) \times X/\mathbf{Z}(X)$, where $X/\mathbf{Z}(X)$ is dihedral of order $2^{m-1}$, with center $\langle x^{2^{m-3}} \rangle/\mathbf{Z}(X)$. Now, if $Q$ denotes the full inverse image of $\mathbf{Z}(P/\mathbf{Z}(P))$ in $P$, so that $Q/\mathbf{Z}(P) = \mathbf{Z}(P/\mathbf{Z}(P)) \cong E/\mathbf{Z}(E) \times \mathbf{Z}(X/\mathbf{Z}(X))$, then $Q = E * \langle x^{2^{m-3}} \rangle$. Thus $\mathbf{Z}(Q) = \langle x^{2^{m-3}} \rangle \cong C_4$ is characteristic abelian, however not central in $Q$, a contradiction. □

LEMMA 1.1.9. *Let $1 \neq G \leq \mathrm{GL}(V)$ be a Zariski closed, irreducible subgroup. Suppose that $G$ satisfies* ($\mathbf{S}-$), $\dim(V) > 1$, *and $\mathbf{Z}(G)$ is finite. Then we have three possibilities:*

(a) *The identity component $G^\circ = L_1 * L_2 * \ldots * L_n$ is a central product of simple algebraic groups, which are permuted transitively by $G$ via conjugation, and $V|_{G^\circ}$ is irreducible.*

(b) *$G$ is finite, $F^*(G) = \mathbf{Z}(G)E(G)$, $E(G) = L_1 * L_2 * \ldots * L_n$ is a central product of quasisimple groups which are permuted transitively by $G$ via conjugation, and $V|_{E(G)}$ is irreducible.*

(c) *$G$ is finite and it is an extraspecial normalizer in characteristic $r$, i.e.* $\dim(V) = r^n$ *for a prime $r$, and $G$ contains a normal $r$-subgroup $R = \mathbf{Z}(R)E$, where $E$ is an extraspecial $r$-group $E$ of order $r^{1+2n}$ acting irreducibly on $V$, and either $R = E$ or $\mathbf{Z}(R) \cong C_4$. Furthermore, $R/\mathbf{Z}(R) = \mathbf{O}_r(G/\mathbf{Z}(G))$ is the unique minimal normal subgroup of $G/\mathbf{Z}(G)$, and $G/\mathbf{Z}(G)R$ embeds in* $\mathrm{Sp}_{2n}(r)$.

PROOF. (i) By Lemma 1.1.3(ii), $\det(G)$ is finite. Now we can apply the arguments in the proof of [**GT3**, Proposition 2.8] to $G$. Suppose $G^\circ \neq 1$. Then $G^\circ$ is semisimple, and so $G^\circ = L_1 * L_2 * \ldots * L_n$ is a central product of simple algebraic groups. Now, $G$ permutes $L_1, L_2, \ldots, L_n$ via conjugation. If this action is not transitive, then we can write $G^\circ = A * B$, where $A$ is the product of the $L_i$'s belonging to one $G$-orbit, and $B$ is the product of the rest. Furthermore, $A, B \lhd G$ and $A, B \not\leq \mathbf{Z}(G)$. Hence $A$ and $B$ are irreducible on $V$ by Lemma 1.1.6, and so $B \leq \mathbf{Z}(G)$ by Schur's lemma, leading to a contradiction. Thus (a) holds if $G^\circ \neq 1$.

(ii) We will now assume that $G$ is finite. As $\dim(V) > 1$, $G > \mathbf{Z}(G)$. Let $\bar{L}$ be a minimal normal subgroup of $G/\mathbf{Z}(G)$. Suppose $\bar{L}$ is non-abelian. Then the arguments in part 2) of the proof of [**GT3**, Proposition 2.8] show that $\bar{L}$ is the unique minimal normal subgroup of $G/\mathbf{Z}(G)$, and $K = L_1 * L_2 * \ldots * L_n$ is a central product of quasisimple groups which are permuted transitively by $G$ via conjugation, if $K = L^{(\infty)}$ and $L$ is the full inverse image of $\bar{L}$ in $G$. The uniqueness of $\bar{L}$ implies that $E(G) = K$, and that $F^*(G) = \mathbf{Z}(G)E(G)$. Furthermore, $V|_{E(G)}$ is irreducible by Lemma 1.1.6, and so (b) holds.

(iii) Suppose now that $\bar{L}$ is an (elementary) abelian $r$-subgroup for a prime $r$, and let $L$ be the full inverse image of $\bar{L}$ in $G$. Then $[L, L] \leq \mathbf{Z}(G)$, whence $L$ is nilpotent and so we can write $L = \mathbf{O}_{r'}(\mathbf{Z}(G)) \times L_1$ for an $r$-subgroup $L_1 \lhd G$. As $L \lhd G$ and $L \not\leq \mathbf{Z}(G)$, $V$ is irreducible over $L$ by Lemma 1.1.6, and so over $L_1$ as well; in particular, $L_1$ is non-abelian.

Since $\dim(V) > 1$, Lemma 1.1.6 implies that any characteristic abelian subgroup of $L_1$ is contained in $\mathbf{Z}(G)$, and so is cyclic and central in $L_1$. By Lemma 1.1.8, $L_1 = E_1 * L_2$, where $E_1$ is extraspecial and $L_2 = \mathbf{Z}(L_1)$ is cyclic.

For any $x, y \in L_1$, we have $x^r \in \mathbf{Z}(G)$ and $[x,y] \in \mathbf{Z}(G)$, whence $[x,y]^r = [x^r, y] = 1$. The latter implies by [**KS**, 5.3.4(b)] that $(xy)^r = x^r y^r$ when $r > 2$ and $(xy)^4 = x^4 y^4$ when $r = 2$. Setting $r' = r$ if $r > 2$ and $r' = 4$ if $r = 2$, we then see that

$$R := \{x \in L_1 \mid x^{r'} = 1\} \tag{1.1.9.1}$$

is a characteristic *subgroup* of $L_1$; in particular, $R \lhd G$. Note that $E_1 \neq 1$ is a central product of extraspecial $r$-group of order $r^3$ and so it contains non-central elements of order $r'$ (see e.g. [**KS**, p. 115]), and thus $R \not\leq \mathbf{Z}(G)$. By Lemma 1.1.6, $V|_R$ is irreducible, and any characteristic abelian subgroup of $R$ is cyclic and central. Again applying Lemma 1.1.8, we obtain that $R = E * C$, where $E$ is extraspecial and $C$ is cyclic. Moreover, $\exp(R)|r'$ by (1.1.9.1), and so $\mathbf{Z}(R) \leq \mathbf{Z}(G)$ is cyclic of order dividing $r'$. It follows that either $R = E$, or $r = 2$ and $C \cong C_4$, i.e. the first statement in (c) holds.

Next, $\mathbf{Z}(R) = R \cap \mathbf{Z}(G) = R \cap \mathbf{Z}(L_1)$, and so $1 \neq R/\mathbf{Z}(R) \hookrightarrow L_1/\mathbf{Z}(L_1) = L/\mathbf{Z}(L) = \bar{L}$. The minimality of $\bar{L}$ then implies that $\bar{L} = R/\mathbf{Z}(R)$. By Schur's lemma, $\mathbf{C}_G(R) = \mathbf{Z}(G)$, so $\bar{G} := G/\mathbf{Z}(G)$ embeds in

$$\mathrm{Aut}_0(R) := \{f \in \mathrm{Aut}(R) \mid f \text{ acts trivially on } \mathbf{Z}(R)\}.$$

According to [**Gri**] (for $r = 2$) and [**Wi**] (for $r > 2$), $\mathrm{Aut}_0(R)$ contains the normal subgroup $\bar{L}$ of all inner automorphisms of $R$ and $\mathrm{Aut}_0(R)/\bar{L} \hookrightarrow \mathrm{Sp}(\bar{L}) \cong \mathrm{Sp}_{2n}(r)$, and thus $G/\mathbf{Z}(G)R \hookrightarrow \mathrm{Sp}_{2n}(r)$. The minimality of $\bar{L}$ implies that $G/\mathbf{Z}(G)R$ acts irreducibly on $\bar{L}$. Next, $\bar{L} \leq \mathbf{O}_r(\bar{G})$, and the $r$-group $\mathbf{O}_r(\bar{G})/\bar{L} < \mathrm{Sp}(\bar{L})$ acting on the $\mathbb{F}_r$-space $\bar{L}$ must have a nonzero fixed point subspace $\bar{X}$ which is $G$-invariant. Hence $\bar{X} = \bar{L}$ by irreducibility, and so $\bar{L} = \mathbf{O}_r(\bar{G})$. Finally, if $\bar{M}$ is any minimal normal subgroup of $\bar{G}$, then the preceding arguments imply that $\bar{M}$ is abelian and equal to $\mathbf{O}_r(\bar{G})$, completing the proof of (c). □

For later use, we prove another result on $p$-groups:

PROPOSITION 1.1.10. *Let $p$ be a prime, $V = \mathbb{C}^n$ with $n > 1$, and let $P \leq \mathrm{GL}(V)$ a finite irreducible $p$-group. Let $\chi$ denote the character of $G$ on $V$. Suppose that every characteristic abelian subgroup of $P$ is central in $P$. Then the following statements hold.*

(i) *$n = p^m$ for some $m \in \mathbb{Z}_{\geq 1}$, $P = E * C$ is a central product of subgroups $E$ and $C$, where $E$ is an extraspecial $p$-group of order $p^{1+2m}$, and $C = \mathbf{Z}(P)$ is cyclic.*

(ii) *If $h \in \mathrm{GL}(V)$ has finite $p'$-order and $h$ normalizes $P$, then the order $M$ of the automorphism $f$ of $P$ induced by $h$ is less than $p^{m+1}/(p-1)$.*

(iii) *Suppose $k \in \mathbb{Z}_{\geq 1}$ and $p \nmid k$. Then $\mathrm{Sym}^k(\chi)$ is a multiple of an irreducible character of degree $p^m$ of $P$. If in addition $1 \leq k \leq n-1$, the same statement holds for $\wedge^k(\chi)$.*

(iv) *Suppose $k \in \mathbb{Z}_{\geq 1}$ and $p|k$. Then $\mathrm{Sym}^k(\chi)$ contains at least $N$ distinct linear characters of $P$, where $N := p^{2m} - 1$ if $p > 2$ and $N := 2^{m-1}(2^m + 1)$ if $p = 2$. If in addition $2 \leq k \leq n-2$, the same statement holds for $\wedge^k(\chi)$, with $N := p^{2m} - 1$ if $p > 2$ and $N := 2^{m-1}(2^m - 1)$ if $p = 2$.*

PROOF. (i) Since $P$ is irreducible, $\mathbf{Z}(P)$ is cyclic, and by hypothesis every characteristic abelian subgroup of $P$ is cyclic. Hence $P = E * C$, with $E$ and $C$ as described in Lemma 1.1.8. Now $V|_E$ is irreducible, so $|E| = p^{1+2m}$ with $n = p^m$.

(ii) Note that $\exp(E) = p$ or $p^2$. Setting

$$P_2 := \{x \in P \mid x^{p^2} = 1\},\ C_2 := \Omega_2(C) := \{z \in C \mid z^{p^2} = 1\},$$

we then see that $P_2 = \{xz \mid x \in E, z \in C_2\}$, whence $P_2 = E * C_2$ is a characteristic *subgroup* of $P$, of exponent $p$ or $p^2$. As $P_2 \geq E$ is irreducible on $V$, $h$ centralizes $\mathbf{Z}(P_2) < \mathbf{Z}(\mathrm{GL}(V))$, so $f|_{P_2}$ belongs to

$$\mathrm{Aut}_0(P_2) = \{y \in \mathrm{Aut}(P_2) \mid y \text{ acts trivially on } \mathbf{Z}(P_2)\}.$$

Moreover, if $f^j$ acts trivially on $P_2$, then $h^j \in \mathbf{C}_{\mathrm{GL}(V)}(P_2) = \mathbf{Z}(\mathrm{GL}(V))$, and so $h^j$ centralizes $P$ as well. Thus $f$ and $f|_{P_2}$ have the same order $M$.

Note that $x^p, [x,y] \in \mathbf{Z}(P_2)$ for all $x, y \in P_2$, and so $[x,y]^p = 1$ . Hence the commutator map $(x,y) \mapsto [x,y]$ induces a non-degenerate symplectic bilinear form on $P_2/\mathbf{Z}(P_2) \cong E/\mathbf{Z}(E) \cong \mathbb{F}_p^{2m}$, taking values in $\Omega_1(\mathbf{Z}(P_2)) := \{z \in \mathbf{Z}(P_2) \mid z^p = 1\} \cong \mathbb{F}_p$. Certainly, $h$ acts on $P_2/\mathbf{Z}(P_2)$ preserving the form, and $h$ acts trivially on $\mathbf{Z}(P_2)$. If some power $h^j$ acts trivially on $P_2/\mathbf{Z}(P_2)$, then, since $p \nmid \mathsf{o}(h)$, we have that $h^j$ centralizes $P$ by [**KS**, 8.2.2]. Thus $M$ is equal to the order of the map in $\mathrm{Sp}(P_2/\mathbf{Z}(P_2))$ induced by $f$. In particular, $M \leq \mathrm{meo}(\mathrm{Sp}_{2m}(p))$, whence $M < p^{m+1}/(p-1)$ by [**GMPS**, Table 3].

(iii) As $E$ is extraspecial, $\mathbf{Z}(E) = \langle \boldsymbol{z} \rangle \cong C_p$, and we may assume $\boldsymbol{z}$ acts on $V$ as $\zeta_p \cdot \mathrm{Id}$. Now, given $p \nmid k$, we see that $\boldsymbol{z}$ acts as the scalar $\zeta_p^k \neq 1$ on $V^{\otimes k}$. Thus, any irreducible constituent of the $E$-character afforded by $V^{\otimes k}$ lies above the character $\boldsymbol{z} \mapsto \zeta_p^k$ of $\mathbf{Z}(E)$, and the extraspecial $p$-group $E$ has a unique such irreducible character, which has degree $p^m$. As both $\mathrm{Sym}^k(V)$ and $\wedge^k(V)$ are inside $V^{\otimes k}$, the statement follows for $E$, and hence for $P = E * C$ (as $C$ acts via scalars on $V$).

(iv) Denote $\Sigma := \mathrm{Sym}$ or $\wedge$, and assume $1 \leq k \leq n-1$ when $\Sigma = \wedge$. It is well-known that $\Sigma^k(V)$ is a nontrivial irreducible module for $\mathrm{SL}(V)$. As $\mathrm{GL}(V) = \mathbf{Z}(\mathrm{GL}(V))\mathrm{SL}(V)$ and $\mathrm{SL}(V)/\mathbf{Z}(\mathrm{SL}(V))$ is simple, the only elements of $\mathrm{GL}(V)$ that can act via scalars on $\Sigma^k(V)$ are the ones in $\mathbf{Z}(\mathrm{GL}(V))$. It follows that $\Sigma^k(\chi)$ cannot be a multiple of a single linear character of $P$. As $p|k$ in this case, the generator $\boldsymbol{z}$ of $\mathbf{Z}(E)$ acts as $\zeta_p^p = 1$ on $V^{\otimes k}$, and thus the character of $E$ on $V^{\otimes k}$ is a sum of $p^{mk}$ linear characters. The previous observation implies that $\wedge^k(\chi)|_E$ must contain at least two distinct linear characters. Since $P = E * C$ with $C < \mathrm{GL}(V)$, $\Sigma^k(\chi)$ must contain at least two distinct linear characters, say $\alpha$ and $\beta$, with $\alpha|_E \neq \beta|_E$.

First we consider the case $p > 2$. Denoting $D := \langle \zeta_{p^2} \cdot \mathrm{Id} \rangle < \mathbf{Z}(\mathrm{GL}(V))$, one readily check that $E * D = P_2 * D = E^+ * D$, where $E^+ \cong p_+^{1+2m}$ is extraspecial of exponent $p$. Extending $\alpha$ to $P_2 * D$, we may assume that $\alpha|_{E^+}$ is nontrivial. It is well-known that

$$\mathbf{N}_{\mathrm{GL}(V)}(E^+) = \mathbf{Z}(\mathrm{GL}(V))E^+ \rtimes \mathrm{Sp}_{2m}(p),$$

and $\mathrm{Sp}_{2m}(p)$ has two orbits on $\mathrm{Irr}(E^+/\mathbf{Z}(E^+))$: $\{1_{E^+}\}$, and one of length $p^{2m}-1$. Also, $\mathbf{Z}(E^+) = \mathbf{Z}(E)$ acts trivially on $V^{\otimes k}$. Since $\mathbf{N}_{\mathrm{GL}(V)}(E^+)$ also acts on $\wedge^k(V)$, Clifford's theorem implies that $\Sigma^k(\chi)|_{E^+}$ contains the $\mathbf{N}_{\mathrm{GL}(V)}(E^+)$-orbit $\mathcal{O}$ of $\alpha|_{E^+}$ which has length $p^{2m}-1$.

Now we can write every element $g \in P_2$ (not uniquely) as $g = xd$ with $x \in E^+$ and $d \in D$. Then $d$ acts on $\Sigma^k(V)$ as $\mu(d)$, where $\mu \in \mathrm{Irr}(D)$ and $\mu(\zeta_{p^2} \cdot \mathrm{Id}) = \zeta_{p^2}^k$. For each $\lambda \in \mathcal{O}$, the $E^+$-eigenspace $W_\lambda$ in $\Sigma^k(V)$ that corresponds to $\lambda$ is invariant under $P_2$, and $g$ acts on this subspace as the scalar $\lambda(x)\mu(d)$. If these actions of each $g \in P_2$ are the same on $W_\lambda$ and $W_{\lambda'}$ for $\mathcal{O} \ni \lambda' \neq \lambda$, then $\lambda(x) = \lambda'(x)$, a contradiction because $E^+ \leq P_2 D$. Hence, $\Sigma^k(\chi)$ must contain at least $|\mathcal{O}| = p^{2m} - 1$ distinct linear characters of $P_2$, whence the statement follows for $P$.

Next we consider the case $p = 2$. It is well known, see e.g. [**Gri**], that either

$$P_2 = E = 2^{1+2m}_\epsilon \text{ for some } \epsilon = \pm \;\text{ and }\; \mathbf{N}_{\mathrm{GL}(V)}(P_2) = \mathbf{Z}(\mathrm{GL}(V))P_2 \cdot \mathrm{O}^\epsilon_{2m}(2),$$

or

$$P_2 = E * C_4 \text{ and } \mathbf{N}_{\mathrm{GL}(V)}(P_2) = \mathbf{Z}(\mathrm{GL}(V))P_2 \cdot \mathrm{Sp}_{2m}(2).$$

Choose $\kappa = +$ if $\Sigma = \mathrm{Sym}$ and $\kappa = -$ if $\Sigma = \wedge$. Since $C_4$ acts via scalars on $\Sigma^k$, arguing as above, we see that it suffices to show that $\Sigma^k(\chi)$ contain at least $N$ distinct linear characters for $C_4 * E$. Repeating the argument and using $C_4 * E = C_4 * E^\kappa$, we see that it suffices to show that $\Sigma^k(\chi)$ contains at least $N$ distinct linear characters for $E^\kappa = 2^{1+2m}_\kappa$. Note that the representation of $E^\kappa$ on $V$ is orthogonal if $\kappa = +$, and symplectic if $\kappa = -$. Moreover, the contraction map shows that $\Sigma^k(V)$ contains $\Sigma^{k-2}(V)$ as modules over $\mathrm{O}(V)$, respectively over $\mathrm{Sp}(V)$, see [**OV**, Table 5]. As $2|k \geq 2$, it suffices to prove the statement for $k = 2$. Now, $V^{\otimes 2} = \mathrm{Sym}^2(V) \oplus \wedge^2(V)$ affords the regular character of $E^\kappa/\mathbf{Z}(E^\kappa)$, which breaks into three $\mathbf{N}_{\mathrm{GL}(V)}(E^\kappa)$-orbits: $\{1_{E^\kappa}\}$, one of length $2^{m-1}(2^m - \kappa)$, and another, say $\mathcal{O}$, of length $(2^{m-1} + \kappa)(2^m - \kappa)$. By the choice of $\kappa$, $\Sigma^2(\chi)|_{E^\kappa}$ contains $1_{E^\kappa}$, and $\dim \Sigma^2(V) = 1 + |\mathcal{O}|$. Since $\mathbf{N}_{\mathrm{GL}(V)}(E^\kappa)$ also acts on $\Sigma^2(V)$, Clifford's theorem implies that $\Sigma^2(V)$ affords $1_{E^\kappa}$ and the orbit $\mathcal{O}$, proving the statement with $N = \dim \Sigma^2(V)$. □

## 1.2. Kloosterman and hypergeometric sheaves

We work in characteristic $p$, and use $\overline{\mathbb{Q}_\ell}$-coefficients for a chosen prime $\ell \neq p$. We fix a nontrivial additive character $\psi$ of $\mathbb{F}_p$, with values in $\mu_p(\overline{\mathbb{Q}_\ell})$. We will consider Kloosterman and hypergeometric sheaves on $\mathbb{G}_m/\overline{\mathbb{F}_p}$ as representations of $\pi_1 := \pi_1(\mathbb{G}_m/\overline{\mathbb{F}_p})$, and prove that, under various hypotheses, they satisfy (**S**+) as representations of $\pi_1$. As noted in Lemma 1.1.7, this is equivalent to their satisfying (**S**+) as representations of their geometric monodromy groups.

On $\mathbb{G}_m/\overline{\mathbb{F}_p}$, we consider a Kloosterman sheaf

$$\mathcal{K}l := \mathcal{K}l_\psi(\chi_1, \ldots, \chi_D)$$

of rank $D \geq 2$, defined by an unordered list of $D$ not necessarily distinct multiplicative characters of some finite subfield $\mathbb{F}_q$ of $\overline{\mathbb{F}_p}$.

One knows that $\mathcal{K}l$ is absolutely irreducible, cf. [**Ka-GKM**, 4.1.2]. One also knows, by a result of Pink [**Ka-MG**, Lemmas 11 and 12] that $\mathcal{K}l$ is primitive so long as it is not Kummer induced. Recall that $\mathcal{K}l$ is Kummer induced if and only if there exists a nontrivial multiplicative character $\rho$ such that the unordered list of the $\chi_i$ is equal to the unordered list of the $\rho\chi_i$. Thus primitivity (or imprimitivity) of $\mathcal{K}l$ is immediately visible.

Recall that for any smooth, geometrically connected $X/\mathbb{F}_q$ and any lisse $\overline{\mathbb{Q}_\ell}$ sheaf on $X$, with geometric monodromy group $G_{\mathrm{geom}}$, a celebrated theorem of Grothendieck [**De2**, 1.3.8] tells us that the radical of $G^\circ_{\mathrm{geom}}$ is unipotent. Thus if $\mathcal{F}$ is geometrically semisimple, then $G^\circ_{\mathrm{geom}}$ is semisimple. Applying this last statement to $\det(\mathcal{F})$, we see that $\det(\mathcal{F})$ is geometrically of finite order, since its $G^{\circ}_{\mathrm{geom}}$, being a semisimple subgroup of $\mathrm{GL}_1(\overline{\mathbb{Q}_\ell})$, is trivial.

THEOREM 1.2.1. [**KT5**, Theorem 1.7] *Let $\mathcal{K}l$ be a Kloosterman sheaf of rank $D \geq 2$ in characteristic $p$ which is primitive. Suppose that $D$ is not 4. If $p = 2$, suppose also that $D \neq 8$. Then $\mathcal{K}l$ satisfies* $(\mathbf{S}+)$.

More generally, we consider a ($\overline{\mathbb{Q}_\ell}$-adic) hypergeometric sheaf $\mathcal{H}$ of type $(D, m)$ with $D > m \geq 0$, thus

$$\mathcal{H} = \mathcal{H}yp_\psi(\chi_1, \ldots, \chi_D; \rho_1, \ldots, \rho_m).$$

[A Kloosterman sheaf is none other than a hypergeometric sheaf $\mathcal{H}$ of type $(D, 0)$.] Here the $\chi_i$ and, if $m > 0$, the $\rho_j$ are (possibly trivial) multiplicative characters of some finite subfield $\mathbb{F}_q^\times$, with the proviso that no $\chi_i$ is any $\rho_j$. [The case $m = 0$ is precisely the $\mathcal{K}l$ case.] One knows [**Ka-ESDE**, 8.4.2, (1)] that such an $\mathcal{H}$ is lisse on $\mathbb{G}_m$, geometrically irreducible. Its local monodromy at 0 is tame, a successive extension of the $\chi_i$. It is of finite order if and only if the $\chi_i$ are pairwise distinct, in which case that local monodromy is their direct sum $\oplus_i \chi_i$, cf. [**Ka-ESDE**, 8.4.2, (5)]. Its local monodromy at $\infty$ is the direct sum of a tame part of rank $m$ which is a successive extension of the $\rho_j$, with a totally wild representation $\mathsf{Wild}_{D-m}$ of rank $D - m$ and Swan conductor one, i.e. it has all $\infty$-breaks $1/(D - m)$. It is of finite order if and only the $\rho_j$, if any, are pairwise distinct, in which case that local monodromy is the direct sum of $\oplus_j \rho_j$ with $\mathsf{Wild}_{D-m}$. We denote by $w := D - m$ the dimension of the wild part $\mathsf{Wild}$, and let

$$J := \text{the image of } I(\infty) \text{ on } \mathcal{H}. \tag{1.2.1.1}$$

THEOREM 1.2.2. [**KT5**, Theorem 4.1] *Let $\mathcal{H}$ be an irreducible $\overline{\mathbb{Q}_\ell}$-hypergeometric sheaf on $\mathbb{G}_m/\overline{\mathbb{F}_p}$, with $p \neq \ell$, and of type $(D, m)$ with $D - m \geq 2$. Denote by $G_0$ the Zariski closure inside the geometric monodromy group $G_{\mathrm{geom}}$ of the normal subgroup generated by all $G_{\mathrm{geom}}$-conjugates of the image of $I(0)$. Then $G_0 = G_{\mathrm{geom}}$. In particular, if $G_{\mathrm{geom}}$ is finite then it is generated by all $G_{\mathrm{geom}}$-conjugates of the image of $I(0)$, and $G_{\mathrm{geom}} = \mathbf{O}^p(G_{\mathrm{geom}})$.*

THEOREM 1.2.3. [**KT5**, Theorem 4.7] *Let $\mathcal{H}$ be an irreducible $\overline{\mathbb{Q}_\ell}$-hypergeometric sheaf on $\mathbb{G}_m/\overline{\mathbb{F}_p}$ definable on $\mathbb{G}_m/\mathbb{F}_q$ for some finite extension $\mathbb{F}_q/\mathbb{F}_p$, with $p \neq \ell$, and of type $(D, m)$ with $D > m$. Denote by $G_{P(\infty)}$ the Zariski closure inside the geometric monodromy group $G_{\mathrm{geom}}$ of the normal subgroup generated by all $G_{\mathrm{geom}}$-conjugates of the image of the wild inertia group $P(\infty)$. Then $G_{\mathrm{geom}}/G_{P(\infty)}$ is a finite cyclic group of order prime to $p$.*

In the case of a hypergeometric sheaf $\mathcal{H}$ with $m > 0$, primitivity is less easy to determine at first glance, because there is also the possibility of Belyi induction, cf. [**KRLT3**, Proposition 1.2]. It is known that an $\mathcal{H}$ of type $(D, 1)$ is primitive unless $D$ is a power of $p$, cf. [**KRLT3**, Cor 1.3]. It is also known [**KRLT3**, Proposition 1.4] that an $\mathcal{H}$ of type $(D, m)$, with $D > m \geq 2$ and $D$ a power of $p$, is primitive.

THEOREM 1.2.4. [**KT5**, Theorem 1.9] *Let $\mathcal{H}$ be a hypergeometric sheaf of type $(D, m)$ with $D > m > 0$, with $D \geq 4$. Suppose that $\mathcal{H}$ is primitive, $p \nmid D$, and $w > D/2$. If $p$ is odd and $D = 8$, suppose $w > 6$. If $p \neq 3$, suppose that either $D \neq 9$, or that both $D = 9$ and $w > 6$. Then $\mathcal{H}$ satisfies* $(\mathbf{S}+)$.

THEOREM 1.2.5. [**KT5**, Theorem 1.12] *Let $\mathcal{H}$ be a hypergeometric of type $(D, m)$ with $D > m > 0$, with $D > 4$. Suppose that $\mathcal{H}$ is primitive. Suppose that $p|D$, and $w > (2/3)(D-1)$. If $p = 2$, suppose $D \neq 8$. If $p = 3$, suppose $(D, m)$ is not $(9, 1)$. Then $\mathcal{H}$ satisfies* $(\mathbf{S}+)$.

These two results will be significantly strengthened in Theorem 5.2.9.

We end this section with the following result, which corrects an inaccuracy in [**KT5**, Theorem 9.19(ii)].

THEOREM 1.2.6. *Let $\mathcal{H}$ be an irreducible hypergeometric sheaf of type $(D, m)$ in characteristic $p$ with $D > m$, $D \geq 10$, such that its geometric monodromy group $G = G_{\mathrm{geom}}$ is a finite extraspecial normalizer in some characteristic $r$. Then $p = r$, $D = p^n$ for some $n \in \mathbb{Z}_{\geq 1}$, and the following statements hold.*

(i) *Suppose $p > 2$. Then $\mathcal{H}$ is Kloosterman, in fact the sheaf $\mathcal{K}l(\mathsf{Char}_{\mathrm{ntriv}}(p^n+1))$ (studied by Pink* [**Pink**] *and Sawin* [**KT1**, p. 841]*).*

(ii) *Suppose $p = 2$. Then the 2-part of $\mathbf{Z}(G)$ has order 2, and so in Lemma 1.1.3(i)(c) we have that $R = E$ is a normal extraspecial 2-group $2^{1+2n}_{\epsilon}$ of $G$ for some $\epsilon = \pm$. Moreover, after tensoring $\mathcal{H}$ with a suitable rank one sheaf $\mathcal{L}_{\chi}$, we obtain $\mathbf{Z}(G) = C_2$.*

PROOF. Part (i) is precisely [**KT5**, Theorem 9.19(i)], and the first claim of part (ii) is also established in the first paragraph of the proof of [**KT5**, Theorem 9.19]. Now, if $V$ denotes the underlying representation, then $V|_E$ is irreducible and self-dual, we have by Gallagher's Theorem [**Is**, (6.17)] that $V^* \cong V \otimes A \otimes B$, with $A$ and $B$ being one-dimensional representations of the finite group $G$; moreover, (the character of) $A$ has odd order and (the character of) $B$ has 2-power order. Since $p = 2$, we can find a one-dimensional representation $L$ of $G$ such that $L^{\otimes 2} = A$, on which the 2-subgroup $E$ acts trivially. Then the $G$-representation $U := V \otimes L$ yields a hypergeometric sheaf $\mathcal{H} \otimes \mathcal{L}_{\chi}$ whose geometric monodromy group is the image $H$ of $G$ in $\mathrm{GL}(U)$, and we also have $U^* \cong U \otimes B$. Now any odd-order element $z \in \mathbf{Z}(H)$ acts on $U$ as some root of unity $\zeta \in \mathbb{C}^{\times}$ with $\zeta^m = 1$ for some odd $m \in \mathbb{Z}$. Evaluating the action of $z$ on $U^*$ and $U$, we see that $\zeta^{-2} = B(z)$ has a 2-power order in $\mathbb{C}^{\times}$ and hence $\zeta = 1$. Thus $\mathbf{O}_{2'}(\mathbf{Z}(H))$ acts trivially on $U$. By the first claim of part (ii), $|\mathbf{O}_2(\mathbf{Z}(H))| \leq 2$. On the other hand, since $E$ acts trivially on $L$ and faithfully on $V$, $E$ embeds in $H$ as an irreducible normal 2-subgroup. in particular, $\mathbf{Z}(E)$ still acts via $\mu_2$ on $U$. It follows that $H$ is an extraspecial 2-normalizer with $\mathbf{Z}(H) = \mathbf{Z}(E) \cong C_2$. □

## 1.3. More on condition (S+) for hypergeometric sheaves

Over a field $k$, a representation $\Phi : G \to \mathrm{GL}(V)$ of a group $G$ is called *tensor decomposable* if there exists a $k$-linear isomorphism $V \cong A \otimes_k B$ with both $A$, $B$ of dimension $\geq 2$, such that $\Phi(G) \leq \mathrm{GL}(A) \otimes_k \mathrm{GL}(B)$, the latter being the image of $\mathrm{GL}(A) \times \mathrm{GL}(B)$ in $\mathrm{GL}(A \otimes_k B)$ by the map $(\phi, \rho) \mapsto \phi \otimes \rho$. Tensor indecomposability is one part of the condition $(\mathbf{S}+)$, which is shown in [**KT5**] to play a central role in the study of hypergeometric sheaves. More precisely, a geometrically irreducible hypergeometric sheaf $\mathcal{H}$ satisfies $(\mathbf{S}+)$ if and only if it is primitive, tensor indecomposable, and not tensor induced.

Various results in [**KRLT3**] on tensor indecomposability for the monodromy groups of hypergeometric sheaves of type $(D, m)$ with $D > m > 0$ are proved relying on the following representation-theoretic fact:

THEOREM 1.3.1. [**KRLT3**, Theorem 2.3] *Let $J$ be a finite group, with normal Sylow $p$-subgroup $P$ and with cyclic quotient $J/P$. Let $V$ be a finite-dimensional $\mathbb{C}J$-module which is the direct sum $T \oplus W$ of a nonzero tame part $T$ (i.e., one on which $P$ acts trivially) and of an irreducible submodule $W$ which is totally wild (i.e., one in which $P$ has no nonzero invariants). Suppose that one of the following conditions holds.*

(a) $\dim(V)$ *is neither* 4 *nor an even power of* $p$.
(b) $\dim(V)$ *is an even power of* $p$ *and* $\dim(T) > 1$.
(c) $\dim(V) = 4$, $p > 2$, *and* $\dim(T) \neq 2$.

*Then $J$ does not stabilize any decomposition $V = A \otimes B$ with* $\dim(A), \dim(B) > 1$.

We offer another result which applies to some situations not covered by Theorem 1.3.1:

THEOREM 1.3.2. *Let $p$ be any prime, $n \geq 1$. Let $G < \mathrm{GL}(V) \cong \mathrm{GL}_{p^n}(\mathbb{C})$ be a finite group with a normal subgroup $P$ which is an extraspecial $p$-group of order $p^{1+2n}$. Suppose that $p^{2n} - 1$ admits a primitive prime divisor $\ell$ (in the sense of* [**Zs**]*) and that $G$ contains an element $g$ of order $\ell$ that does not centralize $P$. Then $G$ is irreducible, primitive on $V$, and cannot fix any nontrivial tensor decomposition or a tensor induced decomposition of $V$.*

PROOF. (i) It suffices to prove the statement in the case $G = P\langle g \rangle \cong P \rtimes C_\ell$. Note that any complex irreducible representation of $P$ is either trivial on $\mathbf{Z}(P) \cong C_p$ or has degree $p^n$. It follows that $V|_P$ is irreducible. Thus $G$ acts irreducibly on $V$, with character say $\varphi$.

By Schur's Lemma, $\mathbf{Z}(P)$ acts on $V$ via scalars, and so $\mathbf{Z}(P) \leq \mathbf{Z}(G)$ and $g$ centralizes $\mathbf{Z}(P)$. Next, the assumption about $\ell = |g|$ implies that the action of $g$ on $P/\mathbf{Z}(P)$ is irreducible. Hence, if $g$ has nonzero fixed points on $P/\mathbf{Z}(P)$, then $g$ acts trivially on $P/\mathbf{Z}(P)$. As $g$ acts coprimely on $P$ and $g$ centralizes both $\mathbf{Z}(P)$ and $P/\mathbf{Z}(P)$, we then have that $g$ centralizes $P$, a contradiction. We have shown that $|\mathbf{C}_{P/\mathbf{Z}(P)}(g)| = 1$, whence $\mathbf{Z}(P)$ is the complete inverse image of $\mathbf{C}_{P/\mathbf{Z}(P)}(g)$ in $P$. It follows by [**GT1**, Lemma 2.4] that

$$|\varphi(g)| = 1. \tag{1.3.2.1}$$

(ii) Next we observe that if $1 \neq P_1 \leq P$ is a $g$-invariant subgroup, then either $P_1 = \mathbf{Z}(P)$ or $P_1 = P$. Indeed, the claim is obvious if $P_1 \leq \mathbf{Z}(P)$. Suppose $P_1 \not\leq \mathbf{Z}(P)$ and $P_1 < P$. Then $P_1\mathbf{Z}(P)/\mathbf{Z}(P)$ is $g$-invariant, and so $P_1\mathbf{Z}(P) = P$ by irreducibility. As $P_1 \cap \mathbf{Z}(P) = 1$, we have $P_1 \cong P/\mathbf{Z}(P)$ is abelian. In this case, $P = P_1 \times \mathbf{Z}(P)$ is also abelian, a contradiction. A similar argument shows that

$$\mathbf{O}^{\ell'}(G) = G. \tag{1.3.2.2}$$

Suppose now that $G$ fixes a nontrivial imprimitive decomposition $V = \oplus_{i=1}^s V_i$ with $s > 1$. As $s|p^n$, $[G : \mathrm{Stab}_G(V_1)] = s$ is coprime to $\ell$, and so we may assume that $g$ fixes $V_1$. Now $\mathrm{Stab}_P(V_1)$ is $g$-invariant, and has order at least $|P|/s \geq p^{n+1}$. It follows by the preceding statement that $\mathrm{Stab}_P(V_1) = P$, i.e. $P$ fixes $V_1$. But in this case $V_1 = V$ by irreducibility, a contradiction. We have shown that $G$ acts primitively on $V$.

(iii) Assume now that $G$ fixes a tensor decomposition $V = A \otimes B$, with

$$1 < p^a := \dim A \leq \dim B < p^n. \tag{1.3.2.3}$$

This leads to projective representations of $G$ on $A$ and on $B$, which are both irreducible over $P$ since $P$ is irreducible on $V$. Since $|G| = p^{2n+1}\ell$, by [**Is**, (11.21)] the Schur multiplier of

$G$ is a $p$-group. Thus we can find a finite group $\hat{G}$ with a central $p$-subgroup $Z_1$, such that $\hat{G}/Z_1 \cong G$ and the projective representations of $G$ on $A$ and $B$ lift to linear representations of $\hat{G}$, with characters $\alpha$ and $\beta$, respectively.

Let $Z_1 \leq T_1 \leq Q \leq \hat{G}$ be such that $Q/Z_1 = P$ and $T_1/Z_1 = \mathbf{Z}(P)$. Note that

$$\hat{G}/Q \cong G/P \cong C_\ell. \tag{1.3.2.4}$$

By irreducibility, $Z_1$ acts via scalars on $A$, so $Z_1 \leq \mathrm{Ker}(\alpha\overline{\alpha})$. Hence, $\alpha\overline{\alpha}|_Q$ can be viewed as a character of $P$, which then contains $1_P$ as an irreducible constituent since $\alpha\overline{\alpha}|_Q$ contains $1_Q$. Now $\alpha\overline{\alpha}|_P - 1_P$ is a $P$-character of degree $p^{2a} - 1 \leq p^n - 1$ (recalling (1.3.2.3)). Inspecting $\mathrm{Irr}(P)$ as we did at the beginning of (i), we see that $\mathbf{Z}(P) \leq \mathrm{Ker}(\alpha\overline{\alpha}|_P - 1_P)$. Thus, for any $t \in T_1$,

$$|\alpha(t)|^2 = (\alpha\overline{\alpha} - 1_Q)(t) + 1 = (\alpha\overline{\alpha} - 1_Q)(1) + 1 = \alpha(1)^2,$$

which means that $T_1$ acts via scalars on $A$.

Let the subgroup $T$ consist of all elements of $\hat{G}$ that acts on $A$ via scalars, so that $T \geq T_1$. We claim that $T \leq Q$. If not, then, keeping in mind (1.3.2.4) and the fact that $Z_1$ is a $p$-group, we may assume that an inverse image $\hat{g}$ of order $\ell$ of $g$ in $\hat{G}$ is contained in $T$. This implies that $\alpha(\hat{g}) = p^a\epsilon$, with $\epsilon \in \mathbb{C}^\times$ a root of unity. Certainly, $\beta(\hat{g})$ is an algebraic integer. It follows that

$$\varphi(g) = \alpha(\hat{g})\beta(\hat{g}) = p^a\gamma$$

for some algebraic integer $\gamma$. This in turn implies that $|\varphi(g)|^2/p^2 = \gamma\overline{\gamma}$ is an algebraic integer, contradicting (1.3.2.1). Thus $T \leq Q$ as stated.

Modding out by $\mathrm{Ker}(\alpha)$ (which is contained in $T$), we may assume that $\alpha$ is faithful. Slightly abusing the notation, we will denote the images of $\hat{G}$, $Q$, $T$ in this quotient by the same letters. Now we have that $\alpha|_Q$ is a faithful irreducible character of the $p$-group $Q$, with $T$ acting via scalars. Let $\Psi$ denote the representation of $Q$ on $A$. Next we show that

$$Q/T \cong C_p^{2n}. \tag{1.3.2.5}$$

Indeed, since $Q/T$ is a quotient of $P/\mathbf{Z}(P) \cong C_p^{2n}$, $Q/T$ is elementary abelian of order $p^c$ for some $c \leq 2n$. Now if $c < 2n$, then the choice of $\ell = |\hat{g}|$ implies that $\hat{g}$ centralizes $Q/T$. As $T$ acts on $A$ via scalars and $\Psi$ is faithful, $\hat{g}$ also centralizes $T$. The coprime action of $\hat{g}$ on the $p$-group $Q$ now yields that $\hat{g}$ centralizes $Q$, and so $g$ centralizes $P$, a contradiction.

Recall we have shown that $Q/T$ acts projectively and irreducibly on $A$. It is well known, cf [**Is**, (11.16), p. 197] that the Schur multiplier of the elementary abelian group $Q/T$ is also elementary abelian. Hence, we can find a $p$-group $R$ with an elementary abelian central subgroup $Z_2$ and with a faithful irreducible linear action $\Theta$ on $A$ that lifts the projective action of $Q/T \cong R/Z_2$. More precisely, if we fix a representative $g \in Q$ of a coset $gT \in Q/T$, then there is a representative $h \in R$ of $gT$ but now viewed as a coset in $R/Z_2$ such that $\Psi(g) = \Theta(h)$. In this case, $\Theta(h)$ can be scalar only when $\Psi(g)$ is, whence $g \in T$ by the choice of $T$. Thus $Z_2$ consists precisely of all elements $h \in R$ such that $\Theta(h)$ is scalar. The faithfulness of $\Theta$ now implies that $Z_2$ is cyclic. Also, $Z_2 \neq 1$ as otherwise $R$ would be abelian and so cannot act irreducibly on $A$. It follows that $\mathbf{Z}(R) = Z_2 \cong C_p$. Since $R/Z_2$ is elementary abelian, it now follows that $[R, R] = \Phi(R) = \mathbf{Z}(R)$ (where $\Phi(R)$ is the Frattini subgroup of $R$). In other words, $R$ is extraspecial, of order $|\mathbf{Z}(R)| \cdot |R/Z_2| = p^{1+2n}$

by (1.3.2.5). As $\Theta$ is a faithful irreducible representation of $R$, we must have that

$$\dim A = \deg \Theta = p^n,$$

contradicting (1.3.2.3).

(iv) We have shown that $G$ fixes no nontrivial tensor decomposition of $V$. Suppose now that $G$ fixes a tensor induced decomposition $V = V_1 \otimes V_2 \otimes \ldots \otimes V_m \cong V_1^{\otimes m}$, where $\dim V_1 = p^d$, $m > 1$, and $dm = n$. Note that the choice of $\ell$ implies that $\ell \geq 2n+1 > m$. Hence, every element of order $\ell$ of $G$ must act trivially on the set $\{V_1, \ldots, V_m\}$. This in turn implies by (1.3.2.2) that $G$ also acts trivially on the same set, that is, $G$ fixes each of the tensor factors $V_i$. But this contradicts the previous result. □

We now state a well-known result which will be useful later.

Theorem 1.3.3. *Let $k$ be a finite field of characteristic $p$, $X/k$ a smooth, geometrically connected scheme, $\ell \neq p$ a prime, and $\mathcal{F}, \mathcal{G}$ two lisse $\overline{\mathbb{Q}_\ell}$ sheaves on $X$, each of which is pure of weight zero. Suppose that $\mathcal{F}$ and $\mathcal{G}$ have identical trace functions: for every finite extension $L/k$, and every point $x \in X(L)$, we have*

$$\mathrm{Trace}(\mathsf{Frob}_{x,L}|\mathcal{F}) = \mathrm{Trace}(\mathsf{Frob}_{x,L}|\mathcal{G}).$$

*Then we have the following results.*

(i) *There exists a geometric isomorphism $\phi$ of $\mathcal{F}$ with $\mathcal{G}$, i.e., an isomorphism of their pullbacks to $X \otimes_k \overline{k}$.*

(ii) *Pick a geometric point $\overline{\eta}$ of $X$, and use $\phi$ to view $\mathcal{F}$ and $\mathcal{G}$ as representations $\rho_{\mathcal{F}}$ and $\rho_{\mathcal{G}}$ of $\pi_1^{\mathrm{geom}} := \pi_1(X \otimes_k \overline{k}, \overline{\eta})$ on the same finite dimensional $\overline{\mathbb{Q}_\ell}$ vector space $V$ ($V$ being the stalk $\mathcal{F}_{\overline{\eta}} = \mathcal{G}_{\overline{\eta}}$ via $\phi$). Then the two image groups $\rho_{\mathcal{F}}(\pi_1^{\mathrm{geom}})$ and $\rho_{\mathcal{F}}(\pi_1^{\mathrm{geom}})$ are conjugate subgroups of the ambient* $\mathrm{GL}(V)$.

(iii) *The geometric monodromy groups $G_{\mathrm{geom},\mathcal{F}}$ and $G_{\mathrm{geom},\mathcal{G}}$ are conjugate subgroups of the ambient* $\mathrm{GL}(V)$.

Proof. Assertion (iii) is obtained from the last sentence of (ii) by passing to Zariski closures of the conjugate image groups. Assertion (ii) is just a concrete spelling out of assertion (i).

To prove (i), we argue as follows. By Chebotarev, the equality of traces implies that $\mathcal{F}$ and $\mathcal{G}$ have isomorphic arithmetic semisimplifications, i.e., isomorphic semisimplifications as representations of $\pi_1^{\mathrm{arith}} := \pi_1(X, \overline{\eta})$. Because $\pi_1^{\mathrm{geom}} \lhd \pi_1^{\mathrm{arith}}$ is a normal subgroup, it follows that $\mathcal{F}$ and $\mathcal{G}$ have isomorphic semisimplifications as representations of $\pi_1^{\mathrm{geom}}$. Because $\mathcal{F}$ and $\mathcal{G}$ are each pure of weight zero, each is semisimple as a representation of $\pi_1^{\mathrm{geom}}$, by [**De2**, 3.4.1 (iii)]. Hence $\mathcal{F}$ and $\mathcal{G}$ are isomorphic as representations of $\pi_1^{\mathrm{geom}}$, i.e., they are geometrically isomorphic. □

To end this section, we give a well-known result for which we do not know an explicit reference.

Theorem 1.3.4. *Let $n \geq 1$ be an integer, $p$ a prime and $k/\mathbb{F}_p$ an algebraically closed field of characteristic $p$. Then for $G$ a finite group of order prime to $p$,*

$$\mathrm{Hom}_{\mathrm{gp}}(\pi_1(\mathbb{A}^n/k), G) = 1.$$

Proof. For $n = 1$, this is Abhyankar's insight [**Abh**, Proposition 6, (I) and (II)]. For $n \geq 2$, we use the "weak Bertini" result of [**Ka-ACT**, Corollary 3.4.2], applied with $V = \mathbb{A}^n, \pi = \mathrm{Id}, f = 0$ there to reduce from $n$ to $n-1$, viewing $\mathbb{A}^{n-1}$ as the zero set of the polynomial $f_{A,b} = Ax + b$ there. □

## 1.4. Moments and monodromy

We first recall the notion of moments. Let $\mathbb{C}$ (sic) be an algebraically closed field of characteristic zero, $V$ a finite dimensional $\mathbb{C}$ vector space, and $G \leq \mathrm{GL}(V)$ a Zariski closed subgroup. For non-negative integers $a, b$, the $(a,b)$-*moment* $M_{a,b}(G, V)$ is the dimension

$$M_{a,b}(G,V) := \dim\big((V^{\otimes a} \otimes (V^\vee)^{\otimes b})^G\big).$$

In applications, $\mathcal{F}$ will be a lisse $\mathbb{Q}_\ell$-sheaf on some geometrically connected $X/\mathbb{F}_q$, $\ell \neq p$, $V$ will be the representation of $G_{\mathrm{geom}}$ attached to $\mathcal{F}$, $G$ will be $G_{\mathrm{geom}}$, and $\overline{\mathbb{Q}_\ell}$ will be the algebraically closed field of characteristic zero. By fundamental results of Grothendieck and Deligne [**De2**, 1.3.8 and 3.4.1 (iii)], $G_{\mathrm{geom}}$ is a semisimple algebraic group (meaning that its identity component $G^0_{\mathrm{geom}}$ is semisimple).

The importance of the $M_{2,2}$ moment is given by *Larsen's Alternative.* First recall the following basic facts. Suppose $G \leq \mathrm{GL}(V)$ and $\dim(V) \geq 2$.

(a) If $\mathrm{SL}(V) \leq G$, and $\dim(V) \geq 2$, then $M_{2,2}(G,V) = 2$.
(b) If $V$ is given with an orthogonal autoduality $\langle \cdot, \cdot \rangle$, and either $G = \mathrm{O}(V)$ or both $\dim(V) \neq 2, 4$ and $G = \mathrm{SO}(V)$, then $M_{2,2}(G,V) = 3$.
(c) If $V$ is given with an alternating autoduality $\langle \cdot, \cdot \rangle$ and $\dim(V) \geq 4$, then $M_{2,2}(\mathrm{Sp}(V), V) = 3$.

Remark 1.4.1. The special behavior in dimensions 2 and 4 is this. The group $\mathrm{SO}_2$ is not semisimple, but rather is $\mathrm{GL}_1$ with the 2-dimensional representation $x \mapsto \mathrm{diag}(x, 1/x)$, and has $M_{2,2} = 6$ in this representation. The group $\mathrm{SO}_4$ has $M_{2,2} = 4$ in its standard representation because it is $(\mathrm{SL}(2) \times \mathrm{SL}(2))/(\pm\mathrm{diag}(\mathrm{id}, \mathrm{id}))$ in the representation $\mathrm{std}_2 \otimes \mathrm{std}_2$. In both cases, this "too large $M_{2,2}$" issue is cured by passing to O instead of SO.

Theorem 1.4.2. (Larsen's Alternative, [**Ka-LAMM**, 1.1.6]) *Suppose $G \leq \mathrm{GL}(V)$ is semisimple and $\dim(V) \geq 2$. Then we have the following results.*

(i) *If $M_{2,2}(G,V) = 2$, then either $G$ is finite or $G^\circ = \mathrm{SL}(V)$.*
(ii) *If $V$ is given with an orthogonal autoduality $\langle \cdot, \cdot \rangle$, $G \leq \mathrm{O}(V)$, and $M_{2,2}(G,V) = 3$, then either $G$ is finite or $\mathrm{SO}(V) \leq G \leq \mathrm{O}(V)$.*
(iii) *If $V$ is given with an alternating autoduality $\langle \cdot, \cdot \rangle$, $\dim(V) \geq 4$, $G \leq \mathrm{Sp}(V)$, and $M_{2,2}(G,V) = 3$, then either $G$ is finite or $G = \mathrm{Sp}(V)$.*

The cases in dimension $\geq 5$ when Larsen's alternative implies finiteness are given by the following theorem.

Theorem 1.4.3. [**GT2**, Theorem 1.5] *Let $V = \mathbb{C}^d$ with $d \geq 5$, $\boldsymbol{G} = \mathrm{GL}(V)$, $\mathrm{Sp}(V)$, or $\mathrm{O}(V)$. Assume $G$ is a semisimple subgroup of $\boldsymbol{G}$. Set $\bar{S} = S/Z(S)$ for $S := F^*(G)$ if $G$ is finite. Then $G$ is irreducible on every $\boldsymbol{G}$-composition factor of $V \otimes V^*$, equivalently, $M_{2,2}(G,V) = M_{2,2}(\boldsymbol{G}, V)$, if and only if one of the following holds.*

(A) $G \geq [\boldsymbol{G}, \boldsymbol{G}]$.

(B) *(Lie-type case) One of the following holds.*
 (i) $\bar{S} = \mathrm{PSp}_{2n}(q)$, $n \geq 2$, $q = 3, 5$, $G = Z(G)S$, *and* $V|_S$ *is a Weil module of dimension* $(q^n \pm 1)/2$.
 (ii) $\bar{S} = \mathrm{PSU}_n(2)$, $n \geq 4$, *and* $V|_S$ *is a Weil module of dimension* $(2^n + 2(-1)^n)/3$ *or* $(2^n - (-1)^n)/3$.

(C) *(Extraspecial cases)* $d = p^a$ *for some prime* $p$, $p > 2$ *if* $\boldsymbol{G} = \mathrm{GL}(V)$ *and* $p = 2$ *otherwise,* $F^*(G) = Z(G)E$ *for some extraspecial subgroup* $E$ *of order* $p^{1+2a}$ *of* $\mathcal{G}$, *and one of the conclusions* (i)–(iii) *of* [**GT2**, Lemma 5.1] *holds.*

(D) *(Exceptional cases)* $(\dim(V), \bar{S}, G, \boldsymbol{G})$ *is as listed in Table I.*

The following two results of [**GT2**] address higher moments of closed subgroups of $\boldsymbol{G}$.

Theorem 1.4.4. [**GT2**, Theorem 1.6] *Let* $V = \mathbb{C}^d$ *with* $d \geq 5$, $\boldsymbol{G} = \mathrm{GL}(V)$, $\mathrm{Sp}(V)$, *or* $\mathrm{O}(V)$. *Assume* $G$ *is a semisimple subgroup of* $\boldsymbol{G}$. *Then* $G$ *is irreducible on every* $\boldsymbol{G}$-*composition factor of* $V^{\otimes 3}$, *equivalently,* $M_{3,3}(G, V) = M_{3,3}(\boldsymbol{G}, V)$, *if and only if one of the following holds.*

(A) $G \geq [\boldsymbol{G}, \boldsymbol{G}]$; *moreover,* $G \neq \mathrm{SO}(V)$ *if* $d = 6$.

(B) *(Extraspecial case)* $d = 2^a$ *for some* $a > 2$. *If* $\boldsymbol{G} = \mathrm{GL}(V)$ *then* $G = \mathbf{Z}(G)E \cdot \mathrm{Sp}_{2a}(2)$ *with* $E = 2^{1+2a}_{+}$. *If* $\boldsymbol{G} = \mathrm{Sp}(V)$, *respectively* $\mathrm{O}(V)$, *then* $E \cdot \Omega^{\epsilon}_{2a}(2) \leq G \leq E \cdot \mathrm{O}^{\epsilon}_{2a}(2)$, *with* $E = 2^{1+2a}_{\epsilon}$ *and* $\epsilon = -$, *resp.* $\epsilon = +$.

(C) *(Exceptional cases)* $G$ *is finite, with the unique nonabelian composition factor*

$$\bar{S} \in \{\mathrm{PSL}_3(4), \mathrm{SU}_3(3), \mathrm{PSU}_4(3), J_2, \mathsf{A}_9, \Omega^+_8(2), \mathrm{SU}_5(2), G_2(4), Suz, J_3, Co_2, Co_1, F_4(2)\},$$

*and* $(\dim(V), \bar{S}, G, \boldsymbol{G})$ *is as listed in the lines marked by* $^{(\star)}$ *in Table I.*

Theorem 1.4.5. [**GT2**, Theorem 1.4] *Let* $V = \mathbb{C}^d$ *with* $d \geq 5$ *and* $\boldsymbol{G}$ *be* $\mathrm{GL}(V)$, $\mathrm{Sp}(V)$, *or* $\mathrm{O}(V)$. *Assume that* $G$ *is a Zariski closed subgroup of* $\boldsymbol{G}$ *such that* $G^\circ$ *is reductive. Then one of the following statements holds.*

(i) $M_{4,4}(G, V) > M_{4,4}(\boldsymbol{G}, V)$.
(ii) $G \geq [\boldsymbol{G}, \boldsymbol{G}]$.
(iii) $d = 6$, $\boldsymbol{G} = \mathrm{Sp}(V)$, *and* $G = 2J_2$.

As in Theorem 1.4.3(C), consider finite groups $G$ with $F^*(G) = \mathbf{Z}(G)E$ of symplectic type, i.e. $E$ is either extraspecial of odd exponent $p$, an extraspecial 2-group of type ±, or a central product of an extraspecial 2-group with a cyclic group of order 4 (with the central involutions identified).

If $E$ is extraspecial of order $p^{1+2a}$, then an irreducible faithful module $V$ over an algebraically closed field $\mathbb{F}$ of characteristic $\ell \neq p$ for $E$ has dimension $p^a$ and is unique once the character of $\mathbf{Z}(E)$ is fixed. Moreover, we consider the following situations: $E \lhd G \leq \boldsymbol{G} \leq \mathrm{GL}(V)$, where $Z := \mathbf{Z}(\boldsymbol{G})$, and

(a) $p$ is odd, $G \leq N := (EZ) \rtimes \mathrm{Sp}_{2a}(p)$ and $\boldsymbol{G} = \mathrm{GL}(V)$;
(b) $p = 2$, $G \leq N := (EZ) \cdot \mathrm{Sp}_{2a}(2)$ and $\boldsymbol{G} = \mathrm{GL}(V)$;
(c) $p = 2$, $G \leq N := E \cdot \mathrm{O}^+_{2a}(2)$ and $\boldsymbol{G} = \mathrm{O}(V)$;
(d) $p = 2$, $G \leq N := E \cdot \mathrm{O}^-_{2a}(2)$ and $\boldsymbol{G} = \mathrm{Sp}(V)$.

We now assume that $E \lhd G \leq N$, $|E| = p^{1+2a}$, $d = \dim(V) = p^a > 4$, $W := \mathbb{F}_p^{2a}$ the natural module for $N/(EZ \cap N)$, and take this opportunity to correct some inaccuracies in the proofs of Propositions 5.2 and 5.3 of [**GT2**].

| $d$ | $\bar{S}$ | $G$ | $\boldsymbol{G}$ | The largest $2k$ with $M_{k,k}(G,V)=M_{k,k}(\boldsymbol{G},V)$ | $M_{k+1,k+1}(G,V)$ vs. $M_{k+1,k+1}(\boldsymbol{G},V)$ |
|---|---|---|---|---|---|
| 6 | $\mathsf{A}_7$ | $6\mathsf{A}_7$ | $\mathrm{GL}_6$ | 4 | 21 vs. 6 |
| 6 | $\mathrm{PSL}_3(4)$ $^{(\star)}$ | $6\cdot\mathrm{PSL}_3(4)\cdot 2_1$ | $\mathrm{GL}_6$ | 6 | 56 vs. 24 |
| 6 | $\mathrm{PSU}_3(3)$ $^{(\star)}$ | $(2\times\mathrm{PSU}_3(3))\cdot 2$ | $\mathrm{Sp}_6$ | 6 | 195 vs. 104 |
| 6 | $\mathrm{PSU}_4(3)$ $^{(\star)}$ | $6_1\cdot\mathrm{PSU}_4(3)$ | $\mathrm{GL}_6$ | 6 | 25 vs. 24 |
| 6 | $J_2$ $^{(\star)}$ | $2J_2$ | $\mathrm{Sp}_6$ | 10 | 10660 vs. 9449 |
| 7 | $\mathrm{SL}_2(8)$ | $\mathrm{SL}_2(8)\cdot 3$ | $\mathrm{O}_7$ | 4 | 81 vs. 15 |
| 7 | $\mathrm{Sp}_6(2)$ | $\mathrm{Sp}_6(2)$ | $\mathrm{O}_7$ | 4 | 16 vs. 15 |
| 8 | $\mathrm{PSL}_3(4)$ | $4_1\cdot\mathrm{PSL}_3(4)$ | $\mathrm{GL}_8$ | 4 | 17 vs. 6 |
| 8 | $\mathsf{A}_9$ $^{(\star)}$ | $2\mathsf{A}_9$ | $\mathrm{O}_8$ | 6 | 191 vs. 106 |
| 8 | $\Omega_8^+(2)$ $^{(\star)}$ | $2\Omega_8^+(2)$ | $\mathrm{O}_8$ | 6 | 107 vs. 106 |
| 10 | $\mathrm{SU}_5(2)$ $^{(\star)}$ | $(2\times\mathrm{SU}_5(2))\cdot 2$ | $\mathrm{Sp}_{10}$ | 6 | 120 vs. 105 |
| 10 | $M_{12}$ | $2M_{12}$ | $\mathrm{GL}_{10}$ | 4 | 15 vs. 6 |
| 10 | $M_{22}$ | $2M_{22}$ | $\mathrm{GL}_{10}$ | 4 | 7 vs. 6 |
| 12 | $G_2(4)$ $^{(\star)}$ | $2G_2(4)\cdot 2$ | $\mathrm{Sp}_{12}$ | 6 | 119 vs. 105 |
| 12 | $Suz$ $^{(\star)}$ | $6Suz$ | $\mathrm{GL}_{12}$ | 6 | 25 vs. 24 |
| 14 | ${}^2B_2(8)$ | ${}^2B_2(8)\cdot 3$ | $\mathrm{GL}_{14}$ | 4 | 90 vs. 6 |
| 14 | $G_2(3)$ | $G_2(3)$ | $\mathrm{O}_{14}$ | 4 | 21 vs. 15 |
| 18 | $\mathrm{Sp}_4(4)$ | $(2\times Sp_4(4))\cdot 4$ | $\mathrm{O}_{18}$ | 4 | 25 vs. 15 |
| 18 | $J_3$ $^{(\star)}$ | $3J_3$ | $\mathrm{GL}_{18}$ | 6 | 238 vs. 24 |
| 22 | $McL$ | $McL$ | $\mathrm{O}_{22}$ | 4 | 17 vs. 15 |
| 23 | $Co_3$ | $Co_3$ | $\mathrm{O}_{23}$ | 4 | 16 vs. 15 |
| 23 | $Co_2$ $^{(\star)}$ | $Co_2$ | $\mathrm{O}_{23}$ | 6 | 107 vs. 105 |
| 24 | $Co_1$ $^{(\star)}$ | $2Co_1$ | $\mathrm{O}_{24}$ | 6 | 106 vs. 105 |
| 26 | ${}^2F_4(2)'$ | ${}^2F_4(2)'$ | $\mathrm{GL}_{26}$ | 4 | 26 vs. 6 |
| 28 | $Ru$ | $2Ru$ | $\mathrm{GL}_{28}$ | 4 | 7 vs. 6 |
| 45 | $M_{23}$ | $M_{23}$ | $\mathrm{GL}_{45}$ | 4 | 817 vs. 6 |
| 45 | $M_{24}$ | $M_{24}$ | $\mathrm{GL}_{45}$ | 4 | 42 vs. 6 |
| 52 | $F_4(2)$ $^{(\star)}$ | $2F_4(2)\cdot 2$ | $\mathrm{O}_{52}$ | 6 | 120 vs. 105 |
| 78 | $Fi_{22}$ | $Fi_{22}$ | $\mathrm{O}_{78}$ | 4 | 21 vs. 15 |
| 133 | $HN$ | $HN$ | $\mathrm{O}_{133}$ | 4 | 21 vs. 15 |
| 248 | $Th$ | $Th$ | $\mathrm{O}_{248}$ | 4 | 20 vs. 15 |
| 342 | $O'N$ | $3O'N$ | $\mathrm{GL}_{342}$ | 4 | 3480 vs. 6 |
| 1333 | $J_4$ | $J_4$ | $\mathrm{GL}_{1333}$ | 4 | 8 vs. 6 |

TABLE I. Exceptional cases with small moments in dimension $d \geq 5$

PROPOSITION 1.4.6. (cf. [**GT2**, Proposition 5.2]). *Assume $\ell = 0$ and $p^a > 4$.*

(i) *Assume $\boldsymbol{G} = \mathrm{GL}(V)$. If $p > 2$ then $M_{3,3}(N,V) - M_{3,3}(\boldsymbol{G},V) \geq 2p-5$. If $p = 2$ then $M_{4,4}(N,V) > M_{4,4}(\boldsymbol{G},V)$ and $M_{3,3}(N,V) = M_{3,3}(\boldsymbol{G},V)$.*

(ii) *Assume $p = 2$, $a \geq 4$, and $\boldsymbol{G} = \mathrm{Sp}(V)$ or $\mathrm{O}(V)$. Then $M_{3,3}(N,V) = M_{3,3}(\boldsymbol{G},V)$ and $M_{4,4}(N,V) > M_{4,4}(\boldsymbol{G},V)$.*

Proof. (i) It was stated at the beginning of the proof of [**GT2**, Proposition 5.2], that

$$M := V^* \otimes V$$

is trivial on $Z$, and, considered as a module over $EZ/Z$, it is the permutation module on $W$ with $E/\mathbf{Z}(E)$ acting by translations, *and, as a module over $N/Z$, it is the permutation module on $W$ with $N/EZ \cong \mathrm{Sp}(W)$ acting naturally.* The emphasized part of the statement is true only when $p > 2$. Indeed, if $p = 2$ then $N/Z$ is non-split over $EZ/Z$, see [**Gri**, Theorem 1]. Assume that $p > 2$. It is well known that $N$ is split over $EZ$ (with a complement $S \cong Sp(W)$ being the centralizer of a suitable involution), and $V|_S$ is reducible (in fact it is a sum of two irreducible Weil modules). Let $M_1 = \mathrm{Ind}_S^{N/Z}(1_S)$ denote the permutation $N/Z$-module on $W$ with $S$ acting naturally. Since the corresponding permutation action is doubly transitive, $M_1 \cong \mathbb{F} \oplus M_2$ with $M_2$ nontrivial irreducible. By Frobenius reciprocity,

$$\mathrm{Hom}_{N/Z}(M, M_1) \cong \mathrm{Hom}_S(M|_S, 1_S) \cong \mathrm{Hom}_S(V|_S, V_S)$$

has dimension at least 2. Since $\mathrm{Hom}_{N/Z}(M, \mathbb{F}) \cong \mathrm{Hom}_N(V, V) \cong \mathbb{F}$, it follows that $M$ contains both $\mathbb{F}$ and $M_2$, and by dimension comparison we conclude that $M \cong M_1$.

Now, if $p > 2$, then all the arguments in part (i) of the proof of [**GT2**, Proposition 5.2] apply, and we are done. Assume $p = 2$. To prove $M_{4,4}(N, V) > M_{4,4}(\boldsymbol{G}, V)$, by [**GT2**, Remark 2.3] it suffices to show that $N$ is reducible on the simple $\boldsymbol{G}$-module $\mathrm{Sym}^4(V)$ of dimension

$$D := 2^{a-2}(2^a + 1)(2^{a-1} + 1)(2^a + 3)/3.$$

Assume the contrary. Recall that $E = C_4 * 2_+^{1+2a}$ and $\mathbf{Z}(E) = C_4$ acts trivially on $\mathrm{Sym}^4(V)$ but $E$ does not (as one can check by computing the trace of some non-central involution). Since $N/EZ$ acts transitively on the $2^{2a} - 1$ nontrivial irreducible characters of $E/(E \cap Z)$, it follows from Clifford's theorem that $2^{2a} - 1$ divides $D$, which is impossible.

Next we observe for $p = 2$ that $M_{3,3}(N, V) \geq M_{3,3}(\boldsymbol{G}, V) = 6$. As mentioned in the proof of [**GT2**, Proposition 5.2], the $E/\mathbf{Z}(E)$-module $M$ affords the character $\rho := \sum_{v \in W} v$, where we again identify $\mathrm{Irr}(E/\mathbf{Z}(E))$ with $W$ as in the proof of [**GT2**, Lemma 5.1]. It follows that $M^{\otimes 3}$ is the permutation module on $W \times W \times W$, and that the fixed point subspace for $ZE$ inside $M^{\otimes 3}$ affords the $E/\mathbf{Z}(E)$-character $1_E \cdot \left(\sum_{u,v,w \in W, u+v+w=0} 1\right)$. On the triples $(u, w, w)$, $u, v, w \in W$, $u + v + w = 0$, $\mathrm{Sp}(W)$ acts with exactly 6 orbits, with the first four orbit representatives being $(0, 0, 0)$; $(u, 0, -u)$, $(u, -u, 0)$, $(0, u, -u)$ with $u \neq 0$; and 2 orbits of $(u, v, u + v)$ with $u, v \in W$ linearly independent and the inner product $(u|v) = \mu \in \mathbb{F}_2$. Each orbit gives rise to an induced module $\mathrm{Ind}_{P_i}^S(L_i)$, $1 \leq i \leq 6$, for $S := \mathrm{Sp}(W)$, with $\dim L_i = 1$. Since

$$\dim \mathrm{Hom}_S(\mathrm{Ind}_{P_i}^S(L_i), \mathbb{F}) = \dim \mathrm{Hom}_{P_i}(L_i, \mathbb{F}) \leq 1,$$

it follows that $M_{3,3}(N, V) \leq 6$, and we are done. In fact, now since $M_{3,3}(N, V) = 6$, the previous inequality must in fact be an equality, and thus $L_i \cong \mathbb{F}$, i.e. all the six induced modules are permutation modules.

(ii) A similar argument as in (i) also applies to show that $M_{4,4}(N, V) > M_{4,4}(\boldsymbol{G}, V)$ in the case $\boldsymbol{G} = \mathrm{Sp}(V)$. Indeed, assume that $N$ is irreducible on the simple $\boldsymbol{G}$-module $\mathrm{Sym}^4(V)$ of the same dimension $D$. Since $\mathbf{Z}(E)$ acts trivially on $\mathrm{Sym}^4(V)$ but $E$ does not, and $N/E$ has two orbits of length $d(d+1)/2$ and $(d-2)(d+1)/2$ on the $2^{2a} - 1$ nontrivial irreducible characters of $E/\mathbf{Z}(E)$, we see from Clifford's theorem that one of these two lengths divides $D$. But this is impossible.

Next we show that $M_{4,4}(N,V) > M_{4,4}(\boldsymbol{G},V)$ in the case $\boldsymbol{G} = \mathrm{O}(V)$. Indeed, assume $N$ is irreducible on the simple $\boldsymbol{G}$-module $\mathrm{Sym}^4(V)/\mathrm{Sym}^2(V)$ of dimension

$$D' := 2^{a-2}(2^a+1)(2^{a-1}+3)(2^a-1)/3.$$

Since $\mathbf{Z}(E)$ acts trivially on $\mathrm{Sym}^4(V)/\mathrm{Sym}^2(V)$ but $E$ does not, and $N/E$ has two orbits of length $d(d-1)/2$ and $(d+2)(d-1)/2$ on the $2^{2a}-1$ nontrivial irreducible characters of $E/\mathbf{Z}(E)$, we see from Clifford's theorem that one of these two lengths divides $D'$. But this is again impossible.

To show that $M_{3,3}(N,V) = M_{3,3}(\boldsymbol{G},V)$, first we observe that $M_{3,3}(N,V) \geq M_{3,3}(\boldsymbol{G},V) = 15$. Next, as mentioned in the proof of [**GT2**, Proposition 5.2], the fixed point subspace of $E$ on $M^{\otimes 3}$, considered as an $N/E$-module, is the direct sum of 15 induced modules (from one-dimensional submodules). Arguing as in (i), we obtain the upper bound $M_{3,3}(N,V) \leq 15$, hence the equality $M_{3,3}(N,V) = 15$, and thus the 15 induced modules are in fact permutation modules. □

Proposition 1.4.7. (cf. [**GT2**, Proposition 5.3].) *Assume $\ell = 0$ and $p^a > 4$. Then $M_{3,3}(\boldsymbol{G},V) = M_{3,3}(G,V)$ if and only if $G$ is as described in case* (B) *of* [**GT2**, Theorem 1.6].

Proof. By Proposition 1.4.6 we may assume $p = 2$. In fact the proof of Proposition 1.4.6 establishes the "if" part of our claim. For the "only if" part, suppose that $M_{3,3}(G,V) = M_{3,3}(\boldsymbol{G},V)$. The decomposition of the $E$-fixed point subspace on $(V^* \otimes V)^{\otimes 3}$ as the sum of permutation $N/(EZ \cap N)$-modules in the proof of Proposition 1.4.6 also shows that $G/\mathbf{Z}(G)E$ has the same orbits on $W \times W$ as of $M := N/(EZ \cap N)$. Now the proof of [**GT2**, Proposition 5.3] shows that $H \geq [M,M]$, yielding the statement. □

CHAPTER 2

# Some basic facts about monodromy groups

## 2.1. Arithmetic semisimplicity

Let $k$ be a finite field of characteristic $p > 0$, $X/k$ a smooth, geometrically irreducible $k$-scheme, $\ell \neq p$ a prime, and $\mathcal{F}$ a lisse $\overline{\mathbb{Q}_\ell}$ sheaf on $X$ which is pure of some weight. By [**De2**, 3.4.1 (iii)], $\mathcal{F}$ is completely reducible (:= semisimple) as a representation of $\pi_1^{\mathrm{geom}}(X)$, or equivalently as a representation of its $G_{\mathrm{geom}}$. However, $\mathcal{F}$ need not be arithmetically semisimple, i.e. semisimple as a representation of $\pi_1^{\mathrm{arith}}(X)$. Equivalently, $\mathcal{F}$ need not be semisimple as a representation of its $G_{\mathrm{arith}}$. However, we have the following fundamental result of Faltings, Mori, and Zarhin, cf. [**Zar1**] and [**Zar2**, Theorem 1.2].

THEOREM 2.1.1. *Let $\mathcal{A}/X$ be an abelian scheme, with structural morphism $f : \mathcal{A} \to X$. Then $R^1 f_\star \overline{\mathbb{Q}_\ell}$ is arithmetically semisimple.*

Passing to Jacobians, we find

COROLLARY 2.1.2. *Let $\mathcal{C}/X$ be a proper smooth family of curves, with geometrically connected fibres of some genus $g \geq 1$, and structural morphism $f : \mathcal{C} \to X$. Then $R^1 f_\star \overline{\mathbb{Q}_\ell}$ is arithmetically semisimple, and hence every direct factor of $R^1 f_\star \overline{\mathbb{Q}_\ell}$ is arithmetically semisimple.*

In what follows, we often deal with the following situation: $X/k$ is an affine dense open set $\mathrm{Spec}\,(R)$ in an affine space $\mathbb{A}^n/k$, and $\mathcal{C}/X$ is either an Artin-Schreier curve of affine equation

$$y^p - y = \text{a polynomial } f_r(x) \in R[x] \text{ of degree } 2g+1,$$

(whose complete nonsingular model has a single point at $\infty$), or an Artin-Schreier-Witt curve (with Witt vectors of length two)

$$[u^p, v^p] - [u, v] = [a_r(x), b_r(x)]$$

with $a_r(x), b_r(x) \in R[x]$ polynomials each of which is Artin-Schreir reduced and of fixed degree $d_a, d_b$. Here too the complete nonsingular model has a single point at $\infty$.

In the Artin-Schreier case, the $R^1 f_\star$ is the direct sum of $p-1$ summands, each of rank $2g$, corresponding to the $p-1$ nontrivial additive characters $\psi$ of $\mathbb{F}_p$. The trace function of the $\psi$ component, call it $\mathcal{F}_\psi$, is given as follows. For $L/k$ a finite extension, and $r_0 \in R \otimes_k L$,

$$\mathrm{Trace}(\mathsf{Frob}_{r_0,L}|\mathcal{F}_\psi) = -\sum_{x \in L} \psi_L(f_{r_0}(x)).$$

In the Artin-Schreier-Witt case, there are $p^2 - p$ summands, each of rank $\max(pd_a, d_b)$, corresponding to the $p^2 - p$ faithful characters $\psi_2$ of $\mathbb{Z}/p^2Z$. The trace function of the $\psi_2$

component, call it $\mathcal{F}_{\psi_2}$, is given as follows. For $L/k$ a finite extension, and $r_0 \in R \otimes_k L$,

$$\mathrm{Trace}(\mathsf{Frob}_{r_0,L}|\mathcal{F}_{\psi_2}) = -\sum_{x \in L} \psi_{2,L}([a_{r_0}(x), b_{r_0}(x)]).$$

We will use without further reminders that these local systems are arithmetically semisimple, and we will refer to each of them simply as "the local system whose trace function is . . .".

## 2.2. Finiteness of $G_{\mathrm{geom}}$ and $G_{\mathrm{arith}}$

In this section, $\mathbb{F}_q$ is a finite field of characteristic $p$, and $X/\mathbb{F}_q$ is a smooth, geometrically connected $\mathbb{F}_q$-scheme. We also fix a choice of prime $\ell \neq p$, and consider lisse $\overline{\mathbb{Q}_\ell}$ sheaves $\mathcal{F}$ on $X$. Taking as base point an algebraic closure of the function field of $X$, we have the (profinite) arithmetic fundamental group

$$\pi_1^{\mathrm{arith}}(X) := \pi_1(X)$$

and its closed normal subgroup

$$\pi_1^{\mathrm{geom}}(X) := \pi_1(X \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}) \lhd \pi_1^{\mathrm{arith}}(X).$$

which sits in the short exact sequence

$$1 \to \pi_1^{\mathrm{geom}}(X) \to \pi_1^{\mathrm{arith}}(X) \to \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) \to 1.$$

A lisse $\overline{\mathbb{Q}_\ell}$ sheaf on $X$ of rank $d$ is a continuous representation $\rho_{\mathcal{F}} : \pi_1^{\mathrm{arith}}(X) \to \mathrm{GL}_d(\overline{\mathbb{Q}_\ell})$. One knows [**Ka-Sar**, 9.0.7] that for any such $\mathcal{F}$, there exists a finite extension $E_\lambda/\mathbb{Q}_\ell$ such that $\rho_{\mathcal{F}}$ has image in $\mathrm{GL}_d(E_\lambda)$, and indeed in a suitable basis has image in $\mathrm{GL}_d(\mathcal{O}_\lambda)$, for $\mathcal{O}_\lambda$ the ring of $\lambda$-adic integers in $E_\lambda$.

We say that $\mathcal{F}$ is *arithmetically semisimple* (respectively *geometrically semisimple*) if it is completely reducible as a representation of $\pi_1^{\mathrm{arith}}(X)$ (respectively $\pi_1^{\mathrm{geom}}(X)$). Similarly for the notions of *arithmetic* and *geometric irreducibility.*

Attached to $\mathcal{F}$ we have two algebraic groups, $G_{\mathrm{arith}}$ and $G_{\mathrm{geom}} \lhd G_{\mathrm{arith}} \subset \mathrm{GL}_d(\overline{\mathbb{Q}_\ell})$, namely

$$G_{\mathrm{geom},\mathcal{F}} := G_{\mathrm{geom}} := \text{the Zariski closure of } \rho_{\mathcal{F}}(\pi_1^{\mathrm{geom}}(X)),$$

$$G_{\mathrm{arith},\mathcal{F}} := G_{\mathrm{arith}} := \text{the Zariski closure of } \rho_{\mathcal{F}}(\pi_1^{\mathrm{arith}}(X)).$$

THEOREM 2.2.1. ([**KRLT1**, Prop. 2.1 and Remark 2.2]) *Suppose $\mathcal{F}$ is arithmetically semisimple and pure of weight zero for all embeddings of $\overline{\mathbb{Q}_\ell}$ into $\mathbb{C}$. Then $\mathcal{F}$ has finite $G_{\mathrm{arith}}$ if and only if for every finite extension $k/\mathbb{F}_q$ and every point $x \in X(k)$, the Frobenius $\mathsf{Frob}_{x,k}$ has* $\mathrm{Trace}(\mathsf{Frob}_{x,k}|\mathcal{F})$ *an algebraic integer.*

REMARK 2.2.2. Here is an example to show that the hypothesis of arithmetic semisimplicity is essential in the above Therem 2.2.1, cf. [**KRLT1**, Remark 2.2]. On $X/\mathbb{F}_q$, take the rank two sheaf $\mathcal{F}$ on which $\pi_1^{\mathrm{geom}}(X)$ acts trivially (so that $\mathcal{F}$ is geometrically isomorphic to $\overline{\mathbb{Q}_\ell} \oplus \overline{\mathbb{Q}_\ell}$), and on which $\pi_1^{\mathrm{arith}}(X)$ acts through its quotient $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ by having $\mathsf{Frob}_q$ act as the upper unipotent automorphism with matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Then $\mathcal{F}$ is arithmetically indecomposable, but its arithmetic semisimplification is trivial. Its $G_{\mathrm{arith},\mathcal{F}}$ is not finite, rather it is the upper unipotent group $\left\{\begin{pmatrix}1 & z\\ 0 & 1\end{pmatrix}\right\}$, but each of its Frobenius traces is the algebraic integer 2.

Conversely, if a sheaf $\mathcal{F}$ has finite $G_{\text{arith}}$, then in particular $G_{\text{arith}}$ is reductive, and hence $\mathcal{F}$ is arithmetically semisimple.

We also remark that if $\mathcal{F}$ has finite $G_{\text{arith}}$, then $\mathcal{F}$ is (trivially) pure of weight zero and (trivially) has $\det(\mathcal{F})$ arithmetically of finite order.

Theorem 2.2.1 implies the following consequence, which allows us to deduce finiteness of $G_{\text{arith}}$ (and $G_{\text{geom}}$) in all the cases we are interested in.

Corollary 2.2.3. *Suppose $\mathcal{F}$ is arithmetically semisimple and pure of weight zero for all embeddings of $\overline{\mathbb{Q}_\ell}$ into $\mathbb{C}$. Suppose further that for some finite extension $K/Q$, all Frobenius traces of $\mathcal{F}$ take values in $\mathcal{O}_K[1/p]$, for $\mathcal{O}_K$ the ring of integers of $K$. Then $\mathcal{F}$ has finite $G_{\text{arith}}$ if and only if all Frobenius traces are $p$-adically integral at all $p$-adic places $\wp$ of $K$.*

Theorem 2.2.4. ([**Ka-ESDE**, 8.14.3.1 and 8.14.4]) *Suppose $\mathcal{F}$ is geometrically irreducible and* $\det(\mathcal{F})$ *is arithmetically of finite order. Then $G_{\text{geom}}$ is finite if and only if $G_{\text{arith}}$ is finite. If $\mathcal{F}$ is pure of weight zero, this finiteness is equivalent to $\mathcal{F}$ having all its Frobenius traces algebraic integers.*

Lemma 2.2.5. *Suppose $\mathcal{F}$ is a finite direct sum $\mathcal{F} := \bigoplus_i \mathcal{F}_i$. Then $\mathcal{F}$ has finite $G_{\text{geom}}$ (respectively finite $G_{\text{arith}}$) if and only if each $\mathcal{F}_i$ has finite $G_{\text{geom}}$ (respectively finite $G_{\text{arith}}$). In general, without assuming finiteness in either of the two cases, i.e. arithmetic or geometric, the relevant group $G_{\mathcal{F}}$ is a subgroup of the product group $\prod_i G_{\mathcal{F}_i}$ which maps onto each factor.*

Proof. In each of the two (geometric and arithmetic) contexts, $\rho_{\mathcal{F}}$ is the direct sum of the $\rho_{\mathcal{F}_j}$. Thus $\text{Ker}(\rho_{\mathcal{F}})$ lies in each $\text{Ker}(\rho_{\mathcal{F}_i})$, so each of the latter groups will be of finite index in the appropriate $\pi_1$ if $\text{Ker}(\rho_{\mathcal{F}})$ is of finite index. Conversely, if each $\text{Ker}(\rho_{\mathcal{F}_i})$ is of finite index, then $\text{Ker}(\rho_{\mathcal{F}})$, being the intersection of these normal subgroups of finite index, is itself of finite index. In the finite monodromy case, each of the relevant monodromy groups is the literal image of $\rho_{\mathcal{F}}$, respectively of the $\rho_{\mathcal{F}_i}$ (the Zariski closure of a finite subgroup of a GL is itself).

In the finite case, the second assertion results from the fact that in each context, i.e. either geometric or arithmetic, $\rho_{\mathcal{F}}$ is the direct sum of the $\rho_{\mathcal{F}_j}$. If we no longer assume finiteness, then we must deal with the Zariski closures of the images on the respective $\pi_1(X)$ (i.e., either geometric or arithmetic) under the homomorphisms $\rho_{\mathcal{F}}$ and the $\rho_{\mathcal{F}_j}$. Let us temporarily denote these literal image groups as $\Gamma_{\mathcal{F}}$ and the $\Gamma_{\mathcal{F}_j}$. Then $\Gamma_{\mathcal{F}}$ is a subgroup of the product group $\prod_i \Gamma_{\mathcal{F}_j}$ which maps onto each factor. So we must check that an inclusion of subgroups $A < B < \text{GL}_d$ gives an inclusion of their Zariski closures, which is immediate from the definition of Zariski closure, and that given a finite product of subgroups $A_i < \text{GL}_{d_i}$, the Zariski closure of the product $\prod_i A_i$ in $\prod_i \text{GL}_{d_i}$ is the product of the individual Zariski closures of the $A_i < \text{GL}_{d_i}$. An obvious induction reduces us to treat the case of two factors, call them $X, Y$. Denoting the Zariski closure of $A$ by $\overline{A}$, we argue as follows. Since $\overline{X} \times \overline{Y}$ is closed and contains $X \times Y$, we have $\overline{X \times Y} \supseteq \overline{X} \times \overline{Y}$. Conversely, suppose a polynomial $f(x, y)$ vanishes on $X \times Y$. Then for any $x' \in X$, the polynomial $f(x', y)$ vanishes on $\{x'\} \times Y$, so it also vanishes on $\{x'\} \times \overline{Y}$. Thus $f$ vanishes on $X \times \overline{Y}$. Hence, for any $y' \in \overline{Y}$, the polynomial $f(x, y')$ vanishes on $X \times \{y'\}$, so it also vanishes on $\overline{X} \times \{y'\}$. Thus $f(x, y)$ vanishes on $\overline{X} \times \overline{Y}$, showing $\overline{X} \times \overline{Y} \subseteq \overline{X \times Y}$. □

Theorem 2.2.4 remains true under a weaker assumption.

THEOREM 2.2.6. *Suppose $\mathcal{F}$ is arithmetically irreducible and* $\det(\mathcal{F})$ *is arithmetically of finite order. Then $G_{\text{geom}}$ is finite if and only if $G_{\text{arith}}$ is finite.*

PROOF. Because $G_{\text{geom}} \leq G_{\text{arith}}$, it is obvious that if $G_{\text{arith}}$ is finite, then $G_{\text{geom}}$ is finite. To prove the converse, we argue as follows. Suppose that $\mathcal{F}$ has finite $G_{\text{geom}}$ and that $\det(\mathcal{F})$ is arithmetically of finite order.

One knows [**De3**, 1.2] that geometrically, $\mathcal{F}$ is the direct sum of pairwise non isomorphic constituents, transitively permuted by $\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$. For $n$ the number of such summands, and $X_n := X \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n}$, the pullback of $\mathcal{F}$ to $X_n$ is the direct sum of $n$ irreducible lisse sheaves $\mathcal{G}_i$ on $X_n$. For any of these, say $\mathcal{G}_1$, denoting by

$$\pi : X_n \to X$$

the projection, we have

$$\mathcal{F} \cong \pi_\star(\mathcal{G}_1).$$

By Lafforgue [**L**, VII.7], cf. also [**De3**, proof of 1.9], one knows that $\mathcal{F}$ is pure of weight zero. Therefore its pullback to $X_n$ is pure of weight zero, and hence each $\mathcal{G}_i$ is pure of weight zero. By Grothendieck's "the radical is unipotent" theorem [**De2**, 1.3.8, 1.3.9], one knows that $\det(\mathcal{G}_1)$ is geometrically of finite order, say of order $d$. Then $\det(\mathcal{G}_1)^{\otimes d}$ is geometrically trivial, so arithmetically of the form $\alpha^{\deg/\mathbb{F}_{q^n}}$. Choosing $\beta$ with $\beta^{nd} = 1/\alpha$, we have that $\mathcal{G}_1 \otimes \beta^{n\deg/\mathbb{F}_{q^n}}$ has determinant which is arithmetically of finite order.

On the other hand, $\mathcal{F}$ has finite $G_{\text{geom}}$, hence so does each $\mathcal{G}_i$, and hence so does $\mathcal{G}_1 \otimes \beta^{n\deg/\mathbb{F}_{q^n}}$ . Then by the previous Theorem 2.2.4, we conclude that$\mathcal{G}_1 \otimes \beta^{n\deg/\mathbb{F}_{q^n}}$ has finite $G_{\text{arith}}$. Therefore its direct image by $\pi$ has finite $G_{\text{arith}}$ (simply because $\pi_1(X_n) \lhd \pi_1(X)$ has finite index). But this direct image is $\mathcal{F} \otimes \beta^{\deg/\mathbb{F}_q}$. Therefore $\det(\mathcal{F} \otimes \beta^{\deg/\mathbb{F}_q})$ is arithmetically of finite order, i.e. $\det(\mathcal{F}) \otimes \beta^{\text{rank}(\mathcal{F})\deg/\mathbb{F}_q}$ is arithmetically of finite order. As $\det(\mathcal{F})$ is arithmetically of finite order by hypothesis, the quantity $\beta$ is itself a root of unity: $\mathcal{G}_1$ itself already had finite $G_{\text{arith}}$. □

REMARK 2.2.7. Here is an example to show that we can have a geometrically irreducible $\mathcal{F}$ which is pure of weight zero and with finite $G_{\text{geom}}$ whose $G_{\text{arith}}$ is not finite. Namely, we start with a geometrically irreducible $\mathcal{G}$ whose $G_{\text{arith}}$ is finite. We then choose an $\ell$-adic unit $\alpha$ which is pure of weight zero but which is not a root of unity. Then the constant field twist $\mathcal{F} := \mathcal{G} \otimes \alpha^{\deg}$ has the same $G_{\text{geom}}$ as $\mathcal{G}$, but its $G_{\text{arith}}$ is not finite, indeed $\det(\mathcal{F})$ is not arithmetically of finite order (precisely because $\alpha$ is not a root of unity). Here is a concrete example. Choose a prime number $r \neq \ell$ with $r \equiv 1 \pmod 4$, so that $r = a^2 + b^2$ for some $a, b \in \mathbb{Z}$. Then take $\alpha := (a + bi)/(a - bi)$.

## 2.3. Geometric and arithmetic determinants

We begin with a general result on geometric determinants.

Proposition 2.3.1. *Let $p$ be a prime, $\ell \neq p$ a second prime, $\mathbb{F}_q/\mathbb{F}_p$ be a finite extension, $d \geq 1$ an integer, and $\mathcal{F}$ a $\overline{\mathbb{Q}_\ell}$-local system on $\mathbb{A}^d/\mathbb{F}_q$. Suppose that all Frobenius traces of $\mathcal{F}$ take values in a field $K$. Define the integer $N \geq 0$ to be the largest integer $n$ such that the group $\mu_{p^n}(\overline{\mathbb{Q}_\ell})$ lies in $K$. Then* $\det(\mathcal{F})$ *is geometrically of order dividing $p^N$.*

Proof. We may replace $\mathcal{F}$ by its determinant, which still takes values in $K$. Thus we are reduced to the case when $\mathcal{F}$ is lisse of rank one, call it $\mathcal{L}$. By Grothendieck's global version of his local monodromy theorem, cf. [**De2**, 1.3.8], the group $G_{\mathrm{geom}}$ for $\mathcal{L}$ is a semisimple subgroup of $\mathrm{GL}_1$, i.e., it is a finite group, hence it is $\mu_A$ for some integer $A \geq 1$. We first observe that $A$ is some power $p^n$ of $p$ for some $n \geq 0$. Indeed, if we write $A = A_0 p^n$ with $p \nmid A_0$, then $\mathcal{L}^{\otimes p^n}$ is geometrically of order $A_0$ prime to $p$. But $\pi_1^{\mathrm{geom}}$ of $\mathbb{A}^d/\mathbb{F}_q$ has no nontrivial prime to $p$ quotient. Thus $A_0 = 1$. Thus $\mathcal{L}$ is geometrically of order $p^n$ for some $n \geq 0$.

Suppose first that $\mathcal{L}$ satisfies the following condition: for every integer $d \geq 1$ and every point $x \in \mathbb{A}^d(\mathbb{F}_{q^d})$, we have

$$\mathrm{Trace}(\mathsf{Frob}_{x,\mathbb{F}_{q^d}}|\mathcal{L}) = (\mathrm{Trace}(\mathsf{Frob}_{0,\mathbb{F}_q}|\mathcal{L}))^d.$$

Then we claim that $\mathcal{L}$ is geometrically trivial, or equivalently that $\mathcal{L}$ as a character of $\pi_1^{\mathrm{arith}}$ is trivial on $\pi_1^{\mathrm{geom}}$, or equivalently that as a character of $\pi_1^{\mathrm{arith}}$ it factors through the quotient $\pi_1^{\mathrm{arith}}/\pi_1^{\mathrm{geom}} \cong \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$, i.e. as a function on $\hat{}\mathbb{Z}$ of the form $d \mapsto \alpha^d$ for some $\alpha$. By Chebotarev, it suffices to check this on Frobenius elements in $\pi_1^{\mathrm{arith}}$, which is exactly the displayed equation, with $\alpha := \mathrm{Trace}(\mathsf{Frob}_{0,\mathbb{F}_q}|\mathcal{L})$.

Thus the minimal $n$ such that $\mathcal{L}$ is geometrically of order $p^n$ is the minimal $n$ such that for every integer $d \geq 1$ and every point $x \in \mathbb{A}^d(\mathbb{F}_{q^d})$, we have

$$(\mathrm{Trace}(\mathsf{Frob}_{x,\mathbb{F}_{q^d}}|\mathcal{L}))^{p^n} = (\mathrm{Trace}(\mathsf{Frob}_{0,\mathbb{F}_q}|\mathcal{L}))^{dp^n}.$$

If this holds, then each ratio

$$\mathrm{Trace}(\mathsf{Frob}_{x,\mathbb{F}_{q^d}}|\mathcal{L})/(\mathrm{Trace}(\mathsf{Frob}_{0,\mathbb{F}_q}|\mathcal{L}))^d$$

must lie in $\mu_{p^n}$, and $n$ is minimal such that this holds. But these ratios all lie in $K$, which therefore contains $\mu_{p^n}$. □

Here is a variant.

Proposition 2.3.2. *Let $p$ be a prime, $\ell \neq p$ a second prime, $\mathbb{F}_q/\mathbb{F}_p$ be a finite extension, $X/\mathbb{F}_q$ a smooth, geometrically connected $\mathbb{F}_q$-scheme, and $\mathcal{F}$ a $\overline{\mathbb{Q}_\ell}$-local system on $X$. Suppose that all Frobenius traces of $\mathcal{F}$ take values in a field $K$ (which we may always take to be a finite extension of $\mathbb{Q}_\ell$, cf.* [**Ka-Sar**, 9.0.7]*). Denote by $A$ the order of the group of all roots of unity in $K$. The* $\det(\mathcal{F})$ *is geometrically of order dividing $A$.*

Proof. The question is geometric, so at the expense of replacing $\mathbb{F}_q$ by a finite extension, we reduce to the case when $X(\mathbb{F}_q)$ is nonempty. Choosing a point $x_0 \in X(\mathbb{F}_q)$, the argument proving Proposition 2.3.1 shows that the geometric order of $\det(\mathcal{F})$ is the order of the subgroup of $K^\times$ generated by all ratios

$$\det(\mathsf{Frob}_{x,\mathbb{F}_{q^d}}|\mathcal{F})/\det(\mathsf{Frob}_{x_0,\mathbb{F}_q}|\mathcal{F})^d$$

for all $d \geq 1$ and all $x \in X(\mathbb{F}_{q^d})$. □

In this section, $p$ is a prime, $\ell$ is a prime $\ell \neq p$ (specified so we can speak of $\overline{\mathbb{Q}_\ell}$-adic cohomology), $\psi$ is a nontrivial additive character of $\mathbb{F}_p$, $k = \mathbb{F}_q$ is a finite extension of $\mathbb{F}_p$, $\chi$ is a (possibly trivial) multiplicative character of $k^\times$, $D \geq 3$ is an integer which is prime to $p$, and a strictly positive integer $d < D$. For an integer $N$ prime to $p$, we denote by $\psi_N$ the additive character $x \mapsto \psi(Nx)$, and by $\psi_{k,N}$ its extension to $k$ by composition with the trace: $\psi_{k,N}(x) := \psi(\mathrm{Tr}_{k/\mathbb{F}_p}(Nx))$. We write

$$\psi_k := \psi_{k,1}.$$

We next recall the notion of Kummer and Artin-Schreier sheaves. The *Artin-Schreier sheaf* $\mathcal{L}_\psi$ is the lisse rank one sheaf on $\mathbb{A}^1/\mathbb{F}_p$ whose trace function at a point $t \in k$, for $k$ a finite extension of $\mathbb{F}_p$, is

$$\mathrm{Trace}(\mathsf{Frob}_{t,k}|\mathcal{L}_\psi) := \psi_k(t),$$

with $\psi_k$ as defined above. For any scheme $X/\mathbb{F}_p$, and any function $f$ on $X$, we view $f$ as a morphism to $\mathbb{A}^1$, and define $\mathcal{L}_{\psi(f)} := f^\star\mathcal{L}_\psi$ as a lisse sheaf on $X$. For $k/\mathbb{F}_p$ a finite extension and $x \in X(k)$, we have

$$\mathrm{Trace}(\mathsf{Frob}_{x,k}|\mathcal{L}_{\psi(f)}) := \psi_k(f(x)).$$

For a multiplicative character $\chi$ of a finite extension $k$ of $\mathbb{F}_p$, the *Kummer sheaf* $\mathcal{L}_\chi$ on $\mathbb{G}_m/k$ is the lisse sheaf of rank one whose trace function at a point $t \in E^\times$, for $E$ a finite extension of $k$, is

$$\mathrm{Trace}(\mathsf{Frob}_{t,E}|\mathcal{L}_\chi) := \chi_E(t),$$

with $\chi_E := \chi \circ \mathrm{Norm}_{E/k}$. By abuse of notation, for $\chi$ nontrivial we also let $\mathcal{L}_\chi$ denote the sheaf $j_!\mathcal{L}_\chi$ on $\mathbb{A}^1/k$ for the inclusion $j : \mathbb{G}_m \to \mathbb{A}^1$: it has trace 0 at time 0. For any scheme $X/k$ and any invertible function $f$ on $X$, we view $f$ as a morphism to $\mathbb{G}_m$, and define $\mathcal{L}_{\chi(f)} := f^\star\mathcal{L}_\chi$ as a lisse sheaf on $X$. For $E/k$ a finite extension and $x \in X(E)$, we have

$$\mathrm{Trace}(\mathsf{Frob}_{x,E}|\mathcal{L}_{\chi(f)}) := \chi_E(f(x)).$$

Theorem 2.3.3. *Fix a monic polynomial*

$$f(X) = X^D + \sum_{i=1}^{d} a_i X^i \in k[X].$$

*We have the following results.*

(i) *If* $D = 2d+1$ *is odd, then*

$$\det\big(\mathsf{Frob}_q|H^1_c(\mathbb{A}^1/\overline{k}, \mathcal{L}_{\psi(f(X))})\big) = q^d$$

(ii) *If* $D = 2d+2$ *is even, then*

$$\det\big(\mathsf{Frob}_q|H^1_c(\mathbb{A}^1/\overline{k}, \mathcal{L}_{\psi(f(X))})\big) = \big(-\mathsf{Gauss}(\psi_{k,D/2}, \chi_2)\big)q^d.$$

(iii) *If* $D = 2d+1$ *is odd and* $\chi$ *is nontrivial, then*

$$\det\big(\mathsf{Frob}_q|H^1_c(G_m/\overline{k}, \mathcal{L}_{\psi(f(X))} \otimes \mathcal{L}_{\chi(X)})\big) = \big(-\mathsf{Gauss}(\psi_{k,D}, \chi)\big)q^d.$$

(iv) *If* $D = 2d+2$ *is even and* $\chi$ *is nontrivial, then*

$$\det\big(\mathsf{Frob}_q|H^1_c(\mathbb{G}_m/\overline{k}, \mathcal{L}_{\psi(f(X))} \otimes \mathcal{L}_{\chi(X)})\big) = \big(-\mathsf{Gauss}(\psi_{k,-D}, \chi)\big)\big(-\mathsf{Gauss}(\psi_{k,D/2}, \chi_2)\big)q^d.$$

PROOF. Exactly as in the proof of [**KT1**, 2.3], we unify the first two cases, where "there is no $\chi$", with cases (iii) and (iv) by replacing $H^1_c(A^1/\overline{k}, \mathcal{L}_{\psi(f(X))})$ by $H^1_c(\mathbb{G}_m/\overline{k}, \mathcal{L}_{\psi(f(X))})$, and allowing $\chi = \mathbb{1}$ in cases (iii) and (iv). This changes the dimension of the cohomology group from $D-1$ to $D$, but does so by adding the extra eigenvalue 1. So this does not change the determinant. In the formulas (iii) and (iv), the factor $(-\mathsf{Gauss}(\psi_k, \mathbb{1}))$ is also 1.

On the one hand, the $L$-function is given cohomologically by

$$L(T) = \det\big(1 - (\mathsf{Frob}_q T | H^1_c(\mathbb{G}_m/\overline{k}, \mathcal{L}_{\psi(f(X))} \otimes \mathcal{L}_{\chi(X)})\big).$$

The Hasse-Davenport method is to write the additive form of the $L$-function:

$$L(T) = 1 + \sum_{n \geq 1} A_n T^n,$$

$$A_n = \sum_{\substack{\text{monic } P(X) \in k[X], \\ \deg(P) = n, P(0) \neq 0}} \chi(P(0)) \psi_k\big(\sum_{\substack{\text{roots } \alpha \\ \text{of } P}} f(\alpha)\big).$$

The "miracle" is that $L(T)$ is not an infinite series, but rather a polynomial of degree $D$. Comparing the coefficients of the term of degree $D$, we get

$$(-1)^D \det(\mathsf{Frob}_q | H^1_c(\mathbb{G}_m/\overline{k}, \mathcal{L}_{\psi(f(X))} \otimes \mathcal{L}_{\chi(X)})) = A_D.$$

Thus our determinant is $(-1)^D A_D$. To compute $A_D$, we argue as follows. To deal with the expression inside the $\psi$, we observe that for each integer $n$, the sum of the $n^{\text{th}}$ powers of the roots of $P$ is simply the $n^{\text{th}}$ Newton function $N_n(\text{roots of } P)$, which is a universal polynomial in the coefficients of $P$ that we also denote by $N_n$. Thus

$$\begin{aligned}\sum_{\text{roots } \alpha \text{ of } P} f(\alpha) &= \sum_{\text{roots } \alpha \text{ of } P} \big(\alpha^D + \sum_{i=1}^{d} a_i \alpha^i\big) \\ &= N_D(\text{roots of } P) + \sum_{i=1}^{d} a_i N_i(\text{roots of } P),\end{aligned}$$

and hence

$$A_D = \sum_{S_1, \ldots, S_D \in k,\, S_D \neq 0} \chi(S_D) \psi_k\big(N_D(S_1, \ldots, S_D) + \sum_{i=1}^{d} a_i N_i(S_1, \ldots, S_D)\big).$$

We compute the $N_i$ as polynomials in the $S_j$ by the identity

$$1/(1 + \sum_{i \geq 1} (-1)^i S_i T^i) = \exp(\sum_{n \geq 1} N_n T^n/n).$$

Applying $d/dT$, we have the identity

$$-(\sum_{i \geq 1} (-1)^i i S_i T^i)/(1 + \sum_{j \geq 1} (-1)^j S_j T^j) = \sum_{n \geq 1} N_n T^n.$$

We now expand the left side, as

$$-(\sum_{i \geq 1} (-1)^i i S_i T^i)(1 + \sum_{m \geq 1} (-\sum_{j \geq 1} (-1)^j S_j T^j)^m).$$

When we ignore all but the first two terms in the geometric series, we find that $N_D$, the coefficient of $T^D$, is thus

$$N_D = (-1)^{D+1}DS_D - \sum_{i+j=D,\, i\geq 1,\, j\geq 1} (-1)^i iS_i(-1)^{j+1}S_j + R,$$

with $R$ a polynomial in which every monomial has usual degree $\geq 3$ in the variables $S_i$.

Let us first look at the case when $D = 2d+1$ is odd. Combining the terms $S_iS_{D-i}$ and $S_{D-i}S_i$, their coefficients add to $(-1)^D D$, we see that

$$N_D = (-1)^{D+1}DS_D + (-1)^D D\sum_{i=1}^{d} S_iS_{D-i} + R_D,$$

with $R_D$ isobaric of weight $D$ in the $S_i$ but in which every monomial has usual degree $\geq 3$. Thus $(-1)^D A_D$ is equal to

$$\sum_{S_1,\ldots,S_D\in k,\, S_D\neq 0} \chi(S_D)\psi_k\big((-1)^{D+1}DS_D + (-1)^D D\sum_{i=1}^{d} S_iS_{D-i} + R_D + \sum_{i=1}^{d} a_iN_i(S_1,\ldots,S_i)\big),$$

where we use the fact that $N_i$ is a polynomial in $S_1,\ldots,S_i$. The variable $S_D$ occurs only once, so $(-1)^D A_D$ is now equal to

$$\big(\sum_{S_D\in k^\times} \chi(S_D)\psi_k((-1)^{D+1}DS_D)\big) \sum_{S_1,\ldots,S_{D-1}\in k} \psi_k\big((-1)^D D\sum_{i=1}^{d} S_iS_{D-i}+R_D+\sum_{i=1}^{d} a_iN_i(S_1,\ldots,S_i)\big).$$

Because $N_D$ is isobaric of degree $D$, for each $i\leq d$, the variable $S_{D-i}$ appears in this sum as

$$(-1)^D DS_{D-i}\big(S_i + \text{a polynomial in only the } S_j, j<i, \text{every monomial of usual degree } \geq 2\big).$$

Summing first over $S_{D-1}$, we get 0 unless $S_1 = 0$, in which case we get $q$. Once we know $S_1 = 0$ in our sum, summing over $S_{D-2}$ gives 0 unless $S_2 = 0$, in which case we get $q$. Continuing in this way we get

$$A_D = q^d\big(\sum_{S_D\in k^\times} \chi(S_D)\psi_k((-1)^{D+1}DS_D)\big)\mathsf{Gauss}(\psi_{k,(-1)^{D+1}D},\chi),$$

and thus $\det(\mathsf{Frob}_k) = (-1)^D\mathsf{Gauss}(\psi_{k,(-1)^{D+1}D},\chi)q^d$.

When $D = 2d+2$ is even, the only difference is that the coefficient of $T^D$ now has the extra term $S_{D/2}S_{D/2}$, which occurs with coefficient $(-1)^D(D/2)$. This extra "middle term" persists, and at the end of the argument getting the previous answer, this "middle term" creates an extra factor $\mathsf{Gauss}(\psi_{k,(-1)^D(D/2)},\chi_2)$.

Thus for $D = 2d+1$ odd, the determinant is $(-\mathsf{Gauss}(\psi_{k,D},\chi))q^d$, while for $D = 2d+2$ even it is $(-\mathsf{Gauss}(\psi_{k,D/2},\chi_2))(-\mathsf{Gauss}(\psi_{k,-D},\chi))q^d$. □

Corollary 2.3.4. *Suppose we are given a prime to $p$ integer $D\geq 3$, and a multiplicative character $\chi$ of a finite extension $k = \mathbb{F}_q$ of $\mathbb{F}_p$, and a strictly positive integer $d < D$. Consider the lisse sheaf $\mathcal{F}(D,\leq d,\chi)$ on $\mathbb{A}^d/k$ whose trace function is given as follows.*

(a) *For $\mathcal{F}(D, \leq d, \mathbb{1})$ on $\mathbb{A}^d/\mathbb{F}_p$, $L/\mathbb{F}_p$ a finite extension, and $(a_1, \ldots, a_d) \in L^d$, the trace is*

$$(a_1, \ldots, a_d) \mapsto -\sum_{x \in L} \psi_L(x^D + \sum_{i=1}^{d} a_i x^i).$$

(b) *For $\mathcal{F}(D, \leq d, \chi)$ with $\chi$ a nontrivial character of $k^\times$, $L/k$ a finite extension, and $(a_1, \ldots, a_d) \in L^d$, the trace is*

$$(a_1, \ldots, a_d) \mapsto -\sum_{x \in L} \psi_L(x^D + \sum_{i=1}^{d} a_i x^i)\chi_L(x).$$

*These local systems are geometrically irreducible, pure of weight one, of ranks $D-1$ and $D$ respectively. For $d := [(D-1)/2]$, their geometric determinants are trivial. Moreover, we have the following results on their arithmetic determinants.*

(i) *If $D = 2d+1$ is odd, then for either choice of $\sqrt{p}$, the local system $\mathcal{F}(D, \leq d, \mathbb{1})(1/2)$ has arithmetically trivial determinant. Indeed, for any choice of $\alpha_{D,\mathbb{1}}$ with $(\alpha_{D,\mathbb{1}})^{D-1} = p^d$, the local system $\mathcal{F}(D, \leq d, \mathbb{1}) \otimes (\alpha_{D,\mathbb{1}})^{-\deg}$ has arithmetically trivial determinant.*

(ii) *If $D = 2d+2$ is even, then for any choice of $\alpha_{D,\mathbb{1}}$ with*

$$(\alpha_{D,\mathbb{1}})^{D-1} = (-\mathsf{Gauss}(\psi_{D/2}, \chi_2))p^d,$$

*the local system $\mathcal{F}(D, \leq d, \mathbb{1}) \otimes (\alpha_{D,\mathbb{1}})^{-\deg}$ has arithmetically trivial determinant.*

(iii) *If $D = 2d+1$ is odd, then for any choice of $\alpha_{D,\chi}$ with*

$$(\alpha_{D,\chi})^D = (-\mathsf{Gauss}(\psi_{k,D}, \chi))q^d,$$

*the local system $\mathcal{F}(D, \leq d, \chi) \otimes (\alpha_{D,\chi})^{-\deg/k}$ has arithmetically trivial determinant.*

(iv) *If $D = 2d+2$ is even, then for any choice of $\alpha_{D,\chi}$ with*

$$(\alpha_{D,\chi})^D = (-\mathsf{Gauss}(\psi_{k,-D}, \chi))(-\mathsf{Gauss}(\psi_{k,D/2}, \chi_2)))q^d,$$

*the local system $\mathcal{F}(D, \leq d, \chi) \otimes (\alpha_D, \chi)^{-\deg/k}$ has arithmetically trivial determinant.*

PROOF. That the sheaves $\mathcal{F}(D, \leq d, \chi)$ are lisse results from the fact that their ranks are constant and they are sheaves of perverse origin in the sense of [**Ka-Scont**]. The purity is due to Weil. The explicit formulas for their determinants, and the behavior of Gauss sums under field extension give the asserted arithmetic triviality of the $\alpha_{D,\chi}$-twisted sheaves. Each is geometrically irreducible because already pulled back to the $\mathbb{A}^1$ which is $(s_1, 0, \ldots, 0)$ each is the Fourier transform of a lissse rank one sheaf on $\mathbb{G}_m$, extended across 0 by direct image (and hence perverse irreducible on $\mathbb{A}^1$). □

REMARK 2.3.5. Suppose we "go too far" in Theorem 2.3.3 when $D$ is even, in the sense that we also allow a term $a_{D/2}X^{D/2}$ in $f(X)$. What changes in the argument is that the involvement of $S_{D/2}$ now comes also from the $N_{D/2}$ term, so that what was previously the sum

$$\sum_{S_{D/2} \in k} \psi_k((-1)^D(D/2)(S_{D/2})^2) = \mathsf{Gauss}(\psi_{k,(-1)^D(D/2)}, \chi_2)$$

now becomes

$$\sum_{S_{D/2}\in k} \psi_k((-1)^D(D/2)(S_{D/2})^2 - (-1)^{D/2}a_{D/2}(D/2)S_{D/2}) =$$

$$= \mathsf{Gauss}(\psi_{k,(-1)^D(D/2)}, \chi_2)\psi_{k,(-1)^D(D/2)}((-a_{D/2})^2/4),$$

the last equality by completing the square. The consequence for the corresponding local systems on $\mathbb{A}^{d+1}$ in cases (ii) and (iv) of Corollary 2.3.4 is that even after the $\alpha_{D,\chi}$ twistings, their arithmetic and geometric determinants are no longer trivial, but are rather $\mathcal{L}_{\psi_{k,(-1)^D(D/2)}((-a_{D/2})^2/4)}$.

Similarly, suppose we "go too far" in Theorem 2.3.3 when $D = 2d + 1$ is odd, in the sense that we also allow a term $a_{d+1}X^{d+1}$ in $f(X)$. What changes now is at the end of the argument, when we have already set $S_1, \ldots, S_{d-1}$ to vanish, the terms involving $S_{d+1}$ and $S_d$, previously just the single term $(-1)^D DS_{d+1}S_d$, are now

$$(-1)^D DS_{d+1}S_d + (-1)^{d+2}(d+1)a_{d+1}S_{d+1} + (-1)^{d+1}da_dS_d =$$

$$= S_{d+1}\big((-1)^D DS_d + (-1)^{d+2}(d+1)a_{d+1}\big) + (-1)^{d+1}da_dS_d.$$

So when we sum over $S_{d+2}$ we solve for $S_d$ and get $q$ times $\psi_k(-d(d+1)a_da_{d+1}/D)$. The consequence for the corresponding local systems on $\mathbb{A}^{d+1}$ in cases (i) and (iii) of Corollary 2.3.4 is that even after the $\alpha_{D,\chi}$ twistings, their arithmetic and geometric determinants are no longer necessarily trivial, but are rather $\mathcal{L}_{\psi_k(-d(d+1)a_da_{d+1}/D)}$.

The second part of the above Remark 2.3.5 gives the following corollary.

Corollary 2.3.6. *For $D = 2d + 1$, and any $\chi$, consider the local system $\mathcal{F}(D, d+1, \le d-1, \chi)$ on $\mathbb{A}^d/\mathbb{F}_q$ whose trace function is given as follows. For $k/\mathbb{F}_q$ a finite extension, and $(a_1, \ldots, a_{d-1}, a_{d+1}) \in \mathbb{A}^d(k)$,*

$$(a_1, \ldots, a_{d-1}, a_{d+1}) \mapsto -\sum_{x\in k^\times} \psi_k(x^D + a_{d+1}x^{d+1} + \sum_{i=1}^{d-1} a_ix^i)\chi_k(x).$$

*Its geometric determinant is trivial, and after an $\alpha_{D,\chi}$ twist, its arithmetic determinant is trivial as well.*

A second, somewhat artificial, corollary is this.

Corollary 2.3.7. *If $p|d(d+1)$, then $\mathcal{F}(D, \le d+1, \chi)$ has geometrically trivial determinant, and its $\alpha_{D,\chi}$ twist has arithmetically trivial determinant.*

The next corollary is an exercise in Gauss sums, left to the reader.

Corollary 2.3.8. *We have the following results about the systems $\mathcal{F}(D, \le d, \chi)$ introduced in Theorem 2.3.3.*

(i) *If $p$ is odd, and $D = 2d+1$ is odd, then for either choice* Gauss *of quadratic Gauss sum over $\mathbb{F}_p$, the local system*

$$\mathcal{F}(D, \le d, \mathbb{1}) \otimes (-\mathsf{Gauss})^{-\deg}$$

*on $\mathbb{A}^d/\mathbb{F}_p$ has arithmetic determinant $(\chi_2(-1)^d)^{\deg}$ (which is trivial if either $d$ is even or if $p \equiv 1 \bmod 4$, otherwise is $(-1)^{\deg}$). In all cases, the pullback of $\mathcal{F}(D, \le d, \mathbb{1}) \otimes (-\mathsf{Gauss})^{-\deg}$ to $\mathbb{A}^d/\mathbb{F}_{p^2}$ has arithmetically trivial determinant.*

(i-bis) *If $p = 2$ and $D = 2d + 1$ is odd, then on $\mathbb{A}^d/\mathbb{F}_{p^2}$, the local system*

$$\mathcal{F}(D, \leq d, \mathbb{1}) \otimes (p)^{-\deg/\mathbb{F}_{p^2}}$$

*has arithmetically trivial determinant.*

(ii) *If $D = 2d + 2$ is even (which forces $p$ to be odd), then the local system*

$$\mathcal{F}(D, \leq d, \mathbb{1}) \otimes (-\mathsf{Gauss}(\psi_{(-1)^d D/2}, \chi_2))^{-\deg}$$

*on $\mathbb{A}^d/\mathbb{F}_p$ has arithmetically trivial determinant.*

(iii) *If $p$ is odd, and $D = 2d + 1$ is odd, then the local system*

$$\mathcal{F}(D, \leq d, \chi_2) \otimes (-\mathsf{Gauss}(\psi_{(-1)^d D}, \chi_2))^{-\deg}$$

*on $\mathbb{A}^d/\mathbb{F}_p$ has arithmetically trivial determinant.*

(iii-bis) *If $D = 2d + 1$ is odd, $q$ a power of $p$ and $\chi$ a nontrivial character of $\mathbb{F}_{q^2}^\times$ of order dividing $q + 1$, then the local system*

$$\mathcal{F}(D, \leq d, \chi) \otimes (-\mathsf{Gauss}(\psi_{\mathbb{F}_{q^2}, -D}, \chi))^{-\deg/\mathbb{F}_{q^2}}$$

*on $\mathbb{A}^d/\mathbb{F}_{q^2}$ has arithmetically trivial determinant.* [Notice that every element of $\mathbb{F}_q^\times$, in particular $-D$, becomes a $(q + 1)^{\text{th}}$ power in $\mathbb{F}_{q^2}$ (surjectivity of the norm), so we could as well use $(-\mathsf{Gauss}(\psi_{\mathbb{F}_{q^2}}, \chi))^{-\deg}$.]

(iii-ter) *If $D = 2d + 1$ is odd, $p = 2$, $q$ a power of $p$ and $\chi$ a nontrivial character of $\mathbb{F}_{q^2}^\times$ of order dividing $q + 1$, then the local system*

$$\mathcal{F}(D, \leq d, \chi) \otimes (-q)^{-\deg/\mathbb{F}_{q^2}}$$

*on $\mathbb{A}^d/\mathbb{F}_{q^2}$ has arithmetically trivial determinant. Indeed, when $p = 2$, then by Stickelberger's theorem* [**BEW**, Theorem.11.6.1], $-\mathsf{Gauss}(\psi_{\mathbb{F}_{q^2}, -D}, \chi) = -q$. *Hence on $\mathbb{A}^d/\mathbb{F}_{q^4}$, the local system*

$$\mathcal{U}_{D,\chi} \otimes (q^2)^{-\deg/\mathbb{F}_{q^4}}$$

*has arithmetically trivial determinant, simply by the Hasse-Davenport relation*

$$-\mathsf{Gauss}(\psi_{\mathbb{F}_{q^4}, -D}, \chi) = (-\mathsf{Gauss}(\psi_{\mathbb{F}_{q^2}, -D}, \chi))^2.$$

(iv) *If $D = 2d + 2$ is even (which forces $p$ to be odd), then for either choice* $\mathsf{Gauss}$ *of quadratic Gauss sum over $\mathbb{F}_p$, the local system*

$$\mathcal{F}(D, \leq d, \chi_2) \otimes (-\mathsf{Gauss}(\psi, \chi_2))^{-\deg}$$

*on $\mathbb{A}^d/\mathbb{F}_p$ has arithmetic determinant $(\chi_2(-2))^{\deg}$.*

(iv-bis) *If $D = 2d + 2$ is even, $q$ a power of $p$ and $\chi$ a nontrivial character of $\mathbb{F}_{q^2}^\times$ of order $m$ dividing $q + 1$, then the local system*

$$\mathcal{F}(D, \leq d, \chi) \otimes q^{-\deg/\mathbb{F}_{q^2}}$$

*on $\mathbb{A}^d/\mathbb{F}_{q^2}$ has arithmetic determinant $\left((-1)^{\frac{q+1}{2} + \frac{q+1}{m}}\right)^{-\deg/\mathbb{F}_{q^2}}$, this last statement using Stickelberger's determination* [**BEW**, 11.6.1] *of* $\mathsf{Gauss}(\psi_{\mathbb{F}_{q^2}, -D}, \chi)$ *as being* $(-1)^{(q+1)/m} q$.

In general, we can only say the following about geometric determinants.

Lemma 2.3.9. *For any character $\chi$ of $k^\times$ for $k/\mathbb{F}_p$ a finite extension, the system $\mathcal{F}(D, \leq D-1, \chi)$ and any pullback of it has geometric determinant of order dividing $p$.*

Proof. This is immediate from Proposition 2.3.1, since the $K$ there for $\mathcal{F}(D, \leq D-1, \chi)$ can be taken to be $\mathbb{Q}(\zeta_p, \text{values of } \chi)$. □

We will now give a variant of the above results. The proof of Theorem 2.3.10 below is a very slight variation on the proof of Theorem 2.3.3, but we include it for the convenience of the reader.

Theorem 2.3.10. *Let $\mathbb{F}_q/\mathbb{F}_p$ be a finite extension, and $D \geq 3$ a prime to $p$ integer. Fix a polynomial*

$$f(X) = a_D X^D + \sum_{i=1}^{d} a_i X^i \in k[X]$$

*with* $\deg(f) = D$. *We have the following results.*

(i) *If $D = 2d+1$ is odd, then*

$$\det\bigl(\mathsf{Frob}_q | H^1_c(\mathbb{A}^1/\overline{k}, \mathcal{L}_{\psi(f(X))})\bigr) = q^d$$

(ii) *If $D = 2d+2$ is even, then*

$$\det\bigl(\mathsf{Frob}_q | H^1_c(\mathbb{A}^1/\overline{k}, \mathcal{L}_{\psi(f(X))})\bigr) = \chi_2((D/2)a_D)(-\mathsf{Gauss}(\psi_k, \chi_2))q^d.$$

(iii) *If $D = 2d+1$ is odd and $\chi$ is nontrivial, then*

$$\det\bigl(\mathsf{Frob}_q | H^1_c(G_m/\overline{k}, \mathcal{L}_{\psi(f(X))} \otimes \mathcal{L}_{\chi(X)})\bigr) = \overline{\chi}(-Da_D)(-\mathsf{Gauss}(\psi_k, \chi))q^d.$$

(iv) *If $D = 2d+2$ is even and $\chi$ is nontrivial, then*

$$\det\bigl(\mathsf{Frob}_q | H^1_c(\mathbb{G}_m/\overline{k}, \mathcal{L}_{\psi(f(X))} \otimes \mathcal{L}_{\chi(X)})\bigr) = \chi_2((D/2)a_D)\overline{\chi}(-Da_D)(-\mathsf{Gauss}(\psi_k\chi_2))(-\mathsf{Gauss}(\psi_k, \chi))q^d.$$

Proof. Exactly as in the proof of [**KT1**, 2.3], we unify the first two cases, where "there is no $\chi$", with cases (iii) and (iv) by replacing $H^1_c(A^1/\overline{k}, \mathcal{L}_{\psi(f(X))})$ by $H^1_c(\mathbb{G}_m/\overline{k}, \mathcal{L}_{\psi(f(X))})$, and allowing $\chi = \mathbb{1}$ in cases (iii) and (iv). This changes the dimension of the cohomology group from $D-1$ to $D$, but does so by adding the extra eigenvalue 1. So this does not change the determinant. In the formulas (iii) and (iv), the factor $(-\mathsf{Gauss}(\psi_k, \mathbb{1}))$ is also 1.

On the one hand, the $L$-function is given cohomologically by

$$L(T) = \det\bigl(1 - \mathsf{Frob}_q T | H^1_c(\mathbb{G}_m/\overline{k}, \mathcal{L}_{\psi(f(X))} \otimes \mathcal{L}_{\chi(X)})\bigr).$$

The Hasse-Davenport method is to write the additive form of the $L$-function:

$$L(T) = 1 + \sum_{n \geq 1} A_n T^n,$$

$$A_n = \sum_{\substack{\text{monic } P(X) \in k[X], \\ \deg(P) = n, P(0) \neq 0}} \chi(P(0))\psi_k\Bigl(\sum_{\substack{\text{roots } \alpha \\ \text{of } P}} f(\alpha)\Bigr).$$

The "miracle" is that $L(T)$ is not an infinite series, but rather a polynomial of degree $D$. Comparing the coefficients of the term of degree $D$, we get

$$(-1)^D \det(\mathsf{Frob}_q | H^1_c(\mathbb{G}_m/\overline{k}, \mathcal{L}_{\psi(f(X))} \otimes \mathcal{L}_{\chi(X)})) = A_D.$$

Thus our determinant is $(-1)^D A_D$. To compute $A_D$, we argue as follows. To deal with the expression inside the $\psi$, we observe that for each integer $n$, the sum of the $n^{\text{th}}$ powers of the roots of $P$ is simply the $n^{\text{th}}$ Newton function $N_n(\text{roots of } P)$, which is a universal polynomial $N_n$ in the coefficients $S_i$ of $P$. Thus

$$\begin{aligned}\sum_{\text{roots } \alpha \text{ of } P} f(\alpha) &= \sum_{\text{roots } \alpha \text{ of } P} \big(a_D\alpha^D + \sum_{i=1}^{d} a_i\alpha^i\big)\\ &= a_D N_D(\text{roots of } P) + \sum_{i=1}^{d} a_i N_i(\text{roots of } P),\end{aligned}$$

and hence

$$A_D = \sum_{S_1,\ldots,S_D\in k,\, S_D\neq 0} \chi((-1)^D S_D)\psi_k\big(a_D N_D(S_1,\ldots,S_D) + \sum_{i=1}^{d} a_i N_i(S_1,\ldots,S_D)\big).$$

We compute the $N_i$ as polynomials in the $S_j$ by the identity

$$\log\Big(1/(1+\sum_{i\geq 1}(-1)^i S_i T^i)\Big) = \sum_{n\geq 1} N_n T^n/n.$$

Applying $d/dT$, we have the identity

$$-(\sum_{i\geq 1}(-1)^i i S_i T^i)/(1+\sum_{j\geq 1}(-1)^j S_j T^j) = \sum_{n\geq 1} N_n T^n.$$

We now expand the left side, as

$$-(\sum_{i\geq 1}(-1)^i i S_i T^i)(1+\sum_{m\geq 1}(-\sum_{j\geq 1}(-1)^j S_j T^j)^m).$$

When we ignore all but the first two terms in the geometric series, we find that $N_D$, the coefficient of $T^D$, is thus

$$N_D = (-1)^{D+1} D S_D - \sum_{i+j=D,\, i\geq 1,\, j\geq 1} (-1)^i i S_i (-1)^{j+1} S_j + R,$$

with $R$ a polynomial in which every monomial has usual degree $\geq 3$ in the variables $S_i$.

Let us first look at the case when $D = 2d+1$ is odd. Combining the terms $S_i S_{D-i}$ and $S_{D-i}S_i$, their coefficients add to $(-1)^D D$, we see that

$$N_D = (-1)^{D+1} D S_D + (-1)^D D \sum_{i=1}^{d} S_i S_{D-i} + R_D,$$

with $R_D$ isobaric of weight $D$ in the $S_i$ but in which every monomial has usual degree $\geq 3$. Thus $(-1)^D A_D$ is equal to

$$\sum_{\substack{S_1,\ldots,S_D\in k,\\ S_D\neq 0}} \chi((-1)^D S_D)\psi_k\big((-1)^{D+1} a_D D S_D + (-1)^D a_D D \sum_{i=1}^{d} S_i S_{D-i} + a_D R_D + \sum_{i=1}^{d} a_i N_i(S_1,\ldots,S_i)\big),$$

where we use the fact that $N_i$ is a polynomial in $S_1, \ldots, S_i$. The variable $S_D$ occurs only once, so $(-1)^D A_D$ is now equal to

$$\Big(\sum_{S_D \in k^\times} \chi((-1)^D S_D)\psi_k((-1)^{D+1} a_D D S_D)\Big) \times$$

$$\sum_{S_1,\ldots,S_{D-1} \in k} \psi_k\Big((-1)^D a_D D \sum_{i=1}^{d} S_i S_{D-i} + a_D R_D + \sum_{i=1}^{d} a_i N_i(S_1, \ldots, S_i)\Big).$$

Because $N_D$ is isobaric of degree $D$, for each $i \leq d$, the variable $S_{D-i}$ appears in this sum as $(-1)^D a_D D S_{D-i}\big(S_i$+a polynomial in only the $S_j, j < i$, every monomial of usual degree $\geq 2\big)$.

We further analyze the case when $D = 2d+1$ is odd as follows. Summing first over $S_{D-1}$, we get 0 unless $S_1 = 0$, in which case we get $q$. Once we know $S_1 = 0$ in our sum, summing over $S_{D-2}$ gives 0 unless $S_2 = 0$, in which case we get $q$. Continuing in this way we get

$$\begin{aligned} A_D &= q^d\Big(\sum_{S_D \in k^\times} \chi((-1)^D S_D)\psi_k((-1)^{D+1} a_D D S_D)\Big) \\ &= q^d \overline{\chi}(-D a_D)\mathsf{Gauss}(\psi_k, \chi), \end{aligned}$$

and thus

$$\det(\mathsf{Frob}_k) = (-1)^D \overline{\chi}(-D a_D)\mathsf{Gauss}(\psi_k, \chi) q^d.$$

When $D = 2d+2$ is even, the only difference is that the coefficient of $T^D$ now has the extra term $S_{D/2}S_{D/2}$, which occurs with coefficient $(-1)^D a_D(D/2) = a_D(D/2)$. This extra "middle term" persists, and at the end of the argument getting the previous answer, this "middle term" creates an extra factor $\chi_2((D/2)a_D)\mathsf{Gauss}(\psi_k, \chi_2)$.

Thus for $D = 2d+1$ odd, the determinant is $\overline{\chi}(-D a_D)(-\mathsf{Gauss}(\psi_k, \chi))q^d$, while for $D = 2d+2$ even it is $\chi_2((D/2)a_D)\overline{\chi}(-D a_D)(-\mathsf{Gauss}(\psi_k \chi_2))(-\mathsf{Gauss}(\psi_k, \chi))q^d$. □

COROLLARY 2.3.11. *Suppose we are given a prime to p integer $D \geq 3$, and a multiplicative character $\chi$ of a finite extension $k = \mathbb{F}_q$ of $\mathbb{F}_p$, and a strictly positive integer $d < D$. Consider the lisse sheaf $\mathcal{F}^\sharp(D, \leq d, \chi)$ on $(\mathbb{G}_m \times \mathbb{A}^d)/k$ whose trace function is given as follows.*

(a) *For $\mathcal{F}^\sharp(D, \leq d, \mathbb{1})$ on $(\mathbb{G}_m \times \mathbb{A}^d)/\mathbb{F}_p$, $L/\mathbb{F}_p$ a finite extension, and $(a_D, a_1, \ldots, a_d) \in L^\times \times L^d$, the trace is*

$$(a_D, a_1, \ldots, a_d) \mapsto -\sum_{x \in L} \psi_L(a_D x^D + \sum_{i=1}^{d} a_i x^i).$$

(b) *For $\mathcal{F}^\sharp(D, \leq d, \chi)$ with $\chi$ a nontrivial character of $k^\times$, $L/k$ a finite extension, and any point $(a_D, a_1, \ldots, a_d) \in L^\times \times L^d$, the trace is*

$$(a_D, a_1, \ldots, a_d) \mapsto -\sum_{x \in L} \psi_L(a_D x^D + \sum_{i=1}^{d} a_i x^i)\chi_L(x).$$

*These local systems are geometrically irreducible, pure of weight one, of ranks $D-1$ and $D$ respectively. For $d := [(D-1)/2]$, their geometric determinants are given as follows.*

(i) *If $D = 2d+1$ is odd, then* $\det(\mathcal{F}^\sharp(D, \leq d, \chi)) = \mathcal{L}_{\overline{\chi}(a_D)}$.

(ii) *If $D = 2d+2$ is even, then* $\det(\mathcal{F}^\sharp(D, \leq d, \chi)) = \mathcal{L}_{\chi_2(a_D)} \otimes \mathcal{L}_{\overline{\chi}(a_D)}$.

Proof. That the sheaves $\mathcal{F}^\sharp(D, \le d, \chi)$ are lisse results from the fact that their ranks are constant and they are sheaves of perverse origin in the sense of [**Ka-Scont**]. The purity is due to Weil. The explicit formulas for their determinants, and the behavior of Gauss sums under field extension give the asserted geometric determinant formulas. Each is geometrically irreducible because already pulled back to the $\mathbb{A}^1$ which is $(1, s_1, 0, \dots, 0)$ each is the Fourier transform of a lissse rank one sheaf on $\mathbb{G}_m$, extended across 0 by direct image (and hence perverse irreducible on $\mathbb{A}^1$). □

## 2.4. Infinite monodromy groups

We begin with an elementary lemma which will be used below.

Lemma 2.4.1. *Let $k$ be an algebraically closed field, $X/k$ and $Y/k$ smooth connected schemes,*

$$f : Y \to X$$

*a finite étale map, $\ell$ a prime invertible in $k$, and $\mathcal{F}$ a lisse $\overline{\mathbb{Q}_\ell}$ sheaf on $Y$. Suppose that the direct image $\mathcal{G} := f_\star\mathcal{F}$ on $X$ has finite $G_{\rm geom}$. Then $\mathcal{F}$ on $Y$ has finite $G_{\rm geom}$.*

Proof. The pullback $f^\star\mathcal{G}$ has finite $G_{\rm geom}$, since $\pi_1(Y) < \pi_1(X)$ is a subgroup (of finite index, a fact we use next). By Frobenius reciprocity, this pullback $f^\star\mathcal{G} = f^\star f_\star\mathcal{F}$ contains $\mathcal{F}$ as a constituent, indeed as a direct factor since in characteristic zero finite-dimensional representations of finite groups are completely reducible. Therefore $\mathcal{F}$ itself has finite $G_{\rm geom}$. □

Proposition 2.4.2. *Let $\mathcal{H}$ be a hypergeometric sheaf $\mathcal{H}yp_\psi(\chi_1, \dots, \chi_D; \rho_1, \dots, \rho_m)$ of type $(D, m)$ in characteristic $p$, with wild part* Wild *of dimension $w = D - m > 0$. Then the action of $I(\infty)$ on* Wild *has finite image.*

Proof. The key points are that Wild is $I(\infty)$-irreducible (because all its slopes are $1/w$) and is the restriction to $I(\infty)$ of a representation of the decomposition group $D(\infty)$ (because $\mathcal{H}$ lives on $\mathbb{G}_m$ over some finite field $k/\mathbb{F}_p$). By the $I(\infty)$-irreducibility, Deligne's monodromy filtration [**Ka-GKM**, 7.0.6] on Wild must be trivial, i.e. the action of $I(\infty)$ must be trivial on some open subgroup. □

Proposition 2.4.3. *Let $\mathcal{H} := \mathcal{H}yp_\psi(\chi_1, \dots, \chi_D; \rho_1, \dots, \rho_m)$ be an irreducible hypergeometric sheaf in characteristic $p$ of type $(D, m)$ with $D > m \ge 0$. Let $G = G_{\rm geom}$ denote the geometric monodromy group of $\mathcal{H}$ and $V$ be the underlying representation. For $g \in G$, we let $\bar{\mathsf{o}}(g)$ denote the order of the element $g\mathbf{Z}(G)$ in $G/\mathbf{Z}(G)$.*

(i) *Suppose $\chi_1, \dots, \chi_D$ are pairwise distinct. Then $I(0)$ has finite cyclic $p'$-image $\langle g_0 \rangle$, and $g_0$ is an* ssp*-element on $V$.*

(ii) *Suppose $\rho_1, \dots, \rho_m$ are pairwise distinct if $m > 0$. The image $J$ of $I(\infty)$ is finite, the image $Q$ of $P(\infty)$ is a normal subgroup $Q \lhd J$, and the quotient $J/Q$ is a finite cyclic $p'$-group, which is generated by the image $g_\infty$ in $G_{\rm geom}$ of any element $\gamma \in I(\infty)$ of order prime to $p$ that generates $I(\infty)/P(\infty)$. The element $g_\infty$ is an* m2sp*-element on $V$. If $m = 0$ then $g_\infty$ is an* ssp*-element on $V$, and if $m = 1$ then $g_\infty$ is an* asp*-element on $V$. Moreover, $\bar{\mathsf{o}}(g_\infty)$ is divisible by $w := D - m$ if $p \nmid w$, and by $w_0(q_0 + 1)$ if $p | w = w_0 q_0$ with $p \nmid w_0$ and $q_0$ a power of $p$.*

PROOF. (i) This is proved in [**Ka-ESDE**, 8.4.2(6)].

(ii) One knows [**Se**, pp. 80-82] that $P(\infty) \lhd I(\infty)$ with pro-cyclic $p'$-quotient. By Proposition 2.4.2, $I(\infty)$ has finite image on $\mathsf{Wild}$. By [**Ka-ESDE**, 8.4.2 (6)], $I(\infty)$ has finite, prime to $p$ cyclic image on $\mathsf{Tame}$. By Propositions 5.8 and 5.9 of [**KRLT4**], $g_\infty$ has simple spectrum on $\mathsf{Wild}$. If $m > 0$, $g_\infty$ also has simple spectrum on $\mathsf{Tame}$ because $\rho_1, \ldots, \rho_m$ are pairwise distinct, cf [**Ka-ESDE**, 8.4.2 (6)]. Next, if $p \nmid w$, then $g_\infty$ permutes the $w$ simple $Q$-summands of $\mathsf{Wild}$ cyclically, so $w|\bar{\mathsf{o}}(g_\infty)$. If $p|w = w_0q_0$, then $g_\infty^{w_0(q_0+1)}$ acts as a scalar on $\mathsf{Wild}$, but $g_\infty$ has $w_0q_0 > w_0(q_0+1)/2$ distinct eigenvalues on $\mathsf{Wild}$. This shows that the central order of the image of $g_\infty$ on $\mathsf{Wild}$ is $w_0(q_0+1)$, hence $w_0(q_0+1)|\bar{\mathsf{o}}(g_\infty)$. Hence the statements follow. □

For an integer $D$ with $p \nmid D$, $\mathsf{Char}(D)$ is the set of all multiplicative characters of order dividing $D$.

THEOREM 2.4.4. *Let $\mathcal{H}$ be a hypergeometric sheaf $\mathcal{H}yp_\psi(\chi_1, \ldots, \chi_D; \rho_1, \ldots, \rho_m)$ of type $(D, m)$ in characteristic $p$, with wild part $w = D - m > 0$. Suppose that $p > 2w + 1$ and $D \geq 2$. Then one of the following statements holds.*

(a) *$G_{\rm geom}$ is infinite.*
(b) *$G_{\rm geom}$ is finite, and $\mathcal{H}$ is imprimitive and Kloosterman. Moreover, $p \nmid D$, and for some tame character $\Lambda$, $\mathcal{H} \cong \mathcal{L}_\Lambda \otimes \mathcal{K}l(\mathsf{Char}(D))$ is Kummer induced from a Kloosterman sheaf of rank 1.*
(c) *$G_{\rm geom}$ is finite, and $(w, p, D) = (1, 5, 2)$.*

PROOF. (i) We will assume that $G = G_{\rm geom}$ is finite, and aim to show that $\mathcal{H}$ is imprimitive unless $(w, p, D) = (1, 5, 2)$. Let $V$ denote the representation underlying $\mathcal{H}$, and let $Q$ denote the image of $P(\infty)$ in $G$. We claim that $Q$ is isomorphic to the additive group of $\mathbb{F}_p(\xi)$, where $\xi$ is a primitive $w^{\rm th}$ root of unity in $\overline{\mathbb{F}_p}^\times$, and that the set of characters of $Q$ on $\mathsf{Wild}$ is

$$x \mapsto \psi\big(\mathrm{Tr}_{\mathbb{F}_p(\xi)/\mathbb{F}_p}(w\xi^j x)\big),\ 0 \leq j \leq w-1. \tag{2.4.4.1}$$

In the special case when our $\mathcal{H}$ has $\prod_i \chi_i / \prod_j \rho_j$ trivial if $w$ is odd, and equal to the quadratic character when $w$ is even, this is proven in [**KRLT3**, Lemma 3.1]. In general, there exists a tame character $\Lambda$ such that $\mathcal{L}_\Lambda \otimes \mathcal{H}$ has the desired ratio. This operation of tensoring replaces $\mathsf{Wild}$ by $\mathsf{Wild} \otimes \Lambda$, a change which does not affect the restriction to $P(\infty)$.

By [**KT5**, Proposition 4.8], $Q \not\leq \mathbf{Z}(G)$. As $Q$ is elementary abelian, we can find a $p$-element $g \in Q$ such that

$$g \in Q \smallsetminus \mathbf{Z}(G),\ g^p = 1. \tag{2.4.4.2}$$

Consider the case $g$ as chosen in (2.4.4.2) has at most $(p-3)/2$ distinct eigenvalues on $V$. By Zalesskii's conjecture, proved in [**Rob**], the normal closure $A := \langle g^G \rangle$ of $\langle g \rangle$ in $G$ is abelian, but not central since $g \notin \mathbf{Z}(G)$. It follows from Clifford's theorem that the restriction of $V$ to $A$ is a sum of at least two $A$-isotypic components, and so $(G, V)$ is imprimitive. In particular, $\mathcal{H}$ is imprimitive if $1 \leq w \leq (p-5)/2$, or if $w = D = (p-3)/2$.

(ii) Now we consider the case $w = (p-3)/2 < D$; in particular $\mathsf{Tame} \neq 0$. If $p = 5$ but $D > 2$, then $G$ is infinite by Theorem 4.1.1. The possibility $(w, p, D) = (1, 5, 2)$ is recorded in (c).

Suppose now that $p \geq 11$. Then $w = (p-3)/2$ does not divide $p-1$, and so $K := \mathbb{F}_p(\xi)$ is a proper extension of $\mathbb{F}_p$. Clearly, $K$ is the $\mathbb{F}_p$-span of the powers $\xi^i$, $0 \leq i \leq w-1$, of $\xi$, and the kernel $K_1$ of $\mathrm{Tr}_{K/\mathbb{F}_p}$ has codimension one in the $\mathbb{F}_p$ vector space $K$. Hence, if for all $x \in K$ we were to have $\mathrm{Tr}_{K/\mathbb{F}_p}(x\xi^i) = 0$ for all $i$, then we would have $K_1 = K$, a contradiction. Thus for any nonzero $z \in K$, there is some power $\xi^j$ with $0 \leq j \leq w-1$, such that $\mathrm{Tr}_{K/\mathbb{F}_p}(z\xi^j) \neq 0$. As $K > \mathbb{F}_p$, we can pick $0 \neq z \in K_1$. Then $z$ has trace zero, but some $z\xi^j$ has nonzero trace. By (2.4.4.1), this means precisely that of the $w$ eigenvalues of $z$ on $\mathsf{Wild}$, at least one eigenvalue is 1, but not all eigenvalues are 1; in particular, $z \notin \mathbf{Z}(G)$. Recall that 1 is the only eigenvalue of $z$ on $\mathsf{Tame}$. It follows that $z$ has at most $w = (p-3)/2$ distinct eigenvalues on $V$, and we are done by the result of (i).

Next, let $p = 7$. Then (2.4.4.1) shows that $Q \cong C_7$ admits two nontrivial characters $\lambda$ and $\lambda^{-1}$ on $\mathsf{Wild}$. In particular, the element $g$ as in (2.4.4.2) can be chosen to have eigenvalues $\zeta_7$ and $\overline{\zeta}_7$ on $\mathsf{Wild}$, and 1 on $\mathsf{Tame}$ as $\mathsf{Tame} \neq 0$. It follows from Blichfeldt's 60-degree theorem [**Bl**, Theorem 8, p. 96] that $G$ is imprimitive.

(iii) Now we may assume that $G$ is finite and imprimitive, and that $(w, p, D) \neq (1, 5, 2)$. Since $(p-1) \nmid w$, $\mathcal{H}$ cannot be Belyi induced, and so it is Kummer induced by [**KRLT3**, Proposition 1.2]. In other words, for some prime to $p$ integer $N > 1$, $\mathcal{H}$ is $[N]_\star\mathcal{H}'$, for $\mathcal{H}'$ a hypergeometric sheaf of type $(D/N, m/N)$. Note that $\mathcal{H}'$ has wild part of dimension $1 \leq w/N < w \leq (p-3)/2$ (in particular $p \geq 7$), and has finite geometric monodromy group, by Lemma 2.4.1 above, applied to the degree $N$ Kummer covering of $\mathbb{G}_m$ by itself.

Choose the largest possible such $N$. If $D > N$, so that $D/N \geq 2$, then, as $p \geq 7$, we can apply the above results to $\mathcal{H}'$, and conclude that $\mathcal{H}'$ is again Kummer induced, contrary to the choice of $N$. It follows that $D = N$ and so $m = 0$, i.e. $\mathcal{H}$ is Kloosterman of rank $D = N$ prime to $p$, $\mathcal{H}'$ is Kloosterman of rank one, and $\mathcal{H}$ is Kummer induced of degree $D$. Hence, by [**Ka-MG**, Lemma 12], $\mathcal{H}$ is $\mathcal{K}l_\psi(\chi_1, \ldots, \chi_D)$ with the $\chi_i$ all the $D^{\text{th}}$ roots of some tame character $\sigma$, which we write as $\sigma = \Lambda^D$. Thus the set of $\chi_i$'s is precisely the set $\Lambda\mathsf{Char}(D)$, and hence $\mathcal{H}$ is $\mathcal{L}_\Lambda \otimes \mathcal{K}l_\psi(\mathsf{Char}(D))$. □

REMARK 2.4.5. (i) Note that (half of) the local systems considered in [**KT1**, Theorem 11.1] have $G_{\text{geom}} = \mathrm{SL}_2(p)$, and they are Kummer pullbacks of hypergeometric sheaves in characteristic $p$ with $w = (p-1)/2$. This example shows that the bound $p > 2w+1$ in Theorem 2.4.4 is best possible. Furthermore, [**KRLT4**, Theorem 30.7(v)] gives a hypergeometric sheaf of type $(2, 1)$ in characteristic $p = 5$ with $G_{\text{geom}} = 5 \times \mathrm{SL}_2(5)$, a finite primitive complex reflection group. Hence case (c) of Theorem 2.4.4 is a real exception.

(ii) In the case of Kloosterman sheaves, Theorem 2.4.4 was already proved in [**Ka-MG**, Proposition 6], which in turn relied on the well-known result of Feit and Thompson [**FT**].

Let us now recall the notion of "Lie irreducible". Given an algebrically closed field $k$ in which $\ell$ is invertible, a smooth, geometrically connected scheme $X/k$, a lisse $\overline{\mathbb{Q}_\ell}$-sheaf $\mathcal{F}$ on $X$ is said to be *Lie irreducible* if, in the given representation of $G_{\text{geom}}$, the identity component $G^\circ_{\text{geom}}$ acts irreducibly. Equivalently, $\mathcal{F}$ is Lie irreducible if, for any finite étale $f : Y \to X$ with $Y$ connected, the pullback $f^\star\mathcal{F}$ on $Y$ remains irreducible. [Just pass to the covering which trivializes $G_{\text{geom}}/G^\circ_{\text{geom}}$.] In a similar vein, we say that $\mathcal{F}$ is Lie self-dual if it is Lie irreducible and if the restriction to $G^{\circ}_{\mathrm{geom}}$ of the given representation is self-dual. Finally, we say that two Lie irreducible sheaves $\mathcal{F}_1$ and $\mathcal{F}_2$ on $X$ are Lie-isomorphic if for some finite étale $f : Y \to X$ with $Y$ connected, the pullbacks $f^{\star}\mathcal{F}_1$ and $f^{\star}\mathcal{F}_2$ on $Y$ are isomorphic.

Lemma 2.4.6. *Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be (geometrically irreducible) hypergeometric sheaves on $\mathbb{G}_m/\overline{\mathbb{F}_p}$, formed using possibly different additive characters $\psi_1$ and $\psi_2$. Denote by $(D_1, m_1)$ and $(D_2, m_2)$, with $D_1 > m_1$ and $D_2 > m_3$, their types. Suppose that $D_2 \geq 2$ and that $(D_2, m_2) \neq (2, 1)$. Suppose further that both $\mathcal{H}_1$ and $\mathcal{H}_2$ are Lie irreducible, and that they are Lie isomorphic. Then there exists a multiplicative character $\chi$ of some $\mathbb{F}_q^{\times}$ and an isomorphism*

$$\mathcal{H}_1 \cong \mathcal{L}_{\chi} \otimes \mathcal{H}_2.$$

Proof. Let $Y \to \mathbb{G}_m$ be a finite étale pullback, with $Y$ connected, on which $\mathcal{H}_1$ and $\mathcal{H}_2$ become isomorphic. Think of $Y$ as corresponding to the open subgroup of finite index in $\pi_1(\mathbb{G}_m/\overline{\mathbb{F}_p})$, namely $\pi_1(Y)$. Then passsing to a smaller open subgroup of finite index which is normal in $\pi_1(\mathbb{G}_m/\overline{\mathbb{F}_p})$, we may reduce to the case when $\pi_1(Y) \lhd \pi_1(\mathbb{G}_m/\overline{\mathbb{F}_p})$ is a normal subgroup. Then $\mathcal{H}_1$ and $\mathcal{H}_2$ are representations of $\pi_1(\mathbb{G}_m/\overline{\mathbb{F}_p})$ whose restrictions to $\pi_1(Y)$ are irreducible and isomorphic. Here there exists a linear character $\Lambda$ of the quotient group $\pi_1(\mathbb{G}_m/\overline{\mathbb{F}_p})/\pi_1(Y)$ such that we have an isomorphism

$$\mathcal{H}_1 \cong \Lambda \otimes \mathcal{H}_2.$$

Let us observe the trivial consequence that $D_1 = D_2$.

We must show that $\Lambda$ is tame at both 0 and $\infty$. It is tame at 0 because both $\mathcal{H}_1$ and $\mathcal{H}_2$ are tame at 0. If $\Lambda$ were not tame at 0, it would have Swan conductor $\geq 1$ at 0, which in turn would force $\mathcal{H}_1$ to be totally wild at 0, which it is not. If If $\Lambda$ were not tame at $\infty$, it would have Swan conductor $\mathsf{Swan}_{\infty}(\Lambda) \geq 1$. Suppose first that $D_2 - m_2 \geq 2$. Then the $\infty$ slopes of $\mathcal{H}_2$, which are either 0 or $1/(D_2 - m_2)$, are all $< 1$, and so $\mathcal{H}_1$ would have all slopes equal to $\mathsf{Swan}_{\infty}(\Lambda) \geq 1$, and hence $\mathsf{Swan}_{\infty}(\mathcal{H}_1) = \mathsf{Swan}_{\infty}(\Lambda) D_2 \geq D_2 \geq 2$, again a contradiction as $\mathsf{Swan}_{\infty}(\mathcal{H}_1) = 1$. Finally, suppose $D_2 - m_2 = 1$. Then by hypothesis $m_2 \geq 2$, so that $\mathcal{H}_2$ has $m_2 \geq 2$ $\infty$ slopes 0. Then $\mathcal{H}_1$ has $m_2 \geq 2$ $\infty$ slopes $\mathsf{Swan}_{\infty}(\Lambda)$, so $\mathsf{Swan}_{\infty}(\mathcal{H}_1) \geq \mathsf{Swan}_{\infty}(\Lambda) m_2 \geq 2$, the same contradiction. □

Corollary 2.4.7. *In the situation of the above Lemma 2.4.6, let $A$ be a prime to $p$ integer such that both Kummer pullbacks $[A]^{\star}\mathcal{H}_1$ and $\mathcal{H}_2$ have unipotent local monodromy at 0. Then we have an isomorphism*

$$[A]^{\star}\mathcal{H}_1 \cong [A]^{\star}\mathcal{H}_2.$$

Proof. Indeed, after the pullback we have an isomorphism

$$[A]^{\star}\mathcal{H}_1 \cong \mathcal{L}_{\chi^A} \otimes [A]^{\star}\mathcal{H}_2.$$

But both $[A]^{\star}\mathcal{H}_1$ and $\mathcal{H}_2$ are unipotent at 0, hence $\mathcal{L}_{\chi^A}$ is trivial at 0. Being a tame character, it is then trivial. □

Corollary 2.4.8. *Suppose that the hypergeometric sheaf $\mathcal{H}$ on $\mathbb{G}_m/\overline{\mathbb{F}_p}$ is Lie self-dual. Let $A$ be a prime to $p$ integer such the Kummer pullback $[A]^{\star}\mathcal{H}$ has unipotent local monodromy at 0. Then $[A]^{\star}\mathcal{H}$ is self-dual.*

Proof. Apply the previous Corollary 2.4.7 to $\mathcal{H}$ and its dual. □

In the same spirit, we have the following lemma.

LEMMA 2.4.9. *Let $\mathcal{H}$ be a geometrically irreducible hypergeometric sheaf of type $(D,m)$ with $D-m\geq 2$. Suppose that $G^{\circ}_{\mathrm{geom}}=\mathrm{SL}_D$. Then the determinant gives an isomorphism $G_{\mathrm{geom}}/G^{\circ}_{\mathrm{geom}}\cong\mu_N(\overline{\mathbb{Q}_\ell})$ for some prime to $p$ integer $N\geq 1$. Equivalently, $\det(\mathcal{H})\cong\mathcal{L}_\chi$ for some tame character $\chi$.*

PROOF. Because $G^{\circ}_{\mathrm{geom}}=\mathrm{SL}_D$, the determinant gives an isomorphism $G_{\mathrm{geom}}/G^{\circ}_{\mathrm{geom}}\cong\mu_N(\overline{\mathbb{Q}_\ell})$ for some integer $N\geq 1$. Because $D-m\geq 2$, we know by [**KT5**, Theorem 4.1] that $G_{\mathrm{geom}}$ is the Zariski closure of the normal subgroup generated by the image of $I(0)$. Therefore the quotient group $\mu_N$, being abelian, is generated by the image of $I(0)$, which is a group of (pro) order prime to $p$. Thus the quotient is a character of $\pi_1(\mathbb{G}_m/\overline{\mathbb{F}_p})$ of finite order prime to $p$, necessarily an $\mathcal{L}_\chi$. Alternatively, by [**Ka-ESDE**, Theorem 8.12.2], $\det(\mathcal{H})=\mathcal{L}_\chi$ for $\chi$ the product of the "upstairs" characters of $\mathcal{H}$. □

COROLLARY 2.4.10. *Let $\mathcal{H}$ be a geometrically irreducible hypergeometric sheaf of type $(D,m)$ with $D-m\geq 2$. Suppose that $G^{\circ}_{\mathrm{geom}}=\mathrm{SL}_D$. Let $A$ be a prime to $p$ integer such that the Kummer pullback $[A]^{\star}\mathcal{H}$ has unipotent local monodromy at $0$. Then $[A]^{\star}\mathcal{H}_1$ has $G_{\mathrm{geom},[A]^{\star}\mathcal{H}}=\mathrm{SL}_D$.*

PROOF. Indeed, if $[A]^{\star}\mathcal{H}$ is unipotent, then each character occuring in the image of $I(0)$ has order dividing $A$, so $N$ divides $A$, i.e., $\chi^A=\mathbb{1}$. □

REMARK 2.4.11. Suppose $\mathcal{H}$ is of type $(D,m)$ with $D-m=1$. Then one knows [**Ka-ESDE**, Theorem 8.12.2] that $\det(\mathcal{H})=\mathcal{L}_\chi\otimes\mathcal{L}_\psi$, with $\chi$ the product of the "upstairs" characters of $\mathcal{H}$. So in this case, if $A$ is a prime to $p$ integer such that the Kummer pullback $[A]^{\star}\mathcal{H}$ has unipotent local monodromy at 0, $\det([A]^{\star}\mathcal{H})=\mathcal{L}_\psi$. In particular, if $\mathcal{H}$ has $G^{\circ}_{\mathrm{geom}}=\mathrm{SL}_D$, then $[A]^{\star}\mathcal{H}$ has $G_{\mathrm{geom},[A]^{\star}\mathcal{H}}=\{\gamma\in\mathrm{GL}_D|\det(\gamma)^p=1\}$.

## 2.5. Estimating the size of $G_{\mathrm{geom}}$ when it is finite

LEMMA 2.5.1. *Let $X/\mathbb{F}_q$ be smooth and geometrically connected. Let $\mathcal{F}$ be a lisse $\overline{\mathbb{Q}_\ell}$-adic sheaf on $\mathbb{G}_m/\mathbb{F}_q$ which is pure of weight zero and for which $G_{\mathrm{arith}}$ is finite. Then $G_{\mathrm{geom}}\lhd G_{\mathrm{arith}}$, and the quotient group $G_{\mathrm{arith}}/\mathbb{G}_{\mathrm{geom}}$ is cyclic of order*

$$\begin{aligned}\#(G_{\mathrm{arith}}/G_{\mathrm{geom}})&=\gcd\big(d\in\mathbb{Z}_{\geq 1}\mid\text{there exists }x\in X(F_{q^d})\text{ with }\mathsf{Frob}_{x,F_{q^d}}|\mathcal{F}=\mathrm{id}\big)\\&=\gcd\big(d\in\mathbb{Z}_{\geq 1}\mid\text{there exists }x\in X(F_{q^d})\text{ with }\mathrm{Trace}(\mathsf{Frob}_{x,F_{q^d}}|\mathcal{F})=\mathrm{rank}(\mathcal{F})\big).\end{aligned}$$

PROOF. The two asserted formulas are equivalent, since in a faithful $\mathbb{C}$-representation $V$ of a finite group, here the action of $G_{\mathrm{arith}}$ on $\mathcal{F}$, only the identity element has trace equal to $\dim(V)$.

The quotient $G_{\mathrm{arith}}/G_{\mathrm{geom}}$ is a finite quotient of the pro-cyclic group $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$, so is itself cyclic. The coset $G_{\mathrm{geom}}$ of $G_{\mathrm{arith}}$ is the unique coset containing the identity element of $G_{\mathrm{geom}}$, and this element is also the identity element of $G_{\mathrm{arith}}$. If some $\mathsf{Frob}_{x,F_{q^d}}|\mathcal{F}=\mathrm{id}$, then over $\mathbb{F}_{q^d}$ we have $G_{\mathrm{geom}}=G_{\mathrm{arith}}$, which is to say that $|G_{\mathrm{arith}}/G_{\mathrm{geom}}|$ divides $d$. So if the asserted gcd is 1, then the index must be 1. Conversely, if $G_{\mathrm{geom}}=G_{\mathrm{arith}}$, then by Deligne's equidistribution theorem in this finite case [**Ka-Sar**, Theorem 9.7.13], we will obtain Frobenii which attain any specified element of $G_{\mathrm{arith}}$ over all extensions of $\mathbb{F}_q$ of sufficiently large degree. □

Lemma 2.5.2. *Let $\mathcal{F}$ be a lisse $\overline{\mathbb{Q}_\ell}$-adic sheaf on $\mathbb{G}_m/\mathbb{F}_q$ which is pure of weight zero and for which $G_{\text{geom}} = G_{\text{arith}}$ is finite. Let $S_0$ and $S_\infty$ be real constants such that all $I(0)$-slopes of $\mathcal{F}$ are $\leq S_0$ and all $I(\infty)$-slopes of $\mathcal{F}$ are $\leq S_\infty$. Then we have the inequality*

$$\left|\frac{\#\{x \in \mathbb{F}_q^\times | \text{Trace}(\mathsf{Frob}_{x,\mathbb{F}_q}|\mathcal{F}) = \text{rank}(\mathcal{F})\}}{q-1} - \frac{1}{|G_{\text{geom}}|}\right| \leq \frac{(S_0+S_\infty)\sqrt{q}}{q-1}.$$

Proof. Let us write $G := G_{\text{geom}}(= G_{\text{arith}})$. Write the regular representation $\text{Rep}_G$ as the usual sum of irreducible representations $\Lambda$ of $G$

$$\text{Rep}_G - \mathbb{1} = \bigoplus_{\Lambda \neq \mathbb{1}} \dim(\Lambda)\Lambda,$$

and recall that $\text{Rep}_G$ is $|G|$ times the characteristic function of $\text{id}_G$.

Sum both sides of this equality over the $\mathsf{Frob}_{x,\mathbb{F}_q}|\mathcal{F}$. We get
(2.5.2.1)

$$|G|\cdot\#\{x \in \mathbb{F}_q^\times|\text{Trace}(\mathsf{Frob}_{x,\mathbb{F}_q}|\mathcal{F}) = \text{rank}(\mathcal{F})\} - (q-1) = \sum_{\Lambda\neq\mathbb{1}} \dim(\Lambda) \sum_{x \in \mathbb{F}_q^\times} \text{Trace}(\Lambda(\mathsf{Frob}_{x,\mathbb{F}_q}|\mathcal{F})).$$

Because each $\Lambda$ is a representation of $G = G_{\text{arith}}$, we may form the pushout sheaf $\Lambda(\mathcal{F})$ on $\mathbb{G}_m/\mathbb{F}_q$. It will be lisse, pure of weight zero, and its $I(0)$ (respectively $I(\infty)$) slopes will be bounded by $S_0$ (respectively $S_\infty$), because each $\Lambda(\mathcal{F})$ is a direct factor of some tensor power $\mathcal{F}^{\otimes a} \otimes (\mathcal{F}^\vee)^{\otimes b}$. By the Lefschetz trace formula, we have

$$\sum_{x\in\mathbb{F}_q^\times} \text{Trace}(\Lambda(\mathsf{Frob}_{x,\mathbb{F}_q}|\mathcal{F})) = \sum_i (-1)^i \text{Trace}\big(\mathsf{Frob}_q|H_c^i(\mathbb{G}_m/\overline{\mathbb{F}_q}, \Lambda(\mathcal{F}))\big).$$

The only possibly nonvanishing $H_c^i$ are $H_c^2$ and $H_c^1$. For $\Lambda$ nontrivial, the $H_c^2$ vanishes, because $\Lambda$ is irreducible nontrivial on $G = G_{\text{geom}}$. By the Euler-Poincare formula on $\mathbb{G}_m$, applied to $\Lambda$ nontrivial, we have

$$\dim\big(H_c^i(\mathbb{G}_m/\overline{\mathbb{F}_q}, \Lambda(\mathcal{F}))\big) = \mathsf{Swan}_0(\Lambda(\mathcal{F})) + \mathsf{Swan}_\infty(\Lambda(\mathcal{F})) \leq (S_0+S_\infty)\dim(\Lambda).$$

By Deligne [**De2**, 3.3.4], each $H_c^1$ is mixed of weight $\leq 1$, so we have the estimate

$$\big|\text{Trace}\big(\mathsf{Frob}_q|H_c^1(\mathbb{G}_m/\overline{\mathbb{F}_q}, \Lambda(\mathcal{F}))\big)\big| \leq \dim(H_c^1)\sqrt{q} \leq (S_0+S_\infty)\dim(\Lambda)\sqrt{q}$$

Thus we have the estimate

$$\big|\sum_{\Lambda\neq\mathbb{1}} \dim(\Lambda) \sum_{x\in\mathbb{F}_q^\times} \text{Trace}\big(\Lambda(\mathsf{Frob}_{x,\mathbb{F}_q}|\mathcal{F})\big)\big| \leq \sum_{\Lambda\neq\mathbb{1}} (\dim(\Lambda)^2(S_0+S_\infty)\sqrt{q} \leq |G|(S_0+S_\infty)\sqrt{q}.$$

Dividing through Equation (2.5.2.1) by $|G|(q-1)$ we get the asserted result. ☐

Corollary 2.5.3. *Let $\mathcal{H}$ be an irreducible hypergeometric sheaf of type $(D,m)$ with $w := D-m > 0$. Suppose that $G_{\text{geom}} = G_{\text{arith}}$ is finite. Then*

$$\left|\frac{\#\{x\in\mathbb{F}_q^\times|\text{Trace}(\mathsf{Frob}_{x,\mathbb{F}_q}|\mathcal{H}) = \text{rank}(\mathcal{H})\}}{q-1} - \frac{1}{|G_{\text{geom}}|}\right| \leq \frac{\sqrt{q}}{(q-1)w}.$$

Proof. Indeed $\mathcal{H}$ is tame at 0, so we may take $S_0 = 0$, and all its $\infty$-slopes are either 0 or $1/w$, so we may take $S_\infty = 1/w$. ☐

Here is a variant on $\mathbb{A}^1$. What we use here is that for $\mathcal{G}$ lisse on $\mathbb{A}^1$ whose $H^2_c$ vanishes, the Euler-Poincaré formula gives

$$\dim\big(H^1_c(\mathbb{A}^1/\overline{\mathbb{F}_q}, \mathcal{G})\big) = \mathsf{Swan}_\infty(\mathcal{G}) - \mathrm{rank}(\mathcal{G}).$$

Lemma 2.5.4. *Let $\mathcal{F}$ be a lisse $\overline{\mathbb{Q}_\ell}$-adic sheaf on $\mathbb{A}^1/\mathbb{F}_q$ which is pure of weight zero and for which $G_{\mathrm{geom}} = G_{\mathrm{arith}}$ is finite. Let $S_\infty$ be a real constant such all $I(\infty)$-slopes of $\mathcal{F}$ are $\leq S_\infty$. Then we have the inequality*

$$\left|\frac{\#\{x \in \mathbb{F}_q | \mathrm{Trace}(\mathsf{Frob}_{x,\mathbb{F}_q}|\mathcal{F}) = \mathrm{rank}(\mathcal{F})\}}{q} - \frac{1}{|G_{\mathrm{geom}}|}\right| \leq \frac{(S_\infty - 1)}{\sqrt{q}}.$$

Proof. The only new point here is that for any $\Lambda(\mathcal{F})$, its $\infty$ slopes are still $\leq S_\infty$, so for $\Lambda \neq \mathbb{1}$ we have

$$\dim\big(H^1_c(\mathbb{A}^1/\overline{\mathbb{F}_q}, \Lambda(\mathcal{F}))\big) = \mathsf{Swan}_\infty(\Lambda(\mathcal{F})) - \dim(\Lambda) \leq S_\infty \dim(\Lambda) - \dim(\Lambda) = (S_\infty - 1)\dim(\Lambda).$$

The rest of the proof proceeds as in the proof of Lemma 2.5.2. □

## 2.6. Limsup formula for moments

Let $X_0/\mathbb{F}_q$ be smooth and geometrically connected, of dimension $d \geq 1$, $\ell \neq p$ a prime, and $\mathcal{F}$ a lisse $\overline{\mathbb{Q}_\ell}$ sheaf on $X_0$ which is pure of weight zero. By fundamental results of Grothendieck and Deligne [**De2**, 1.3.8 and 3.4.1 (iii)], $G_{\mathrm{geom}}$ is a semisimple algebraic group (meaning that its identity component $G^0_{\mathrm{geom}}$ is semisimple). For $V$ the representation of $G_{\mathrm{geom}}$ attached to $\mathcal{F}$, $a, b$ nonnegative integers, and

$$X := X_0 \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q},$$

we have

$$\begin{aligned} M_{a,b}(\mathcal{F}) &:= \dim\big((V^{\otimes a} \otimes (V^\vee)^{\otimes b})^{G_{\mathrm{geom}}}\big) \\ &= \dim\big(H^{2d}_c(X, \mathcal{F}^{\otimes a} \otimes (\mathcal{F}^\vee)^{\otimes b})\big). \end{aligned}$$

Because $\mathcal{F}$ is pure of weight zero, the trace function of $\mathcal{F}^\vee$ is the complex conjugate of the trace function of $\mathcal{F}$.

Theorem 2.6.1. *As $L/\mathbb{F}_q$ runs over finite extensions, we have the limsup formula*

$$M_{a,b}(\mathcal{F}) = \limsup_{L/\mathbb{F}_q} \Big|\frac{1}{(\#L)^d} \sum_{x \in X_0(L)} \mathrm{Trace}(\mathsf{Frob}_{x,L}|\mathcal{F})^a \mathrm{Trace}(\mathsf{Frob}_{x,L}|\mathcal{F}^\vee)^b)\Big|.$$

Proof. For the auxiliary sheaf $\mathcal{G} := \mathcal{F}^{\otimes a} \otimes (\mathcal{F}^\vee)^{\otimes b}$, which is lisse and pure of weight zero on $X_0$, this is the statement that we recover $\dim(H^{2d}_c(X, \mathcal{G}))$ as the limsup

$$\limsup_{L/\mathbb{F}_q} \Big|\frac{1}{(\#L)^d} \sum_{x \in X_0(L)} \mathrm{Trace}(\mathsf{Frob}_{x,L}|\mathcal{G})\Big|.$$

By the Lefschetz trace formula, we have

$$\sum_{x \in X_0(L)} \mathrm{Trace}(\mathsf{Frob}_{x,L}, \mathcal{G}) = \sum_{0 \leq i \leq 2d} (-1)^i \mathrm{Trace}(\mathsf{Frob}_L | H^i_c(X, \mathcal{G})).$$

For $i < 2d$, the group $H^i_c(X, \mathcal{G})$ is mixed of weight $\leq i$, by Deligne's fundamental estimate [**De2**, 3.3.4], so for every finite extension $L/\mathbb{F}_q$ we have

$$\big|\sum_{0\leq i\leq 2d-1}(-1)^i\mathrm{Trace}(\mathsf{Frob}_L|H^i_c(X,\mathcal{G})\big| \leq (\#L)^{d-1/2}\big(\sum_{0\leq i\leq 2d-1} h^i_c(X,\mathcal{G})\big).$$

So if $H^{2d}(X, \mathcal{G})$ vanishes, we are done. When $H^{2d}(X, \mathcal{G})$ is nonzero, we must show that

$$\dim H^{2d}(X,\mathcal{G}) = \limsup_{L/\mathbb{F}_q}\big|\frac{1}{(\#L)^d}\mathrm{Trace}(\mathsf{Frob}_L|H^{2d}(X,\mathcal{G}))\big|.$$

The key point here is that $H^{2d}(X, \mathcal{G})$ is pure of weight $2d$: the eigenvalues of $\mathsf{Frob}_{\mathbb{F}_q}$ on $H^{2d}(X, \mathcal{G})$ are of the form $q^d\alpha_j$, for $1 \leq j \leq \dim H^{2d}(X, \mathcal{G})$, with each $|\alpha_j| = 1$. For $L/\mathbb{F}_q$ of degree $n$, the eigenvalues of $\mathsf{Frob}_L$ on this space are $(\#L)^d\alpha_j^n$. Thus we are reduced to the statement that given $D \geq 1$ points $\alpha_j \in S^1$, we recover $D$ as

$$\limsup_{n}\big|\sum_{1\leq j\leq D}\alpha_j^n\big|,$$

which holds because in the compact group $(S^1)^D$, powers of any point $(\alpha_1, \ldots, \alpha_D)$ come arbitrarily close to the identity element $(1, \ldots, 1)$. □

CHAPTER 3

# Representations of reductive groups containing elements with special spectra

## 3.1. Almost quasisimple groups containing elements with simple spectra

One of the main goals of [**KT5**] was to describe triples $(G, V, g)$ subject to the following condition:

(3.1.0.1)
$G$ is an almost quasisimple finite group, with $S$ the unique non-abelian composition factor, $V$ a faithful irreducible $\mathbb{C}G$-module, and $g \in G$ has simple spectrum on $V$.

With $G$ as in (3.1.0.1), let $E(G)$ denote the *layer* of $G$, so that $E(G)$ is quasisimple and $S \cong E(G)/\mathbf{Z}(E(G))$. On the other hand, $G/\mathbf{Z}(G)$ is almost simple: $S \lhd G/\mathbf{Z}(G) \leq \mathrm{Aut}(S)$. We will frequently identify $G$ with its image in $\mathrm{GL}(V)$. Let $\mathfrak{d}(S)$ denote the smallest degree of faithful projective irreducible complex representations of $S$, and let $\bar{\mathsf{o}}(g)$ denote the order of the element $g\mathbf{Z}(G)$ in $G/\mathbf{Z}(G)$. Adopting the notation of [**GMPS**], let $\mathrm{meo}(X)$ denote the largest order of elements in a finite group $X$. An element $g \in G \leq \mathrm{GL}(V)$ is called an $\mathsf{ssp}$-element, or an element with simple spectrum, if the multiplicity of any eigenvalue of $g$ acting on $V$ is 1. (Note that in (3.1.0.1), we do *not* (yet) assume that $V|_{E(G)}$ is irreducible.)

We begin with a useful observation:

Lemma 3.1.1. [**KT5**, Lemma 6.1] *In the situation of* (3.1.0.1)*, we have*

$$\mathfrak{d}(S) \leq \dim(V) \leq \bar{\mathsf{o}}(g) \leq \mathrm{meo}(G/\mathbf{Z}(G)) \leq \mathrm{meo}(\mathrm{Aut}(S)).$$

Let $S^{(n-1,1)}$ denote the *deleted permutation module* of $\mathsf{S}_n$. We will also need to consider the so-called *basic spin modules* (acted on faithfully by the double cover $\hat{\mathsf{A}}_n$), see e.g. [**KlT**, §2].

Theorem 3.1.2. [**KT5**, Theorem 6.2] *In the situation of* (3.1.0.1)*, assume that* $S = \mathsf{A}_n$ *with* $n \geq 8$*. Then one of the following statements holds.*

(i) $E(G) = \mathsf{A}_n$ *and one of the following holds.*
   (a) $\dim V = n-1$, $V|_{\mathsf{A}_n} \cong S^{(n-1,1)}|_{\mathsf{A}_n}$*, and, up to a scalar,* $g$ *is either an* $n$*-cycle, or a disjoint product of a* $k$*-cycle and an* $(n-k)$*-cycle for some* $1 \leq k \leq n-1$ *coprime to* $n$*.*
   (b) $n = 8$, $\dim V = 14$*, and, up to a scalar,* $g$ *is an element of order* 15 *in* $\mathsf{A}_8$*.*

(ii) $E(G) = \hat{\mathsf{A}}_n$ *and one of the following holds.*
   (a) $n = 8$, $\dim V = 8$, $V|_{E(G)}$ *is a basic spin module, and* $\bar{\mathsf{o}}(g) = 10$, 12*, or* 15*.*
   (b) $G/\mathbf{Z}(G) \cong \mathsf{A}_9$, $\dim V = 8$, $V|_{E(G)}$ *is a basic spin module, and* $\bar{\mathsf{o}}(g) = 9$, 10, 12*, or* 15*.*

(c) $G/\mathbf{Z}(G) \cong \mathsf{S}_9$, $\dim V = 16$, $V|_{E(G)}$ *is the sum of two basic spin modules, and* $\bar{\mathsf{o}}(g) = 20$.
(d) $G/\mathbf{Z}(G) \cong \mathsf{S}_{10}$, $\dim V = 16$, $V|_{E(G)}$ *is a basic spin module, and* $\bar{\mathsf{o}}(g) = 20$ *or* $30$.
(e) $G/\mathbf{Z}(G) \cong \mathsf{A}_{11}$, $\dim V = 16$, $V|_{E(G)}$ *is a basic spin module, and* $\bar{\mathsf{o}}(g) = 20$.
(f) $G/\mathbf{Z}(G) \cong \mathsf{S}_{12}$, $\dim V = 32$, $V|_{E(G)}$ *is a basic spin module, and* $\bar{\mathsf{o}}(g) = 60$.

Table II, reproduced from [**KT5**], summarizes the classification of ssp-elements in the non-generic cases of sporadic groups and $\mathsf{A}_7$ and some small rank Lie-type groups, *under the additional condition that* $V|_{E(G)}$ *is irreducible.* For each $V$, we list all almost quasisimple groups $G$ with common $E(G)$ that act on $V$, and we list the number of isomorphism classes of such representations in a given dimension, for a largest possible $G$ up to scalars (if no number is given, it means the representation is unique up to equivalence in given dimension). For each representation, we list the names of conjugacy classes of ssp-elements in a largest possible $G$, as listed in [**GAP**], and/or the total number of them. We also give a reference where a local system realizing the given representation is constructed. The indicator (-) means that no hypergeometric sheaf with $G$ as monodromy group can exist.

THEOREM 3.1.3. [**KT5**, Theorem 6.4] *In the situation of* (3.1.0.1), *assume that $S$ is one of* 26 *sporadic simple groups, or* $\mathsf{A}_7$, *and that* $V|_{E(G)}$ *is irreducible. Then* $(S, G, V, g)$ *are as listed in* Table II.

LEMMA 3.1.4. *Let* $q = p^f > p$ *and* $q \neq 4, 8, 9, 25$. *Suppose that* $S = \mathrm{PSL}_2(q)$ *and* $g \in \mathrm{Aut}(S)$ *has order at least* $(q-1)/\gcd(2, q-1)$. *Then* $g \in \mathrm{PGL}_2(q)$.

PROOF. Suppose that $g \notin H := \mathrm{PGL}_2(q)$, and thus the coset $gH$ is an element of order $e \geq 2$ in the cyclic quotient $\mathrm{Aut}(S)/H \cong C_f$. As shown on [**GMPS**, p. 7679], we then have that $\mathsf{o}(g) \leq e(q^{1/e} + 1)$.

Suppose $p = 2$. Then one can check that $e(q^{1/e} + 1) < q - 1$, unless $(e, q) = (2, 4), (3, 8)$.

Suppose $p > 2$. Then one can check that $e(q^{1/e} + 1) < (q-1)/2$, unless $(e, q) = (2, 9)$, $(2, 25)$. □

THEOREM 3.1.5. *In the situation of* (3.1.0.1), *assume that $S$ is a finite simple group of Lie type. Then one of the following statements holds.*

(i) $S \cong \mathrm{PSL}_2(q)$ *and* $\dim(V) \leq \bar{\mathsf{o}}(g) \leq q + 1$. *Moreover, if* $q \geq 11$ *then the image of $g$ in* $\mathrm{Aut}(S)$ *lies in* $\mathrm{PGL}_2(q)$.
(ii) $S = \mathrm{PSL}_n(q)$, $n \geq 3$, $E(G)$ *is a quotient of* $\mathrm{SL}_n(q)$, *and* $V|_{E(G)}$ *is one of* $q - 1$ *Weil modules, of dimension* $(q^n - 1)/(q - 1)$ *or* $(q^n - q)/(q - 1)$. *Moreover,* $\dim(V) \leq \bar{\mathsf{o}}(g) \leq (q^n - 1)/(q - 1)$.
(iii) $S = \mathrm{PSU}_n(q)$, $n \geq 3$, $E(G)$ *is a quotient of* $\mathrm{SU}_n(q)$, *and* $V|_{E(G)}$ *is one of* $q + 1$ *Weil modules, of dimension* $(q^n - (-1)^n)/(q + 1)$ *or* $(q^n + q(-1)^n)/(q + 1)$.
(iv) $S = \mathrm{PSp}_{2n}(q)$, $n \geq 2$, $2 \nmid q$, $E(G)$ *is a quotient of* $\mathrm{Sp}_{2n}(q)$, *every irreducible constituent of* $V|_{E(G)}$ *is one of four Weil modules, of dimension* $d := (q^n \pm 1)/2$, *and* $\dim(V) = d$ *or* $2d$.
(v) *Non-generic cases:*
   (a) *$S$ is one of the following groups:* $\mathrm{PSL}_3(4)$, $\mathrm{PSU}_4(3)$, $\mathrm{Sp}_6(2)$, $\Omega_8^+(2)$, ${}^2B_2(8)$, $G_2(3)$, $G_2(4)$, $V|_{E(G)}$ *is simple, and the classification of* ssp*-elements in $G$ can be read off from Table I.*

| $S$ | meo(Aut($S$)) | $\mathfrak{d}(S)$ | $G$ | dim($V$) | $\mathsf{ssp}$-classes |
|---|---|---|---|---|---|
| $\mathsf{A}_7$ | 12 | 4 | $2\mathsf{A}_7$ | 4 (2 reps) [**KRLT4**] | 9 classes |
| | | | $\mathsf{S}_7$ | 6 (2 reps) [**KT5**] | $7A$, $6C$, $10A$, $12A$ (4 classes) |
| | | | $3\mathsf{A}_7$ | 6 (2 reps) [**KRLT4**] | 6 classes |
| | | | $6\mathsf{A}_7$ | 6 (4 reps) [**KRLT4**] | 15 classes |
| $\mathrm{M}_{11}$ | 11 | 10 | $\mathrm{M}_{11}$ | 10 (3 reps) [**KRLT4**] | $11AB$ (2 classes) |
| | | | | 11 [**KRLT4**] | $11AB$ (2 classes) |
| $\mathrm{M}_{12}$ | 12 | 10 | $2\mathrm{M}_{12} \cdot 2$ | 10 (4 reps) (-) | 11 classes |
| | | | $\mathrm{M}_{12}$ | 11 (2 reps) (-) | $11AB$ (2 classes) |
| | | | $2\mathrm{M}_{12} \cdot 2$ | 12 (2 reps) (-) | $24AB$ (2 classes) |
| $\mathrm{M}_{22}$ | 14 | 10 | $2\mathrm{M}_{22} \cdot 2$ | 10 (4 reps) [**KRLT4**] | 10 classes |
| $\mathrm{M}_{23}$ | 23 | 22 | $\mathrm{M}_{23}$ | 22 [**KRLT4**] | $23AB$ (2 classes) |
| $\mathrm{M}_{24}$ | 23 | 23 | $\mathrm{M}_{24}$ | 23 [**KRLT4**] | $23AB$ (2 classes) |
| $\mathrm{J}_2$ | 24 | 6 | $2\mathrm{J}_2$ | 6 (2 reps) [**KRL**] | 17 classes |
| | | | $2\mathrm{J}_2 \cdot 2$ | 14 (2 reps) [**KRLT4**] | $28AB$, $24CDEF$ (6 classes) |
| $\mathrm{J}_3$ | 34 | 18 | $3\mathrm{J}_3$ | 18 (4 reps) [**KRLT4**] | $19AB$, $57ABCD$ (6 classes) |
| HS | 30 | 22 | $\mathrm{HS} \cdot 2$ | 22 (2 reps) (-) | $30A$ |
| McL | 30 | 22 | $\mathrm{McL} \cdot 2$ | 22 (2 reps) [**KRLT4**] | $30A$, $22AB$ (3 classes) |
| Ru | 29 | 28 | 2Ru | 28 [**KRLT4**] | $29AB$, $58AB$ (4 classes) |
| Suz | 40 | 12 | 6Suz | 12 (2 reps) [**KRLT3**] | 57 classes |
| $\mathrm{Co}_1$ | 60 | 24 | $2\mathrm{Co}_1$ | 24 [**KRLT3**] | 17 classes |
| $\mathrm{Co}_2$ | 30 | 23 | $\mathrm{Co}_2$ | 23 [**KRLT2**] | $23AB$, $30AB$ (4 classes) |
| $\mathrm{Co}_3$ | 30 | 23 | $\mathrm{Co}_3$ | 23 [**KRLT1**] | $23AB$, $30A$ (3 classes) |
| $\mathrm{PSL}_3(4)$ | 21 | 6 | $6S \cdot 2_1$ | 6 (4 reps) [**KRLT4**] | many classes |
| | | | $4_1S \cdot 2_3$ | 8 (8 reps) [**KRLT4**] | 12 classes |
| | | | $2S \cdot 2_2$ | 10 (4 reps) [**KRLT4**] | $14CDEF$ (4 classes) |
| $\mathrm{PSU}_4(3)$ | 28 | 6 | $6_1S \cdot 2_2$ | 6 (4 reps) [**KRLT4**] | many classes |
| $\mathrm{Sp}_6(2)$ | 15 | 7 | $\mathrm{Sp}_6(2)$ | 7 [**KRLT4**] | $7A$, $8B$, $9A$, $12C$, $15A$ |
| | | | $2\mathrm{Sp}_6(2)$ | 8 [**KRLT4**] | 8 classes |
| | | | $\mathrm{Sp}_6(2)$ | 15 (-) | $15A$ |
| $\Omega_8^+(2)$ | 30 | 8 | $2\Omega_8^+(2) \cdot 2$ | 8 [**KRLT4**] | 22 classes |
| ${}^2B_2(8)$ | 15 | 14 | ${}^2B_2(8) \cdot 3$ | 14 (6 reps) [**KRLT4**] | $15AB$ (2 classes) |
| $G_2(3)$ | 18 | 14 | $G_2(3) \cdot 2$ | 14 (2 reps) [**KRLT4**] | $14A$, $18ABC$ (4 classes) |
| $G_2(4)$ | 24 | 12 | $2G_2(4) \cdot 2$ | 12 (2 reps) [**KRLT4**] | 20 classes |

TABLE II. Elements with simple spectra in non-generic cases

(b) $V|_{E(G)}$ *is the direct sum of two simple modules of equal dimension, and one of the following possibilities occurs.*

($\alpha$) $E(G) = S = \mathrm{SU}_4(2)$*,* $G/\mathbf{Z}(G) = \mathrm{Aut}(S)$*, either* $\dim(V) = 8$ *and* $\bar{\mathsf{o}}(g) = 9, 10, 12$*, or* $\dim(V) = 10$ *and* $\bar{\mathsf{o}}(g) = 10, 12$.

($\beta$) $S = \mathrm{SU}_5(2)$*,* $G/\mathbf{Z}(G) = \mathrm{Aut}(S)$*,* $\dim(V) = 22$*, and* $\bar{\mathsf{o}}(g) = 24$.

Proof. If $S \not\cong \mathrm{PSL}_2(q)$, then the theorem is just [**KT5**, Theorem 6.6], which also gives the first statement in (i) when $S = \mathrm{PSL}_2(q)$. For the second claim in (i), assume $q \geq 11$. Then

$$\bar{\mathsf{o}}(g) \geq \dim(V) \geq (q-1)/\gcd(2, q-1)$$

by Lemma 3.1.1, and so we are done unless $q = 25$. If $q = 25$, but the image of $g$ is not contained in $\mathrm{PGL}_2(25)$, then using [**CCNPW**] we can check that $\bar{\mathsf{o}}(g) \leq 12$; on the other hand, $V|_{E(G)}$ is either irreducible of dimension $\geq 24$, or a sum of two simple summands of dimension 12 or 13 that are fused by $g$. Thus $\bar{\mathsf{o}}(g) < \dim(V)$, a contradiction. □

Theorem 3.1.6. *In the situation of* (3.1.0.1), *assume in addition that* $V|_{E(G)}$ *is irreducible and that* $\dim(V) \neq 4, 6$. *Then the following statements hold.*

(i) *The action of* $G$ *on* $V$ *is tensor indecomposable and not tensor induced.*

(ii) *Either* $(G, V)$ *satisfies* (**S**+), *or* $(G, V)$ *is imprimitive and one of the following cases occurs.*

(a) $E(G)/\mathbf{Z}(E(G)) \cong \mathrm{PSL}_n(q)$, $n \geq 2$, $q \geq 3$, *and* $\dim(V) = (q^n - 1)/(q-1)$.

(b) $E(G) = \mathrm{PSL}_2(7)$ *and* $\dim(V) = 7$.

(c) $E(G) = \mathrm{M}_{11}$ *and* $\dim(V) = 11$.

(d) $E(G) = 2\mathrm{M}_{12}$ *and* $\dim(V) = 12$.

Proof. (i) The statement is obvious in the case $\dim(V)$ is a prime, so we may assume that $\dim(V) \geq 8$. In particular, using [**CCNPW**] we see that $S \not\cong \mathsf{A}_5$ and so $\mathfrak{d}(S) \geq 3$.

If $S \cong \mathsf{A}_6$, then we can check directly using [**CCNPW**] that $\dim(V) \neq 9$ (because $G$ possesses an $\mathsf{ssp}$-element), and $\mathfrak{d}(S) = 3$. If furthermore $\dim(V) \geq 10$, then we get $E(G) \cong \mathrm{SL}_2(9)$, $\dim(V) = 10$, and $G/\mathbf{Z}(G)E(G) \leq C_2$, in which case one can check the statements readily. Hence we may assume $\dim(V) \leq 8$ when $S \cong \mathsf{A}_6$. Now, Theorems 10.3.5, 3.1.3, and 3.1.5 imply that $\dim(V) < \mathfrak{d}(S)^2$ in all remaining cases. Hence, if $(G, V)$ is tensor decomposable: $G \leq \mathrm{GL}(A) \otimes \mathrm{GL}(B)$ with $1 < \dim(A) < \dim(B)$, then we may assume that $\dim(A) < \mathfrak{d}(S)$, and so the projective representation of $E(G)$ on $A$ is reducible, contradicting the irreducibility of $E(G)$ on $V = A \otimes B$. Thus $(G, V)$ is tensor indecomposable.

Assume now that $(G, V)$ is tensor induced and let $H \lhd G$ be the subgroup of $G$ that stabilizes each of the $n \geq 2$ tensor factors, each of dimension $d$ so that $\dim(V) = d^n$. Then $\dim(V) < \mathfrak{d}(S)^2$ again implies that $d < \mathfrak{d}(S)$ and so $E(G) \not\leq H$ (because otherwise $E(G)$ would stabilize each of the tensor factor and act reducibly on each of them). As $E(G)$ is quasisimple, we must have that $E(G) \cap H = \mathbf{Z}(E(G))$. Thus $S = E(G)/\mathbf{Z}(E(G))$ embeds in $G/H \hookrightarrow \mathsf{S}_n$ and acts faithfully on the set of $n$ tensor factors. However, as $\mathfrak{d}(S) \geq 3$ we have

$$n = \log_d \dim(V) < \log_2 \mathfrak{d}(S)^2 < \mathfrak{d}(S) + 1 \leq P(S),$$

where $P(S)$ denotes the smallest index of proper subgroups in $S$, contradicting $S \hookrightarrow \mathsf{S}_n$.

We have shown that $(G, V)$ is not tensor induced, whence the statement follow. For a later application in Theorem 5.2.12, we also note that when $\dim(V) = 6$ and $\mathfrak{d}(S) < 3$, $S = \mathsf{A}_5$ and $V$ is imprimitive by [**CCNPW**]. Hence, (**S**+) also holds if $\dim(V) = 6$ and $V$ is primitive.

(ii) Note by Lemma 1.1.6 that (**S**+) necessarily implies that $E(G)$ is irreducible on $V$. In view of (i), it suffices to determine whether the $G$-module is primitive.

Assume that $G$ fixes an imprimitive decomposition $V = \oplus_{i=1}^{t} V_i$ with $t > 1$. Since $\mathbf{Z}(E(G)) \leq \mathbf{Z}(G)$ by irreducibility of $E(G)$, we see that $\mathbf{Z}(G)$ acts trivially on $\{V_1, \ldots, V_t\}$.

Now irreducibility of $E(G)$ on $V$ implies that $S := E(G)/\mathbf{Z}(E(G))$ acts transitively on this set, when $S$ has a proper subgroup of index $t$ that divides $\dim(V)$. Using [**KlL**, Table 5.2.A] and [**CCNPW**], and going through the cases listed in Theorems 10.3.5, 3.1.3, and 3.1.5, we can check that when $\dim(V) > 12$, the latter is possible only when $(S, \dim(V)) \neq (\mathrm{PSL}_n(q), (q^n-1)/(q-1))$, leading to (a). Assume now that $\dim(V) \leq 12$ and we are not in (a). Now we have

$$5 \leq P(S) \leq t \leq \dim(V),$$

and that $\dim(V) \neq 6$ by assumption. We will use [**GAP**] to check this condition for the modules listed in Theorems 10.3.5, 3.1.3, and 3.1.5 when $S \not\cong \mathsf{A}_5, \mathsf{A}_6$, and in [**GAP**] when $S = \mathsf{A}_5$, $\mathsf{A}_6$.

When $S = \mathsf{A}_5 \cong \mathrm{PSL}_2(4)$, the possibility $\dim(V) = 5$ is already included in (a) (indeed, if $\chi \in \mathrm{Irr}(S)$ has degree 5, then $\chi = \mathrm{Ind}_M^S(\alpha)$ for a non-principal linear character $\alpha$ of $M \cong \mathsf{A}_4$).

When $S = \mathsf{A}_6 \cong \mathrm{PSL}_2(9)$, any proper subgroup of $S$ has index 6 or $\geq 10$ whereas $\dim(V) \leq \mathrm{meo}(\mathrm{Aut}(S)) = 10$ [**CCNPW**], so, in view of (a) and the assumption $\dim(V) \neq 6$, no further consideration is needed.

When $S = \mathsf{A}_7$, any proper subgroup of $S$ has index 7 or $\geq 15$ whereas $\dim(V) \leq \mathrm{meo}(\mathrm{Aut}(S)) = 12$ [**CCNPW**], so $V$ can only have dimension 7 which is impossible.

When $S = \mathsf{A}_8$, any proper subgroup of $S$ has index 8 or $\geq 15$ whereas $\dim(V) \leq \mathrm{meo}(\mathrm{Aut}(S)) = 15$ [**CCNPW**], so $V$ can only have dimension 8 or 15. There is no $V$ of dimension 15, see [**CCNPW**], and the ones of dimension 8 are primitive (since any subgroup of index 8 of $E(G) = 2\mathsf{A}_8$ is isomorphic to $2\mathsf{A}_7$, which is perfect, and so any linear character of it is trivial and cannot induce to $E(G)$ to yield $V|_{E(G)}$).

When $S = \mathrm{PSL}_2(7)$, we only need to look at the case $\dim(V) = 7$, which leads to (b); (indeed, if $\chi \in \mathrm{Irr}(S)$ has degree 7, then $\chi = \mathrm{Ind}_M^S(\alpha)$ for a non-principal linear character $\alpha$ of $M \cong \mathsf{S}_4$).

When $S = \mathrm{PSL}_2(11)$, $P(S) = 11$ and $\dim(V) \leq \mathrm{meo}(\mathrm{Aut}(S)) = 12$ [**CCNPW**], so in view of (a), $V$ can only have dimension 11. However, such a module is primitive (since any subgroup of index 11 of $E(G) = S$ is isomorphic to $\mathsf{A}_5$, which is perfect, and so any linear character of it is trivial and cannot induce to $S$ to yield $V|_S$).

When $S = \mathrm{M}_{11}$, $P(S) = 11 = \mathrm{meo}(\mathrm{Aut}(S))$ [**CCNPW**], so $\dim(V) = 11$, leading to (c); indeed, if $\chi \in \mathrm{Irr}(S)$ has degree 11, then $\chi = \mathrm{Ind}_M^S(\alpha)$ for a non-principal linear character $\alpha$ of $M \cong \mathsf{A}_6 \cdot 2_3$.

When $S = \mathrm{M}_{12}$, $P(S) = 12 = \mathrm{meo}(\mathrm{Aut}(S))$ [**CCNPW**], so $\dim(V) = 12$, leading to (d); indeed, if $\chi \in \mathrm{Irr}(E(G))$ has degree 12, then $E(G) \cong 2\mathrm{M}_{12}$ and $\chi = \mathrm{Ind}_M^{E(G)}(\alpha)$ for a non-principal linear character $\alpha$ of $M \cong 2 \times \mathrm{M}_{11}$. □

Using the aforementioned results on representations of almost quasisimple groups admitting ssp-elements, we now prove

THEOREM 3.1.7. *Let $H < \mathrm{GL}(V) \cong \mathrm{GL}_d(\mathbb{C})$ be a finite almost quasisimple group that admits an element $h$ with simple spectrum. Assume in addition that $V$ is irreducible over $L := E(H)$. Then either*

$$\bar{\mathsf{o}}(h) < d^2/2$$

*or one of the following cases occurs.*

(a) *$d = 2$, $H = \mathrm{SL}_2(5)$, and $\bar{\mathsf{o}}(h) = 2$, 3, or 5.*

(b) *$d = 3$, $H = \mathsf{A}_5$, and $\bar{\mathsf{o}}(h) = 5$.*
(c) *$d = 3$, $H = \mathrm{PSL}_2(7)$, and $\bar{\mathsf{o}}(h) = 7$.*
(d) *$d = 3$, $H = 3\mathsf{A}_6$, and $\bar{\mathsf{o}}(h) = 5$.*
(e) *$d = 4$, $H = \mathrm{Sp}_4(3)$, and $\bar{\mathsf{o}}(h) = 9$ or $12$.*
(f) *$d = 6$, $L = 6_1 \cdot \mathrm{PSU}_4(3)$, $H/\mathbf{Z}(H) \cong \mathrm{PSU}_4(3) \cdot 2_2$, and $\bar{\mathsf{o}}(h) = 18$.*

Proof. We will assume that

$$\bar{\mathsf{o}}(h) \geq d^2/2. \tag{3.1.7.1}$$

The list of possible $H$ in the case $d = 2$, $3$ is well known, see e.g. [**HM**], and we easily arrive at (a)–(d). From now on, we will assume $d \geq 4$, and let $S = L/\mathbf{Z}(L)$ be the unique non-abelian composition factor of $H$. Also, let $\mathrm{meo}(\mathrm{Aut}(S))$ denote the largest order of elements in $\mathrm{Aut}(S)$.

(i) Here we consider the case $S = \mathsf{A}_n$ with $n \geq 5$. If $n = 5$, then $\bar{\mathsf{o}}(h) \leq \mathrm{meo}(\mathrm{Aut}(S)) = 6 < d^2/2$, contrary to (3.1.7.1). If $n = 6$, then $\bar{\mathsf{o}}(h) \leq \mathrm{meo}(\mathrm{Aut}(S)) = 10$, so (3.1.7.1) implies that $d = 4$. In this case, we have by [**CCNPW**] that $L = 2\mathsf{A}_6$ and $S \lhd H/\mathbf{Z}(H) \leq S \cdot 2_1$, which then implies that $\bar{\mathsf{o}}(h) \leq 6$, again contradicting (3.1.7.1). If $n = 7$, then $\bar{\mathsf{o}}(h) \leq \mathrm{meo}(\mathrm{Aut}(S)) = 12$, so (3.1.7.1) again implies that $d = 4$. In this case, we have by [**CCNPW**] that $H = 2\mathsf{A}_7$ and so $\bar{\mathsf{o}}(h) \leq 7$, again contradicting (3.1.7.1).

Assume now that $n \geq 8$. Then we can apply Theorem 10.3.5 to see that (3.1.7.1) implies that we are in case (i)(a) of Theorem 10.3.5, and so $\bar{\mathsf{o}}(h) \leq n^2/4 < (n-1)^2/2 = d^2$, a contradiction.

(ii) Assume now that $S$ is one of 26 sporadic simple groups, and apply Theorem 3.1.3. Using the information on $(V, \mathrm{meo}(\mathrm{Aut}(S))$ listed in Table 1, we see that (3.1.7.1) implies that $H = 2\mathrm{J}_2$ and $d = 6$, in which case we also have $\bar{\mathsf{o}}(h) \leq 15$, violating (3.1.7.1).

(iii) From now on we may assume that $S$ is a simple group of Lie type, and apply Theorem 3.1.5. First consider the case $S = \mathrm{PSL}_2(q)$ with $q \geq 7$ and $q \neq 9$ (note that the cases $\mathrm{SL}_2(4) \cong \mathrm{PSL}_2(5) \cong \mathsf{A}_5$ and $\mathrm{PSL}_2(9) \cong \mathsf{A}_6$ have already been considered in (i)). If $q = 7$, then $\bar{\mathsf{o}}(h) \leq 8$, and so (3.1.7.1) implies that $d = 4$, whence $H = L = \mathrm{SL}_2(7)$ and $\bar{\mathsf{o}}(h) \leq 7$ (see [**CCNPW**]), a contradiction. If $q = 8$, then $\bar{\mathsf{o}}(h) \leq 9$ whereas $d \geq 7$, see [**CCNPW**], contradicting (3.1.7.1). If $q \geq 11$, then $\bar{\mathsf{o}}(h) \leq q + 1$ by Theorem 3.1.5(i), whereas $d \geq (q-1)/2$ (see [**TZ1**, Theorem 1.1]), and this again violates (3.1.7.1).

Suppose $S = \mathrm{PSL}_n(q)$ with $n \geq 3$ and $(n, q) \neq (3, 2), (3, 4)$. Then $d \geq (q^n - q)/(q-1)$ and $\mathrm{meo}(\mathrm{Aut}(S)) = (q^n - 1)/(q-1) \leq d + 1$ by [**GMPS**, Theorem 2.16], contradicting (3.1.7.1). The case $\mathrm{SL}_3(2) \cong \mathrm{PSL}_2(7)$ has already been treated. Suppose now that $S = \mathrm{PSL}_3(4)$. Then $\mathrm{meo}(\mathrm{Aut}(S)) = 21$, so (3.1.7.1) yields that $d = 6$, $L = 6S$, $S \lhd H/\mathbf{Z}(H) \leq S \cdot 2_1$ (see [**CCNPW**]), in which case we have $\bar{\mathsf{o}}(h) \leq 8$, a contradiction.

Suppose next that $S = \mathrm{PSp}_{2n}(q)$ with $n \geq 2$ and $(n, q) \neq (2, 3)$. Then $d \geq (q^n - 1)/2$ and $\mathrm{meo}(\mathrm{Aut}(S)) \leq q^{n+1}/(q-1)$ by [**GMPS**, Theorem 2.16], again violating (3.1.7.1). Assume now that $S = \mathrm{PSp}_4(3)$. Then $\mathrm{meo}(\mathrm{Aut}(S)) = 12$, so (3.1.7.1) yields that $d = 4$, $H = \mathrm{Sp}_4(3)$, $\bar{\mathsf{o}}(h) = 9$ or $12$ (see [**CCNPW**]), and we arrive at (e).

Suppose $S = \mathrm{PSU}_n(q)$ with $n \geq 3$ and $(n, q) \neq (3, 2)$, $(3, 3)$, $(4, 2)$, $(4, 3)$, $(5, 2)$. Then $d \geq (q^n - q)/(q+1)$ and $\mathrm{meo}(\mathrm{Aut}(S)) \leq q^{n-1} + q^2$ by [**GMPS**, Theorem 2.16], again contradicting (3.1.7.1). Note that $\mathrm{PSU}_3(2)$ is solvable, and $\mathrm{PSU}_4(2) \cong \mathrm{PSp}_4(3)$ has already been handled. If $S = \mathrm{SU}_5(2)$, then $d \geq 10$ and $\mathrm{meo}(\mathrm{Aut}(S)) = 24$, contrary to (3.1.7.1).

If $S = \mathrm{SU}_3(3)$, then $d \geq 6$ and $\mathrm{meo}(\mathrm{Aut}(S)) = 12$, again contradicting (3.1.7.1). Suppose next that $S = \mathrm{PSU}_4(3)$. Then $\mathrm{meo}(\mathrm{Aut}(S)) = 28$, so (3.1.7.1) yields that $d = 6$, $L = 6_1 \cdot S$, $S \lhd H/\mathbf{Z}(H) \leq S \cdot 2_2$, and $\bar{\mathsf{o}}(h) = 18$ (see [**CCNPW**]), leading to (f).

Finally, in the exceptional cases $S = \mathrm{Sp}_6(2)$, $\Omega_8^+(2)$, ${}^2B_2(8)$, $G_2(3)$, and $G_2(4)$ of Theorem 3.1.5(v), using the information on $(V, \mathrm{meo}(\mathrm{Aut}(S))$ listed in Table 1, we can check that $\mathrm{meo}(\mathrm{Aut}(S)) < d^2/2$, violating (3.1.7.1). □

THEOREM 3.1.8. [**KT5**, Corollary 8.4] *Suppose* (3.1.0.1) *gives rise to a hypergeometric sheaf $\mathcal{H}$ of type $(D, m)$ with $D - m \geq 2$, with $G = G_{\mathrm{geom}}$, $g$ a generator of the image of $I(0)$ in $G$, and $V$ realizes the action of $G$ on $\mathcal{H}$. Suppose in addition that we are in the cases* (ii)–(iv) *of Theorem 3.1.5, and that $V|_{E(G)}$ is irreducible. Then $G/\mathbf{Z}(G) \cong \mathrm{PGL}_n(q)$, respectively $\mathrm{PSp}_{2n}(q)$, $\mathrm{PGU}_n(q)$.*

THEOREM 3.1.9. [**KT5**, Theorem 8.5] *Let $p$ be a prime. Let $G$ be a finite irreducible subgroup of $\mathrm{GL}(V) \cong \mathrm{GL}_{p^n}(\mathbb{C})$ that satisfies* ($\mathbf{S}+$) *and is an extraspecial normalizer, so that $G \rhd R = \mathbf{Z}(R)E$ for some some extraspecial $p$-group $E$ of order $p^{1+2n}$ that acts irreducibly on $V$, and furthermore either $R = E$ or $\mathbf{Z}(R) \cong C_4$, as in* [**GT3**, Proposition 2.8(iii)]. *Suppose that a $p'$-element $g \in G$ has simple spectrum on $V$ and that $p^n \geq 11$. Then the following statements hold.*

(i) *Suppose $p > 2$. Then $\exp(R) = p$, $\bar{\mathsf{o}}(g) = p^n + 1$, and the coset $g\mathbf{Z}(G)R$ as an element of $G/\mathbf{Z}(G)R \hookrightarrow \mathrm{Sp}_{2n}(p)$ generates a cyclic maximal torus $C_{p^n+1}$ of $\mathrm{Sp}_{2n}(p)$.*
(ii) *Suppose $p = 2$. Then one can find integers $a_1 > a_2 > \ldots > a_t \geq 1$ such that $n = \sum_{i=1}^t a_i$, $\gcd(2^{a_i}+1, 2^{a_j}+1) = 1$ if $i \neq j$, $\bar{\mathsf{o}}(g) = \prod_{i=1}^t (2^{a_i}+1)$, and the coset $g\mathbf{Z}(G)R$ as an element of $G/\mathbf{Z}(G)R \hookrightarrow \mathrm{Sp}_{2n}(2)$ generates a cyclic maximal torus $C_{2^{a_1}+1} \times \ldots \times C_{2^{a_t}+1}$ of $\mathrm{Sp}_{2n}(2)$.*

Our next result offers an optimal refinement of [**KT5**, Theorem 7.3]:

THEOREM 3.1.10. *Let $\mathcal{H}$ be a hypergeometric sheaf in characteristic $p$ of type $(D, m)$ with $D > m$ and with finite geometric monodromy group $G = G_{\mathrm{geom}}$. Suppose that $G$ is an almost quasisimple group of Lie type:*

$$S \lhd G/\mathbf{Z}(G) \leq \mathrm{Aut}(S)$$

*for some finite simple group $S$ of Lie type in characteristic $r$, and either $\mathcal{H}$ is* ($\mathbf{S}+$), *or $G^{(\infty)}$ is irreducible on $\mathcal{H}$. Then at least one of the following statements holds.*

(i) *$p = r$, i.e. $\mathcal{H}$ and $S$ have the same characteristic.*
(ii) *$D \leq 10$ and $S$ is one of the following simple groups:* $\mathsf{A}_5$, $\mathsf{A}_6$, $\mathsf{A}_8$, $\mathrm{PSL}_2(7)$, $\mathrm{SL}_2(8)$, $\mathrm{PSL}_2(11)$, $\mathrm{PSL}_3(4)$, $\mathrm{SU}_3(3)$, $\mathrm{SU}_4(2) \cong \mathrm{PSp}_4(3)$, $\mathrm{SU}_5(2)$, $\mathrm{PSU}_4(3)$, $\mathrm{Sp}_6(2)$, $\Omega_8^+(2)$. *More precisely, one of the following statements holds.*
  (ii-2) *$D = 2$, and $S = \mathsf{A}_5$.*
  (ii-3) *$D = 3$, and $S = \mathsf{A}_5$, $\mathsf{A}_6$, $\mathrm{PSL}_2(7)$.*
  (ii-4) *$D = 4$, and $S = \mathsf{A}_5$, $\mathsf{A}_6$, $\mathrm{PSL}_2(7)$, $\mathrm{SU}_4(2)$.*
  (ii-5) *$D = 5$, and $S = \mathsf{A}_5$, $\mathsf{A}_6$, $\mathrm{PSL}_2(11)$, $\mathrm{SU}_4(2)$.*
  (ii-6) *$D = 6$, and $S = \mathsf{A}_5$, $\mathsf{A}_6$, $\mathrm{PSL}_2(7)$, $\mathrm{PSL}_2(11)$, $\mathrm{PSL}_3(4)$, $\mathrm{SU}_3(3)$, $\mathrm{SU}_4(2)$, $\mathrm{PSU}_4(3)$.*
  (ii-7) *$D = 7$, and $S = \mathsf{A}_8$, $\mathrm{PSL}_2(7)$, $\mathrm{SL}_2(8)$, $\mathrm{SU}_3(3)$, $\mathrm{Sp}_6(2)$.*
  (ii-8) *$D = 8$, and $S = \mathsf{A}_6$, $\mathsf{A}_8$, $\mathrm{PSL}_2(7)$, $\mathrm{SL}_2(8)$, $\mathrm{PSL}_3(4)$, $\mathrm{Sp}_6(2)$, $\Omega_8^+(2)$.*
  (ii-9) *$D = 9$, and $S = \mathsf{A}_6$, $\mathrm{SL}_2(8)$.*

(ii-10) *$D = 10$, and $S = \mathsf{A}_6$, $\mathrm{PSL}_2(11)$, $\mathrm{PSL}_3(4)$, $\mathrm{SU}_4(2)$, $\mathrm{SU}_5(2)$.*

(iii) *$D = 12$, $S = \mathrm{SU}_3(4)$, and $p = 5$ or $13$.*

(iv) *$D = 14$, $p = 13$, and $S = {}^2B_2(8)$ or $G_2(3)$.*

Proof. Assume $(\mathcal{H}, G)$ is as in the theorem, but $p \neq r$. Note that $(\mathbf{S}+)$ implies by Lemma 1.1.6 that the central cover $L := G^{(\infty)}$ of $S$ is irreducible on the underlying representation $V = V_{\mathcal{H}}$ of $\mathcal{H}$; in paricular $\mathbf{Z}(G) = \mathbf{C}_G(L)$ and $G/\mathbf{Z}(G) \hookrightarrow \mathrm{Aut}(S)$. Recall that a generator $g_0$ of the image of $I(0)$ in $G$, a $p'$-element, has simple spectrum on $V$, which implies

$$D \leq \bar{\mathsf{o}}(g_0) \leq \mathrm{meo}(\mathrm{Aut}(S)). \tag{3.1.10.1}$$

Let $Q$ denote the image of $I(\infty)$ in $G$, and let $\varphi$ denote the character of the $G$-module $V$. Suppose that there exists a constant $0 < \alpha < 1$ such that $|\varphi(x)|/\varphi(1) \leq \alpha$ for all $x \in Q \smallsetminus \mathbf{Z}(G)$. We will frequently use the following lower bound

$$|Q| > w \geq D(1-\alpha)(1-1/|Q|) \tag{3.1.10.2}$$

for $w := \dim \mathsf{Wild} = D - m$. [Indeed, the action of $Q$ on $\mathsf{Wild}$ implies by Propositions 5.8 and 5.9 of [**KRLT4**] that $w < |Q|$, and the second inequality in (3.1.10.2) is reproduced from [**KT5**, (7.2.2)].] Furthermore, in the cases where $Q/(Q \cap \mathbf{Z}(G))$ is cyclic, in particular when Sylow $p$-subgroups of $\mathrm{Aut}(S)$ are cyclic, we must have that

$$w \leq [Q : Q \cap \mathbf{Z}(G)]. \tag{3.1.10.3}$$

Indeed, the cyclic assumption implies that $Q$ is abelian. By Propositions 5.8 and 5.9 of [**KRLT4**], the character of the $Q$-module $\mathsf{Wild}$ is a sum of $w$ distinct linear characters $\lambda_i$, $1 \leq i \leq w$. Note that $Q \cap \mathbf{Z}(G)$ acts on $V_{\mathcal{H}}$ via a central character $\nu$, and $Q$ has exactly $[Q : Q \cap \mathbf{Z}(G)]$ linear characters lying above $\nu$. Hence the claim follows.

Now we can apply [**KT5**, Theorem 7.4] to see that $D \leq 22$, and arrive at the following possibilities for $S$:

$$\begin{gathered}\mathrm{PSL}_2(5,7,8,9,11,25),\ \mathsf{A}_8,\ \mathrm{PSL}_3(3,4),\ \mathrm{PSU}_{4,5,6}(2),\ \mathrm{PSU}_{3,4}(3)\\ \mathrm{PSU}_3(4,5),\ \mathrm{Sp}_6(2),\ \mathrm{PSp}_6(3),\ \mathrm{PSp}_4(5),\ \Omega_8^+(2),\ {}^2B_2(8),\ G_2(3,4),\end{gathered}$$

which we will analyze individually. We also let $g_\infty \in G$ be a $p'$-element that generates the image of $I(\infty)$ in $G$ modulo $Q$, and note that the cases $S = G_2(4)$ and $S = \mathrm{SU}_3(4)$ are treated by Theorem 24.6, respectively Corollary 24.7, of [**KRLT4**].

(a) If $S = \mathrm{PSL}_2(q)$ with $q = 4, 5, 7, 8$, then $\mathrm{meo}(\mathrm{Aut}(S)) \leq 9$ [**CCNPW**], so $D \leq 9$ by (3.1.10.1), and (ii) holds. If $S = \mathsf{A}_6 \cong \mathrm{PSL}_2(9) \cong \mathrm{Sp}_6(2)'$, then $\mathrm{meo}(\mathrm{Aut}(S)) \leq 10$, so again $D \leq 10$ and (ii) holds. In addition, if $D = 10$, then $\bar{\mathsf{o}}(g_0) = 10$ by (3.1.10.1), whence $p = 3$ since $g_0$ is a $p'$-element. More generally, the list of possibilities in (ii-2)–(ii-10) can be verified using [**HM**].

Suppose $S = \mathrm{PSL}_2(11)$, but $p \neq 11$ and $D > 10$. Note that $S \leq G/\mathbf{Z}(G) \leq \mathrm{Aut}(S) = S{\cdot}2$, and both $S$ and $S \cdot 2$ inject in $\mathrm{GL}_3(\overline{\mathbb{F}_{11}})$ as irreducible subgroups. By [**KT5**, Theorem 4.14], this implies that $w \leq 3$. On the other hand, $D \leq \mathrm{meo}(\mathrm{Aut}(S)) = 12$, and using [**GAP**] we can check that $|\varphi(x)| \leq 2$ for all $x \in G \smallsetminus \mathbf{Z}(G)$. Thus we can take $\alpha = 1/5$, and as $|Q| \geq 2$, (3.1.10.2) implies $w > 4$, a contradiction.

Suppose $S = \mathrm{PSL}_2(25)$, but $p \neq 5$ and $D \leq 22$. Since $V|_L$ is irreducible, we have $D = 12$ or 13 by [**GAP**], and so $S \leq G/\mathbf{Z}(G) \leq S{\cdot}2_2$. Next, each of $S$ and $S{\cdot}2_2$ injects in $\mathrm{GL}_d(\overline{\mathbb{F}_5})$ as an irreducible subgroup for some $d \leq 4$. By [**KT5**, Theorem 4.14], this implies that $w \leq 4$.

Using [**GAP**] we can check that $|\varphi(x)| \leq 5$ for all $x \in G \smallsetminus \mathbf{Z}(G)$, and thus we can take $\alpha = 5/12$. Hence (3.1.10.2) yields $|Q| > w \geq 4$. Since $|Q| \geq 5$, (3.1.10.2) now implies $w \geq 6$, a contradiction.

Suppose $S = \mathsf{A}_8 \cong \mathrm{SL}_4(2)$, but $p \neq 2$ and $D > 8$. Since $\mathrm{meo}(\mathrm{Aut}(S)) = 15$ [**GAP**] and $V|_L$ is irreducible, we see that $D = 14$ and $\bar{\mathsf{o}}(g_0) = 15$. The latter rules out $p = 3, 5$. In the remaining case $p = 7$, the Sylow $p$-subgroups of $\mathrm{Aut}(S)$ are of order 7, so $w \leq 7$ by (3.1.10.3). However, $\varphi(x) = 0$ for all $x \in Q \smallsetminus \mathbf{Z}(G)$, yielding $\alpha = 0$ and so $w \geq 12$ by (3.1.10.2), a contradiction.

Suppose $S = \mathrm{SL}_3(3)$, but $p \neq 3$. Since $V|_L$ is irreducible and $D \leq \mathrm{meo}(\mathrm{Aut}(S)) = 13$, we have $D = 12$ or 13 by [**GAP**], $L = S$ and $S \leq G/\mathbf{Z}(G) \leq S \cdot 2$. Next, each of $S$ and $S \cdot 2$ injects in $\mathrm{GL}_d(\overline{\mathbb{F}_3})$ as an irreducible subgroup for some $d \leq 6$. By [**KT5**, Theorem 4.14], this implies that $w \leq 6$. Using [**GAP**] we can check that $|\varphi(x)| \leq 4$ for all $x \in G \smallsetminus \mathbf{Z}(G)$, and thus we can take $\alpha = 1/3$. Hence (3.1.10.2) yields $|Q| > w \geq 4$. Since $|Q| \geq 5$, (3.1.10.2) now implies $w > 6$, a contradiction.

Suppose $S = \mathrm{PSL}_3(4)$, but $p \neq 2$ and $D \geq 11$. Since $V|_L$ is irreducible and $D \leq \mathrm{meo}(\mathrm{Aut}(S)) = 21$, we have $D \in \{15, 20, 21\}$ by [**GAP**]. Now, since $\bar{\mathsf{o}}(g_0) \geq D \geq 15$, we can see that 3 always divides $\bar{\mathsf{o}}(g_0)$, showing $p \neq 3$. We can then check using [**GAP**] that $|\varphi(x)| \leq 1$ for all $x \in Q \smallsetminus \mathbf{Z}(G)$. Thus we can take $\alpha = 1/15$, which implies $w \geq 12$. This however contradicts (3.1.10.3), since Sylow $p$-subgroups of $\mathrm{Aut}(S)$ have order $p$.

Suppose $S = \mathrm{SU}_4(2)$ and $D \geq 11$. Then $D \leq \mathrm{meo}(\mathrm{Aut}(S)) = 12$, and $L$ has no irreducible characters of degree 11 or 12 [**GAP**], a contradiction.

Suppose $S = \mathrm{SU}_5(2)$, but $p \neq 2$ and $D \geq 11$. Since $V|_L$ is irreducible, we actually have $D = 11$ and $G = \mathbf{Z}(G)S$ by [**GAP**]. Now $S$ is an irreducible subgroup of $\mathrm{GL}_5(\overline{\mathbb{F}_2})$, so $w \leq 5$ by [**KT5**, Theorem 4.14]. If $p = 5$ or 11, then by [**GAP**] we have that $|\varphi(x)| \leq 1$ for all $x \in Q \smallsetminus \mathbf{Z}(G)$. Thus we can take $\alpha = 1/11$, which implies $w \geq 8$ by (3.1.10.2), a contradiction. Suppose $p = 3$. Again using [**GAP**] and (3.1.10.2), we see that $|Q| > w \geq 4$, whence $|Q| \geq 9$, yielding $w \geq 5$. Thus $w = 5$ and so $W \cong 3^4$ is elementary abelian by [**KRLT4**, Proposition 5.8]. Next, $3 \nmid |\mathbf{Z}(G)|$ by [**KT5**, Proposition 4.8(iv)], hence $Q \leq S$. Also, $5 | \bar{\mathsf{o}}(g_\infty)$ by [**KRLT4**, Proposition 5.8], and thus an element of order 5 of $S$ acts nontrivially on $Q$. It follows that $Q$ is a maximal torus of $S$ and hence contains an element of class $3c$ in the notation of [**GAP**], which however has eigenvalue 1 only with multiplicity 2 on $V$, showing $w \geq 9$, a contradiction.

Suppose $S = \mathrm{PSU}_6(2)$, but $p \neq 2$. Since $V|_L$ is irreducible and $D \leq \mathrm{meo}(\mathrm{Aut}(S)) = 36$, we have $D = 21$ or 22 by [**GAP**]. Now, since $\bar{\mathsf{o}}(g_0) \geq 21$, we can see that 3 always divides $\bar{\mathsf{o}}(g_0)$, showing $p \neq 3$. We can then check using [**GAP**] that $|\varphi(x)| \leq 2$ for all $x \in Q \smallsetminus \mathbf{Z}(G)$. Thus we can take $\alpha = 2/21$, which implies $w \geq 16$. This however contradicts (3.1.10.3), since Sylow $p$-subgroups of $\mathrm{Aut}(S)$ have order $p$.

Suppose $S = \mathrm{SU}_3(3)$ and $D \geq 8$. Then $D \leq \mathrm{meo}(\mathrm{Aut}(S)) = 12$, and $L$ has no irreducible characters of degree $9 \leq D \leq 12$ [**GAP**], a contradiction.

Suppose $S = \mathrm{PSU}_4(3)$, but $p \neq 3$ and $7 \leq D \leq 22$. Since $V|_L$ is irreducible, we have $D \in \{15, 20, 21\}$ by [**GAP**]. Now, since $\bar{\mathsf{o}}(g_0) \geq D \geq 15$, we can see that 2 always divides $\bar{\mathsf{o}}(g_0)$, showing $p \neq 2$. We can then check using [**GAP**] that $|\varphi(x)| \leq 1$ for all $x \in Q \smallsetminus \mathbf{Z}(G)$. Thus we can take $\alpha = 1/15$, which implies $w \geq 12$. This however contradicts (3.1.10.3), since Sylow $p$-subgroups of $\mathrm{Aut}(S)$ have order $p$.

Suppose $S = \mathrm{SU}_3(4)$, but $p \neq 2$. Since $V|_L$ is irreducible and $D \leq \mathrm{meo}(\mathrm{Aut}(S)) = 16$, we actually have $D = 12$ or $13$ by [**GAP**]. First we consider the case $D = 13$, which implies that $G = \mathbf{Z}(G) \times S$. In particular, $G$ admits an irreducible representation $G \to \mathrm{GL}_3(\overline{\mathbb{F}_4})$, hence [**KT5**, Theorem 4.14] implies that $w \leq 3$. For $p \neq 5$, we can check that $|\varphi(x)| \leq 1$ for all $x \in Q \smallsetminus \mathbf{Z}(G)$. Thus we can take $\alpha = 1/13$, which implies $w \geq 8$ by (3.1.10.2), a contradiction. If $p = 5$, then using [**GAP**] we see that any element $x \in Q \smallsetminus \mathbf{Z}(G)$ has all eigenspaces of dimension $\leq 4$, which implies that $w \geq D - 4 = 9$, again a contradiction. Now suppose that $D = 12$. Note that the cases $p = 5$ and $p = 13$ are recorded in (iii), so we have $p = 3$. Since the Sylow 3-subgroups of $\mathrm{Aut}(S)$ are of order 3, by (3.1.10.3) we have that $w \leq 3$. On the other hand, applying (3.1.10.2) with $\alpha = 0$ we have $w \geq 8$, a contradiction.

Suppose $S = \mathrm{PSU}_3(5)$, but $p \neq 5$. Since $V|_L$ is irreducible and $D \leq \mathrm{meo}(\mathrm{Aut}(S)) = 30$, we actually have $D = 20$ or $21$ by [**GAP**]. Now we can use [**GAP**] to check that no $3'$-element can have a simple spectrum on $V$, ruling out the case $p = 3$. For $p \neq 3, 5$, we can check that $|\varphi(x)| \leq 5$ for all $x \in Q \smallsetminus \mathbf{Z}(G)$. Thus we can take $\alpha = 1/4$, which implies $|Q| > w \geq 8$ by (3.1.10.2). Applying (3.1.10.2) with $|Q| \geq 9$, we actually have $w \geq 14$. Also, since $g_0$ has simple spectrum on $V$, we see that $g_0\mathbf{Z}(G) \in S \cdot 3$. Hence we can apply Theorem 1.2.2 to get that $S \leq G/\mathbf{Z}(G) \leq S \cdot 3$. Since each of $S$ and $S \cdot 3$ is an irreducible subgroup of $\mathrm{GL}_d(\overline{\mathbb{F}_5})$ for some $d \leq 8$, it follows from [**KT5**, Theorem 4.14] that $w \leq 8$, a contradiction.

Suppose $S = \mathrm{Sp}_6(2)$. Then $D \leq \mathrm{meo}(\mathrm{Aut}(S)) = 15$, and so $D \leq 8$ since $V|_L$ is irreducible, see [**GAP**]. Thus (ii) holds in this case.

Suppose $S = \mathrm{PSp}_4(5)$, but $p \neq 5$. Since $V|_L$ is irreducible and $D \leq \mathrm{meo}(\mathrm{Aut}(S)) = 30$, we actually have $D = 12$ or $13$ and $G/\mathbf{Z}(G) = S$ by [**GAP**]. Since $S$ is an irreducible subgroup of $\mathrm{GL}_5(\overline{\mathbb{F}_5})$, it follows from [**KT5**, Theorem 4.14] that $w \leq 5$. Using [**GAP**] we can check that $|\varphi(x)| \leq 5$ for all $x \in Q \smallsetminus \mathbf{Z}(G)$. Thus we can take $\alpha = 5/12$, which implies $|Q| > w \geq 4$ by (3.1.10.2). Applying (3.1.10.2) with $|Q| \geq 5$, we actually have $w \geq 6$, a contradiction.

Next suppose $S = \Omega^+_8(2)$ and $D \geq 9$. As $D \leq \mathrm{meo}(\mathrm{Aut}(S)) = 30$, we have $D = 28$ since $V|_L$ is irreducible, see [**GAP**]. Now (3.1.10.1) implies that $\bar{\mathsf{o}}(g_0) = 30$, but such elements do not have simple spectrum on $V$, a contradiction.

(b) The last three cases of $\mathrm{PSp}_6(3)$, ${}^2B_2(8)$, and $G_2(3)$ require a more substantial analysis. Suppose $S = \mathrm{PSp}_6(3)$, but $p \neq 3$. Since $V|_L$ is irreducible and $D \leq \mathrm{meo}(\mathrm{Aut}(S)) = 40$, we actually have $D = 13$ or $14$ and $G/\mathbf{Z}(G) = S$ by [**GAP**]. For $p \neq 2$, we can check that $|\varphi(x)| \leq 2$ for all $x \in Q \smallsetminus \mathbf{Z}(G)$. Thus we can take $\alpha = 2/13$, which implies $w \geq 9$ by (3.1.10.2). Since the Sylow 5-subgroups and 7-subgroups of $S$ have order 5, respectively, this bound rules out the cases $p = 5$ and $7$ by (3.1.10.3). Assume $p = 13$. Then any $x \in Q \smallsetminus \mathbf{Z}(G)$ has central order 13 and spectrum $\beta \cdot \mu_{13}$ on $V$ for some $\beta \in \mathbb{C}^\times$. This implies that $w \geq 12$. Since Sylow 13-subgroups of $S$ have order 13, $Q$ is abelian, and so $w \neq 13$ by [**KRLT4**, Proposition 5.9] and $w \neq 14$ by (3.1.10.3). Thus $w = 12$, in which case $12|\bar{\mathsf{o}}(g_\infty)$ and $g_\infty$ has spectrum $\gamma \cdot \mu_{12}$ on $\mathsf{Wild}$ for some $\gamma \in \mathbb{C}^\times$ by [**KRLT4**, Proposition 5.8]. However, using [**GAP**] one can check that no such element exists in $G = \mathbf{Z}(G)L$.

We have shown that $p = 2$. Then the $2'$-element $g_0$ has simple spectrum on $V$. Using [**GAP**] we can check that $\bar{\mathsf{o}}(g_0) = 13 = D$, so $L = S$, and $G = \mathbf{Z}(G)S = \mathbf{Z}(G) \times S$. Also, $2 \nmid |\mathbf{Z}(G)|$ by [**KT5**, Proposition 4.8(iv)]. By [**KT5**, Corollary 5.2], we can replace $\mathcal{H}$ by another hypergeometric sheaf of the same type $(D, m)$ but now with $G = S$. So we may assume $G = S = \mathrm{PSp}_6(3)$; in particular, $|Q| \leq 2^9$. Checking the spectrum of $g_0$ on $V$, we see that the set of "upstairs" characters of $\mathcal{H}$ is $\mathsf{Char}(13)$. Using [**GAP**] we can check that $|\varphi(x)| \leq 5$ for all $1 \neq x \in Q$. Thus we can take $\alpha = 5/13$, which implies $|Q| > w \geq 4$ by (3.1.10.2). This in turn implies that $|Q| \geq 8$, and so $w \geq 7$ by (3.1.10.2). If $w = 13$, then $Q \cong 2^{12}$ by [**KRLT4**, Proposition 5.8], a contradiction. The case $w = 11$ is impossible since $g_\infty \in S$ would have order divisible by 11. If $w = 7$, then $Q \cong 2^3$ and each $1 \neq x \in Q$ has trace $-1$ on $\mathsf{Wild}$ by [**KRLT4**, Proposition 5.8]. It follows that these involutions $x$ have trace $m - 1 = 5$ on $V$, which is impossible by [**GAP**]. Suppose $w = 9$. Then $Q \cong 2^6$ by [**KRLT4**, Proposition 5.8], and consists of, say $A$ involutions of class $2a$ and $B$ involutions of class $2b$, in the notation of [**GAP**]. Then $A + B = 63$, and

$$4 = m = [\varphi|_Q, 1_Q]_Q = (13 - 3A + B)/64,$$

yielding $A = -45$, a contradiction.

Suppose $w = 10$. By [**KRLT4**, Proposition 5.9], $g_\infty \in S$ has order divisible by 5; in particular, $g^{15} = \mathrm{Id}$, and spectrum all the 5th roots of $\beta \cdot (\mu_3 \smallsetminus \{1\})$ on $\mathsf{Wild}$ for some $\beta \in \mathbb{C}^\times$. It follows that $\beta^3 = 1$, and $g_\infty^3$ has order 5 and spectrum all the 5th roots of unity on $\mathsf{Wild}$, each with multiplicity 2, which can be seen to be impossible by [**GAP**].

Suppose $w = 8$. By [**KRLT4**, Proposition 5.9], $g_\infty \in S$ has order divisible by 9; in particular, $g^9 = \mathrm{Id}$, and spectrum all the 9th roots of $\gamma \cdot (\mu_9 \smallsetminus \{1\})$ on $\mathsf{Wild}$ for some $\gamma \in \mathbb{C}^\times$. It follows that $\gamma^9 = 1$, and the spectrum of $g_\infty$ on $\mathsf{Wild}$ is $\mu_9 \smallsetminus \{\gamma\}$. On the other hand, since $G$ is finite, $g_\infty$ also has simple spectrum on $\mathsf{Tame}$. Checking the spectra of elements of order 9 of $S$ on $V$ and replacing $g_\infty$ by its inverse if necessary, we see that the spectrum of $g_\infty$ on $V$ is $\mu_9 \sqcup \{\zeta_9^j \mid j = 1, 4, 6, 7\}$ as a multi-set, and so the spectrum of $g_\infty$ on $\mathsf{Tame}$ is $\{\zeta_9^j \mid j = 1, 4, 6, 7, j_0\}$ for some $j_0 \in \{0, 2, 3, 5, 8\}$. The irreducibility of $\mathcal{H}$ implies $j_0 \neq 0$ (as $\mathbb{1}$ already appears "upstairs"), and $\mathbb{Q}(\varphi) = \mathbb{Q}(\zeta_3)$ implies that the spectrum of $g_\infty$ is stable under the unique subgroup $C_3$ of $\mathrm{Gal}(\mathbb{Q}(\zeta_9)/\mathbb{Q})$, whence $j_0 = 3$. Thus the set of "downstairs" characters of $\mathcal{H}$ is $\{\xi_9^j \mid j = 1, 3, 4, 6, 7\}$. However, the resulting $\mathcal{H}$ now fails the $V$-test, as can be shown by direct computation.

Suppose $w = 12$. By [**KRLT4**, Proposition 5.9], $g_\infty \in S$ has order divisible by 3 and spectrum all the 3rd roots of $\delta \cdot (\mu_5 \smallsetminus \{1\})$ on $\mathsf{Wild}$ for some $\delta \in \mathbb{C}^\times$. It follows that 5 divides $\mathsf{o}(g^3)$ and in fact $\mathsf{o}(g) = 15$. Checking the spectra of elements of order 15 of $S$ on $V$, we see that the spectrum of $g_\infty$ on $V$ contains 4 eigenvalues with multiplicity 2, which is a contradiction since $g_\infty$ has simple spectra on both $\mathsf{Wild}$ (of dimension 12) and $\mathsf{Tame}$ (of dimension 1).

(c) Suppose $S = {}^2B_2(8)$. Since $D \leq \mathrm{meo}(\mathrm{Aut}(S)) = 15$ and $V|_L$ is irreducible, we have $D = 14$ and $L = S$ by [**GAP**]. Now, (3.1.10.1) implies that $\bar{\mathsf{o}}(g_0) = 15$, ruling out $p = 3, 5$. The case $p = 13$ can indeed arise, see [**KRLT4**, Theorem 26.2], leading to possibility (iv). We can also rule out $p = 2$ as follows. Using [**GAP**] we can check that $|\varphi(x)| \leq 2$ for all 2-elements $x \in Q \smallsetminus \mathbf{Z}(G)$, and thus we can take $\alpha = 1/7$. Hence (3.1.10.2) yields $|Q| > w \geq 6$. Hence $|Q| \geq 8$, and (3.1.10.2) now implies $w \geq 11$. We also note by [**KT5**, Proposition 4.8(v)] that $|\mathbf{Z}(G)|_2 \leq 2$, and so $|Q| \leq 2^7$. The case $w = 11$ is now impossible by [**KRLT4**, Proposition 5.8], since no element in $\mathrm{Aut}(S)$ has order 11. If $w = 13$, then $|Q| = 2^{12}$ by [**KRLT4**, Proposition 5.8], again a contradiction. Suppose $w = 14$. Applying [**KRLT4**, Proposition 5.8] again, we see that $7|\bar{\mathsf{o}}(g_\infty)$, which implies that $g_\infty$ and $Q$ are both contained in $\mathbf{Z}(G)S$. In this case, $G = \mathbf{Z}(G)S$ by [**KT5**, Theorem 4.6]. But this is a contradiction, since $g_0 \notin \mathbf{Z}(G)S$. Finally, suppose $w = 12$. In this case, $Q$ has an irreducible summand of dimension 4 on $\mathsf{Wild}$ by [**KRLT4**, Proposition 5.8]. However, $Q \leq \mathbf{Z}(G)P$ for a Sylow 2-subgroup $P$ of $S$, and all irreducible characters of $P$ are of degree 1 or 2, again a contradiction.

(d) Finally, we consider $S = G_2(3)$. Since $D \leq \mathrm{meo}(\mathrm{Aut}(S)) = 18$ and $V|_L$ is irreducible, we have $D = 14$ and $L = S$ by [**GAP**]. Now, (3.1.10.1) implies that $\mathsf{o}(g_0) = 14$ or 18, ruling out $p = 2$. The case $p = 13$ can indeed arise, see [**KRLT4**, Theorem 23.2], leading to possibility (iv). If $p = 7$, then $\varphi(x) = 0$ for all $x \in Q \smallsetminus \mathbf{Z}(G)$, which implies $w \geq 12$ by (3.1.10.2). But this contradicts (3.1.10.3), since Sylow 7-subgroups of $\mathrm{Aut}(S)$ have order 7. Next we rule out $p = 3$ as follows. Using [**GAP**] we can check that $|\varphi(x)| \leq 5$ for all 3-elements $x \in Q \smallsetminus \mathbf{Z}(G)$, and thus we can take $\alpha = 5/14$. Hence (3.1.10.2) yields $|Q| > w \geq 6$. Hence $|Q| \geq 9$, and (3.1.10.2) now implies $w \geq 8$. We also note by [**KT5**, Proposition 4.8(iv)] that $3 \nmid |\mathbf{Z}(G)|$, and so $|Q| \leq 3^6$ and $Q \leq S$. The case $w = 10$, respectively 11, is impossible by [**KRLT4**, Proposition 5.8], since no element in $\mathrm{Aut}(S)$ has order 5 or 11. If $w = 14$, then $Q = 3^6$ is elementary abelian by [**KRLT4**, Proposition 5.8], again a contradiction (since Sylow 3-subgroups of $S$ have order $3^6$ but exponent 9). Suppose $w = 9$. Then $Q$ is irreducible on $\mathsf{Wild}$ by [**KRLT4**, Proposition 5.9]. Since $Q$ acts trivially on $\mathsf{Tame}$ (of dimension 5) and faithfully on $V$, an element $z \in \mathbf{Z}(Q)$ of order 3 will act as scalar $\zeta_3$ on $\mathsf{Wild}$ and thus $\varphi(z) = 9\zeta_3 + 5$, which is impossible by [**GAP**]. Suppose $w = 8$, respectively 13. Applying [**KRLT4**, Proposition 5.8] again, we see that $w|\mathsf{o}(g_\infty)$, which implies that $g_\infty$ and $Q$ are both contained in $\mathbf{Z}(G)S$. In this case, $G = \mathbf{Z}(G)S$ by [**KT5**, Theorem 4.6]. But this is a contradiction, since $g_0 \notin \mathbf{Z}(G)S$. Finally, suppose $w = 12$. As in the previous case, we have $g_\infty \notin \mathbf{Z}(G)S$. On the other hand, $4|\mathsf{o}(g_\infty)$ by [**KRLT4**, Proposition 5.9]. So, modulo $\mathbf{Z}(G)$, $g_\infty$ belongs to class $4b$ in the notation of [**GAP**], and has traces 0 on $\mathsf{Wild}$ and on $V$, whence on $\mathsf{Tame}$ as well. Since $\dim \mathsf{Tame} = 2$, it follows that the set $\{\rho_1, \rho_2\}$ of "downstairs" characters of $\mathcal{H}$ is stable under multiplication by the quadratic character $\xi_2$. As $p = 3$ and $\mathsf{o}(g_0) \geq D$, we also see that, modulo $\mathbf{Z}(G)$, $g_0$ belongs to class $14a$ in the notation of [**GAP**], and so has spectrum $\beta \cdot \mu_{14}$ on $V$, for some $\beta \in \mathbb{C}^\times$. It follows that the set $\{\chi_1, \ldots, \chi_{14}\}$ of "upstairs" characters of $\mathcal{H}$ is stable under multiplication by $\xi_2$, and so $\mathcal{H}$ is Kummer induced by [**KRLT4**, Proposition 3.7], a contradiction. □

Remark 3.1.11. In the case where $D \neq 4, 8, 9$, it is shown in Theorem 5.2.9 (below) that if $\mathcal{H}$ is primitive then it is $(\mathbf{S}+)$. Also, the construction of particular hypergeometric sheaves with $(p, D, S)$ as indicated in cases (iii)–(iv), and in various subcases of (ii), of Theorem 3.1.10, is carried out in [**KRLT4**]. Our proof of Theorem 3.1.10 also shows that, conversely, if $S = {}^2B_2(8)$ or $G_2(3)$, then $(D, p) = (14, 13)$.

## 3.2. Modules with small weight multiplicities

Let $\boldsymbol{G}$ be a simple, simply connected Lie group over $\mathbb{C}$, of rank $r$. With respect to a fixed maximal torus $\boldsymbol{T}$ in $\boldsymbol{G}$, let $\{\alpha_1, \alpha_2, \ldots, \alpha_r\}$ be a system of simple roots, $\{\varpi_1, \varpi_2, \ldots, \varpi_r\}$ be the corresponding fundamental weights, with the same labeling as given [**Hum**, §11.4]. For a dominant integral weight $\lambda \in \langle \varpi_1, \varpi_2, \ldots, \varpi_r \rangle_{\mathbb{Z}_{\geq 0}}$, let $L(\lambda)$ denote the irreducible rational $\mathbb{C}\boldsymbol{G}$-module with highest weight $\lambda$.

Definition 3.2.1. (i) In the above notation, $L(\lambda)$ is called *weight multiplicity-free*, or WMF, if the largest multiplicity of any weight in $L(\lambda)$ is at most 1. Similarly, $L(\lambda)$ is called WM2, respectively WM3, if the largest multiplicity of any weight in $L(\lambda)$ is at most 2, respectively 3.

(ii) A semisimple element $g \in \boldsymbol{G}$ is called WMF, respectively WM2, WM3, on $L(\lambda)$, if the largest multiplicity of any eigenvalue of $g$ on $L(\lambda)$ is at most 1, 2, or 3, respectively.

WMF modules were classified by Howe in [**HS**, Theorem 4.6.3]. In the cases where $\boldsymbol{G}$ admits a (nontrivial) graph automorphism $\tau$ of order 2, i.e. when $\boldsymbol{G}$ is of type $A_r$ with $r \geq 2$, $D_r$ with $r \geq 4$, and $E_6$, we need to extend Howe's result to deal with WM2 modules that are $\tau$-invariant. When $\boldsymbol{G}$ is of type $D_4$, we also need to classify WM3 modules.

In theory, the multiplicity $m_\lambda(\mu)$ of any weight $\mu$ in $L(\lambda)$ can be determined using Freudenthal's formula, or Kostant's formula, see [**Hum**]. Based on these formulas, algorithms are developed and implemented in various computer packages to compute $m_\lambda(\mu)$, see [**Lie**] in particular. However, it is highly nontrivial to deduce a closed, effective formula for all $m_\lambda(\mu)$. In practice, the following reduction formula turns out to be useful in many cases:

Proposition 3.2.2. [**Cav**, Proposition A] *Let $\lambda = \sum_{i=1}^r a_i\varpi_i$ be a dominant integral weight and let $\mu$ be a dominant weight such that $\mu = \lambda - \sum_{i=1}^r c_i\alpha_i$ with $c_1, \dots, c_r \in \mathbb{Z}_{\geq 0}$. Also, assume that $J$ is a subset $J$ of $\{1, \dots, r\}$ with the property that $c_j \leq a_j$ for all $j \in J$. Set $\lambda' := \lambda - \sum_{j\in J}(a_j - c_j)\varpi_j$ and $\mu' := \mu - \sum_{j\in J}(a_j - c_j)\varpi_j$. Then $m_\lambda(\mu) = m_{\lambda'}(\mu')$.*

First we treat type $A_3$:

Lemma 3.2.3. *Let $\boldsymbol{G}$ be of type $A_3$ and let $L(\lambda)$ be* WM2. *Then $\lambda$ is one of the following weights: $a\varpi_1$ or $a\varpi_3$ with $a \in \mathbb{Z}_{\geq 0}$, $a\varpi_2$ with $1 \leq a \leq 3$, $\varpi_1 + \varpi_2$, $\varpi_2 + \varpi_3$.*

Proof. Recall (see e.g.[**Hum**, Table 1, p. 69])

$$\varpi_1 = (3\alpha_1 + 2\alpha_2 + \alpha_3)/4,\ \varpi_2 = (2\alpha_1 + 4\alpha_2 + 2\alpha_3)/4,\ \varpi_3 = (\alpha_1 + 2\alpha_2 + 3\alpha_3)/4.$$

Write $\lambda = a\varpi_1+b\varpi_2+c\varpi_3$ also as $(a, b, c)$. We will also write $m_{x,y,z}(a, b, c)$ for the multiplicity of the weight $(x, y, z) = x\varpi_1 + y\varpi_2 + z\varpi_3$ in $L(a, b, c) = L(\lambda)$.

(i) First we consider the case $a, c \geq 1$ and let $\mu := \lambda - (\varpi_1 + \varpi_3) = (a - 1, b, c - 1)$. Note that $\varpi_1 + \varpi_3 = \alpha_1 + \alpha_2 + \alpha_3$. Assume $b \geq 1$. Then, by Proposition 3.2.2 we can take $J = \{1, 2, 3\}$ and get $m_\lambda(\mu) = m_{\lambda_1}(\mu_1)$ for

$$\lambda_1 = \lambda - (a - 1, b - 1, c - 1) = (1, 1, 1),\ \mu_1 = \mu - (a - 1, b - 1, c - 1) = (0, 1, 0).$$

Thus $m_\lambda(\mu) = m_{1,1,1}(0, 1, 0) = 4$, with the second equality checked using [**Lie**].

Assume now that $b = 0$. By Proposition 3.2.2 we can take $J = \{1, 3\}$ and get $m_\lambda(\mu) = m_{\lambda_2}(\mu_2)$ for

$$\lambda_2 = \lambda - (a - 1, 0, c - 1) = (1, 0, 1),\ \mu_2 = \mu - (a - 1, b - 1, c - 1) = (0, 0, 0).$$

Thus $m_\lambda(\mu) = m_{1,0,1}(0, 0, 0) = 3$ (with the second equality again checked using [**Lie**] – in what follows we will skip similar references to [**Lie**]).

(ii) We have shown that at least one of $a, c$ is 0, and may therefore assume $a = 0$. Assume in addition that $b \geq 2$ and $c \geq 1$, and take $\mu := \lambda - 2\varpi_2 = (0, b - 2, c)$, noting

$2\varpi_2 = \alpha_1 + 2\alpha_2 + \alpha_3$. By Proposition 3.2.2 we can take $J = \{2, 3\}$ and get $m_\lambda(\mu) = m_{\lambda_3}(\mu_3)$ for

$$\lambda_3 = \lambda - (0, b-2, c-1) = (0, 2, 1),\ \mu_3 = \mu - (0, b-2, c-1) = (0, 0, 1).$$

Thus $m_\lambda(\mu) = m_{0,2,1}(0, 0, 1) = 3$.

Suppose now that $b = 1$ but $c \geq 2$, and take $\mu := \lambda - (\varpi_2 + 2\varpi_3) = (0, 0, c-2)$. As $\varpi_2+2\varpi_3 = \alpha_1+2\alpha_2+2\alpha_3$, by Proposition 3.2.2 we can take $J = \{3\}$ and get $m_\lambda(\mu) = m_{\lambda_4}(\mu_4)$ for

$$\lambda_4 = \lambda - (0, 0, c-2) = (0, 1, 2),\ \mu_4 = \mu - (0, 0, c-2) = (0, 0, 0).$$

Thus $m_\lambda(\mu) = m_{0,1,2}(0, 0, 1) = 3$.

Finally, assume that $a = c = 0$ but $b \geq 4$, and take $\mu := \lambda - 4\varpi_2 = (0, b-4, 0)$. As $4\varpi_2 = 2\alpha_1 + 4\alpha_2 + 2\alpha_3$, by Proposition 3.2.2 we can take $J = \{2\}$ and get $m_\lambda(\mu) = m_{\lambda_5}(\mu_5)$ for

$$\lambda_4 = \lambda - (0, b-4, 0) = (0, 4, 0),\ \mu_4 = \mu - (0, b-4, 0) = (0, 0, 0).$$

Thus $m_\lambda(\mu) = m_{0,4,0}(0, 0, 0) = 3$. □

Recall we label the simple roots for type $D_4$ in such a way that a triality graph automorphism fixes $\alpha_2$ and permutes $\alpha_1$, $\alpha_3$, and $\alpha_4$.

LEMMA 3.2.4. *Let $\boldsymbol{G}$ be of type $D_4$ and let $L(\lambda)$ be* WM3. *Then $\lambda$ is one of the following weights: $a\varpi_i$ with $i \in \{1, 3, 4\}$ and $0 \leq a \leq 3$, $\varpi_1 + \varpi_3$, $\varpi_1 + \varpi_4$, $\varpi_3 + \varpi_4$. If moreover $L(\lambda)$ is* WM2*, then $\lambda \in \{0, \varpi_1, \varpi_3, \varpi_4\}$.*

PROOF. Recall (see e.g. [**Hum**, Table 1, p. 69])

$$\varpi_1 = (2\alpha_1 + 2\alpha_2 + \alpha_3 + \alpha_4)/2,\ \varpi_2 = \alpha_1 + 2\alpha_2 + \alpha_3 + \alpha_4,$$
$$\varpi_3 = (\alpha_1 + 2\alpha_2 + 2\alpha_3 + \alpha_4)/2,\ \varpi_4 = (\alpha_1 + 2\alpha_2 + \alpha_3 + 2\alpha_4)/2.$$

Write $\lambda = a\varpi_1 + b\varpi_2 + c\varpi_3 + d\varpi_4$ also as $(a, b, c, d)$. We will also write $m_{x,y,z,t}(a, b, c, d)$ for the multiplicity of the weight $(x, y, z, t) = x\varpi_1 + y\varpi_2 + z\varpi_3 + t\varpi_4$ in $L(a, b, c, d) = L(\lambda)$.

(i) First we consider the case $b \geq 1$ and let $\mu := \lambda - \varpi_2 = (a, b-1, c, d)$. Also set

$$a_1 := \min(a, 1),\ c_1 := \min(c, 1),\ d_1 = \min(d, 1),$$

so that

$$a = a_1 a,\ c = c_1 c,\ d = d_1 d,\ 0 \leq a_1, c_1, d_1 \leq 1. \tag{3.2.4.1}$$

Note that $\varpi_2 = \alpha_1 + 2\alpha_2 + \alpha_3 + \alpha_4$.

Assume in addition that $b \geq 2$. Then by Proposition 3.2.2 we can always put 2 in $J$. Moreover, we will put 1 in $J$ if and only if $a_1 = 1$, and similarly for 3 and 4. With this convention and using (3.2.4.1), we now have $m_\lambda(\mu) = m_{\lambda_1}(\mu_1)$ for

$$\lambda_1 = \lambda - (a_1(a-1), b-2, c_1(c-1), d_1(d-1)) = (a_1, 2, c_1, d_1),$$
$$\mu_1 = \mu - (a_1(a-1), b-2, c_1(c-1), d_1(d-1)) = (a_1, 1, c_1, d_1).$$

Thus $m_\lambda(\mu) = m_{a_1,2,c_1,d_1}(a_1, 1, c_1, d_1) \geq 5$, with the latter inequality checked using [**Lie**].

Assume now that $b = 1$. Then, we will put 1 in $J$ if and only if $a_1 = 1$, and similarly for 3 and 4. With this choice of $J$ and using Proposition 3.2.2 and (3.2.4.1), we now have $m_\lambda(\mu) = m_{\lambda_2}(\mu_2)$ for

$$\lambda_2 = \lambda - (a_1(a-1), 0, c_1(c-1), d_1(d-1)) = (a_1, 1, c_1, d_1),$$
$$\mu_2 = \mu - (a_1(a-1), 0, c_1(c-1), d_1(d-1)) = (a_1, 0, c_1, d_1).$$

Thus $m_\lambda(\mu) = m_{a_1,1,c_1,d_1}(a_1, 0, c_1, d_1) \geq 4$, with the latter inequality checked using [**Lie**] again.

(ii) We have shown that $b = 0$. Assume in addition that $a \geq 4$ and let $\mu := \lambda - 4\varpi_1 = (a-4, 0, c, d)$. Also set

$$c_2 := \min(c, 2),\ d_2 := \min(d, 2),$$

and choose $\gamma, \delta \in \{0, 1\}$ so that $\gamma = 1$ if and only $c \geq 2$ and $\delta = 1$ if and only $d \geq 2$. Note that $4\varpi_2 = 4\alpha_1 + 4\alpha_2 + 2\alpha_3 + 2\alpha_4$. We will put 1 in $J$. In addition, we will put 3 in $J$ if and only if $c_2 = 2$ (i.e. $\gamma = 1$) and similarly for 4. With this choice of $J$ and using Proposition 3.2.2, we now have $m_\lambda(\mu) = m_{\lambda_3}(\mu_3)$ for

$$\lambda_3 = \lambda - (a-4, 0, \gamma_2(c-2), \delta_2(d-2)) = (4, 0, c_2, d_2),$$
$$\mu_1 = \mu - (a-4, 0, \gamma_2(c-2), \delta_2(d-2)) = (0, 0, c_2, d_2).$$

Thus $m_\lambda(\mu) = m_{4,0,c_2,d_2}(0, 0, c_2, d_2)$. Using [**Lie**], we can check that $m_{4,0,c_2,d_2}(0, 0, c_2, d_2) \geq 6$ for $0 \leq c_2, d_2 \leq 2$.

We have therefore shown that $0 \leq a, c, d \leq 3$ and $b = 0$. A direct check using [**Lie**] shows that, if $\lambda$ is one of these 64 weights, but not listed in the lemma's first statement, then $L(\lambda)$ has some weight multiplicity $\geq 6$. The second statement is then checked using [**Lie**]. □

LEMMA 3.2.5. *Let* $\boldsymbol{G}$ *be of type* $A_2$ *or* $A_4$*, with graph automorphism* $\tau$*, and let* $L(\lambda)$ *be* WM2 *and* $\tau$*-invariant. Then either* $\lambda = 0$*, or* $\boldsymbol{G}$ *is of type* $A_2$ *and* $\lambda = \varpi_1 + \varpi_2$.

PROOF. (i) First we consider the case of $A_4$. Using [**Hum**, Table 1, p. 69] one can see that

$$\varpi_1 + \varpi_4 = \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4,\ \varpi_2 + \varpi_3 = \alpha_1 + 2\alpha_2 + 2\alpha_3 + \alpha_4. \tag{3.2.5.1}$$

Since $\tau$ interchanges $\varpi_1$ with $\varpi_4$ and $\varpi_2$ with $\varpi_3$, we can write $\lambda = a(\varpi_1 + \varpi_4) + b(\varpi_2 + \varpi_3)$; abbreviate it as $(a, b)$. We will also write $m_{x,y}(a, b)$ for the multiplicity of the weight $(x, y) = x(\varpi_1 + \varpi_4) + y(\varpi_2 + \varpi_3)$ in $L(a, b) = L(\lambda)$.

First we consider the case $a \geq 1$ and let $\mu := \lambda - (\varpi_1 + \varpi_4) = (a-1, b)$; also set $b_1 := \min(b, 1)$. By Proposition 3.2.2 we can always put 1 and 4 in $J$. Moreover, we will put both 2 and 3 in $J$ if $b_1 = 1$, and none of them if $b_1 = 0$. With this choice of $J$ and using Proposition 3.2.2, we now have $m_\lambda(\mu) = m_{\lambda_1}(\mu_1)$ for

$$\lambda_1 = \lambda - (a-1, b_1(b-1)) = (1, b_1),\ \mu_1 = \mu - (a-1, b_1(b-1)) = (0, b_1)$$

Thus $m_\lambda(\mu) = m_{1,b_1}(0, b_1) \geq 4$, with the latter inequality checked using [**Lie**].

We have shown that $a = 0$. Assume now that $b \geq 2$, and let $\mu := \lambda - (\varpi_2 + \varpi_3) = (0, b-1)$. By (3.2.5.1) and Proposition 3.2.2, we can choose $J = \{2, 3\}$ and obtain $m_\lambda(\mu) = m_{\lambda_2}(\mu_2)$ for

$$\lambda_2 = \lambda - (0, b-2) = (0, 2),\ \mu_2 = \mu - (0, b-2) = (0, 1).$$

Thus $m_\lambda(\mu) = m_{0,2}(0, 1) = 7$, with the latter equality checked using [**Lie**].

Finally, $m_{0,1}(0,0) = 5$, and the statement follows.

(ii) For $A_2$, an analogous argument shows that $m_{a(\varpi_1+\varpi_2)}((a-2)(\varpi_1+\varpi_2) = m_{2(\varpi_1+\varpi_2)}(0) = 3$ when $a \geq 2$. □

Lemma 3.2.6. *Let $\boldsymbol{G}$ be of type $A_5$, with graph automorphism $\tau$, and let $L(\lambda)$ be* WM2 *and $\tau$-invariant. Then $\lambda = 0$ or $\lambda = \varpi_3$ (and corresponds to the middle node of the Dynkin diagram).*

Proof. Using [**Hum**, Table 1, p. 69] one can see that

$$\begin{aligned} \varpi_1 + \varpi_5 &= \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 + \alpha_5, \\ \varpi_2 + \varpi_4 &= \alpha_1 + 2\alpha_2 + 2\alpha_3 + 2\alpha_4 + \alpha_5, \\ 2\varpi_3 &= \alpha_1 + 2\alpha_2 + 3\alpha_3 + 2\alpha_4 + \alpha_5. \end{aligned} \tag{3.2.6.1}$$

Since $\tau$ interchanges $\varpi_1$ with $\varpi_5$ and $\varpi_2$ with $\varpi_4$, we can write $\lambda = a(\varpi_1 + \varpi_5) + b(\varpi_2 + \varpi_4) + c\varpi_3$; abbreviate it as $(a, b, c)$. We will also write $m_{x,y,z}(a, b, c)$ for the multiplicity of the weight $(x, y, z) = x(\varpi_1 + \varpi_5) + y(\varpi_2 + \varpi_4) + z\varpi_3$ in $L(a, b, c) = L(\lambda)$.

First we consider the case $a \geq 1$ and let $\mu := \lambda - (\varpi_1 + \varpi_5) = (a - 1, b, c)$. Also set $b_1 := \min(b, 1)$ and $c_1 := \min(c, 1)$. By Proposition 3.2.2 we can always put 1 and 5 in $J$. Moreover, we will put both 2 and 4 in $J$ if $b_1 = 1$, and none of them if $b_1 = 0$, and similarly for 3. With this choice of $J$ and using Proposition 3.2.2, we now have $m_\lambda(\mu) = m_{\lambda_1}(\mu_1)$ for

$$\begin{aligned} \lambda_1 &= \lambda - (a - 1, b_1(b - 1), c_1(c - 1)) = (1, b_1, c_1), \\ \mu_1 &= \mu - (a - 1, b_1(b - 1), c_1(c - 1)) = (0, b_1, c_1). \end{aligned}$$

Thus $m_\lambda(\mu) = m_{1,b_1,c_1}(0, b_1, c_1) \geq 5$, with the latter inequality checked using [**Lie**].

We have shown that $a = 0$. Assume now that $b \geq 1$, and let

$$\mu := \lambda - (\varpi_2 + \varpi_4 - \varpi_1 - \varpi_5) = (1, b - 1, c).$$

Note from (3.2.6.1) that $\varpi_2 + \varpi_4 - \varpi_1 - \varpi_5 = \alpha_2 + \alpha_3 + \alpha_4$. Hence, by Proposition 3.2.2 we can always put 2 and 4 in $J$. Moreover, we will put 3 in $J$ if and only if $c_1 = 1$, but none of $1, 5$. With this choice of $J$ and using Proposition 3.2.2, we now have $m_\lambda(\mu) = m_{\lambda_2}(\mu_2)$ for

$$\lambda_2 = \lambda - (0, b - 1, c_1(c - 1)) = (0, 1, c_1),\ \mu_2 = \mu - (0, b - 1, c_1(c - 1)) = (1, 0, c_1).$$

Thus $m_\lambda(\mu) = m_{0,1,c_1}(1, 0, c_1) \geq 3$, with the latter inequality checked using [**Lie**].

We have therefore shown that $a = b = 0$. Assume now that $c \geq 3$, and let $\mu := \lambda - 2\varpi_3 = (0, 0, c - 2)$. Using Proposition 3.2.2 with $J = \{3\}$, we now have $m_\lambda(\mu) = m_{\lambda_3}(\mu_3)$ for

$$\lambda_3 = \lambda - (0, 0, c - 3) = (0, 0, 3),\ \mu_3 = \mu - (0, 0, c - 3) = (0, 0, 1).$$

Thus $m_\lambda(\mu) = m_{0,0,3}(0, 0, 1) = 6$. Finally, $m_{0,0,2}(0, 0, 0) = 5$, and the statement follows. □

Proposition 3.2.7. *Let $\boldsymbol{G}$ be of type $E_6$, with graph automorphism $\tau$, and let $L(\lambda)$ be* WM2 *and $\tau$-invariant. Then $\lambda = 0$.*

Proof. In the chosen labeling, $\tau$ interchanges $\varpi_1$ with $\varpi_6$, $\varpi_3$ with $\varpi_5$, and fixes $\varpi_2$ and $\varpi_4$. Hence we can write $\lambda = a(\varpi_1 + \varpi_6) + b(\varpi_3 + \varpi_5) + c\varpi_2 + d\varpi_4$; abbreviate it as $(a, b, c, d)$. We will also write $m_{x,y,z,t}(a, b, c, d)$ for the multiplicity of the weight

$$(x, y, z, t) = x(\varpi_1 + \varpi_6) + y(\varpi_3 + \varpi_5) + z\varpi_2 + d\varpi_4$$

in $L(a,b,c,d) = L(\lambda)$.

Note that there is a positive root $\alpha_0$ such that $\{-\alpha_0, \alpha_1, \dots, \alpha_6\}$ is the set of vertices for the extended Dynkin diagram $E_6^{(1)}$; moreover, $\alpha_0$ is connected only to $\alpha_2$ in this diagram. Consider the subsystem subgroup

$$\boldsymbol{H} := \langle X_{\alpha_i}, X_{-\alpha_i} \mid 0 \le i \le 6,\ i \ne 2 \rangle,$$

where as usual $X_\beta$ is the root subgroup corresponding to the root $\beta$. Then $\boldsymbol{H}$ is the direct product $\boldsymbol{H}_0 \times \boldsymbol{H}_1$ of semisimple subgroups $\boldsymbol{H}_0$ of type $A_1$ with simple root system $\{\alpha_0\}$, and $\boldsymbol{H}_1$ with simple root system $A_5$, and $\tau$ induces a graph automorphism of $\boldsymbol{H}_1$. We can choose a maximal torus $\boldsymbol{T} = \boldsymbol{T}_0 \times \boldsymbol{T}_1$, where $\boldsymbol{T}_0$ is a maximal torus in $\boldsymbol{H}_0$ and $\boldsymbol{T}_1$ is a maximal torus in $\boldsymbol{H}_1$. Then, without loss of generality, we may identify the set of fundamental weights of $\boldsymbol{H}_1$ with $\{\varpi_i \mid 1 \le i \le 6,\ i \ne 2\}$. As shown in [**GLT**, Lemma 4.1], the restriction of $L(\lambda)$ to $\boldsymbol{H}$ contains a simple subquotient $U_0 \otimes U_1$, where $U_0$ is a simple $\mathcal{H}_0$-module, and $U_1$ is the simple $\mathcal{H}_1$-module with highest weight $a(\varpi_1 + \varpi_6) + b(\varpi_3 + \varpi_5) + d\varpi_4$, which is $\tau$-invariant. Now, since the $\boldsymbol{T}$-module $L(\lambda)$ is $\mathsf{WM2}$, the same holds for $U_0 \otimes U_1$, and so for the $\boldsymbol{T}_1$-module $U_1$ as well. Applying Lemma 3.2.6, we obtain that $a = b = 0$ and $d \in \{0,1\}$.

Using [**Hum**, Table 1, p. 69] one can see that

$$\begin{aligned} \varpi_1 + \varpi_6 &= 2\alpha_1 + 2\alpha_2 + 3\alpha_3 + 4\alpha_4 + 3\alpha_5 + 2\alpha_6, \\ \varpi_2 &= \alpha_1 + 2\alpha_2 + 2\alpha_3 + 3\alpha_4 + 2\alpha_5 + \alpha_6, \\ \varpi_4 &= 2\alpha_1 + 3\alpha_2 + 4\alpha_3 + 6\alpha_4 + 4\alpha_5 + 2\alpha_6. \end{aligned} \tag{3.2.7.1}$$

Consider the case $d = 1$ but $c \ge 1$, and let $\mu := \lambda - (\varpi_4 - \varpi_1 - \varpi_6) = (1,0,c,0)$. Applying Proposition 3.2.2 with $J = \{2\}$, we have $m_\lambda(\mu) = m_{\lambda_1}(\mu_1)$ for

$$\lambda_1 = \lambda - (0,0,c-1,0) = (0,0,1,1),\ \mu_1 = \mu - (0,0,c-1,0) = (1,0,1,0).$$

Thus $m_\lambda(\mu) = m_{0,0,1,1}(1,0,1,0) = 6$, with the latter equality checked using [**Lie**].

Since $m_{0,0,0,1}(1,0,0,0) = 4$, we have shown that $d = 0$. Assume now that $c \ge 2$, and let $\mu := \lambda - (2\varpi_2 - \varpi_1 - \varpi_6) = (1,0,c-2,0)$. Again applying Proposition 3.2.2 with $J = \{2\}$, we have $m_\lambda(\mu) = m_{\lambda_2}(\mu_2)$ for

$$\lambda_2 = \lambda - (0,0,c-2,0) = (0,0,2,0),\ \mu_2 = \mu - (0,0,c-2,0) = (1,0,0,0).$$

Thus $m_\lambda(\mu) = m_{0,0,2,0}(1,0,0,0) = 3$, with the latter equality checked using [**Lie**]. Also, by [**Lie**] we have $m_{0,0,1,0}(0,0,0,0) = 6$, whence the statement follows. □

Recall we label the simple roots for type $D_r$ with $r \ge 5$ in such a way that the graph automorphism $\tau$ interchanges $\alpha_{r-1}$ and $\alpha_r$, and fixes every other simple root $\alpha_i$, $1 \le i \le r-2$.

Lemma 3.2.8. *Let $\boldsymbol{G}$ be of type $D_5$ and let $L(\lambda)$ be $\tau$-invariant. Suppose $\boldsymbol{G}$ contains a semisimple element $g$, whose image in $\mathrm{SO}_{10}(\mathbb{C})$ has an eigenvalue equal to $1$, such that $g$ is $\mathsf{WM2}$ on $L(\lambda)$. Then $\lambda = 0$ or $\varpi_1$.*

Proof. (i) Write $\lambda = a\varpi_1 + b\varpi_2 + c\varpi_3 + d\varpi_4 + e\varpi_5$. Since $\lambda$ is $\tau$-invariant, we have that $d = e$. It is well known, see e.g. [**Lu**, Appendix A.2] that $\mathbf{Z}(\boldsymbol{G}) = \langle \boldsymbol{z} \rangle \cong C_4$, with $\varpi_4(\boldsymbol{z}) = \zeta_4 = \varpi_5(\boldsymbol{z})^{-1}$ and $\varpi_i(\boldsymbol{z}^2) = 1$ when $1 \le i \le 3$; in particular, $\lambda(\boldsymbol{z}^2) = 1$. Next, any simple root takes value $\pm 1$ on $\boldsymbol{z}$, (see e.g. [**Hum**, Table 1, p. 59]), and any weight of $L(\lambda)$ is $\lambda - \sum_{i=1}^{5} b_i\alpha_i$ with $b_i \in \mathbb{Z}_{\ge 0}$, (see e.g. [**Lu**, Theorem 2.1]). Hence, any weight of $L(\lambda)$ takes value 1 on $\boldsymbol{z}^2$, and so, without loss, we may replace $\boldsymbol{G} = \mathrm{Spin}_{10}(\mathbb{C})$ by $\mathrm{Spin}_{10}(\mathbb{C})/\langle \boldsymbol{z}^2\rangle = \mathrm{SO}_{10}(\mathbb{C}) = \mathrm{SO}(V)$ with $V = \mathbb{C}^{10}$.

(ii) Let $(e_1, e_2, \ldots, e_5, f_1, f_2, \ldots, f_5)$ be a hyperbolic basis for the $\boldsymbol{G}$-invariant bilinear form on $V$. By assumption, we may assume that

$$g = \mathrm{diag}(x_1, x_2, x_3, x_4, 1, x_1^{-1}, x_2^{-1}, x_3^{-1}, x_4^{-1}, 1) \tag{3.2.8.1}$$

with $x_i \in \mathbb{C}^\times$ in this basis. In particular, $g$ belongs to a Levi subgroup $\boldsymbol{L}_2 \cong \mathrm{SO}_6(\mathbb{C}) \times \mathrm{GL}_2(\mathbb{C})$ of the parabolic subgroup $\boldsymbol{P}_2 := \mathrm{Stab}_{\boldsymbol{G}}(\langle e_4, e_5\rangle_{\mathbb{C}})$ of $\boldsymbol{G}$. We also choose the maximal torus

$$\boldsymbol{T} = \big\{\mathrm{diag}(y_1, y_2, y_3, y_4, y_5, y_1^{-1}, y_2^{-1}, y_3^{-1}, y_4^{-1}, y_5^{-1}) \mid y_i \in \mathbb{C}^\times\big\}.$$

By Smith's theorem [**Sm**], $L(\lambda)|_{\mathcal{L}_2}$ contains a simple submodule $U_1 \otimes U_0$, where the $\mathrm{SO}_6(\mathbb{C})$-module $U_1$ has highest weight $d\varpi'_1 + c\varpi'_2 + d\varpi'_3$, with $\{\varpi'_1, \varpi'_2, \varpi'_3\}$ being the set of fundamental weights of $\mathrm{SL}_4(\mathbb{C})$ (a double cover of $\mathrm{SO}_6(\mathbb{C})$). In particular, $U_1$, viewed as an $\mathrm{SL}_4(\mathbb{C})$-module, is invariant under the graph automorphism of $\mathrm{SL}_4(\mathbb{C})$. Writing $g = g_2h_2$ with $g_2 := \mathrm{diag}(x_4, 1, x_4^{-1}, 1) \in \mathrm{GL}_2(\mathbb{C})$ and $h_2 := \mathrm{diag}(x_1, x_2, x_3, x_1^{-1}, x_2^{-1}, x_3^{-1}) \in \mathrm{SO}_6(\mathbb{C})$, and using the assumption that $g$ is $\mathsf{WM2}$ on $L(\lambda)$, we see that $h_2$ is $\mathsf{WM2}$ on $U_1$. This in turn implies that $U_1$ is $\mathsf{WM2}$, whence

$$d = e = 0 \text{ and } 0 \le c \le 3 \tag{3.2.8.2}$$

by Lemma 3.2.3.

(iii) Note that $g$ also belong to a Levi subgroup $\boldsymbol{L}_5 \cong \mathrm{GL}_5(\mathbb{C})$ of the parabolic subgroup $\boldsymbol{P}_5 := \mathrm{Stab}_{\boldsymbol{G}}(W)$ of $\boldsymbol{G}$, where $W := \langle e_1, e_2, \ldots, e_5\rangle_{\mathbb{C}}$. Next we claim that every composition factor $X$ of the restriction of $L(\lambda)$ to any standard subgroup $\boldsymbol{H} \cong \mathrm{SL}_4(\mathbb{C})$ of $\boldsymbol{L}_5$ is $\mathsf{WM2}$. (Here, by an $\mathrm{SL}_4(\mathbb{C})$ *standard subgroup* of $\mathrm{GL}_5(\mathbb{C}) = \mathrm{GL}(W)$ we mean any subgroup of $\mathrm{GL}(W)$ that is isomorphic to $\mathrm{SL}_4(\mathbb{C})$, fixes $w$ and stabilizes $W'$ for some decomposition $W = \langle w\rangle \oplus W'$ with $0 \neq w \in W$.) Indeed, we may assume that the element $g$ in (3.2.8.1) is represented by $\mathrm{diag}(x_1, x_2, x_3, x_4, 1)$ in $\mathrm{GL}(W)$, and take the standard subgroup $\mathcal{H}$ to fix $e_5$ and stabilize $\langle e_1, e_2, e_3, e_4\rangle_{\mathbb{C}}$. Consider any composition factor $Y$ of the restriction of $L(\lambda)$ to $\boldsymbol{L}_5$ and any composition factor $X$ of the restriction of $Y$ to $\boldsymbol{H}$. Also, fix $z \in \mathbb{C}^\times$ such that $z^{20} = x_1x_2x_3x_4$, and inside $\mathcal{L}_5$ we write $g = \mathrm{diag}(x_1, x_2, x_3, x_4, 1) = h_5h'_5g_5$, where

$$h_5 := z^4{\cdot}\mathrm{Id} \in \mathbf{Z}(\mathcal{L}_5),\ h'_5 := \mathrm{diag}(z, z, z, z, z^{-4}),\ g_5 := \mathrm{diag}(x_1z^{-5}, x_2z^{-5}, x_3z^{-5}, x_4z^{-5}, 1) \in \boldsymbol{H}.$$

Then $h_5$ acts as a scalar on $Y$. Furthermore, $h'_5$ centralizes $\boldsymbol{H}$, with

$$\boldsymbol{H} * \langle h'_5\rangle = \mathrm{Stab}_{\mathrm{SL}(W)}(\langle e_5\rangle_{\mathbb{C}}, \langle e_1, e_2, e_3, e_4\rangle_{\mathbb{C}}) \cong \mathrm{GL}_4(\mathbb{C}).$$

So without loss we may assume $X$ is $h'_5$-invariant and so $h'_5$ acts as a scalar on $X$. As $g = h_5h'_5g_5$ is $\mathsf{WM2}$ on $L(\lambda)$ and $h_5h'_5$ is scalar on $X$, $g_5$ is $\mathsf{WM2}$ on $X$, whence $X$ is $\mathsf{WM2}$ as claimed.

(iv) By Smith's theorem [**Sm**], the restriction of $L(\lambda)$ to $[\boldsymbol{L}_5, \boldsymbol{L}_5] \cong \mathrm{SL}_5(\mathbb{C})$ contains a direct summand which is simple of highest weight $a\omega_1 + b\omega_2 + c\omega_3 + d\omega_4$, with $\{\omega_1, \omega_2, \omega_3, \omega_4\}$ being the set of fundamental weights of $\mathrm{SL}_5(\mathbb{C})$. Similarly, the restriction of the latter to the standard subgroup $\boldsymbol{H}$ that fixes $e_5$ and stabilizes $\langle e_1, e_2, e_3, e_4\rangle_{\mathbb{C}}$ contains a direct summand $X$ which is simple with highest weight $a\omega'_1 + b\omega'_2 + c\omega'_3$, with $\{\omega'_1, \omega'_2, \omega'_3\}$ being the set of fundamental weights of $\mathrm{SL}_4(\mathbb{C})$. Applying (iii) to $X$ and using Lemma 3.2.3, we see that one of the following occurs:

- $a = b = 0$, $1 \le c \le 3$;
- $a = 0$, $b = c = 1$;
- $b = c = 0$, $0 \le a \le 3$;
- $a = b = 1$, $c = 0$; or
- $a = c = 0$, $1 \le b \le 3$.

Recall $d = e = 0$ by (3.2.8.2). Now using [**Lie**] we can check that in the 12 listed above cases, there is some $\mu$ such that $m_\lambda(\mu) \ge 4$, unless $\lambda = 0$ or $\varpi_1$. □

PROPOSITION 3.2.9. *Let $\boldsymbol{G}$ be of type $D_r$ with $r \ge 5$ and let $L(\lambda)$ be $\tau$-invariant. Suppose $\boldsymbol{G}$ contains a semisimple element $g$, whose image in $\mathrm{SO}_{2r}(\mathbb{C})$ has an eigenvalue equal to* 1, *such that $g$ is* WM2 *on $L(\lambda)$. Then $\lambda = 0$ or $\varpi_1$.*

PROOF. (i) We proceed by induction, with induction base $r = 5$ proved in Lemma 3.2.8. For the induction step $r \ge 6$, since $\lambda = \sum_{i=1}^r a_i\varpi_i$ is $\tau$-invariant, $a_{r-1} = a_r$. If $2 \nmid r$, then the same arguments as in part (i) of the proof of Lemma 3.2.8 shows that $\mathbf{Z}(\boldsymbol{G}) = \langle \boldsymbol{z} \rangle \cong C_4$ with $\boldsymbol{z}^2$ acting trivially on $L(\lambda)$. Suppose $2|r$. Then $\mathbf{Z} = \langle \boldsymbol{z}_1, \boldsymbol{z}_2 \rangle \cong C_2^2$ with $\boldsymbol{G}/\langle \boldsymbol{z}_1\boldsymbol{z}_2 \rangle \cong \mathrm{SO}_{2r}(\mathbb{C})$. Now we can check using [**Lu**, Appendix A.2] that each of $\varpi_{r-1}\varpi_r$ and $\varpi_i$, $1 \le i \le r-2$, takes value 1 at $\boldsymbol{z}_1\boldsymbol{z}_2$. Arguing as in the proof of Lemma 3.2.8, we again see that $\boldsymbol{z}_1\boldsymbol{z}_2$ acts trivially on $L(\lambda)$.

Thus, regardless of the parity of $r$, we may replace $\boldsymbol{G}$ by $\mathrm{SO}_{2r}(\mathbb{C})$. Let $(e_1, e_2, \ldots, e_r, f_1, f_2, \ldots, f_r)$ be a hyperbolic basis for the $\boldsymbol{G}$-invariant bilinear form on $\mathbb{C}^{2r}$. By assumption, we may assume that

$$g = \mathrm{diag}(x_1, x_2, \ldots, x_{r-1}, 1, x_1^{-1}, x_2^{-1}, \ldots, x_{r-1}^{-1}, 1) \tag{3.2.9.1}$$

with $x_i \in \mathbb{C}^\times$ in this basis. In particular, $g$ belongs to a Levi subgroup $\boldsymbol{L} \cong \mathrm{SO}_{2r-2}(\mathbb{C}) \times \mathrm{GL}_1(\mathbb{C})$ of the parabolic subgroup $\boldsymbol{P} := \mathrm{Stab}_{\boldsymbol{G}}(\langle e_1 \rangle_\mathbb{C})$ of $\boldsymbol{G}$. We also choose the maximal torus

$$\boldsymbol{T} = \left\{ \mathrm{diag}(y_1, y_2, \ldots, y_r, y_1^{-1}, y_2^{-1}, \ldots, y_r^{-1}) \mid y_i \in \mathbb{C}^\times \right\}.$$

By Smith's theorem [**Sm**], $L(\lambda)|_{\mathcal{L}}$ contains a simple submodule $U$, where the $\mathrm{SO}_{2r-2}(\mathbb{C})$-module $U$ has highest weight $\sum_{i=2}^r a_i\varpi'_{i-1}$, with $\{\varpi'_1, \varpi'_2, \ldots, \varpi'_{r-1}\}$ being the set of fundamental weights of $\mathrm{Spin}_{2r-2}(\mathbb{C})$. In particular, $U$ is invariant under the graph automorphism of $\mathrm{SO}_{2r-2}(\mathbb{C})$. We can also write the element $g$ in (3.2.9.1) as $g = hg'$, with

$$h := \mathrm{diag}(x_1, 1, \ldots, 1, x_1^{-1}, 1, \ldots, 1) \in \mathrm{GL}_1(\mathbb{C}) \le \mathbf{Z}(\boldsymbol{L})$$

and

$$g' := \mathrm{diag}(1, x_2, \ldots, x_{r-1}, 1, 1, x_2^{-1}, \ldots, x_{r-1}^{-1}, 1) \in \mathrm{SO}_{2r-2}(\mathbb{C}).$$

In particular, as an element of $\mathrm{SO}_{2r-2}(\mathbb{C})$, $g'$ has eigenvalue 1 on $\mathbb{C}^{2r-2}$. Furthermore, $h$ acts as a scalar on $U$. Hence, since $g$ is WM2 on $L(\lambda)$, $g'$ is WM2 on $U$. By the induction hypothesis,

$$a_3 = a_4 = \ldots = a_r = 0,\ 0 \le a_2 \le 1.$$

(ii) Consider the case $a_2 = 1$. First we note, see [**OV**, Table 5] that $L(\varpi_2) = \wedge^2(V)$ for $V := L(\varpi_1) = \mathbb{C}^{2r}$, and it is easy to see that $m_{\varpi_2}(0) = r \ge 6$.

So we may assume that $a_1 \ge 1$, and let $\mu := \lambda - \varpi_2 = a_1\varpi_1$. Note that

$$\varpi_2 = \alpha_1 + 2\sum_{i=2}^{r-2} \alpha_i + \alpha_{r-1} + \alpha_r,$$

see [**Hum**, Table 1, p. 69]. Hence, applying Proposition 3.2.2 with $J = \{1\}$, we obtain that

$$m_\lambda(\mu) = m_{\varpi_1+\varpi_2}(\varpi_1).$$

Again by [**OV**, Table 5],

$$V \otimes \wedge^2(V) = \wedge^3(V) \oplus V \oplus L(\varpi_1 + \varpi_2).$$

Analyzing the action of $\boldsymbol{T}$ on these modules, we see that $\varpi_1$ has multiplicity 1 in $V$, $r-1$ in $\wedge^3(V)$, and $3r-2$ in $V \otimes \wedge^2(V)$. Thus $m_\lambda(\mu) = m_{\varpi_1+\varpi_2}(\varpi_1) = 2(r-1) \geq 10$.

(iii) Now we consider the case $a_2 = 0$ but $a_1 \geq 2$, and let $\mu := \lambda - 2\varpi_1 = (a_1-2)\varpi_1$. Note that

$$2\varpi_2 = 2\sum_{i=1}^{r-2} \alpha_i + \alpha_{r-1} + \alpha_r,$$

see [**Hum**, Table 1, p. 69]. Applying Proposition 3.2.2 with $J = \{1\}$, we obtain that $m_\lambda(\mu) = m_{2\varpi_1}(0)$. Again by [**OV**, Table 5],

$$\mathrm{Sym}^2(V) = \mathbb{C} \oplus L(2\varpi_1).$$

Analyzing the action of $\boldsymbol{T}$ on these modules, we see that 0 has multiplicity 1 in $\mathbb{C}$ and $r$ in $\mathrm{Sym}^2(V)$. Thus $m_\lambda(\mu) = m_{2\varpi_1}(0) = r-1 \geq 5$. □

PROPOSITION 3.2.10. *Let $\boldsymbol{G} = \mathrm{SL}_{r+1}$ with $r \geq 4$ and let $L(\lambda)$ be $\tau$-invariant. Write $r+1 = 2m+j$ with $j \in \{0,1\}$. Suppose $\boldsymbol{G}$ contains a semisimple element*

$$g = \mathrm{diag}\big(t_1, t_2, \ldots, t_m, \underbrace{1}_{j \text{ times}}, t_m^{-1}, t_{m-1}^{-1}, \ldots, t_1^{-1}\big)$$

*with $t_i \in \mathbb{C}^\times$ such that $g$ is* WM2 *on $L(\lambda)$. Then $\lambda = 0$, or $r = 5$ and $\lambda = \varpi_3$.*

PROOF. We proceed by induction on $r \geq 4$. The induction base $r = 4, 5$ is already established in Lemma 3.2.5 and Lemma 3.2.6.

For the induction step $r \geq 6$, assume $\lambda \neq 0$. Let $W = \langle e_1, e_2, \ldots, e_{r+1}\rangle_{\mathbb{C}}$, so that $\boldsymbol{G} = \mathrm{SL}(W)$. We can extend $L(\lambda)$ to a $\mathrm{GL}(W)$-module $V$, and write

(3.2.10.1)
$$g = \mathrm{diag}(t_1, h, t_1^{-1}), \text{ with } h := \mathrm{diag}\big(t_2, t_3, \ldots, t_m, \underbrace{1}_{j \text{ times}}, t_m^{-1}, t_{m-1}^{-1}, \ldots, t_2^{-1}, 1\big) \in \mathrm{SL}_{r-1}.$$

Note that $g$ belongs to the Levi subgroup $\boldsymbol{L} = \mathrm{GL}_1 \times \mathrm{GL}_{r-1} \times \mathrm{GL}_1$ of the parabolic subgroup

$$\boldsymbol{P} = \mathrm{Stab}_{\mathrm{GL}(W)}\big(\langle e_1\rangle_{\mathbb{C}}, \langle e_1, \ldots, e_r\rangle_{\mathbb{C}}\big),$$

and $[\boldsymbol{L}, \boldsymbol{L}] = \{1\} \times \mathrm{SL}_{r-1} \times \{1\}$ in $\boldsymbol{L}$. Let $\boldsymbol{T}$ denote the diagonal torus of $\boldsymbol{G}$. By Smith's theorem, $V|_{\boldsymbol{L}}$ contains a simple submodule $U$, which, as $[\boldsymbol{L}, \boldsymbol{L}]$-module, has highest weight $\nu$, which is the restriction of $\lambda$ to $\boldsymbol{T} \cap [\boldsymbol{L}, \boldsymbol{L}]$ and hence invariant under the graph automorphism $\tau'$ of $[\boldsymbol{L}, \boldsymbol{L}]$.

Since $g$ is WM2 on $V$, it is WM2 on $U$. By (3.2.10.1) we have $g = zh$, with $h \in [\boldsymbol{L}, \boldsymbol{L}]$ and $z = \mathrm{diag}(t_1, I_{r-1}, t_1^{-1}) \in \mathbf{Z}(\boldsymbol{L})$. Hence, $h$ is also WM2 on $U$. By the induction hypothesis applied to $r-2$, either $\nu = 0$, and so $\lambda = a(\varpi_1 + \varpi_r)$ with $a \geq 1$, or $r = 7$, $\nu = \varpi_4$, and so $\lambda = a(\varpi_1 + \varpi_7) + \varpi_4$ with $a \geq 0$.

Suppose $a \geq 1$ in either case, and consider $\mu := \lambda - (\varpi_1 + \varpi_r)$. By Proposition 3.2.2, we can choose $J = \{1, r\}$ and obtain $m_\lambda(\nu) = m_{\lambda_1}(\mu_1)$ for

$$\lambda_1 = \lambda - (a-1)(\varpi_1 + \varpi_r) = \varpi_1 + \varpi_r, \ \mu_1 = \mu - (a-1)(\varpi_1 + \varpi_r) = 0$$

in the first case, and

$$\lambda_1 = \lambda - (a-1)(\varpi_1 + \varpi_7) = \varpi_1 + \varpi_7 + \varpi_4, \ \mu_1 = \mu - (a-1)(\varpi_1 + \varpi_7) = \varpi_4$$

Direct computation shows that $m_{\lambda_1}(\mu_1) = r \geq 5$ in the first case. In the second case, $m_{\lambda_1}(\mu_1) = 16$ by [**Lie**]. In either case, $g$ cannot be WM2 on $V$.

Finally, we consider the case $(r, \lambda) = (7, \varpi_4)$. Then $L(\lambda) = \wedge^4(W)$, and direct computation shows that $g$ has eigenvalue 1 with multiplicity $\geq 6$ on $L(\lambda)$, again a contradiction. □

## 3.3. Regular spectrum and simple spectrum elements

Let $V$ be a finite dimensional $\mathbb{C}$-vector space. Recall from Definition 1.1.5 that an element $g \in \mathrm{GL}(V)$ is said to have *regular spectrum* if each eigenvalue of $g$ occurs with a single Jordan block. We have the following elementary lemma of linear algebra, whose proof is left to the reader.

Lemma 3.3.1. *For a given element $g \in \mathrm{GL}(V)$, the following conditions are equivalent.*

(i) *$g$ has regular spectrum.*

(ii) *The minimal polynomial of $g$ is equal to the characteristic polynomial of $g$.*

(iii) *The powers $g^0 := \mathrm{Id}_V, g, g^2, \ldots, g^{\dim(V)-1}$ are linearly independent in $\mathrm{End}(V)$.*

Recall also from Definition 1.1.5 that an element $g \in \mathrm{GL}(V)$ is said to have *simple spectrum* if it has $\dim(V)$ distinct eigenvalues. Thus an element with simple spectrum has regular spectrum, but not conversely. For example, a single Jordan block of size $\dim(V)$ has regular spectrum, but not simple spectrum so long as $\dim(V) \geq 2$.

Proposition 3.3.2. *Let $V$ be a finite dimensional $\mathbb{C}$-vector space, and $G \leq \mathrm{GL}(V)$ a Zariski closed subgroup which is reductive. Let the connected components of $G$ be denoted $G^{(i)}$, with the identity component denoted $G^\circ$. Suppose a given connected component $G^{(i)}$ contains an element $g$ which has regular spectrum. Then this component $G^{(i)}$ contains an element with simple spectrum, and the set of simple spectrum elements in $G^{(i)}$ is Zariski dense in $G^{(i)}$ .*

Proof. By Lemma 3.3.1, the powers $g^0 := \mathrm{Id}, g, g^2, \ldots, g^{\dim(V)-1}$ are linearly independent in $\mathrm{End}(V)$, or equivalently the vector

$$g^0 \wedge g \wedge g^2 \wedge \ldots \wedge g^{\dim(V)-1} \in \wedge^{\dim(V)}(\mathrm{End}(V))$$

is nonzero. Thus the wedge map

$$A \in G^{(i)} \mapsto A^0 \wedge A \wedge A^2 \wedge \ldots \wedge A^{\dim(V)-1} \in \wedge^{\dim(V)}(\mathrm{End}(V)) \tag{3.3.2.1}$$

is a morphism from $G^{(i)}$ to $\wedge^{\dim(V)}(\mathrm{End}(V))$ which is not identically zero, and hence is nonzero on a dense open set of $G^{(i)}$.

Now choose a maximal compact subgroup $K$ of the complex Lie group $G(\mathbb{C})$. One knows, cf. [**Mos**, p. 44] or [**Ho**, Theorem 3.1], that topologically $G(\mathbb{C})$ is the product of $K$ with a Euclidean space, and (hence) that $K$ meets each $G^{(i)}$, and that the intersections $K \cap G^{(i)}(\mathbb{C})$

are precisely the connected components of $K$. Because $G$ is reductive, $K^\circ$ is a maximal compact subgroup of $G^\circ(\mathbb{C})$, and hence $K^\circ$ is Zariski dense in $G^\circ$ (Weyl's unitarian trick). Now pick elements $k_i \in K \cap G^{(i)}(\mathbb{C})$. Then the connected components of $K$ are the cosets $K^{(i)} = k_i K^\circ$, the connected components of $G$ are the $G^{(i)} = k_i G^\circ$, and thus each $K^{(i)} = k_i K^\circ$ is Zariski dense in $G^{(i)} = k_i G^\circ$. Because the wedge map (3.3.2.1) above is nonzero on the given $G^{(i)}$, it must be nonzero on $K^{(i)}$ (by Zariski density). Thus $K^{(i)}$ contains elements with regular spectrum. But every element in $K^{(i)}$, being an element of the compact group $K$, is diagonalizable. For diagonalizable elements, the notions of regular spectrum and simple spectrum coincide. Thus $K^{(i)}$ contains elements with simple spectrum. As $K^{(i)} \subset G^{(i)}$, $G^{(i)}$ contains elements with simple spectrum. In $G^{(i)}$, the set of elements with simple spectrum is open (this being an open condition on the characteristic polynomial), and being nonempty will necessarily be Zariski dense in $G^{(i)}$. □

Theorem 3.3.3. *Let $V = \mathbb{C}^N$ and let $G \leq \mathrm{GL}(V)$ be a reductive subgroup such that $G^\circ$ is a simple algebraic group of rank $r \geq 4$, $V|_{G^\circ}$ is irreducible, and some element $g \in G \smallsetminus \mathbf{Z}(G)G^\circ$ has a regular spectrum on $V$. Then one of the following holds.*

(a) *$G^\circ \cong \mathrm{SO}_{2r}$ is of type $D_r$, $N = 2r$, and $V|_{G^\circ} \cong L(\varpi_1)$.*
(b) *$G^\circ$ is of type $A_5$, $N = 20$, and $V|_{G^\circ} \cong L(\varpi_3)$.*

Proof. (i) Since $V|_{G^\circ}$ is irreducible, $\mathbf{C}_G(G^\circ) = \mathbf{Z}(G)$. It follows that, modulo $\mathrm{Inn}(G^\circ)$, the conjugation by $g$ induces a graph automorphism $\tau$ of $G^\circ$ of order $e > 1$; in particular, $G^\circ$ is of type $A_r$, $D_r$, or $E_6$. By Proposition 3.3.2, we may replace $g$ by another element in the same $gG^\circ$-coset and assume that $g$ has simple spectrum on $V$; in particular, $g$ is semisimple. If $V|_{G^\circ} = L(\lambda)$ has highest weight $\lambda$, then $\lambda$ is $\tau$-invariant. We also note that $h := g^e \in \mathbf{Z}(G)G^\circ$ (because $g^e$ induces an inner automorphism of $G^\circ$), $h$ is semisimple, and that the multiplicity of any eigenvalue of $h$ on $V$ is at most $e$, as $g$ has simple spectrum on $V$. Writing $h = zh_1$ with $z \in \mathbf{Z}(G)$ and $h_1 \in G^\circ$, we also have that the multiplicity of any eigenvalue of $h_1$ on $V$ is at most $e$. Furthermore, $e \leq 2$, or $e = 3$ and $G^\circ$ is of type $D_4$.

(ii) Now, if $G^\circ$ is of type $E_6$, then $e = 2$ and so $L(\lambda)$ is $\mathsf{WM2}$. Hence $\lambda = 0$ by Proposition 3.2.7, a contradiction.

Next, suppose that $G^\circ$ is of type $D_4$. If $e = 3$, then $L(\lambda)$ is $\mathsf{WM3}$, and $\lambda$ can be identified by Lemma 3.2.4; however, none of these weights is $\tau$-invariant. So $e = 2$, $L(\lambda)$ is $\mathsf{WM2}$, and so (a) holds by Lemma 3.2.4 (with the proviso that $V|_{G^\circ} \cong L(\varpi_1)$ up to a twist by $\mathrm{Aut}(G^\circ)$).

Now assume that $G^\circ$ is of type $D_r$ with $r \geq 5$, so that $e = 2$, and $\mathrm{Aut}(G^\circ) \cong \mathrm{O}_{2r}/C_2$. Hence the image of $g$ in $\mathrm{Aut}(G^\circ)$ is the image of some $g_1 \in \mathrm{O}_{2r} \smallsetminus \mathrm{SO}_{2r}$. Such an element $g_1$ must have eigenvalue $-1$ on $\mathbb{C}^{2r}$. Now the image of $h_1$ in $\mathrm{Aut}(G^\circ)$ is the image of $g_1^2$, and the latter belongs to $\mathrm{SO}_{2r}$ and has eigenvalue 1 on $\mathbb{C}^{2r}$. Also, $h_1$ is $\mathsf{WM2}$ on $V$. Hence (a) holds by Proposition 3.2.9.

(iii) Finally, we consider the case $G^\circ$ is of type $A_r$, so without loss we may assume that $G^\circ = \mathrm{SL}_{r+1}$ and $\tau(X) = {}^tX^{-1}$. Then the image of $g$ in $\mathrm{Aut}(G^\circ)$ is the map $X \mapsto \tau(AXA^{-1})$ for some $A \in G^\circ$, and the image of $g^2$ and $h_1$ is the map $X \mapsto (\tau(A)A)X(\tau(A)A)^{-1}$. Hence, we may assume that the semisimple element $h_1$ is $\tau(A)A$, the *cosquare* of $A$. The possible Jordan canonical form of cosquares are known, see e.g. [**Bal**, Theorem 3.6]. In particular, since $\tau(A)A$ is semisimple, it is similar to

$$\operatorname{diag}\bigl(a_1, a_1^{-1}, \dots, a_m, a_m^{-1}, \underbrace{1, \dots, 1}_{n \text{ times}}\bigr)$$

for some $a_i, b_j \in \mathbb{C}^\times$. As $h_1$ is WM2 on $L(\lambda)$, we can apply Proposition 3.2.10 to arrive at (b). □

Now we are ready to classify irreducible representations of (possibly disconnected) simple algebraic groups that admit elements with regular spectrum. See also [**Za2**] (and references therein) for related results.

THEOREM 3.3.4. *Let $G$ be a (not necessarily connected) reductive group over $\mathbb{C}$ with $G^\circ$ being simple. Let $V$ be a finite-dimensional faithful representation of $G$ such that $V|_{G^\circ}$ is irreducible. Then $G$ admits an element $g$ with regular spectrum on $V$ if and only if one of the following statements holds.*

(A) *$g \in \mathbf{Z}(G)G^\circ$, and $V|_{G^\circ} = L(\lambda)$ is* WMF *and classified in* [**HS**, Theorem 4.6.3]*, see also* [**Seitz**, §6] *and* [**ZS**]*. Specifically, one of the following holds.*
   (a) *$G^\circ$ is of type $A_r$ with $r \geq 1$, and $L(\lambda) = L(a\varpi_1)$ or $L(a\varpi_r)$ with $a \in \mathbb{Z}_{\geq 0}$, or $L(\lambda) = L(\varpi_i)$ with $2 \leq i \leq r-1$.*
   (b) *$G^\circ$ is of type $B_r$ with $r \geq 1$, and $L(\lambda) = L(\varpi_1)$, the natural representation of degree $2r+1$, or $L(\varpi_r)$, the spin representation of degree $2^r$.*
   (c) *$G^\circ$ is of type $C_r$ with $r \geq 3$, and $L(\lambda) = L(\varpi_1)$, the natural representation of degree $2r$, or $L(\lambda) = L(\varpi_3)$ of degree 14 when $r = 3$.*
   (d) *$G^\circ$ is of type $D_r$ with $r \geq 4$, and $L(\lambda) = L(\varpi_1)$, the natural representation of degree $2r$, or $L(\lambda)$ is one of the two half-spin representations $L(\varpi_{r-1})$ and $L(\varpi_r)$ of degree $2^{r-1}$.*
   (e) *$(G^\circ, V|_{G^\circ}, \dim(V)) = (G_2, L(\varpi_1), 7)$, $(E_6, L(\varpi_1 \text{ or } \varpi_6), 27)$, $(E_7, L(\varpi_7), 56)$.*

(B) *$g \notin \mathbf{Z}(G)G^\circ$, and one of the following holds.*
   (a) *$G^\circ$ is of type $D_r$ with $r \geq 4$ and $V|_{G^\circ} = L(\varpi_1)$.*
   (b) *$(G^\circ, V|_{G^\circ}, \dim(V)) = (\mathrm{SL}_6, L(\varpi_3), 20)$, $(\mathrm{SL}_4, L(\varpi_2), 6)$, $(\mathrm{SL}_3, L(\varpi_1 + \varpi_2), 8)$.*

PROOF. (i) For the "only if" direction, by Proposition 3.3.2, we can replace $g$ by another element from the same $G^\circ$-coset and assume that $g$ has simple spectrum on $V$. Now, if $g = zh \in \mathbf{Z}(G)G^\circ$ with $z \in \mathbf{Z}(G)$ and $h \in G^\circ$, then $h$ also has simple spectrum on $V$, and it is semisimple. Hence $V|_{G^\circ}$ is WMF, and (A) follows from Howe's result [**HS**, Theorem 4.6.3].

Consider the case $g \notin \mathbf{Z}(G)G^\circ$. If $G^\circ$ has rank $r \geq 4$, then (B) follows from Theorem 3.3.3. As $g$ induces a non-inner automorphism of $G^\circ$, it remains to consider the case $G^\circ$ is of type $A_2$ or $A_3$, and $V|_{G^\circ} = L(\lambda)$ is invariant under the graph automorphism $\tau$. Arguing as in the proof of Theorem 3.3.3, we see that $L(\lambda)$ is WM2, and $\lambda \neq 0$ by faithfulness. Now the statement follows from Lemma 3.2.5 for type $A_2$. Suppose $G^\circ$ is of type $A_3$. By Lemma 3.2.3, $\lambda = a\varpi_2$ with $1 \leq a \leq 3$. Arguing as in the proof of Theorem 3.3.3, we may assume that $g^2$ is a scalar multiple of $h_1 := \operatorname{diag}(t_1, t_2, t_1^{-1}, t_2^{-1})$. Viewing $G^\circ = \mathrm{SL}(W)$, we have

$$L(\varpi_2) \cong \wedge^2(W),\ L(2\varpi_2) \cong \mathrm{Sym}^2(\wedge^2(W))/L(0),\ L(3\varpi_2) \cong \mathrm{Sym}^3(\wedge^2(W))/\wedge^2(W).$$

Using these identifications, one easily checks that the multiplicity of 1 as an eigenvalue for $h_1$ on $L(2\varpi_2)$ is $\geq 4$, and on $L(3\varpi_2)$ is $\geq 6$. As $g$ is WM2 on $V$, we conclude that $\lambda = \varpi_2$.

(ii) For the "if" direction, in the case of (A), $L(\lambda)$ is $\mathsf{WMF}$ and so some element in a maximal torus of $G^\circ$ has simple spectrum on $L(\lambda)$.

Suppose we are in (B). In the case of (a), twisting $L(\lambda)$ by a suitable automorphism of $G^\circ$ when $G^\circ$ is of type $D_4$, we may assume that $L(\lambda) = L(\varpi_1)$, and $G/\mathbf{C}_G(G^\circ) \cong \mathrm{PO}_{2r}$. Now, we may take $g$ to be a multiple of $\mathrm{diag}(-1, 1, h)$, where $h \in \mathrm{SO}_{2r-2}$ has simple spectrum and no eigenvalue $\pm 1$ on $\mathbb{C}^{2r-2}$, and such $g$ has simple spectrum on $V$.

The case of $\mathrm{SL}_4$ in (B)(b) then also occurs, because $A_3 \cong D_3$. Next, as shown in [**Ka-ESDE**, 10.7.1 (4)], a hypergeometric sheaf $\mathcal{H}$ of type $(8, 2)$ in (any) characteristic $p > 7$ has $G_{\mathrm{geom}} = \mathrm{PSL}_3 \cdot 2$. By Theorem 1.2.2, the image of $I(0)$ in $G_{\mathrm{geom}}$ cannot be contained in $G^\circ_{\mathrm{geom}}$, hence a generator $g_0$ of it is in $G_{\mathrm{geom}} \smallsetminus G^\circ_{\mathrm{geom}}$ and has regular spectrum on $\mathcal{H}$, and thus the case of $\mathrm{SL}_3$ in (B)(b) occurs.

Finally, we show that the case of $G^\circ = \mathrm{SL}_6$ in (B)(b) also occurs. Consider $J := \begin{pmatrix} 0 & I_3 \\ -I_3 & 0 \end{pmatrix}$ and the outer automorphism $\tau : X \to J^{-1}{}^tX^{-1}J$ of $G^\circ$. Then $H := \mathbf{C}_{G^\circ}(\tau) \cong \mathrm{Sp}_6$. As $L(\varpi_3)$ is $\tau$-invariant, $L(\varpi_3)$ extends to a module $V$ over $G := G^\circ \rtimes \langle \tau \rangle$. Next, $V|_H \cong A \oplus B$, a direct sum of irreducible $H$-modules $A = L(\varpi'_1) \cong L(\varpi_1)|_H$ of dimension 6 and $B = L(\varpi'_3)$ of dimension 14. As $\tau$ centralizes $H$ but not $G^\circ$, and has order 2, it must act on $V$ as

$$\epsilon \cdot \mathrm{diag}(\mathrm{Id}_A, -\mathrm{Id}_B) \tag{3.3.4.1}$$

for some $\epsilon = \pm 1$. Now consider $h = \mathrm{diag}(a, b, c, a^{-1}, b^{-1}, c^{-1}) \in H$ with $a, b, c \in \mathbb{C}^\times$. Then $h$ acts on $V$ as $\wedge^3(h)$, which is conjugate to

$$\mathrm{diag}\big((abc)^{[\pm 1]}, a^{[\pm 1]}, a^{[\pm 1]}, b^{[\pm 1]}, b^{[\pm 1]}, c^{[\pm 1]}, c^{[\pm 1]}, (abc^{-1})^{[\pm 1]}, (ab^{-1}c)^{[\pm 1]}, (a^{-1}bc)^{[\pm 1]}\big),$$

(here the notation $d^{[\pm 1]}$ means that the matrix has two consecutive entries $d$ and $d^{-1}$ on the diagonal). As $A \cong L(\varpi_1)|_H$, $h$ acts on $A$ as

$$\mathrm{diag}(a, b, c, a^{-1}, b^{-1}, c^{-1}). \tag{3.3.4.2}$$

Hence, $h$ acts on $B$ as

$$\mathrm{diag}\big((abc)^{[\pm 1]}, a^{[\pm 1]}, b^{[\pm 1]}, c^{[\pm 1]}, (abc^{-1})^{[\pm 1]}, (ab^{-1}c)^{[\pm 1]}, (a^{-1}bc)^{[\pm 1]}\big). \tag{3.3.4.3}$$

Choosing $a, b, c$ suitably (say $a = \zeta_3$, $b = \zeta_5$, and $c = \zeta_7$), we see from (3.3.4.1)–(3.3.4.3) that $g := h\tau \in G \smallsetminus G^\circ$ has simple spectrum on $V$. □

CHAPTER 4

# Hypergeometric sheaves with wild part of dimension one

In this chapter, we consider hypergeometric sheaves $\mathcal{H}$ in characteristic $p$ of type $(D, D-1)$. Recall that a *complex reflection* is an element $\gamma \in \mathrm{GL}_D$ that is conjugate to $\mathrm{diag}(\zeta, 1, \dots, 1)$ for some $1 \neq \zeta \in \mathbb{C}^\times$; $\gamma$ is a (true) *reflection* if $\zeta = -1$.

## 4.1. General situation

THEOREM 4.1.1. *Let $\mathcal{H}$ be a hypergeometric sheaf in odd characteristic $p$ of type $(D, D-1)$. If $G_{\mathrm{geom}}$ is infinite, then $G_{\mathrm{geom}}^\circ = \mathrm{SL}_D$, $G_{\mathrm{geom}} = \mu_N * \mathrm{SL}_D$ for some $N \in \mathbb{Z}_{\geq 1}$, and $\mathcal{H}$ satisfies* (**S**+)*. If $D > 4$ when $p = 3$, $D > 2$ when $p = 5$, or $D \geq 2$ when $p \geq 7$, then $G_{\mathrm{geom}}$ is infinite.*

PROOF. In odd characteristic $p$, any hypergeometric sheaf of type $(D, D-1)$ satisfies (**S**−). To see that it is primitive, notice that it cannot be Kummer induced because $\gcd(D, D-1) = 1$. It cannot be Belyi induced because its wild part has dimension $w = 1$, which is not divisible by $p - 1$, cf. [**KT5**, proof of Theorem 3.13]. By [**KT5**, Lemma 2.4], it is tensor indecomposable.

Because $w = 1$, $P(\infty)$ acts through complex reflections of order $p$. By Mitchell's theorem [**Mit**, Theorem 1], no finite primitive group containing complex reflections of order $\geq 4$ exists in any dimension $> 2$, and none containing complex reflections of order 3 exists in any dimension $> 4$. Moreover, no finite primitive linear groups of degree 2 can contain noncentral elements of prime order $p \geq 7$. Therefore $G_{\mathrm{geom}}$ is infinite. Because the given representation $V_{\mathcal{H}}$ of $G_{\mathrm{geom}}$ is both primitive and tensor-indecomposable, it results from [**Ka-MG**, Prop. 1] that the action of $G_{\mathrm{geom}}$ is Lie-irreducible, i.e. $G_{\mathrm{geom}}^\circ$ acts irreducibly. By Deligne [**De2**, 3.4.1(iii) and 1.3.9], $G_{\mathrm{geom}}$ is a semisimple algebraic group, and hence $\mathrm{Lie}(G_{\mathrm{geom}})$ is a semisimple Lie subalgebra of $\mathrm{End}(V_{\mathcal{H}})$ which acts irreducibly on $V_{\mathcal{H}}$. But $\mathrm{Lie}(G_{\mathrm{geom}})$ is normalized by the image of $P(\infty)$, so in particular by a complex reflection of order $p$. As $p \geq 3$, one knows, cf. [**Ka-ESDE**, 1.5] or [**BH**, Proposition 6.4] that $\mathrm{Lie}(G_{\mathrm{geom}})$ must be $\mathrm{Lie}(\mathrm{SL}(V_{\mathcal{H}}))$, and hence that $G_{\mathrm{geom}}^\circ = \mathrm{SL}(V_{\mathcal{H}}) = \mathrm{SL}_D$. Now $\mathrm{GL}_D = \mathrm{GL}_1 * \mathrm{SL}_D$, and $\mathbf{Z}(G_{\mathrm{geom}})$ is finite (see Lemma 1.1.3(iii)). Hence $G_{\mathrm{geom}}$ is the central product $\mu_N * \mathrm{SL}_D$ for some integer $N \geq 1$. Also, note that $\mathrm{SL}_D$ has no finite quotient and has no nontrivial projective representation of degree $< D$, see [**KlL**, Proposition 5.4.11]. It follows that $\mathcal{H}$ is not tensor induced, and thus satisfies (**S**+). □

REMARK 4.1.2. As shown in [**KRLT4**, Theorem 30.7], there are hypergeometric sheaves of type $(D, D-1)$, of rank $D = 2, 4$ in characteristic $p = 3$ and of rank $D = 2$ in characteristic $p = 5$, with $G_{\mathrm{geom}}$ a finite, primitive complex reflection group. This shows that the bounds $D > 4$ for $p = 3$ and $D > 2$ for $p = 5$ in Theorem 4.1.1 are best possible.

Corollary 4.1.3. *Let $p$ be a prime and $A \in \mathbb{Z}_{\geq 3}$ be such that $p \nmid A(A-1)$. For $\chi$ a character of $E^\times$ for some finite extension $E/\mathbb{F}_p$, consider the local system*

$$\mathcal{F}(A, A-1, \chi)$$

*of rank $A$ on $\mathbb{A}^1/\mathbb{F}_p$ whose trace function for $K/\mathbb{E}$ a finite extension and $t \in K$ is*

$$t \mapsto -\sum_{x \in K^\times} \psi_K(x^A - tx^{A-1})\chi_K(x).$$

*Then we have the following results.*

(i) *Suppose that $A \geq 3$ when $p \geq 7$, $A \geq 4$ when $p = 5$, and $A \geq 6$ when $p = 3$. Then the $G_{\rm geom}$ of $\mathcal{F}(A, A-1, \mathbb{1})$ has $G^\circ_{\rm geom} = \mathrm{SL}_{A-1}$.*

(ii) *Suppose that $A \geq 2$ when $p \geq 7$, $A \geq 3$ when $p = 5$, and $A \geq 5$ when $p = 3$. Then for any nontrivial $\chi$, the $G_{\rm geom}$ of $\mathcal{F}(A, A-1, \chi)$ has $G^\circ_{\rm geom} = \mathrm{SL}_A$.*

Proof. At the expense of replacing $\psi$ by the additive character $x \mapsto \psi(-Ax)$, these local systems are geometrically isomorphic to multiplicative translates of the $[A]^\star$ Kummer pullbacks of hypergeometric sheaves of types $(A-1, A-2)$ and $(A, A-1)$ respectively, cf. [**KT6**, Corollary 3.10, (i) and (ii)]. Because $p \nmid A(A-1)$, $p$ must be odd. Finite pullback does not change the identity component $G^\circ_{\rm geom}$ of $G_{\rm geom}$, so the result follows from Theorem 4.1.1. □

Remark 4.1.4. Unlike the case $p > 2$, hypergeometric sheaves of type $(D, D-1)$ in characteristic $p = 2$ can be imprimitive. No such sheaf can be Kummer induced (simply because $\gcd(D, D-1) = 1$), but it can be Belyi induced. By [**KRLT4**, Proposition 3.7], this can happen precisely when there are characters $\Lambda$ and $\sigma$ such that one of the following holds for $\mathcal{H} = \mathcal{H}yp(\chi_1, \ldots, \chi_D; \rho_1, \ldots, \rho_{D-1})$:

(a) $D = 2$, $\{\chi_1, \chi_2\} = \{\Lambda, \sigma\}$, $\rho_1 = (\Lambda\sigma)^{1/2}$.

(b) $2 \nmid D \geq 3$, $\{\chi_1, \ldots, \chi_D\}$ is the set of all $D^{\rm th}$ roots of $\Lambda\sigma$, $\{\rho_1, \ldots, \rho_{D-2}\}$ is the set of all $(D-2)^{\rm th}$ roots of $\Lambda$, and $\rho_{D-1} = \sigma$.

Such a Belyi induced sheaf is induced, by the map $x \mapsto 1/x^A(x-1)^B$ with $(A, B)$ either $(1, 1)$ or $(2, D-2)$, from the rank one sheaf $\mathcal{L}_{\Lambda(x)} \otimes \mathcal{L}_{\sigma(x-1)}$ which has finite $G_{\rm geom}$, and hence any Belyi induced sheaf has finite $G_{\rm geom}$. Thus, when $p = 2$, a hypergeometric sheaf of type $(D, D-1)$ with $D > 1$ is either primitive, or has finite $G_{\rm geom}$. [In the trivial case $D = 1$, the sheaf is $\mathcal{L}_\chi \otimes \mathcal{L}_\psi$, which is both primitive and has finite $G_{\rm geom}$.]

Theorem 4.1.5. *Let $\mathcal{H}$ be a hypergeometric sheaf in characteristic $p = 2$ of type $(D, D-1)$. Suppose $G_{\rm geom}$ is infinite. Then $G^\circ_{\rm geom}$ is either $\mathrm{SL}_D$ or $\mathrm{SO}_D$. If furthermore $D \neq 4$, then $\mathcal{H}$ satisfies* (**S**+).

Proof. Since $G_{\rm geom}$ is finite when $D = 1$, so we will assume $D > 1$. Now $\mathcal{H}$ is primitive by Remark 4.1.4, and tensor indecomposable by [**KT5**, Lemma 2.4]. Thus $G_{\rm geom}$ is infinite, primitive, and tensor indecomposable, so it results from [**Ka-MG**, Prop. 1] that the action of $G_{\rm geom}$ is Lie-irreducible, i.e. $G^\circ_{\rm geom}$ acts irreducibly. Just as in the proof of Proposition 4.1.1 above, we see that $\mathrm{Lie}(G_{\rm geom})$ is a semisimple Lie subalgebra of $\mathrm{End}(V_\mathcal{H})$ which acts irreducibly on $V_\mathcal{H}$. But $\mathrm{Lie}(G_{\rm geom})$ is normalized by the image of $P(\infty)$, so in particular by a reflection. In this case, one knows [**Ka-ESDE**, 1.5] that $\mathrm{Lie}(G_{\rm geom})$ is either $\mathrm{Lie}(\mathrm{SL}_D)$ or $\mathrm{Lie}(\mathrm{SO}_D)$, and hence that $G^\circ_{\rm geom}$ is either $\mathrm{SL}_D$ or $\mathrm{SO}_D$.

When $D \neq 4$ and $\mathcal{H}$ is primitive, we need to show that $\mathcal{H}$ is not tensor induced, which is obvious unless $D$ is a proper power. We may therefore assume that $D \geq 8$. The same arguments as at the end of the proof of Theorem 4.1.1 yield the result when $G^\circ = \mathrm{SL}_D$ or $\mathrm{SO}_D$. (Note $\mathrm{Spin}_D$ has no nontrivial projective representation of dimension $< D$, see [**KlL**, Proposition 5.4.11].) □

## 4.2. Further analysis

Here is a way to distinguish the two cases of SL and SO in Theorem 4.1.5.

THEOREM 4.2.1. *Let $\mathcal{H}$ be a hypergeometric sheaf in characteristic $p = 2$ of type $(D, D-1)$. Suppose $D > 2$ and $G_{\mathrm{geom}}$ is infinite. If $G^\circ_{\mathrm{geom}} = \mathrm{SO}_D$, then there exists a tame character $\chi$ such that $\mathcal{H} \otimes \mathcal{L}_\chi$ is orthogonally self-dual, and has $G_{\mathrm{geom},\mathcal{H}\otimes\mathcal{L}_\chi} = \mathrm{O}_D$. If there exists no tame character $\chi$ that makes $\mathcal{H} \otimes \mathcal{L}_\chi$ self-dual, then $G^\circ_{\mathrm{geom}} = \mathrm{SL}_D$.*

PROOF. Suppose that $G^\circ_{\mathrm{geom}} = \mathrm{SO}_D$. As $G_{\mathrm{geom}}$ contains a reflection, we have $\mathrm{O}_D \leq G_{\mathrm{geom}}$. The normalizer of $\mathrm{SO}_D$ in $\mathrm{GL}_D$ is the central product $\mathrm{GL}_1 * \mathrm{O}_D$. Thus $G_{\mathrm{geom}}$ is the central product $\mu_N * \mathrm{O}_D$ for some integer $N \geq 1$; each element in $G_{\mathrm{geom}}$ can be written as $\lambda\gamma$ with $\lambda \in \mu_N$ and $\gamma \in \mathrm{O}_D$. If $N$ is odd, this writing is unique, but if $N$ is even then there is precisely one other writing of this element, namely $(-\lambda)(-\gamma)$. In either case, $\lambda^2$ is well defined as a character $\Lambda$ of $G_{\mathrm{geom}}$. Viewed as a character of $\pi_1(\mathbb{G}_m/\overline{\mathbb{F}_2})$, $\Lambda$ is tame at 0 and has $\mathsf{Swan}_\infty(\Lambda) \leq 1$.

Suppose first that $\mathsf{Swan}_\infty(\Lambda) = 0$. Then $\Lambda$ is a tame character, so has a unique tame square root, which we write $\overline{\chi}$. Then for $\mathcal{H} \otimes \mathcal{L}_\chi$, this "formation of $\lambda^2$" character is trivial, which is to say that $G_{\mathrm{geom},\mathcal{H}\otimes\mathcal{L}_\chi} \leq \mathrm{O}_D$. Tensoring with a tame character does not change the identity component of $G_{\mathrm{geom}}$ (because it disappears after a Kummer pullback). Thus we have

$$\mathrm{SO}_D \leq G_{\mathrm{geom},\mathcal{H}\otimes\mathcal{L}_\chi} \leq \mathrm{O}_D.$$

But the geometric determinant of $\mathcal{H} \otimes \mathcal{L}_\chi$ is always of order divisible by $p$ (here 2) in the $w = 1$ case, cf. [**Ka-ESDE**, 8.12.2 (2)], which rules out the $\mathrm{SO}_D$ possibility.

We now argue by contradiction, to show that the case when $\mathsf{Swan}_\infty(\Lambda) = 1$ cannot occur.

Suppose that $\Lambda$ has $\mathsf{Swan}_\infty(\Lambda) = 1$. Then we may again choose a square root $\overline{L}$ of $\Lambda$, but now $L$ has $\mathsf{Swan}_\infty(L) = 2$, and $\mathsf{Swan}_\infty(L^2) = \mathsf{Swan}_\infty(\overline{\Lambda}) = 1$. Just as in the previous paragraph, $L \otimes \mathcal{H}$ has its $G_{\mathrm{geom},L\otimes\mathcal{H}} < \mathrm{O}_D$. Now look at the $I(\infty)$-representation of $\mathcal{H}$; it is

$$\mathsf{Wild}_1 \oplus \rho_1 \oplus \ldots \oplus \rho_{D-1},$$

for some wild part of rank one and some list of length $D-1$ of tame characters $\rho_i$. After tensoring with $L$, the $I(\infty)$-representation of $L \otimes \mathcal{H}$ is

$$L\mathsf{Wild}_1 \oplus L\rho_1 \oplus \ldots \oplus L\rho_{D-1}.$$

This $I(\infty)$-representation is now self-dual, so the set of characters which occur must be stable by complex conjugation (i.e. by inversion). So we may pair up pairs of inverses, with at most two singletons left over.

If there are two singletons left over, at least one of them must be one of the $L\rho_i$, say $L\rho_1$. Then $L\rho_1 = (L\rho_1)^{-1}$, i.e., $L^2 = (\rho_1)^{-2}$. But $(\rho_1)^{-2}$ is tame, hence $L^2$ is tame, but $L^2 = \overline{\Lambda}$ has $\mathsf{Swan}_\infty = 1$, contradiction.

If there is one singleton left over, then either that singleton is an $L\rho_1$ and we get a contradiction as in the previous paragraph, or the singleton is $L\mathsf{Wild}_1$, and, as $D \geq 3$, there is at least one pair, say $L\rho_1$ and $L\rho_2$, of inverses. In this case we have $L\rho_1 = (L\rho_2)^{-1}$, hence $L^2$ is tame, being $(\rho_1\rho_2)^{-1}$, again a contradiction.

If there are no singletons, there is at least one pair, say $L\rho_1$ and $L\rho_2$, of inverses, and we get the same contradiction. □

Remark 4.2.2. In contrast to the situation in Theorem 4.1.1, where we only need $D > 4$, in the situation of Theorem 4.1.5 the assumption that $G_{\rm geom}$ is infinite is essential, because we can have finite $G_{\rm geom}$ for all even $D \geq 4$. For any **odd** integer $n \geq 5$, the hypergeometric sheaf of type $(n-1, n-2)$ in characteristic $p = 2$,

$$\mathcal{H} := \mathcal{H}yp(\mathsf{Char}_{\rm ntriv}(n); \mathsf{Char}(n-2)),$$

whose "upstairs" characters are all the nontrivial characters of order dividing $n$, and whose "downstairs" characters are all the characters of order dividing $n-2$, has $G_{\rm geom}$ the full symmetric group $\mathsf{S}_n$ in its deleted permutation representation, cf. [**KT5**, 9.3(i) and its proof].

Theorem 4.2.3. *Let $\mathcal{H}$ be a (geometrically irreducible) hypergeometric sheaf in characteristic $p = 2$ of type $(D, D-1)$ which is primitive. Suppose that $D \geq 5$ and that $G_{\rm geom}$ is finite. Then $D$ is even, and one of the following statements holds.*

(a) *There exists a tame character $\chi$ such that $\mathcal{H} \otimes \mathcal{L}_\chi$ is geometrically isomorphic to the sheaf*

$$\mathcal{H} := \mathcal{H}yp(\mathsf{Char}_{\rm ntriv}(D+1); \mathsf{Char}(D-1))$$

*of Remark 4.2.2, whose $G_{\rm geom}$ is the symmetric group $\mathsf{S}_{D+1}$ in its deleted permutation representation.*

(b) *$G = \mathbf{Z}(G)G_0$, $G_0$ is a complex reflection group, and either $D = 6$ and $G_0$ is $W(E_6) = \mathrm{SU}_4(2) \cdot 2$ or the Mitchell group $6_1 \cdot \mathrm{PSU}_4(3) \cdot 2_2$, or $D = 8$ and $G_0 = W(E_8)$.*

Proof. (i) Since $p = 2$ and $w = 1$, the image of $P(\infty)$ in $G = G_{\rm geom}$ is generated by a single element $h$, which acts as $-1$ on $\mathsf{Wild}$ and $1$ on $\mathsf{Tame}$, i.e. a (true) reflection. Let $G_0$ denote the normal closure of $\langle h \rangle$ in $G$. By Theorem 1.2.3, $G/G_0$ is cyclic of odd order.

By assumption, $G$ is a finite primitive subgroup of $\mathrm{GL}_D(\mathbb{C})$ that contains the reflection $g$. We will need the following refinement of Mitchell's theorem [**Mit**] (which is [**Ka-LAMM**, 1.4.4] in the case $D > 8$):

*$G = \mathbf{Z}(G)G_0$, and either $G_0$ is $\mathsf{S}_{D+1}$ in its deleted permutation representation, or $(D, G_0) = (5, 2 \times \mathrm{SU}_4(2))$, $(6, W(E_6))$, $(6, 6_1 \cdot \mathrm{PSU}_4(3) \cdot 2_2)$, $(7, W(E_7))$, or $(8, W(E_8))$.*

Indeed, let $H < \mathrm{GL}_D(\mathbb{C})$ denote the complex reflection group $\mathsf{S}_{D+1}$ (in its deleted permutation representation), or $2 \times \mathrm{SU}_4(2)$, $W(E_6)$, $6_1 \cdot \mathrm{PSU}_4(3) \cdot 2_2$, $W(E_7)$, $W(E_8)$, when $D = 5$, 6, 6, 7, or 8, respectively. Correspondingly, let $S := \mathsf{A}_{D+1}$, $\mathrm{SU}_4(2)$, $\mathrm{SU}_4(2)$, $\mathrm{PSU}_4(3)$, $\mathrm{Sp}_6(2)$, or $\Omega_8^+(2)$, so that $S$ is the unique non-abelian composition factor of $H$. Then Mitchell's theorem implies that $G/\mathbf{Z}(G) \cong H/\mathbf{Z}(H)$. Note that $H/\mathbf{Z}(H) \cong S \cdot 2$, $S$, $S \cdot 2$, $S \cdot 2_2$, $S$, and $S \cdot 2$ in the above cases. As $G/G_0$ is cyclic, it follows that $S$ is also the unique non-abelian composition factor of $G_0$. Now we can apply the Shephard-Todd classification [**ST**] to $G_0$ to see that $G_0 \cong H$; in particular, $G_0/\mathbf{Z}(G_0) \cong H/\mathbf{Z}(H) \cong G/\mathbf{Z}(G)$. Now, since $\mathbf{Z}(G) \cap G_0 \leq \mathbf{Z}(G_0)$, we have that $\mathbf{Z}(G)G_0/\mathbf{Z}(G) \cong G_0/(\mathbf{Z}(G) \cap G_0)$ has order divisible by $|G_0/\mathbf{Z}(G_0)| = |G/\mathbf{Z}(G)|$. Hence $G = \mathbf{Z}(G)G_0$, and the claim is proved.

Also note that $\mathbf{Z}(G)$ is a finite group of scalars $\mu_N$ for some $N \geq 1$.

(ii) Here we consider the case $G_0 = \mathsf{S}_{D+1}$. Then $h$ is a 2-cycle in $\mathsf{S}_{D+1}$, whence $G_{P(\infty)} \leq \mathsf{S}_{D+1}$, and so a fortiori the quotient $G_{\rm geom}/\mathsf{S}_{D+1} = \mu_N$ has order prime to $p = 2$. So the projection of $G_{\rm geom} = \mathsf{S}_{D+1} \times \mu_N$ onto the $\mu_N$ factor is a character of odd order, so tame, say $\chi^{-1}$. Then $\mathcal{H} \otimes \mathcal{L}_\chi$ has $G_{\rm geom} = \mathsf{S}_{D+1}$.

Thus we are reduced to treating the case when $\mathcal{H}$ has $G_{\rm geom} = \mathsf{S}_{D+1}$ in its deleted permutation representation. Without loss, we may assume $h = (n-1, n) \in \mathsf{S}_{D+1}$. As usual, let $g_0$ generate the image of $I(0)$ and let $g_\infty$, of odd order, generate the image of $I(\infty)$ modulo $P(\infty)$. Since $\dim \mathsf{Wild} = 1$, $g_\infty$ centralizes the 2-cycle $h$, hence $g_\infty$ belongs to the subgroup $\mathsf{S}_{D-1}$ that fixes both $n-1$ and $n$, and has simple spectrum on $\mathsf{Tame}$ which is now the permutation module for $\mathsf{S}_{D-1}$. By [**KT5**, Theorem 6.2], $g_\infty$ is either a $(D-1)$-cycle and $2|D$, or the disjoint product of an $a$-cycle and a $b$-cycle, with $a + b = D - 1$ and $\gcd(a, D-1) = 1$. However, in the latter case, the spectrum of $g_\infty$ on $\mathsf{Tame}$ would contain 1 twice, a contradiction. Hence we are in the former case, and so $2|D$ and the set of "downstairs" characters of $\mathcal{H}$ is $\mathsf{Char}(D-1)$. As $g_0$ has simple spectrum, again by [**KT5**, Theorem 6.2], $g_0$ is either a $(D+1)$-cycle, or the disjoint product of a $c$-cycle and a $d$-cycle, with $c + d = D + 1$ and $\gcd(c, D+1) = 1$. However, in the latter case, the spectrum of $g_0$ on $\mathcal{H}$ would contain 1, and so $\mathbb{1}$ would occur both "upstairs" and "downstairs". Hence we are in the former case, and so the set of "upstairs" characters of $\mathcal{H}$ is $\mathsf{Char}_{\rm ntriv}(D+1)$, as stated.

(iii) Next we consider the additional possibilities in the cases with $D = 5, 7$. Then $\mathbf{Z}(G) \cap G_0 = \mathbf{Z}(G_0) \cong C_2$; in particular, $N = 2N_0$. Furthermore, $G/G_0 = \mathbf{Z}(G)G_0/G_0 \cong \mathbf{Z}(G)/\mathbf{Z}(G_0)$ is cyclic of odd order, which equals $N_0$. It follows that $2 \nmid N_0$, and $G = Z_0 \times G_0$ with $Z_0 := \mathbf{O}_{2'}(\mathbf{Z}(G)) = \mu_{N_0}$. Arguing as in (ii), we may tensor $\mathcal{H}$ with a suitable $\mathcal{L}_\chi$ to get $G_{\rm geom} = G_0$. As in (ii), we also get an odd-order element $g_\infty$ that centralizes $h$ and has simple spectrum on $\mathsf{Tame}$ of dimension $D - 1$.

Suppose $D = 7$, so that $G_0 = W(E_7) = 2 \times \mathrm{Sp}_6(2)$. As $2 \nmid \mathsf{o}(g_\infty)$, $g_\infty \in \mathrm{Sp}_6(2)$, of order $\geq 6$ since it has simple spectrum on $\mathsf{Tame}$. Thus $g_\infty$ has order 7, 9, or 15, see [**GAP**]. On the other hand, $g_\infty$ centralizes $-\mathrm{Id} \cdot h$, an involution in $\mathrm{Sp}_6(2)$, and this is impossible.

A similar argument rules out the case of $D = 5$. □

Remark 4.2.4. It is shown in [**KRLT4**] that the three cases listed in Theorem 4.2.3(b) do indeed give rise to primitive hypergeometric sheaves with $w = 1$ in characteristic $p = 2$ and with $G_{\rm geom} = G_0$.

We find the following result amazing, for which it would be nice to find a conceptual, rather than a case-by-case, explanation.

Theorem 4.2.5. *Let $\mathcal{H}$ be a (geometrically irreducible) hypergeometric sheaf in characteristic $p$ of type $(D, D-1)$ with $D > 1$, which is primitive. If $G_{\rm geom}$ is finite, then $D$ is even.* [But notice that, as explained in Remark 4.1.4, there are such sheaves in characteristic $p = 2$ of any odd rank $D \geq 3$ which are imprimitive.]

Proof. (i) Assume the contrary: there exists such a sheaf $\mathcal{H}$, but of odd rank $D \geq 3$. By Theorem 4.1.1, if $p \geq 3$, then we actually have $p = D = 3$. By Theorem 4.2.3, we also have $D = 3$ when $p = 2$. Thus $D = 3$ and $p = 2$ or 3. We will consider the elements $g_0$ and $g_\infty$ as in the proof of Theorem 4.2.3, and a complex reflection $1 \neq h$ in the image of $P(\infty)$.

Since $\mathcal{H}$ is primitive and $D = 3$, $\mathcal{H}$ satisfies ($\mathbf{S}+$), and so $G = G_{\mathrm{geom}}$ is either almost quasisimple, or an extraspecial normalizer, by Lemma 1.1.3. Suppose we are in the former case. Then it is well known, see also [**HM**], that $G = \mathbf{Z}(G) \times L$, where $L = \mathsf{A}_5$, $\mathrm{SL}_3(2)$, or $3 \cdot \mathsf{A}_6$. Write $h = zt$, with $z \in \mathbf{Z}(G)$ and $t \in L$, so that $t$ is a scalar multiple of a complex reflection of order $p$. Checking the spectra of elements of $L$ in a 3-dimensional irreducible representation, we see that $\mathsf{o}(t) = 2$ and so $p = 2$. Now $g_\infty$ has odd order, centralizes $t$, and is not central, since it has two distinct eigenvalues on $\mathsf{Tame}$. But this is a contradiction, since $\mathbf{C}_L(t)$ is a 2-group in all three possibilities.

(ii) So we are in the extraspecial normalizer case. As $D = 3$, we get $G < ZG_0$, where $Z := \mathbf{Z}(\mathrm{GL}_3(\mathbb{C}))$ and $G_0 = 3^{1+2}_+ \rtimes \mathrm{SL}_2(3)$. Again write $h = zt$, with $z \in Z$ and $t \in G_0$. Suppose $p = 3$, so that $t$ is a scalar multiple of a complex reflection of order 3. As $g_\infty$ has $3'$-order, centralizes $t$, and is non-central, we see that $g_\infty = z_\infty t_\infty$, where $z_\infty \in Z$ and $t_\infty \in G_0$ has order 2. Similarly, as $g_0$ has $3'$-order and simple spectrum on $\mathcal{H}$, we see that $g_0 = z_0 t_0$, where $z_0 \in Z$ and $t_0 \in G_0$ has order 4. Now, the spectra of elements of order 2 and 4 of $G_0$ on $\mathbb{C}^3$ are $\{-1, -1, 1\}$, respectively $\{\zeta_4, \overline{\zeta_4}, 1\}$ (with counting multiplicities); in particular, $t_\infty$ has to admit both 1 and $-1$ as eigenvalues on $\mathsf{Tame}$. By tensoring $\mathcal{H}$ with $\mathcal{L}_\chi$ for a suitable multiplicative character $\chi$, which does not change the finiteness and irreducibility of $G_{\mathrm{geom}}$, see [**KRLT4**, Lemma 5.10], we may assume that

$$\mathcal{H} = \mathcal{H}yp(\mathbb{1}, \xi_4, \overline{\xi_4}; \gamma, \gamma\xi_2) \tag{4.2.5.1}$$

for some multiplicative character $\gamma$. By [**Ka-ESDE**, 8.12.2(2)], the determinant of $\mathcal{H}$ is $\mathcal{L}_\psi$; in particular, any $p'$-element in $G$ has determinant equal to 1. With this identification (4.2.5.1) of $\mathcal{H}$, $g_\infty$ has spectrum $\alpha, -\alpha, -\alpha$ for some $\alpha \in \mathbb{C}^\times$. Hence $1 = \det(g_\infty) = \alpha^3$, but $3 \nmid \mathsf{o}(g_\infty)$, so $\alpha = 1$. This forces $\gamma \in \{\mathbb{1}, \xi_2\}$, and so $\mathbb{1}$ occurs both "upstairs" and "downstairs" in $\mathcal{H}$, violating the irreducibility of $\mathcal{H}$.

We have shown that $p = 2$, so that $t$ is a scalar multiple of a complex reflection of order 2. As $g_\infty$ has odd order, centralizes $t$, and is non-central, we see that $g_\infty = z_\infty t_\infty$, where $z_\infty \in Z$ and $t_\infty \in G_0$ has order 3. Similarly, as $g_0$ has odd order and simple spectrum on $\mathcal{H}$, we see that $g_0 = z_0 t_0$, where $z_0 \in Z$ and $t_0 \in G_0$ has order 9. Now, the spectra of elements of order 3 and 9 of $G_0$ on $\mathbb{C}^3$ are $\{\alpha, \alpha, \beta\}$ with $\alpha \neq \beta$ and $\alpha^3 = \beta^3 = 1$, respectively $\{\zeta_9^{1,4,7}\}$ or $\{\zeta_9^{2,5,8}\}$. By again tensoring $\mathcal{H}$ with $\mathcal{L}_\chi$ for a suitable multiplicative character $\chi$ and dualizing it if necessary, which do not change the finiteness and irreducibility of $G_{\mathrm{geom}}$, we may assume that

$$\mathcal{H} = \mathcal{H}yp(\xi_9, \xi_9^4, \xi_9^7; \gamma, \gamma\xi_3) \tag{4.2.5.2}$$

for some multiplicative character $\gamma$. By [**Ka-ESDE**, 8.12.2(2)], the determinant of $\mathcal{H}$ is $\mathcal{L}_{\xi_3}\mathcal{L}_\psi$; in particular, any $p'$-element in $G$ has determinant a cubic root of 1. With this identification (4.2.5.2) of $\mathcal{H}$, $g_\infty$ has spectrum $\delta, \delta, \delta\zeta_3$ or $\delta, \delta\zeta_3, \delta\zeta_3$ for some $\delta \in \mathbb{C}^\times$. Hence $1 = \det(g_\infty)^3 = \delta^9$. This forces $\gamma = \xi_9^j$ for some $0 \leq j \leq 8$. Since the "upstairs" and "downstairs" characters of $\mathcal{H}$ do not intersect, $j \neq 1, 4, 7$. Now, if $j = 0, 3, 6$, then choose $\Lambda := \xi_9^{3+j} = \gamma\xi_3$ and $\sigma := \xi_9^{2j}$, so that $\gamma = \sigma^{1/2}$ and $\Lambda\sigma = \xi_9^{3j+3} = \xi_3$. If $j = 2, 5, 8$, then choose $\Lambda := \xi_9^j = \gamma$ and $\sigma := \xi_9^{2j+6}$, so that $\gamma\xi_3 = \sigma^{1/2}$ and $\Lambda\sigma = \xi_9^{3j+6} = \xi_3$. In both cases, the "upstairs" characters in (4.2.5.2) are cubic roots of $\Lambda\sigma$, and the "downstairs" characters are $\Lambda$ and $\sigma^{1/2}$. This shows by [**KRLT3**, Proposition 1.2] that $\mathcal{H}$ is imprimitive, a final contradiction. $\square$

A further note is that the reflection representation of the Weyl group $W(F_4)$ cannot give rise to primitive hypergeometric sheaves with $w = 1$ in any characteristic $p$ (for the reason that every complex reflection in $W(F_4)$ has order 2, forcing $p = 2$ if such a sheaf exists, but no odd-order elements of $W(F_4)$ can have simple spectrum in this representation, contradicting the existence of the element $g_0$). Finally, the Weyl groups of type $B/C$ and $D$ are ruled out in the following lemma:

LEMMA 4.2.6. *Let $n \geq 3$ and let $G$ be the Weyl group of type $B_n$ or $D_n$. Then there is no hypergeometric sheaf $\mathcal{H}$ of type $(n, n-1)$ in any characteristic $p$ with $G_{\mathrm{geom}}$ realizing $G$ in its reflection representation.*

PROOF. Assume the contrary. Note that the complex reflections in $G$ are of order 2, in particular the non-identity element $h$ in the image of $P(\infty)$ in $G$ has order 2. Hence $p = 2$, and we can consider the elements $g_0$ and $g_\infty$ of odd order in $G$ as in the proof of Theorem 4.2.3. Note that $G = E \rtimes S$, where $E$ is a 2-group (of order $2^n$ if $G = W(B_n)$ and of order $2^{n-1}$ if $G = W(D_n)$), and $S \cong \mathsf{S}_n$, acting in its natural permutation representation $\Pi$. Now $E_0 := E\langle g_0 \rangle$ is a subgroup of order $|E| \cdot \mathsf{o}(g_0)$, with $2 \nmid \mathsf{o}(g_0)$. Thus $\langle g_0 \rangle$ is a complement to $E$ in $E_0$, and so by the Schur-Zassenhaus theorem, all such complements are conjugate in $E_0$. As $E_0 = E \rtimes (E_0 \cap S)$, we see that $g_0$ is conjugate to an element $h_0 \in S$. Thus $h_0$ acts on $\Pi$ with simple spectrum, and this is possible only when $h_0$ is an $n$-cycle. It follows that $2 \nmid n$, and the set of "upstairs" characters of $\mathcal{H}$ is $\mathsf{Char}(n)$; in particular, no "downstairs" character is $\mathbb{1}$. Similarly, $g_\infty$ is conjugate to some $h_\infty \in S$, and $g_\infty$ acts on $\mathsf{Tame}$ with $n-1$ distinct eigenvalues, none of which is 1. On the other hand, $h_\infty$ acting on $\Pi$ admits eigenvalue 1, and so it must have $n$ distinct eigenvalues on $\mathcal{H}$. This again implies that $h_\infty$ is an $n$-cycle, and the set of "downstairs" characters of $\mathcal{H}$ is $\mathsf{Char}(n) \smallsetminus \{\mathbb{1}\}$, which intersects the upstairs set nontrivially, violating the irreducibility of $\mathcal{H}$. $\square$

CHAPTER 5

# Tensor induced local systems

## 5.1. 2-tensor induced sheaves

Given a representation $\Phi : G \to \mathrm{GL}(V)$, and an integer $n \geq 2$, we say that $(G, V)$ is *$n$-tensor induced* if $\dim(V)$ is an $n^{\mathrm{th}}$ power $d^n$ with $d \geq 2$ and there exists a tensor factorization of $V$ as

$$V = V_1 \otimes V_2 \otimes \cdots \otimes V_n$$

with each $\dim(V_i) = d$, such that

$$G \leq (\otimes_{i=1}^n \mathrm{GL}(V_i)) \rtimes \mathsf{S}_n,$$

with the symmetric group $\mathsf{S}_n$ acting by permuting the tensor factors $V_i$ transitively.

One says that $(G, V)$ is *not tensor induced* if it is not $n$-tensor induced for any $n \geq 2$.

We have the following obvious but useful lemmas.

Lemma 5.1.1. *Given $(G, V)$ whose dimension $D := \dim(V) \geq 2$ not a power (i.e., not an $n^{\mathrm{th}}$ power for any $n \geq 2$), then $(G, V)$ is not tensor induced.*

Lemma 5.1.2. *Let $V = A \otimes_{\mathbb{C}} B$ be a tensor product of two $\mathbb{C}$-vector spaces $A$ and $B$, both of dimension $\geq 2$. Suppose $h = X \otimes Y$ with $X \in \mathrm{End}(A)$ and $Y \in \mathrm{End}(B)$.*

(i) *If $h$ has almost simple spectrum on $V$, then $X$ has simple spectrum on $A$ and $Y$ has simple spectrum on $B$.*

(ii) *If $h$ has almost regular spectrum on $V$, then $X$ has regular spectrum on $A$ and $Y$ has regular spectrum on $B$.*

Proof. (i) Suppose for instance that $X$ acts as $\begin{pmatrix} \alpha & * \\ 0 & \alpha \end{pmatrix}$ on some 2-dimensional subspace $A_1 \subseteq A$, for some $\alpha \in \mathbb{C}$. We may assume that $Y$ acts as $\begin{pmatrix} \beta & * \\ 0 & \gamma \end{pmatrix}$ on some 2-dimensional subspace $B_1 \subseteq B$, for some $\beta, \gamma \in \mathbb{C}$. If $\beta = \gamma$, then $\alpha\beta$ is the unique eigenvalue for $h$ on $A_1 \otimes B_1$ of dimension 4. If $\beta \neq \gamma$, then both $\alpha\beta$ and $\alpha\gamma$ are eigenvalues of multiplicity 2 for $h$ on $A_1 \otimes B_1$. It follows that $h$ cannot have almost simple spectrum on $V$.

(ii) Assume that $X$ does not have regular spectrum on $A$. Then the Jordan canonical form for $X$ on $A$ contains $\alpha J_a \oplus \alpha J_b$ for some $a, b \geq 1$ and some $\alpha \in \mathbb{C}$, where $J_a$ denotes the Jordan block of size $a$ and with eigenvalue 1. In particular, $X$ has two linearly independent eigenvectors $u_1, u_2$ on $B$, with eigenvalue $\alpha$. Now, if $Y$ has two linearly independent eigenvectors $v_1, v_2$ on $B$, with (not necessarily distinct) eigenvalues $\beta_1, \beta_2$, then $u_1 \otimes v_1, u_2 \otimes v_1$ are $h$-eigenvectors with eigenvalue $\alpha\beta_1$, and $u_1 \otimes v_2, u_2 \otimes v_2$ are $h$-eigenvectors with eigenvalue $\alpha\beta_2$, contradicting the assumption that $h$ has almost regular spectrum. So we may assume that $Y$ is represented by a single Jordan block $J_c$ on $B$, with $c := \dim(B) \geq 2$. Recall, see [**F1**, Theorem VIII.2.7], that

$$J_m \otimes J_n \cong J_{m+n-1} \oplus J_{m+n-3} \oplus \ldots \oplus J_{m-n+1} \tag{5.1.2.1}$$

when $m \geq n \geq 1$. It follows that $h$ has Jordan blocks $\alpha J_{a+c-1}$ and $\alpha J_{b+c-1}$ with $a+c-1, b+c-1 \geq 2$, again a contradiction. □

To deal with the case when $D$ is a power, we begin with recalling the following lemma.

Lemma 5.1.3. [**KT5**, Lemma 3.2] *Let $\mathcal{F}$ be either a Kloosterman sheaf $\mathcal{K}l$ of rank $D \geq 4$ or a hypergeometric sheaf $\mathcal{H}$ of type $(D, m)$ with $D > m > 0$ and $D \geq 4$. Suppose $\mathcal{F}$ is $n$-tensor induced for a given $n \geq 2$. Consider the composite homomorphism*

$$\pi_1(\mathbb{G}_m/\overline{\mathbb{F}_p}) \to (\otimes_{i=1}^n \mathrm{GL}(A_i)) \rtimes \mathsf{S}_n \to \mathsf{S}_n,$$

*obtained by projecting onto the last factor. Suppose we are in either of the following four situations.*

(i) *$\mathcal{F}$ is a Kloosterman sheaf of rank $D \geq 4$.*

(ii) *$\mathcal{F}$ is a hypergeometric sheaf $\mathcal{H}$ of type $(D, m)$ with $D \neq 4$. Denote by $p_0$ the least prime dividing $D$, and suppose we have the inequality $D - m > D/p_0^2$.*

(iii) *$\mathcal{F}$ is a hypergeometric sheaf $\mathcal{H}$ of type $(4, 1)$ and $p$ is odd.*

(iv) *$\mathcal{F}$ is a hypergeometric sheaf $\mathcal{H}$ of type $(4, 2)$ and $p = 2$.*

*Then this composite homomorphism factors through the tame quotient $\pi_1(\mathbb{G}_m/\overline{\mathbb{F}_p})^{\text{tame at } 0,\infty}$, and its image is an $n$-cycle in $\mathsf{S}_n$. Moreover, $n$ is prime to $p$.*

Now we will focus on 2-tensor induced sheaves. In this case, we can do much better.

Lemma 5.1.4. *Suppose that $p = 2$. Let $\mathcal{H}$ be a hypergeometric sheaf of type $(D, m)$ with $w := D - m \geq 2$ and $D > 4$. Then $\mathcal{H}$ is not 2-tensor induced.*

Proof. Suppose $\mathcal{H}$ is 2-tensor induced. The projection of $G_{\text{geom}}$ onto $\mathsf{S}_2$ is a linear character of $\pi_1(\mathbb{G}_m/\overline{\mathbb{F}_2})$ which is tame at 0 and whose $\infty$-slope is $\leq 1/w < 1$ (because $w \geq 2$). Hence (by the integrality of Swan conductors) this character is tame at both 0 and $\infty$. But $\pi_1(\mathbb{G}_m/\overline{\mathbb{F}_2})^{\text{tame at } 0,\infty}$ is a group of profinite order prime to 2, so admits no nontrivial homomorphism to $\mathsf{S}_2$. Thus $\mathcal{H}$ is tensor decomposed, impossible if $D > 4$ by [**KT5**, Lemmas 2.2 and 2.3]. □

Remark 5.1.5. The case when $p = 2$ and $w := D - m = 1$ is dealt with in Theorem 5.2.9.

Lemma 5.1.6. *Suppose that $p$ is odd. Let $\mathcal{H}$ be a hypergeometric sheaf of type $(D, m)$ with $D > m$. Suppose that $\mathcal{H}$ is 2-tensor induced. Consider the composite homomorphism*

$$\pi_1(\mathbb{G}_m/\overline{\mathbb{F}_p}) \to (\otimes_{i=1}^2 \mathrm{GL}(A_i)) \rtimes \mathsf{S}_2 \to \mathsf{S}_2,$$

*obtained by projecting onto the last factor. Then this composite homomorphism factors through the tame quotient $\pi_1(\mathbb{G}_m/\overline{\mathbb{F}_p})^{\text{tame at } 0,\infty}$. If in addition $D > 4$, its image is an 2-cycle in $\mathsf{S}_2$.*

Proof. If $p$ is odd, any homomorphism from $\pi_1(\mathbb{G}_m/\overline{\mathbb{F}_p})$ to a group of order 2 is tame at both 0 and $\infty$. This homomorphism must be nontrivial if $D > 4$, otherwise $\mathcal{H}$ would be tensor decomposed, and this is not the case, cf. [**KT5**, Lemmas 2.2 and 2.3]. □

Corollary 5.1.7. *Suppose that $p$ is odd. Let $\mathcal{H}$ be a hypergeometric sheaf of type $(D, m)$ with $D > m$. Suppose that $\mathcal{H}$ is 2-tensor induced. Then the Kummer pullback $[2]^\star\mathcal{H}$ is tensor decomposable.*

Proof. Immediate from Lemma 5.1.6. □

Lemma 5.1.8. *Suppose $p$ is odd. Let $\mathcal{H}$ be an (irreducible) hypergeometric on $\mathbb{G}_m/\overline{\mathbb{F}_p}$ of type $(D, m)$ with $D > m$. Denote by $W$ the wild part of the $I(\infty)$-representation, and $w := \dim(W) = D - m$. Then we have the following results.*

(i) *If $w$ is odd, then the Kummer pullback $[2]^\star W$ is irreducible (as $I(\infty)$-representation).*
(ii) *If $w$ is even, then $[2]^\star W$ is the direct sum $W_a \oplus W_b$ of two non-isomorphic irreducible $I(\infty)$-representations, each of which is totally wild of dimension $w/2$ with all slopes $2/w$.*

Proof. All slopes of $[2]^\star W$ are $2/w$. If $w$ is odd, then $\gcd(2, w) = 1$, and the asserted irreducibility is [**Ka-GKM**, 1.14 (1)]. If $w$ is even, then we apply [**Ka-GKM**, 1.14 (2)]; write $w = 2n_0p^e$ with $n_0$ prime to $p$ (which is odd) and with $e \geq 0$. Then $W$ is $[2n_0]_\star V$ for an irreducible $I(\infty)$-representation of rank $p^e$ and all slopes $1/p^e$. Thus $W$ is $[2]_\star W_0$ for $W_0 := [n_0]_\star V$. The rank of $W_0$ is $w/2$. and all its slopes are $2/w$. Then

$$[2]^\star W = [2]^\star[2]_\star W_0 = W_0 \oplus [x \mapsto -x]^\star W_0.$$

Because $W_0$ has $\mathsf{Swan}_\infty(W_0) = 1$, it is inequivalent to any nontrivial multiplicative translate of itself, cf. [**Ka-GKM**, 4.1.4]. □

Proposition 5.1.9. *Suppose $p$ is odd. If $D > m > 0$ and $w$ is odd, then $\mathcal{H}$ is not 2-tensor induced.*

Proof. Because $m > 0$, the $I(\infty)$-representation of $\mathcal{H}$ is $T \oplus W$, with $T$ tame and nonzero (because of dimension $m$). Therefore the $I(\infty)$-representation of $[2]^\star\mathcal{H}$ is of the form $T_1 \oplus W_1$ with $T_1$ tame and nonzero, and $W_1$ irreducible and totally wild. By [**KRLT3**, Proposition 10.1], the $I(\infty)$-representation of $[2]^\star\mathcal{H}$ is tensor indecomposable, and hence a fortiori $[2]^\star\mathcal{H}$ is itself tensor indecomposable as a lisse sheaf on $\mathbb{G}_m/\overline{\mathbb{F}_p}$. One knows, by Corollary 5.1.7, that if $\mathcal{H}$ were 2-tensor induced, then $[2]^\star\mathcal{H}$ would be tensor decomposable. □

Proposition 5.1.10. *Suppose $p$ is odd. Suppose $\mathcal{H}$ is primitive, of type $(D, m)$ wth $D > m > 0$, and $w := D - m$ even. Then $\mathcal{H}$ is not 2-tensor induced under any of the following three conditions.*

(i) *$D > 9$.*
(ii) *$D = 9$, $p \neq 3$, and $m \neq 3$.*
(iii) *$D = 9$, $p = 3$, and $m \neq 1$.*

Proof. If $\mathcal{H}$ is 2-tensor induced, then $D$ is a square, $D = d^2$ with $d \geq 3$ (because $D \geq 9$ by hypothesis), and $[2]^\star\mathcal{H}$ is isomorphic to $\mathcal{A}_1 \otimes \mathcal{A}_2$ with $\mathcal{A}_1$ and $\mathcal{A}_2$ local systems on $\mathbb{G}_m/\overline{\mathbb{F}_p}$, each of rank $d$. Passing to the $I(\infty)$-representations, let

$$\mathcal{A}_1|I(\infty) = T_1 \oplus W_1, \quad \mathcal{A}_2|I(\infty) = T_2 \oplus W_2,$$

with the $T_i$ tame and the $W_i$ totally wild $I(\infty)$-representations.

On the other hand, by Lemma 5.1.8, (2), when $w$ is even the $I(\infty)$-representation of $[2]^\star\mathcal{H}$ is of the form

$$\mathcal{H}|I(\infty) = T + W_a + W_b,$$

with $T$ tame and nonzero, and $W_a$ and $W_b$ nonisomorphic irreducible $I(\infty)$-representations, each of dimension $w/2$ with all slopes $2/w$. Thus we have an isomorphism of $I(\infty)$-representations

$$T + W_a + W_b = (T_1 + W_1) \otimes (T_2 + W_2).$$

We next replace each term by its $I(0)$-semisimplification (but don't change their names). We still have this tensor decomposition, simply because for characteristic zero representations, semisimplification commutes with tensor products.

We wish to derive a contradiction. Suppose first that $T_1 \neq 0$. Then

$$T + W_a + W_b = T_1 \otimes W_2 + W_1 \otimes W_2 + \text{other terms}.$$

Because each totally wild irreducible on the left hand side occurs with multiplicity 1, either $W_2 = 0$ or $\dim(T_1) = 1$ and $T_1 \otimes W_2$ is either $W_a$ or $W_b$ or $W_a + W_b$.

If $T_1 \neq 0$ but $W_2 = 0$, then

$$T + W_a + W_b = (T_1 + W_1) \otimes T_2 = T_1 \otimes T_2 + T_2 \otimes W_1.$$

Thus $\dim(T_2) = 1$, and the second factor has dimension 1, not $d$.

If $T_1 \neq 0$ and $W_2 \neq 0$, then as above we have that $\dim(T_1) = 1$ and $T_1 \otimes W_2$ is either $W_a$ or $W_b$ or $W_a + W_b$.

We cannot have $T_1 \otimes W_2 = W_a + W_b$, for then $W_1 \otimes W_2$ is totally tame. This could happen if $W_1 = 0$, but then the first factor $T_1 + W_1$ has dimension 1, not $d$. Thus $W_1$ and $W_2$ are both nonzero, and their tensor product is totally tame. Write the decompositions of $W_1 = \sum_i W_{1,i}$, $W_2 = \sum_j W_{2,j}$ as sums of $I(\infty)$ irreducibles. Then every tensor product $W_{1,i} \otimes W_{2,j}$ is totally tame. By [**KRLT3**, Lemma 10.2], this can only happen when each $W_{1,i}$ and each $W_{2,j}$ has dimension 1, and each $W_{2,j}$ is (a tame character)$\otimes W_{1,i}^\vee$ for every $i, j$. Thus

$$W_1 = (\text{tame } T_3) \otimes W_{1,1}, W_2 = (\text{tame } T_4) \otimes W_{1,1}^\vee.$$

Then we would have

$$T + W_a + W_b = (T_1 + T_3 \otimes W_{1,1}) \otimes (T_2 + T_4 \otimes W_{1,1}^\vee).$$

In this case, each of $W_a, W_b$ is one-dimensional, so both $T_1 \otimes T_4$ and $T_2 \otimes T_3$ are one-dimensional. Then both tensor factors have dimension 2, not $d \geq 3$.

Thus we have $T_1 \otimes W_2$ is either $W_a$ or $W_b$, say $T_1 \otimes W_2 = W_a$. We next claim that $T_2 \neq 0$. For if $T_2 = 0$, then the second factor has dimension $\dim(W_a) = w/2$. But each factor has dimension $d$. Thus $w/2 = d$, and $2/w = 1/d$. The first factor $T_1 + W_1$ has dimension $1+\dim(W_1)$, which is necessarily $d$. This $\dim(W_1) = d-1$. Thus every irreducible constituent of $W_1$ is totally wild of rank $\leq d-1$, and so has all its slopes $\geq 1/(d-1)$. Then every slope of $W_1$ is $\geq 1/(d-1)$. Then in

$$T + W_a + W_b = (T_1 + W_1) \otimes (T_2 + W_2),$$

we have

$$T + W_a + W_b = (T_1 + W_1) \otimes W_2 = W_a + W_1 \otimes W_2.$$

Here $W_a$ and $W_2$ have all slopes $1/d$, but $W_1$ has all slopes $\geq 1/(d-1)$, hence[**Ka-GKM**, 1.3] $W_1 \otimes W_2$ has all slopes $\geq 1/(d-1)$. But every nonzero slope in $T + W_a + W_b$ is $1/d$.

Thus if $T_1 \neq 0$, then also $T_2 \neq 0$, and (by symmetry) both $T_1, T_2$ have dimension 1, and both $W_1, W_2$ are nonzero. Tensoring our putative decomposition by the inverse of the tame character $T_1 \otimes T_2$, we reduce to the case of a decomposition

$$T + W_a + W_b = (\mathbb{1} \oplus W_1) \otimes (\mathbb{1} \oplus W_2).$$

Then both $W_2$ and $W_1$ are nonzero totally wild summands of $T + W_a + W_b$. Therefore we must have, up to interchanging $a, b$, $W_1 = W_a, W_2 = W_b$. But then $W_a \otimes W_b$ is totally tame, which implies [**KRLT3**, Lemma 10.2] that each of $W_a, W_b$ has dimension 1. Then each tensor factor has dimension 2. But each factor has dimension $d \geq 3$, contradiction.

Thus in order to have a tensor decomposition, we must have $T_1 = T_2 = 0$, and

$$T + W_a + W_b = W_1 \otimes W_2$$

is the tensor product of two totally wild $I(\infty)$-representations, each of rank $d$.

We next show that both $W_1$ and $W_2$ must be irreducible as $I(\infty)$-representations. Write

$$W_1 = W_{1,1} + W_{1,2} + \cdots + W_{1,f}$$

as the sum of irreducibles, with $\dim(W_{1,1}) \geq \dim(W_{1,2}) \geq \cdots \geq \dim(W_{1,f})$. Similarly, write

$$W_2 = W_{2,1} + \cdots + W_{2,e}$$

as the sum of irreducibles, with $\dim(W_{2,1}) \geq \cdots \geq \dim(W_{2,e})$.

We first rule out the case when $f \geq 2$ and $\dim(W_{2,1}) = 1$. Then every irreducible constituent of $W_2$ has dimension 1, hence there are $d$ constituents. Let us call them $\mathcal{L}_1, \ldots, \mathcal{L}_d$. If $\dim(W_{1,1}) \geq 2$, then each of the $d$ tensor product $W_{1,1} \otimes \mathcal{L}_j$ is $I(\infty)$-irreducible, and having dimension $\geq 2$ must be totally wild (otherwise it would be totally tame, because the $P(\infty)$ invariants are a subrepresentation, and this can only happen [**KRLT3**, Lemma 10.2] when both factors have dimension one). So we would have at least $d \geq 4$ totally wild irreducible summands in $W_1 \otimes W_2$, contradiction. If both $\dim(W_{1,1}) = 1$ and $\dim(W_{2,1}) = 1$, then also $W_1$ is the sum of $d$ one-dimensional summands, say $\mathcal{N}_1, \ldots, \mathcal{N}_d$. Then of the $d^2$ tensor products $\mathcal{N}_i \otimes \mathcal{L}_j$, precisely two of them are wild (namely the $W_a$ and $W_b$ pieces), and the other $d^2 - 2$ are tame.

This leads to a contradiction, as follows. Renumbering, we may suppose that $\mathcal{N}_1 \otimes \mathcal{L}_1$ is wild. If also $\mathcal{N}_1 \otimes \mathcal{L}_j$ is wild for some $j_0 > 2$, then every $\mathcal{N}_i \otimes \mathcal{L}_j$ with $i \geq 2$ is tame. In particular, taking $i = 2$, every $\mathcal{L}_j$ is

$$\mathcal{N}_2^\vee \otimes (\text{some one} - \text{dimensional tame } T_{2,j}).$$

But for $j \neq 1, j_0$, and there are such $j$, because $d \geq 3$ $\mathcal{N}_1 \otimes \mathcal{L}_j$ is tame, hence $\mathcal{N}_1$ is a tame character times $\mathcal{L}_j^\vee$, i.e. $\mathcal{N}_1$ is a tame character times $\mathcal{N}_2$. Thus all the $\mathcal{N}_i$ are tame twists of each other, all the $\mathcal{L}_j$ are tame twists of the dual, and $W_1 \otimes W_2$ is totally tame, contradiction. If $\mathcal{N}_1 \otimes \mathcal{L}_1$ is wild but $\mathcal{N}_1 \otimes \mathcal{L}_j$ is tame for all $j \geq 2$, a similar argument, left to the reader, leads to the same contradiction.

We now treat the case when $f \geq 2$ and $\dim(W_{2,1}) \geq 2$. In this case, we again get a contradiction if $\dim(W_{1,1}) = 1$. Thus

$$W_1 = W_{1,1} + W_{1,2} + (\text{other terms}), \quad W_2 = W_{2,1} + (\text{other terms}),$$

with both $W_{1,1}, W_{2,1}$ of dimension $\geq 2$. We first show that $W_2$ must be irreducible. Otherwise

$$W_2 = W_{2,1} + W_{2,2} + (\text{other terms}),$$

and so $W_1 \otimes W_2$ contains at least three constituents, namely

$$W_{1,1} \otimes W_{2,1}, \quad W_{1,1} \otimes W_{2,2}, \quad W_{1,2} \otimes W_{2,1},$$

none of which is totally tame, a contradiction.

We now treat the case when $W_2$ is irreducible. Then we have the a priori inequality $f \leq 2$ on the number of irreducible constituents of $W_1$. If $f = 2$, so that \$$W_1 = W_{1,1} + W_{1,2}$, then at least one of $W_{1,1} \otimes W_2$ or $W_{1,2} \otimes W_2$ has a tame part, since $T + W_a + W_b$ has nonzero tame part $T$. Say $W_{1,i} \otimes W_2$ has a tame part. Then for $\chi$ a tame character in this tame part, $W_{1,i} \otimes (W_2 \otimes \overline{\chi}$ contains $\mathbb{1}$, which means that $W_{1,i}$ is the dual of $W_2 \otimes \overline{\chi}$. So in this case already the single component $W_{1,i}$ of $W_1$ has full dimension $d$. Thus $W_1$ is irreducible, and its dual is $W_2 \otimes \overline{\chi}$.

Tensoring with $\chi$, we have the following situation. $W$ is a totally wild ireducible $I(\infty)$-representation of dimension $d \geq 3$, and $\mathrm{End}(W)$ is of the form $T + W_a + W_b$ with a nonzero tame part $T$, and two inequivalent totally wild ireducible $I(\infty)$-representations $W_a$ and $W_b$, each of the same dimension $w/2$, and each with all slopes $2/w$.

Suppose first that $p \nmid d$. The argument of the end of the proof of [**KRLT3**, Lemma 10.2] shows that $\mathrm{End}(W)$ has a tame summand of rank $d$ and $d-1$ totally wild summands, each of rank $d$. If $d \geq 4$, this is a contradiction. If $d = 3$ and $p > 3$, then the tame part of $\mathcal{H}$ has dimension $d = m = 3$, which is a contradiction because we assume $m \neq 3$ when $D = 9$ and $p \neq 3$.

Suppose next that $p|d$. Write $d = n_0 q$ with $p \nmid n_0$ and with $q$ a strictly positive power of $p$. The argument of [**KRLT3**, Lemma 10.2] shows that $\mathrm{End}(W)$ has $n_0$ summands, each of which has a nonzero wild part, and that the tame part of $\mathrm{End}(W)$ has dimension $n_0$. Thus if $n_0 \geq 3$, we have a contradiction.

If $n_0 = 2$, then the argument shows that we have two summands, one of which is totally wild and the other of which has a tame part of dimension 2. In this case, our $\mathcal{H}$ of type $(D = d^2, m)$ has $m = 2$, and hence a wild part of dimension $w = d^2 - 2$. But as $d \geq 3$ by hypothesis, we have $w > (2/3)(D-1)$, i.e., $d^2 - 2 > (2/3)(d^2 - 1)$, i.e., $3d^2 - 6 > 2d^2 - 2$, i.e. $d^2 > 8$, which holds because $d \geq 3$. So in this case, $\mathcal{H}$ satisfies (**S**+), by [**KT5**, Theorem 1.12], and in particular is not 2-tensor induced.

If $n_0 = 1$, then as explained at the end of the proof of [**KRLT3**, Lemma 10.2], $\mathrm{End}(W)$ has a tame part of dimension 1. Thus $m = 1$, our $\mathcal{H}$ is of type $(D, 1)$, with $w = D - 1$, and again we trivially have $D - 1 = w > (2/3)(D-1)$. Except in the case $q = p = 3$, which is the excluded case $(D, m) = (9, 1)$ and $p = 3$, once again $\mathcal{H}$ satisfies (**S**+), by [**KT5**, Theorem 1.12], and in particular is not 2-tensor induced. □

Remark 5.1.11. The excluded cases really can be 2-tensor induced, cf. [**Ka-ESDE**, 10.9.1] for the case $D = 9, m = 3$ and cf. [**Ka-CC**, Theorems 6.3 and 6.5] for the cases $D = 4, m = 0$ or 2.

## 5.2. Tensor induced sheaves: General case

PROPOSITION 5.2.1. *Let $V = V_1 \otimes \ldots \otimes V_n$ be a tensor product of $n \geq 2$ $\mathbb{C}$-vector spaces each of dimension $d \geq 2$. Suppose $g \in \big(\mathrm{GL}(V_1) \otimes \ldots \otimes \mathrm{GL}(V_n)\big) \rtimes \mathsf{S}_n$ permutes the $n$ tensor factors $V_i$ cyclically and that $g$ has almost simple spectrum and finite order on $V$. Then the following statements hold.*

(i) *The action of $g^n$ on $V_1$ has simple spectrum.*
(ii) *If $d \geq 3$ then $n = 2$.*
(iii) *If $d = 2$ then $n \leq 3$.*

PROOF. The automorphism $g$ is, by hypothesis, the composition of isomorphisms $g_i : V_i \to V_{i+1}$ for $i < n$ with an isomorphism $g_n : V_n \to V_1$. If we use $g_1, \ldots, g_{n-1}$ to identify the $V_i$ with each other, then $V$ is $V_1^{\otimes n}$, and $g$ is the map $v_1 \otimes v_2 \otimes \ldots \otimes v_n \mapsto g_n(v_n) \otimes v_1 \otimes \ldots \otimes v_{n-1}$. And the automorphism $g^n$ of $V_1^{\otimes n}$ is $g_n^{\otimes n}$, i.e. $g^n(v_1 \otimes \ldots \otimes v_n) = g_n(v_1) \otimes \ldots \otimes g_n(v_n)$. Since $g$ has finite order on $V_1^{\otimes n}$, so also does $g^n$, and hence $g_n$ has finite order on $V_1$. By "the action of $g^n$ on $V_1$" we mean the action of $g_n$ on $V_1$. Since $\mathsf{o}(g) < \infty$, we can diagonalize the action of $g^n$ on $V_1$: $g^n(e^1_j) = \alpha_j e^1_j$ for a basis $(e^1_1, \ldots, e^1_d)$ of $V_1$ and $\alpha_j \in \mathbb{C}^\times$. Now we can fix bases $(e^i_1, \ldots, e^i_d)$ of $V_i$ such that

$$
\begin{aligned}
g : {} & e^1_1 \mapsto e^2_1 \mapsto e^3_1 \mapsto \ldots \mapsto e^n_1 \mapsto \alpha_1 e^1_1,\\
& e^1_2 \mapsto e^2_2 \mapsto e^3_2 \mapsto \ldots \mapsto e^n_2 \mapsto \alpha_2 e^1_2,\\
& \ldots\\
& e^1_d \mapsto e^2_d \mapsto e^3_d \mapsto \ldots \mapsto e^n_d \mapsto \alpha_d e^1_d.
\end{aligned}
\tag{5.2.1.1}
$$

(a) Note that

$$g(e^1_j \otimes e^2_j \otimes \ldots \otimes e^n_j) = \alpha_i e^1_j \otimes e^2_j \otimes \ldots \otimes e^n_j.$$

Assume now that $\alpha_1 = \alpha_2$. Then by (5.2.1.1), $e^1_j \otimes e^2_j \otimes \ldots \otimes e^n_j$ with $j = 1, 2$ are eigenvectors for $g$ with eigenvalue $\alpha$, and in fact

$$e^1_1 \otimes e^2_2 \otimes e^3_2 \otimes \ldots \otimes e^n_2 + e^1_2 \otimes e^2_1 \otimes e^3_2 \otimes \ldots \otimes e^n_2 + \ldots + e^1_2 \otimes e^2_2 \otimes \ldots \otimes e^{n-1}_2 \otimes e^n_1$$

is a third such an eigenvector, with all three being linearly independent. Thus $\alpha$ is an eigenvalue of $g$ with multiplicity at least 3, a contradiction. Hence (i) follows.

(b) Using (5.2.1.1), we can see that

$$g^n\big(e^1_{j_1} \otimes e^2_{j_2} \otimes \ldots \otimes e^n_{j_n}\big) = \alpha_{j_1}\alpha_{j_2} \ldots \alpha_{j_n} e^1_{j_1} \otimes e^2_{j_2} \otimes \ldots \otimes e^n_{j_n}.$$

Thus, every eigenvalue of $g^n$ on $V$ is of the form $\beta = \alpha_{j_1}\alpha_{j_2} \ldots \alpha_{j_n}$ with $1 \leq j_i \leq d$. Hence, the number $N$ of distinct eigenvalues (without counting multiplicities) of $g^n$ on $V$ is at most the number of ordered $d$-tuples $(k_1, k_2, \ldots, k_d)$, where $k_j$, $1 \leq j \leq d$, is the number of indices $i$, $1 \leq i \leq n$, such that $j_i = j$. Thus

$$N \leq N(n, d),$$

where $N(n, d)$ the number of ordered $d$-tuples $(k_1, k_2, \ldots, k_d)$, where $k_j \in \mathbb{Z}_{\geq 0}$ and $\sum_{j=1}^d k_j = n$. We now prove by induction on $d \geq 1$ that

$$N(n, d) = \binom{n + d - 1}{n}. \tag{5.2.1.2}$$

Clearly, $N(n,1)=1$, proving the induction base $d=1$. To prove the induction step from $d-1$ to $d$, we proceed by another induction on $n \geq 1$, with the obvious induction base $N(1,d)=d=\binom{d}{1}$. By counting tuples with a fixed value $0 \leq k_1 \leq n$ (and noting there is exactly one tuple with $k_1 = n$) we get

$$N(n,d) = 1 + N(1,d-1) + \ldots + N(n-1,d-1) + N(n,d-1)$$

and similarly

$$N(n-1,d) = 1 + N(1,d-1) + \ldots + N(n-1,d-1).$$

It follows that $N(n,d) = N(n-1,d) + N(n,d-1)$. By the two induction hypotheses, we have

$$N(n,d) = \binom{n+d-2}{n-1} + \binom{n+d-2}{n} = \binom{n+d-2}{d-1} + \binom{n+d-2}{d-2} = \binom{n+d-1}{d-1} = \binom{n+d-1}{n},$$

completing the proof of (5.2.1.2).

Since each eigenvalue of $g$ on $V$ is an $n^{\text{th}}$ root of some eigenvalue of $g^n$, we have shown that $g$ has at most $n\binom{n+d-1}{n}$ distinct eigenvalues on $V$. As $g$ has almost simple spectrum on $V$, it follows that

$$d^n - 1 = \dim(V) - 1 \leq n\binom{n+d-1}{n}. \tag{5.2.1.3}$$

Suppose now that $d \geq 4$ and $n \geq 3$. Then $3\binom{d+2}{3} = d(d+1)(d+2)/2 \leq d^3 - d$. In general, if $j \geq 2$, then $(d+j)/j < d$, whence

$$n\binom{n+d-1}{n} = \frac{d(d+1)\ldots(d+n-1)}{1\cdot 2\ldots\cdot(n-1)} = 3\binom{d+2}{3}\cdot\prod_{j=3}^{n-1}\frac{d+j}{j} \leq (d^3-d)d^{n-3} < d^n - 3,$$

violating (5.2.1.3).

We have shown that $n=2$ if $d \geq 4$. If $d=3$, then (5.2.1.3) implies that

$$3^n - 1 \leq n(n+1)(n+2)/2,$$

and so $n \leq 3$. If $d=2$, then (5.2.1.3) implies that $2^n - 1 \leq n(n+1)$, and so $n \leq 4$.

(c) Assume now that $d=n=3$. Using (5.2.1.1), we see that

$$g: e^1_1 \otimes e^2_2 \otimes e^3_3 \mapsto \alpha_3 e^1_3 \otimes e^2_1 \otimes e^3_2 \mapsto \alpha_2\alpha_3 e^1_2 \otimes e^2_3 \otimes e^3_1 \mapsto \alpha_1\alpha_2\alpha_3 e^1_1 \otimes e^2_2 \otimes e^3_3.$$

Thus $g$ stabilizes the 3-dimensional subspace

$$\langle e^1_1 \otimes e^2_2 \otimes e^3_3,\ e^1_3 \otimes e^2_1 \otimes e^3_2,\ e^1_2 \otimes e^2_3 \otimes e^3_1 \rangle_{\mathbb{C}}$$

and admits all the 3 cubic roots of $\alpha_1\alpha_2\alpha_3$ as eigenvalues on this subspace. The same is however also true for the subspace

$$\langle e^1_1 \otimes e^2_3 \otimes e^3_2,\ e^1_2 \otimes e^2_1 \otimes e^3_3,\ e^1_3 \otimes e^2_2 \otimes e^3_1 \rangle_{\mathbb{C}},$$

contradicting the assumption that $g$ has almost simple spectrum. Hence $n=2$ if $d=3$, proving (ii).

Next we consider the case $d=2$ and $n=4$. Again using (5.2.1.1), we see that

$$g: e^1_1 \otimes e^2_2 \otimes e^3_1 \otimes e^4_2 \mapsto \alpha_2 e^1_2 \otimes e^2_1 \otimes e^3_2 \otimes e^4_1 \mapsto \alpha_1\alpha_2 e^1_1 \otimes e^2_2 \otimes e^3_1 \otimes e^4_2.$$

Thus $g$ stabilizes the 2-dimensional subspace

$$\langle e_1^1 \otimes e_2^2 \otimes e_1^3 \otimes e_2^4,\ e_2^1 \otimes e_1^2 \otimes e_2^3 \otimes e_1^4 \rangle_{\mathbb{C}}$$

and has both square roots of $\alpha_1\alpha_2$ as eigenvalues on this subspace. On the other hand, $g$ also maps

$$e_1^1{\otimes}e_2^2{\otimes}e_2^3{\otimes}e_1^4 \mapsto \alpha_1 e_1^1{\otimes}e_1^2{\otimes}e_2^3{\otimes}e_2^4 \mapsto \alpha_1\alpha_2 e_2^1{\otimes}e_1^2{\otimes}e_1^3{\otimes}e_2^4 \mapsto \alpha_1\alpha_2^2 e_2^1{\otimes}e_2^2{\otimes}e_1^3{\otimes}e_1^4 \mapsto \alpha_1^2\alpha_2^2 e_1^1{\otimes}e_2^2{\otimes}e_2^3{\otimes}e_1^4.$$

Thus $g$ stabilizes the 4-dimensional subspace

$$\langle e_1^1 \otimes e_2^2 \otimes e_2^3 \otimes e_1^4,\ e_1^1 \otimes e_1^2 \otimes e_2^3 \otimes e_2^4,\ e_2^1 \otimes e_1^2 \otimes e_1^3 \otimes e_2^4,\ e_2^1 \otimes e_2^2 \otimes e_1^3 \otimes e_1^4 \rangle_{\mathbb{C}}$$

and has all four quartic roots of $\alpha_1^2\alpha_2^2$ as eigenvalues on this subspace. In particular, each of $\sqrt{\alpha_1\alpha_2}$ and $-\sqrt{\alpha_1\alpha_2}$ has multiplicity $\geq 2$ as $g$-eigenvalue on $V$, again a contradiction. Hence $n \leq 3$ if $d = 2$, establishing (iii). □

Lemma 5.2.2. *Let $V = V_1 \otimes \ldots \otimes V_n$ be a tensor product of $n = a + b$ $\mathbb{C}$-vector spaces each of dimension $d \geq 2$, with $a, b \in \mathbb{Z}_{\geq 2}$. Suppose $g \in \big(\mathrm{GL}(V_1) \otimes \ldots \otimes \mathrm{GL}(V_n)\big) \rtimes \mathsf{S}_n$ permutes the first $a$ tensor factors $V_i$, $1 \leq i \leq a$, cyclically, and the next $b$ tensor factors $V_i$, $a + 1 \leq i \leq a + b$, cyclically, and that $g$ has almost simple spectrum and finite order on $V$. Then $(a, b) \neq (2, 2)$ and $(a, b) \neq (3, 3)$.*

Proof. Assume that $(a, b) = (2, 2)$. Arguing as in the proof of Proposition 5.2.1, but changing the notation for simplicity, we may assume that in some bases $(e_i \mid 1 \leq i \leq d)$ for $V_1$, $(f_i \mid 1 \leq i \leq d)$ for $V_2$, $(g_i \mid 1 \leq i \leq d)$ for $V_3$, and $(h_i \mid 1 \leq i \leq d)$ for $V_4$, we have

$$g : e_i \mapsto f_i \mapsto \alpha_i e_i,\ g_i \mapsto h_i \mapsto \beta_i g_i$$

for some $\alpha_i, \beta_i \in \mathbb{C}^\times$. It follows by inspecting the action of $g$ on $\langle e_1 {\otimes} f_2, e_2 {\otimes} f_1 \rangle_{\mathbb{C}}$ that $g$ admits both $\gamma := \sqrt{\alpha_1\alpha_2}$ and $-\gamma$ as eigenvalues on $V_1 \otimes V_2$. Similarly, $g$ admits both $\delta := \sqrt{\beta_1\beta_2}$ and $-\delta$ as eigenvalues on $V_3 \otimes V_4$. Since $\gamma\delta = (-\gamma)(-\delta)$ and $(-\gamma)\delta = \gamma(-\delta)$, it follows that both $\gamma\delta$ and $-\gamma\delta$ are eigenvalues with multiplicity $\geq 2$ for $g$ on $V$, a contradiction.

Assume now that $(a, b) = (3, 3)$. As above, we may assume that in some bases $(e_i \mid 1 \leq i \leq d)$ for $V_1$, $(f_i \mid 1 \leq i \leq d)$ for $V_2$, $(g_i \mid 1 \leq i \leq d)$ for $V_3$, we have

$$g : e_i \mapsto f_i \mapsto g_i \mapsto \alpha_i e_i$$

for some $\alpha_i \in \mathbb{C}^\times$. It follows by inspecting the action of $g$ on

$$\langle e_1 \otimes f_1 \otimes g_2, e_2 \otimes f_1 \otimes g_1, e_1 \otimes f_2 \otimes g_1 \rangle_{\mathbb{C}}$$

that $g$ admits all three roots $\gamma, \gamma\zeta_3, \gamma\zeta_3^2$ of $\gamma^3 := \alpha_1^2\alpha_2$ as eigenvalues on $V_1 {\otimes} V_2 {\otimes} V_3$. Similarly, $g$ admits all $\delta, \delta\zeta_3, \delta\zeta_3^2$ for some $\delta \in \mathbb{C}^\times$ as eigenvalues on $V_4 \otimes V_5 \otimes V_6$. Since

$$\gamma\delta = (\gamma\zeta_3)(\delta\zeta_3^2) = (\gamma\zeta_3^2)(\delta\zeta_3),$$

it follows that $\gamma\delta$ is an eigenvalue with multiplicity $\geq 3$ for $g$ on $V$, again a contradiction. □

Proposition 5.2.3. *Let $V = V_1 \otimes \ldots \otimes V_n$ be a tensor product of $n \geq 2$ $\mathbb{C}$-vector spaces each of dimension $d \geq 2$. Suppose $g \in \big(\mathrm{GL}(V_1) \otimes \ldots \otimes \mathrm{GL}(V_n)\big) \rtimes \mathsf{S}_n$ induces a nontrivial permutation $\pi$ on the set of $n$ tensor factors $V_i$ and that $g$ has almost simple spectrum and finite order on $V$. Then the following statements hold.*

(i) *Suppose $d \geq 3$. Then $\pi$ is a 2-cycle. Suppose that $g$ interchanges $V_1$ and $V_2$. Then the action $h$ of $g^2$ on $V_1$* (which is defined uniquely up to a scalar) *has simple spectrum. Moreover, if $n \geq 3$ or if $g$ has simple spectrum on $V$, then $\bar{\mathsf{o}}(h) \geq d^2/2$.*

(ii) *If $d = 2$, then $\pi$ is either a 2-cycle, a 3-cycle, or a disjoint product of a 2-cycle and a 3-cycle.*

Proof. Write $\pi = \sigma_1\sigma_2 \ldots \sigma_l$ as a product of disjoint cycles of non-increasing lengths

$$k_1 \geq k_2 \geq \ldots \geq k_l \geq 1.$$

Suitably conjugating $g$ in $\mathrm{GL}(V)$, we may assume that

$$\pi = (1, 2, \ldots, k_1)(k_1 + 1, k_1 + 2, \ldots, k_1 + k_2) \ldots \big(\sum_{i=1}^{l-1} k_1 + 1, \sum_{i=1}^{l-1} k_2 + 2, \ldots, n\big).$$

By Lemma 5.1.2(i), $g$ has almost simple spectrum on $V_1 \otimes V_2 \otimes \ldots \otimes V_{k_1}$, $V_1 \otimes V_2 \otimes \ldots \otimes V_{k_1+k_2}$ (if $l \geq 2$), and on $V_1 \otimes V_2 \otimes \ldots \otimes V_{k_1+k_2+k_3}$ if $l \geq 3$. Applying Proposition 5.2.1 to the action of $g$ on $V_1 \otimes V_2 \otimes \ldots \otimes V_{k_1}$, we see that $k_1 = 2$ if $d \geq 3$ and $k_1 \leq 3$ if $d = 2$.

Suppose $d = 2$ but $l \geq 2$ and $k_2 \geq 2$. By applying Lemma 5.2.2 to the action of $g$ on $V_1 \otimes V_2 \otimes \ldots \otimes V_{k_1+k_2}$, we see that $(k_1, k_2) = (3, 2)$. Again applying Lemma 5.2.2, we conclude that $k_3 = 1$ if $l \geq 3$. Hence (ii) follows.

Assume now that $d \geq 3$. If $l \geq 2$, then by applying Lemma 5.2.2 to the action of $g$ on $V_1 \otimes V_2 \otimes \ldots \otimes V_{k_1+k_2}$, we see that $(k_1, k_2) = (2, 1)$. Thus $\pi = (1, 2)$ is a 2-cycle. By Proposition 5.2.1(i), $h$ has simple spectrum on $V_1$. To bound $m := \bar{\mathsf{o}}(h)$, we follow the proof of Proposition 5.2.1 and consider an eigenbasis $(e_1, \ldots, e_d)$ of $g^2$ on $V_1$ and the basis $(f_1 = g(e_1), \ldots, f_d := g(e_d))$ of $V_2$. By the choice of $m$, $g^{2m} = \gamma \cdot \mathrm{Id}$ on $V_1$ for some $\gamma \in \mathbb{C}^\times$. Now

$$g^{2m}(f_i) = g^{2m}\big(g(e_i)\big) = g\big(g^{2m}(e_i)\big) = g(\gamma e_i) = \gamma f_i$$

for all $i$, i.e. $g^{2m} = \gamma \cdot \mathrm{Id}$ on $V_2$ as well. Thus $g^{2m} = \gamma^2 \cdot \mathrm{Id}$ on $V_1 \otimes V_2$, and so $\epsilon^{2m} = \gamma^2$ for all eigenvalues $\epsilon$ of $g$ on $V_1 \otimes V_2$. However, by Lemma 5.1.2, $g$ has simple spectrum on $V_1 \otimes V_2$. It follows that $d^2 = \dim(V_1 \otimes V_2) \leq 2m$, as stated in (i). □

Proposition 5.2.4. *Let $V = V_1 \otimes \ldots \otimes V_n$ be a tensor product of $n \geq 2$ $\mathbb{C}$-vector spaces each of dimension $d \geq 2$. Suppose $g \in \big(\mathrm{GL}(V_1) \otimes \ldots \otimes \mathrm{GL}(V_n)\big) \rtimes \mathsf{S}_n$ permutes the $n$ tensor factors $V_i$ cyclically and that $g$ has almost regular spectrum on $V$. Then the following statements hold.*

(i) *The action of $g^n$ on $V_1$ has regular spectrum.*

(ii) *$n = 2$ if $d \geq 3$, and $n \leq 3$ if $d = 2$.*

Proof. (i) Assume that $g^n$ does not have regular spectrum on $V_1$. Then we can find linearly independent eigenvectors $e_1^1$ and $e_2^1$ for $g^n$ on $V_1$, for the same eigenvalue $\alpha \in \mathbb{C}$. The arguments in (a) of the proof of Proposition 5.2.1 show that $\dim \mathrm{Ker}(g - \alpha \cdot \mathrm{Id}) \geq 3$. Hence the statement follows.

(ii) Replacing $g$ by a scalar multiple, we may assume that $g^n$ is unipotent on each $V_i$, and hence acts as the single Jordan block $J_d$ (with eigenvalue 1) on each of them by (i). In general, if $J_a$ denotes the Jordan block of size $a$ with eigenvalue 1, then $J_a \otimes J_b$ is conjugate to

$$J_{a+b-1} \oplus J_{a+b-3} \oplus \ldots \oplus J_{a-b+1},$$

when $a \geq b \geq 1$, see [**F1**, Theorem VIII.2.7]. An induction on $n$ shows that the Jordan canonical form of $g^n$ on $V$ consists of one block $J_{n(d-1)+1}$ and some other blocks of size at most $n(d-1)-1$.

As $g^n$ is unipotent, all distinct eigenvalues $\epsilon_i$, $1 \leq i \leq l$, of $g$ on $V$ are $n^{\text{th}}$ roots of unity. But $g$ has almost regular spectrum, so, aside from possibly one additional Jordan block of size 1, each of these eigenvalues $\epsilon_i$ gives rise to a unique Jordan block of $g$, say of size $d_i$ and with eigenvalue $\epsilon_i$, which then yields a Jordan block of same size (but with eigenvalue 1) for $g^n$. By the above analysis, one of these blocks has size $n(d-1)+1$, and all others have size $\leq n(d-1)-1$, and possibly one extra of size 1. It follows that

$$\begin{aligned} d^n = \sum_{i=1}^{l} d_i &\leq (n(d-1)+1)+(l-1)(n(d-1)-1)+1 \\ &\leq (n(d-1)+1)+(n-1)(n(d-1)-1)+1 = n^2(d-1)+3-n. \end{aligned}$$

Hence $n=2$ if $d \geq 3$, and $n \leq 3$ if $d=2$.

Now we consider the general case, and let $e$ denote the number of distinct eigenvalues of $g^{k_1}$ on $V_1$ (without counting multiplicities). If $e \geq 3$, then $n=2$ by Proposition 5.2.1 (applied to $g$ on $U^{\otimes n}$, where $U \subseteq V_1$ is spanned by three eigenvectors for three distinct eigenvalues of $g^n$). If $e=1$, then we are done by the unipotent case.

Consider the case $e=2$. If $d=2$, then $g^n$ has simple spectrum on $V_1$, and so $n \leq 3$ by Proposition 5.2.1. Suppose now that $d \geq 3$ but $n \geq 3$. As $e=2$, the largest size of Jordan blocks of $g^n$ on $V_1$ is at most $d-1$, and $g^n$ has two distinct eigenvalues $\alpha \neq \beta$ on $V_1$. Hence, arguing as above, $g^n$ has on $V$ at most one Jordan block of size $n(d-2)+1$ and all others of size at most $n(d-2)-1$. Up to a scalar, the eigenvalues of $g^n$ on $V$ are $\alpha^{n-i}\beta^i$, $0 \leq i \leq n$, a total of at most $n+1$ distinct eigenvalues. Thus $g$ has at most $n(n+1)$ eigenvalues on $V$. As $g$ has almost regular spectrum on $V$, they lead to at most $n(n+1)$ Jordan blocks for $g^n$, and possibly one extra of size 1. We now have that

$$d^n \leq n(n+1)(n(d-2)-1)+2+1,$$

which is impossible unless $(n,d)=(3,3)$. In this remaining case, $g^3$ has 3 Jordan blocks of size 3 with eigenvalue $\alpha\beta^2$ and 3 Jordan blocks of size 1 with eigenvalue $\alpha\beta^2$, if we assume that $g^3$ acts on $V_1$ as $\alpha J_1 \oplus \beta J_2$. These six Jordan blocks of $g^3$ come from six Jordan blocks of $g$ with eigenvalues among the three cubic roots of $\alpha\beta^2$. Thus either some such cubic root leads to at least 3 Jordan blocks of $g$, or each of them leads to two Jordan blocks. Both of these possibilities contradict the assumption that $g$ has almost regular spectrum on $V$. □

LEMMA 5.2.5. *Let $V = V_1 \otimes \ldots \otimes V_n$ be a tensor product of $n = a+b$ $\mathbb{C}$-vector spaces each of dimension $d \geq 2$, with $a, b \in \mathbb{Z}_{\geq 2}$. Suppose $g \in \big(\mathrm{GL}(V_1) \otimes \ldots \otimes \mathrm{GL}(V_n)\big) \rtimes \mathsf{S}_n$ permutes the first $a$ tensor factors $V_i$, $1 \leq i \leq a$, cyclically, and the next $b$ tensor factors $V_i$, $a+1 \leq i \leq a+b$, cyclically, and that $g$ has almost regular spectrum on $V$. Then $(a,b) \neq (2,2)$ and $(a,b) \neq (3,3)$.*

PROOF. (i) Assume that $(a,b)=(2,2)$. We may assume that in some bases $(e_i \mid 1 \leq i \leq d)$ for $V_1$ and $(f_i \mid 1 \leq i \leq d)$ for $V_2$ we have

$$g : e_1 \mapsto f_1 \mapsto \alpha_1 e_1,\ e_2 \mapsto f_2 \mapsto \alpha_2 e_2$$

for some $\alpha_1 \neq \alpha_2 \in \mathbb{C}^\times$, or

$$g : e_1 \mapsto f_1 \mapsto \alpha_1 e_1,\ e_2 \mapsto f_2 \mapsto \alpha_1(e_1 + e_2)$$

for some $\alpha_1 \in \mathbb{C}^\times$. As shown in the proof of Lemma 5.2.2, in the former case $g$ admits both $\gamma := \sqrt{\alpha_1\alpha_2}$ and $-\gamma$ as eigenvalues on $V_1 \otimes V_2$. Direct computation shows that in the latter case $g$ admits both $\gamma := \alpha_1$ and $-\gamma$ as eigenvalues on $V_1 \otimes V_2$. Similarly, there is some $\delta \in \mathbb{C}^\times$ such that $g$ admits both $\delta$ and $-\delta$ as eigenvalues on $V_3 \otimes V_4$. Since $\gamma\delta = (-\gamma)(-\delta)$ and $\gamma(-\delta) = (-\gamma)\delta$, it follows that $\dim \mathrm{Ker}(g - \gamma\delta \cdot \mathrm{Id}) \geq 2$ and $\dim \mathrm{Ker}(g + \gamma\delta \cdot \mathrm{Id}) \geq 2$, a contradiction.

(ii) Assume now that $(a, b) = (3, 3)$. As above, we may assume that in some bases $(e_i \mid 1 \leq i \leq d)$ for $V_1$, $(f_i \mid 1 \leq i \leq d)$ for $V_2$, $(g_i \mid 1 \leq i \leq d)$ for $V_3$, we have

$$g : e_1 \mapsto f_1 \mapsto g_1 \mapsto \alpha_1 e_1,\ e_2 \mapsto f_2 \mapsto g_2 \mapsto \alpha_2 e_2$$

for some $\alpha_1 \neq \alpha_2 \in \mathbb{C}^\times$, or

$$g : e_1 \mapsto f_1 \mapsto g_1 \mapsto \alpha_1 e_1,\ e_2 \mapsto f_2 \mapsto g_2 \mapsto \alpha_1(e_1 + e_2)$$

for some $\alpha_1 \in \mathbb{C}^\times$. As shown in the proof of Lemma 5.2.2, in the former case $g$ admits all three roots $\gamma, \gamma\zeta_3, \gamma\zeta_3^2$ of $\gamma^3 := \alpha_1^2\alpha_2$ as eigenvalues on $V_1 \otimes V_2 \otimes V_3$. Direct computation shows that in the latter case $g$ admits all three roots $\gamma, \gamma\zeta_3, \gamma\zeta_3^2$ of $\gamma^3 := \alpha_1^3$ as eigenvalues on $V_1 \otimes V_2 \otimes V_3$. Similarly, there exists some $\delta \in \mathbb{C}^\times$ such that $g$ admits all $\delta, \delta\zeta_3, \delta\zeta_3^2$ as eigenvalues on $V_4 \otimes V_5 \otimes V_6$. Since $\gamma\delta = (\gamma\zeta_3)(\delta\zeta_3^2) = (\gamma\zeta_3^2)(\delta\zeta_3)$, it follows that $\dim \mathrm{Ker}(g - \gamma\delta \cdot \mathrm{Id}) \geq 3$, again a contradiction. □

Proposition 5.2.6. *Let $V = V_1 \otimes \ldots \otimes V_n$ be a tensor product of $n \geq 2$ $\mathbb{C}$-vector spaces each of dimension $d \geq 2$. Suppose $g \in \big(\mathrm{GL}(V_1) \otimes \ldots \otimes \mathrm{GL}(V_n)\big) \rtimes \mathsf{S}_n$ induces a nontrivial permutation $\pi$ on the set of $n$ tensor factors $V_i$ and that $g$ has almost regular spectrum on $V$. Then the following statements hold.*

(i) *Suppose $d \geq 3$. Then $\pi$ is a 2-cycle.*

(ii) *If $d = 2$, then $\pi$ is either a 2-cycle, a 3-cycle, or a disjoint product of a 2-cycle and a 3-cycle.*

Proof. (a) Write $\pi = \sigma_1\sigma_2 \ldots \sigma_l$ as a product of disjoint cycles of non-increasing lengths

$$k_1 \geq k_2 \geq \ldots \geq k_l \geq 1.$$

Suitably conjugating $g$ in $\mathrm{GL}(V)$, we may assume that

$$\pi = (1, 2, \ldots, k_1)(k_1 + 1, k_1 + 2, \ldots, k_1 + k_2) \ldots \Big(\sum_{i=1}^{l-1} k_1 + 1, \sum_{i=1}^{l-1} k_2 + 2, \ldots, n\Big).$$

By Lemma 5.1.2(ii), $g$ has almost regular spectrum on $V_1 \otimes V_2 \otimes \ldots \otimes V_{k_1}$, $V_1 \otimes V_2 \otimes \ldots \otimes V_{k_1+k_2}$ (if $l \geq 2$), and on $V_1 \otimes V_2 \otimes \ldots \otimes V_{k_1+k_2+k_3}$ if $l \geq 3$.

Applying Proposition 5.2.4 to the action of $g$ on $V_1 \otimes V_2 \otimes \ldots \otimes V_{k_1}$, we see that $k_1 = 2$ if $d \geq 3$ and $k_1 \leq 3$ if $d = 2$.

Suppose $d = 2$ but $l \geq 2$ and $k_2 \geq 2$. By applying Lemma 5.2.5 to the action of $g$ on $V_1 \otimes V_2 \otimes \ldots \otimes V_{k_1+k_2}$, we see that $(k_1, k_2) = (3, 2)$. Again applying Lemma 5.2.5, we conclude that $k_3 = 1$ if $l \geq 3$. Hence (ii) follows.

Assume now that $d \geq 3$. If $l \geq 2$, then by applying Lemma 5.2.5 to the action of $g$ on $V_1 \otimes V_2 \otimes \ldots \otimes V_{k_1+k_2}$, we see that $(k_1, k_2) = (2, 1)$. Thus $\pi = (1, 2)$ is a 2-cycle. □

PROPOSITION 5.2.7. *Let $\mathcal{H}$ be a hypergeometric sheaf in characteristic $p$ of type $(D, m)$ with $D - m \geq 1$. Suppose that $\mathcal{H}$ satisfies* $(\mathbf{S}-)$ *but is $n$-tensor induced:*

$$G_{\mathrm{geom}} \leq \big(\mathrm{GL}(V_1) \otimes \mathrm{GL}(V_2) \otimes \ldots \otimes \mathrm{GL}(V_n)\big) \rtimes \mathsf{S}_n$$

*with $d := \dim(V_i) \geq 2$ and $n \geq 2$. Then one of the following statements holds.*

(a) *The action of $G$ on $\{V_1, V_2, \ldots, V_n\}$ induces a subgroup $C_n \leq \mathsf{S}_n$, generated by an $n$-cycle, and furthermore $p \nmid n$.*

(b) *$p = 2$ and $d = 2$. Furthermore, $D = 4$ if $D - m = 1$ or if $m > 0$.*

PROOF. Let $\varphi$ denote the character of the representation $\Phi : G_{\mathrm{geom}} \to \mathrm{GL}(V)$ realized by $\mathcal{H}$, and let $Q$ denote the image in $G_{\mathrm{geom}}$ of $P(\infty)$; note that $Q$ is finite. Also let $G_0 \lhd G$ consist of all elements in $G := G_{\mathrm{geom}}$ that fix every tensor factor $V_i$. Then $G_0$ is Zariski closed.

(i) First we consider the case $Q \leq G_0$. Then the Zariski closure of the normal closure of $Q$ in $G$ is contained in $G_0$, and so $G/G_0$ is a finite cyclic $p'$-group by Theorem 1.2.3. On the other hand, $G/G_0$ is a transitive subgroup of $\mathsf{S}_n$, since $(G, V)$ is tensor indecomposable. Hence, $G/G_0$ is generated by an $n$-cycle and $p \nmid n$, as stated in (a).

(ii) We may now assume that $Q_0 := Q \cap G_0$ is a proper subgroup of $Q$. Consider any element $x \in Q \smallsetminus Q_0$. Then the $p$-element $x$ induces a nontrivial permutation of $p$-power order of $\mathsf{S}_n$, which then has at least one orbit of length $\geq p$ on $\{V_1, V_2, \ldots, V_n\}$. The formula [**GI**, 2.1] for tensor induced characters implies that $|\varphi(x)| \leq D/d^{p-1}$.

Assume in addition that $D - m = 1$. Then $x$ acts trivially on $\mathsf{Tame}$ of dimension $D - 1$, whence

$$d^{n-1} \geq D/d^{p-1} \geq |\varphi(x)| \geq D - 2 = d^n - 2,$$

and so $D = 4$ and $p = 2$, as stated in (b).

Now we may assume that $D - m \geq 2$. Using the obvious estimates $|\varphi(y)| \leq D$ for $y \in Q_0$ and $|Q_0| \leq |Q|/p$, for the dimension $m$ of the tame part $\mathsf{Tame}$ we have

$$\begin{aligned} m = [\varphi|_Q, 1_Q]_Q &= \Big|\frac{1}{|Q|}\sum_{x \in Q} \varphi(x)\Big| \\ &\leq \frac{D|Q_0| + Dd^{1-p}(|Q| - |Q_0|)}{|Q|} \qquad (5.2.7.1) \\ &< \frac{D}{|Q/Q_0|} + \frac{D}{d^{p-1}} \leq D(1/p + d^{1-p}), \end{aligned}$$

and thus $m/D < 1/p + d^{1-p}$.

• If $p \geq 3$, then $m/D < 1/3 + 1/4 < 3/4$.

• Suppose $p = 2$. Then $m/D < 1/2 + 1/4 = 3/4$ when $d \geq 4$, $m/D < 1/2 + 1/3 = 5/6$ when $d = 3$, and $m/D < 1/4 + 1/2 = 3/4$ when $|Q/Q_0| \geq 4$.

• Finally, assume that $p = 2 = d = |Q/Q_0|$, $D > 4$, and $m > 0$. In this case, all elements $x \in Q \smallsetminus Q_0$ induce the same permutation $\sigma$ of order 2 on the set $\{V_1, V_2, \ldots, V_n\}$. On the other hand, by [**KRLT3**, Corollary 10.4], $I(\infty)$ does not preserve any nontrivial tensor decomposition of $V$, and so it must induce a transitive subgroup of $\mathsf{S}_n$ while permuting $V_1, V_2, \ldots, V_n$. As $P(\infty) \lhd I(\infty)$ and $\mathsf{o}(\sigma) = 2$, it follows that $\sigma$ is a product of disjoint cycles of the same length 2. The number of $\sigma$-orbits on $\{V_1, V_2, \ldots, V_n\}$ is $n/2 \geq 2$ since $D = 2^n > 4$. Hence the formula for tensor induced characters implies that $|\varphi(x)| \leq D/d^2$ for all $x \in Q \smallsetminus Q_0$, and the estimates in (5.2.7.1) again imply that $m/D < 1/|Q/Q_0| + 1/d^2 = 3/4$.

In all three cases, $w = D - m > D/p_0^2$, where $p_0$ is the smallest prime divisor of $D$. Hence (a) holds by Lemma 5.1.3. □

Corollary 5.2.8. *Let $\mathcal{H}$ be a hypergeometric sheaf in characteristic $p$ of type $(D, m)$ with $D - m \geq 2$. Suppose that $\mathcal{H}$ satisfies ($\mathbf{S}-$) but is $n$-tensor induced:*

$$G_{\mathrm{geom}} \leq \big(\mathrm{GL}(V_1) \otimes \mathrm{GL}(V_2) \otimes \ldots \otimes \mathrm{GL}(V_n)\big) \rtimes \mathsf{S}_n$$

*with $d := \dim(V_i) \geq 2$ and $n \geq 2$. If $p = d = 2$, assume in addition that $m > 0$ and $D \geq 8$. Then one of the following statements holds.*

(a) *$n = 2$ i.e. $(G, V)$ is 2-tensor induced, and $p > 2$.*

(b) *$D = 8$, and $(G, V)$ is 3-tensor induced.*

Proof. Note that the action of $G = G_{\mathrm{geom}}$ induces a transitive subgroup $\bar{G} \leq \mathsf{S}_n$, since $\mathcal{H}$ is tensor indecomposable. Furthemore, $\bar{G}$ is generated by an $n$-cycle by Proposition 5.2.7. Using $D - m \geq 2$, we see by Theorem 1.2.2 that $G_{\mathrm{geom}}$ is the Zariski closure of the normal closure of the image $\langle g_0 \rangle$ of $I(0)$ in it. In particular, this implies that the permutation $\pi$ induced by the action of $g_0$ on $\{V_1, V_2, \ldots, V_n\}$ is nontrivial. Next, one knows [**Ka-ESDE**, Theorem 8.4.2 (6)] that $g_0$ has regular spectrum on $V$, and so we can apply Proposition 5.2.6. In the case of 5.2.6(i), $\pi$ is a 2-cycle. When $g_0$ has finite order, i.e. when the "upstairs" characters are all distinct, that order is prime to $p$, so the cyclic group $\langle g_0 \rangle$ cannot map onto $\mathbb{Z}/2\mathbb{Z}$ unless $p$ is odd. In the general case, when the "upstairs" characters have repetitions but each characters has finite order dividing $q - 1$ for $q$ some power of $p$, $g_0^{q-1}$ is unipotent, and hence of pro-$\ell$ order (remember we are dealing with an $\ell$-adic representation). If $p$ were 2, then $\ell$, being $\neq p$, must be odd, and $\langle g_0 \rangle$ is a group whose pro-order is odd, so cannot map onto $\mathbb{Z}/2\mathbb{Z}$ if $p = 2$. Thus we must have that $p > 2$. Since $\pi \in \bar{G}$, we conclude that $n = 2$.

In the case of 5.2.6(ii), $d = 2$, and $\pi$ is either a 2-cycle, a 3-cycle, or a disjoint product of a 2-cycle and a 3-cycle. also, $\pi$ is a power of an $n$-cycle. As $D = 2^n \geq 8$, we must have that $n = 3$, as stated in (b). □

One of the main results of the book is the following theorem:

Theorem 5.2.9. *Let $\mathcal{H}$ be a hypergeometric sheaf in characteristic $p$ of type $(D, m)$ with $D > m$. Suppose that $D \neq 4, 8, 9$ and $\mathcal{H}$ is primitive. Then $\mathcal{H}$ satisfies ($\mathbf{S}+$).*

Proof. First we note that, by Lemmas 2.3 and 2.4 of [**KT5**], $\mathcal{H}$ is tensor indecomposable, and thus satisfies ($\mathbf{S}-$). It remains to show that $\mathcal{H}$ is not tensor induced. Since the statement follows from Theorem 1.2.1 when $m = 0$ and from Lemma 5.1.1 when $D$ is not a proper power, we will assume that $m > 0$ and that $D > 9$. Assume the contrary: $\mathcal{H}$ is $n$-tensor induced.

First we consider the case $D - m \geq 2$. Then, by Corollary 5.2.8 we have that $n = 2$ and $p > 2$. But this contradicts Propositions 5.1.9 and 5.1.10.

Next assume that $D - m = 1$. Choose a $p'$-element in $I(\infty)$ which topologically generates a complement to $P(\infty)$, with image $g_\infty$. Then Proposition 5.2.7 and its proof imply that

$G_{\rm geom}$ induces a subgroup $\bar{G} = C_n$ generated by an $n$-cycle $\sigma$ in $\mathsf{S}_n$, which is induced by the action of $g_\infty$. One knows [**Ka-ESDE**, Theorem 8.4.2,(6)] that $g_\infty$ has regular spectrum on the tame part $\mathsf{Tame}$ of dimension $m = D - 1$ and fixes the wild part of dimension 1, and so $g_\infty$ has almost regular spectrum on $\mathcal{H}$. Thus we can apply Proposition 5.2.6 to $g_\infty$ to determine the permutation $\sigma$. Let $d$ denote the common dimension $d$ of the tensor factors in $\mathcal{H}$.

Suppose $d \geq 3$. Then $\sigma$ is a 2-cycle. We claim that $p$ must be odd. Indeed, $g_\infty$ stabilizes the wild part and has finite order [**Ka-GKM**, Lemma 1.11 (3)] on the wild part. On the tame part $\mathsf{Tame}$, if say all its characters have order dividing $q-1$ for a power $q$ of $p$, then $g_\infty^{q-1}$ is pro-$\ell$ on $\mathsf{Tame}$. Thus a prime-to-$p$ power of $g_\infty$ is pro-$\ell$ on the entire $I(\infty)$-representation. So, using the fact $\sigma$ is a 2-cycle and arguing as in the proof of Corollary 5.2.8, we conclude that $p \neq 2$. This is a contradiction, by Propositions 5.1.9 and 5.1.10. [Alternatively, we can also apply Theorem 4.1.1.]

Suppose now that $d = 2$. As $D > 8$, we have $n \geq 4$. By Proposition 5.2.6, $\sigma \in \mathsf{S}_n$ is either a 2-cycle, a 3-cycle, or a disjoint product of a 2-cycle and a 3-cycle. As $n \geq 4$, none of these permutations can be an $n$-cycle, again a contradiction. □

REMARK 5.2.10. The excluded cases can be tensor induced, cf. [**Ka-ESDE**, 10.9.1] for the case $D = 9$, $m = 3$, cf. [**Ka-ESDE**, 10.8.1] for the case $D = 8$, $m = 2$, and cf. [**Ka-CC**, Theorems 6.3 and 6.5] for the cases $D = 4$, $m = 0$ or 2. And there are $D = 4$ cases which are tensor decomposable, cf. [**Ka-CC**, Theorems 5.1 and 5.3] for the cases $D = 4$, $m = 1$ or 2.

LEMMA 5.2.11. *Let $X < \mathrm{PGL}_2(\mathbb{C})$ be a finite, elementary abelian 2-group, which is the image of some irreducible subgroup of $\mathrm{GL}_2(\mathbb{C})$. Suppose that $h \in \mathrm{PGL}_2(\mathbb{C})$ is an element of odd order that normalizes $X$. Then $h^3$ centralizes $X$.*

PROOF. Since the Schur multiplier of any finite 2-group is a finite 2-group, see [**Is**, Corollary (11.21)], we may assume that $X$ is the image in $\mathrm{PGL}_2(\mathbb{C})$ of a finite irreducible 2-group $\hat{X} < \mathrm{GL}_2(\mathbb{C})$: $X = \hat{X}/\mathbf{Z}(\hat{X})$. Let $\varphi$ denote the character of $\hat{X}$ (acting on $\mathbb{C}^2$), and consider any $y \in \hat{X} \smallsetminus \mathbf{Z}(\hat{X})$. Then $y$ is not a scalar matrix, but $y^2 \in \mathbf{Z}(\hat{X})$ is, since $X$ is elementary abelian. Thus $y$ is conjugate to $\mathrm{diag}(a, -a)$ for some $a \in \mathbb{C}^\times$, and so $\varphi(y) = 0$. It follows that

$$1 = [\varphi, \varphi]_{\hat{X}} = \frac{1}{|\hat{X}|} \sum_{y \in \hat{X}} |\varphi(y)|^2 = \frac{1}{|\hat{X}|} \sum_{y \in \mathbf{Z}(\hat{X})} |\varphi(y)|^2 = \frac{4|\mathbf{Z}(\hat{X})|}{|\hat{X}|},$$

i.e. $|X| = |\hat{X}/\mathbf{Z}(\hat{X})| = 4$. Thus $X \cong C_2^2$, and so $\mathrm{Aut}(X) \cong \mathsf{S}_3$. Now the conjugation by $h$ induces an element of odd order of $\mathrm{Aut}(X)$, hence the cube of the latter is trivial, i.e. $h^3$ centralizes $X$. □

The next result overlaps with Theorem 5.2.9, but we will give an independent proof which does not rely on the analysis of 2-tensor induced sheaves:

THEOREM 5.2.12. *Let $\mathcal{H}$ be a geometrically irreducible hypergeometric sheaf in characteristic $p$ of type $(D, m)$ with $D - m \geq 1$. Suppose that $\mathcal{H}$ has finite geometric monodromy group $G = G_{\rm geom}$ and is primitive. Suppose in addition that $D \neq 4, 8, 9$. Then one of the following statements holds.*

(a) *$G$ is an almost quasisimple group and satisfies* (**S+**).

(b) *$D = 3, 5, 7$ and $G$ satisfies* ($\mathbf{S}+$).

(c) *$p > 2$, $D = p^n$, and $\mathcal{H}$ is Kloosterman, in fact the sheaf $\mathcal{K}l(\mathsf{Char}_{\rm ntriv}(p^n+1))$ (studied by Pink* [**Pink**] *and Sawin* [**KT1**, p. 841]*).*

(d) *$p = 2$, $D = 2^n$, $G$ satisfies* ($\mathbf{S}+$) *and is an extraspecial normalizer as in Lemma 1.1.3(i)(c) with $r = 2$.*

Proof. (A) Let $\Phi : G \to \mathrm{GL}(V)$ be the faithful representation realized by $\mathcal{H}$. Again by Lemmas 2.3 and 2.4 of [**KT5**], $(G, V)$ is tensor indecomposable, and hence satisfies ($\mathbf{S}-$). Note that if $G$ is almost quasisimple, then ($\mathbf{S}-$) implies by Lemma 1.1.6 that $E(G)$ is irreducible on $\mathcal{H}$, and so ($\mathbf{S}+$) holds by Theorem 3.1.6. So we will assume that $G$ is not almost quasisimple. The arguments in the proof of [**GT3**, Proposition 2.8] (but assuming only that $\Phi$ is primitive and tensor indecomposable) show that $G/\mathbf{Z}(G)$ has a unique minimal normal subgroup $\bar{L}$, which is either a direct product $S^n$ of $n \geq 2$ copies of a finite non-abelian simple group $S$, or an elementary abelian $r$-group of order $r^{2n} = D^2$ for some prime $r$. Our proof will be divided into cases according to this dichotomy. Let $g_0$ denote a generator of the image of $I(0)$ in $G$ and note that $g_0$ has finite order coprime to $p$. Clearly, $\mathcal{H}$ satisfies ($\mathbf{S}+$) when $D$ is a prime number, and so we may assume $D \geq 10$ or $D = 6$.

First we consider the case $D - m = 1$. Then any nontrivial element $x$ in the image of $P(\infty)$ in $G$ acts trivially on the tame part $\mathsf{Tame}$ of dimension $D - 1$ and nontrivially on the wild part of dimension 1 and thus is a complex reflection. Applying Mitchell's theorem [**Mit**], we see that $G = \mathbf{Z}(G)G_0$, where either $G_0 = \mathsf{S}_{D+1}$ in its deleted permutation module, or $D = 6$ and $G_0 = \mathrm{PSp}_4(3) \cdot 2$ or $6_1 \cdot \mathrm{PSU}_4(3) \cdot 2_2$) (recall we are excluding $D = 7, 8$). But this violates the above dichotomy. [Alternatively, we can also apply Theorem 5.2.9 to rule out this case.]

From now on we may therefore assume that $D - m \geq 2$.

(B) Here we assume that $\bar{L} \cong S^n$ with $S$ simple non-abelian and $n > 1$. Let $L$ denote the full inverse image of $\bar{L}$ in $G$ and let $R := L^{(\infty)}$. As shown in part 2) of the proof of [**GT3**, Proposition 2.8] (see also Lemma 1.1.9(b)), $R = R_1 * R_2 * \ldots * R_n$ is a central product of $n$ quasisimple groups $R_1 \cong R_2 \cong \ldots \cong R_n$, which are transitively permuted by $G$. Furthermore, the $R$-module $V$ decomposes as $V_1 \otimes V_2 \otimes \ldots \otimes V_n$, where $V_i$ is an irreducible $R_i$-module, $R_j$ acts trivially on $V_i$ with $i \neq j$ (since $R_j$ is perfect), and $G$ permutes the spaces $V_i$ transitively, that is,

$$G \leq \big(\mathrm{GL}(V_1) \otimes \mathrm{GL}(V_2) \otimes \ldots \otimes \mathrm{GL}(V_n)\big) \rtimes \mathsf{S}_n$$

and $(G, V)$ is $n$-tensor induced. Moreover, the arguments in the proof of [**GT3**, Proposition 2.8] (and of [**GT3**, Lemma 2.6]) show that the image of $G$ in the resulting homomorphism $\Theta : G \to \mathsf{S}_n$ agrees with the homomorphism $G \to \mathsf{S}_n$ induced by the conjugation action of $G$ on $\{R_1, R_2, \ldots, R_n\}$.

Let $d := \dim(V_1)$, so that $D = d^n$. Since $W = D - m \geq 2$, by Theorem 1.2.2, $G$ is the normal closure of $\langle g_0 \rangle$. It follows that $g_0$ induces a nontrivial permutation $\pi = \Theta(g_0)$ on the set $\{V_1, V_2, \ldots, V_n\}$.

(i) First we consider the case $d \geq 3$. By Proposition 5.2.3, $\pi$ is a 2-cycle, and we may assume that $g_0$ interchanges $V_1$ and $V_2$. Furthermore, if $h$ denotes the action of $g_0^2$ on $V_1$, then $h$ has simple spectrum and

$$\bar{\mathsf{o}}(h) \geq d^2/2. \tag{5.2.12.1}$$

Correspondingly, $g_0$ interchanges $R_1$ and $R_2$ and normalizes each $R_j$ with $j > 2$; in particular, $g_0^2$ normalizes $R_1$. Recall that the quasisimple group $R_1$ acts irreducibly on $V_1$, via a representation $\Phi_1$. Now $\Phi_1(R_1)$ is quasisimple, and $\tilde{R}_1 := \langle \Phi_1(R_1), h\rangle$ is an irreducible, finite (since $R_1$ and $g$ have finite order), almost quasisimple (since any element that centralizes it is a scalar) subgroup of $\mathrm{GL}(V_1)$. Applying Theorem 3.1.7 and using (5.2.12.1), we see that one of the conclusions (b)–(f) of Theorem 3.1.7 must hold.

(ii) Assume we are in the case of (e), so that $d = 4$ and $\tilde{R}_1 = \mathrm{Sp}_4(3)$. First consider the case $\bar{\mathsf{o}}(h) = 9$. Using [**GAP**] we can check that $h$ has eigenvalues

$$\{\alpha_j \mid 1 \leq j \leq 4\} = \gamma \cdot \{\zeta_9^i \mid i = 1, 4, 6, 7\}$$

for some $\gamma \in \mathbb{C}^\times$. Arguing as in the proof of Lemma 5.2.2, we see that the spectrum of $g_0$ on $V_1 \otimes V_2$ consists of

$$\alpha_j,\ 1 \leq j \leq 4,\ \pm\sqrt{\alpha_i\alpha_j},\ 1 \leq i < j \leq 4.$$

In particular, $\gamma\zeta_9^4 = \sqrt{(\gamma\zeta_9)(\gamma\zeta_9^7)}$ is a multiple eigenvalue for $g_0$ on $V_1 \otimes V_2$, which is impossible by Lemma 5.1.2, since $g$ has simple spectrum on $V$.

Next we consider the case $\bar{\mathsf{o}}(h) = 12$. Using [**GAP**] we can check that $h$ has eigenvalues

$$\{\beta_j \mid 1 \leq j \leq 4\} = \delta \cdot \{\zeta_{12}^i \mid i = 0, 1, 4, 7\}$$

for some $\gamma \in \mathbb{C}^\times$. As above, the spectrum of $g_0$ on $V_1 \otimes V_2$ consists of

$$\beta_j,\ 1 \leq j \leq 4,\ \pm\sqrt{\beta_i\beta_j},\ 1 \leq i < j \leq 4.$$

In particular, $\delta\zeta_{12}^4 = \sqrt{(\delta\zeta_{12})(\delta\zeta_{12}^7)}$ is a multiple eigenvalue for $g_0$ on $V_1 \otimes V_2$, again contradicting Lemma 5.1.2.

(iii) Now we consider the case of (f), so that $d = 6$, $\tilde{R}_1/\mathbf{Z}(\tilde{R}_1) = \mathrm{PSU}_4(3) \cdot 2_2$, and $\bar{\mathsf{o}}(h) = 18$. Using [**GAP**] we can check that $h$ has eigenvalues

$$\{\alpha_j \mid 1 \leq j \leq 6\} = \gamma \cdot \{\zeta_{18}^i \mid i = 1, 3, 6, 7, 13, 15\}$$

for some $\gamma \in \mathbb{C}^\times$. As above, the spectrum of $g_0$ on $V_1 \otimes V_2$ consists of

$$\alpha_j,\ 1 \leq j \leq 6,\ \pm\sqrt{\alpha_i\alpha_j},\ 1 \leq i < j \leq 6.$$

In particular, $\gamma\zeta_{18}^7 = \sqrt{(\gamma\zeta_{18})(\gamma\zeta_{18}^{13})}$ is a multiple eigenvalue for $g_0$ on $V_1 \otimes V_2$, which is impossible by Lemma 5.1.2.

(iii) Assume now that we are in the cases (b) or (d) of Theorem 3.1.7, so that $\bar{\mathsf{o}}(h) = 5$. Using [**GAP**] we can check that $h$ has eigenvalues

$$\{\alpha_j \mid 1 \leq j \leq 3\} = \gamma \cdot \{\zeta_5^i \mid i = 0, 1, 4\}$$

for some $\gamma \in \mathbb{C}^\times$. As above, the spectrum of $g_0$ on $V_1 \otimes V_2$ consists of

$$\alpha_j,\ 1 \leq j \leq 3,\ \pm\sqrt{\alpha_i\alpha_j},\ 1 \leq i < j \leq 3.$$

In particular, $\gamma = \sqrt{(\gamma\zeta_5)(\gamma\zeta_5^4)}$ is a multiple eigenvalue for $g_0$ on $V_1 \otimes V_2$, which is impossible by Lemma 5.1.2.

Next, consider the case (c) of Theorem 3.1.7, so that $\tilde{R}_1 = \mathrm{PSL}_2(7)$ and $\bar{\mathsf{o}}(h) = 7$. As $R_1$ acts trivially on $V_j$ with $j \geq 2$, we see that $R_i \cong R_1 \cong \mathrm{PSL}_2(7)$. As shown in the proof of Proposition 5.2.3, the action on $g_0$ on $V_1 \otimes V_2$ has order $2\bar{\mathsf{o}}(h) = 14$. For any $j \geq 3$, $g_0$ normalizes $R_j$ and fixes $V_j$. As the 3-dimensional representation of $R_j \cong \mathrm{PSL}_2(7)$ on $V_j$ is not fixed by any outer automorphism of $R_j$, $g_0|_{V_j}$ is a multiple scalar of an element in $R_j$, and so has central order 2, 3, 4, or 7. It follows that

$$\bar{\mathsf{o}}(g_0) \text{ divides 84 and is divisible by 14.} \tag{5.2.12.2}$$

In particular, we have by Lemma 3.1.1 that $D = 3^n \leq 84$, and $p \neq 2, 7$. By assumption, $n \geq 3$. If moreover $p \neq 3$, then by Proposition 5.2.7, we get that $\Theta(G)$ is a cyclic transitive subgroup of $\mathsf{S}_n$, generated by an $n$-cycle. But this is impossible, since $\Theta(g_0)$ is a 2-cycle. Now if $D = 3^4$, then $\bar{\mathsf{o}}(g_0) = 84$ by Lemma 3.1.1 and (5.2.12.2), forcing $p \neq 3$, and we arrive at a contradiction. Suppose $D = 3^3$ and $p = 3$. Then we must have $\bar{\mathsf{o}}(g_0) = 28$ by Lemma 3.1.1 and (5.2.12.2). In particular, we may assume that the simple-spectrum (by Lemma 5.1.2) element $g|_{V_3}$ has central order 4, and so has eigenvalues $1, \zeta_4, \zeta_4^3$ on $V_3$. On the other hand, if $h$ has eigenvalues $\beta_j$, $1 \leq j \leq 3$, on $V_1$, then, as above, $g_0$ has both $\pm\sqrt{\beta_1\beta_2}$ as eigenvalues on $V_1 \otimes V_2$. It follows that $\zeta_4\sqrt{\beta_1\beta_2}$ is a multiple eigenvalue for $g_0$ on $V_1 \otimes V_2 \otimes V_3 = V$, again a contradiction.

(iv) Now we consider the case $e = 2$. As mentioned in the proof of Theorem 3.1.7, we now have that the almost quasisimple group $\tilde{R}_1$ in $\mathrm{GL}_2(\mathbb{C})$ must be $\mathrm{SL}_2(5)$, and so $R_i \cong R_1 \cong \mathrm{SL}_2(5)$. As the 2-dimensional representation of $R_j \cong \mathrm{SL}_2(5)$ on $V_j$ is not fixed by any outer automorphism of $R_j$, if $g_0$ fixes $V_j$ then $g_0|_{V_j}$ is a multiple scalar of an element in $R_j$, and so has central order 2, 3, or 5. By Proposition 5.2.3, $\pi = \Theta(g_0)$ is a 2-cycle, a 3-cycle, or a disjoint product of a 2-cycle with a 3-cycle. Given any orbit of length $e$ of $\Theta(g_0)$, we know that the action of $g^e$ on each tensor factor in this orbit has central order 2, 3, or 5. It follows that

$$\bar{\mathsf{o}}(g_0) \in \{6, 12, 18, 30, 36, 60, 90\}. \tag{5.2.12.3}$$

By Lemma 3.1.1, $D = 2^n \leq \bar{\mathsf{o}}(g_0) \leq 90$, and $D \neq 4, 8$ by assumption. Hence $D = 2^n$ with $4 \leq n \leq 6$. Assume $D = 2^5$ or $2^6$, and $\bar{\mathsf{o}}(g_0) \in \{36, 60, 90\}$ by Lemma 3.1.1 and (5.2.12.3). In particular, $p \neq 2, 3$ as $g_0$ is a $p'$-element. Again applying Proposition 5.2.7, we see that $\Theta(G) \cong C_n$ is generated by an $n$-cycle in $\mathsf{S}_n$. For $n = 5$ or 6, this however contradicts the given shape of $\pi = \Theta(g_0)$.

Finally, assume $n = 4$. Then $\pi = \Theta(g_0)$ can be only a 2-cycle, or a 3-cycle. Hence instead of (5.2.12.3), we now have that $\bar{\mathsf{o}}(g_0) \in \{4, 6, 9, 10, 15\}$. Hence $\bar{\mathsf{o}}(g_0) < 16 = D$, contrary to Lemma 3.1.1.

(C) Now we consider the case where $\bar{L}$ is an elementary abelian $r$-group of order $r^{2n} = D^2$. Note that in this case, by Lemma 1.1.9, we have that $G$ admits a normal $r$-subgroup $R$ as in Lemma 1.1.9(c); in particular, $R$ acts irreducibly on $V$, and

$$R/\mathbf{Z}(R) \text{ is elementary abelian of order } r^{2n}. \tag{5.2.12.4}$$

It is clear that $G$ cannot be tensor induced and hence satisfies $(\mathbf{S}+)$ when $D = 2, 3, 5, 7$. Assuming $D = r^n \notin \{2, 3, 4, 5, 7, 8, 9\}$, we then have $D \geq 11$ and therefore can apply Theorem 1.2.6. Assuming furthermore that conclusion (c) does not hold, we must then have that $p = r = 2$. If $(G, V)$ is moreover $(\mathbf{S}+)$, then we arrive at (d). Hence we may assume that $(G, V)$ is $k$-tensor induced for some $k \geq 2$, and that

$$G \leq \bigl(\mathrm{GL}(V_1) \otimes \mathrm{GL}(V_2) \otimes \ldots \otimes \mathrm{GL}(V_k)\bigr) \rtimes \mathsf{S}_k.$$

Let $\Theta : G \to \mathsf{S}_k$ denote the corresponding homomorphism, and let $\pi := \Theta(g_0)$. If $\pi = \mathrm{Id}$, then we can again apply Theorem 1.2.2 to conclude that $\Theta(G) = \{\mathrm{Id}\}$, a contradiction. So $\pi$ is a nontrivial permutation of **odd** order. By Proposition 5.2.3, this implies that $\dim(V_i) = 2$, $2^n = D = 2^k$, i.e. $k = n$, and $\pi$ is a 3-cycle.

Let $K := \mathrm{Ker}(\Theta)$, so that $K \geq \mathbf{Z}(G)$. Assume that $K = \mathbf{Z}(G)$. Then, as $R \cap \mathbf{Z}(G) = \mathbf{Z}(R)$ by Schur's lemma, we have by (5.2.12.4) that

$$C_2^{2n} = R/\mathbf{Z}(R) = R/(R \cap \mathbf{Z}(G)) \cong R\mathbf{Z}(G)/\mathbf{Z}(G) \leq G/\mathbf{Z}(G) = G/K \leq \mathsf{S}_n,$$

which is impossible, since the 2-part of $|\mathsf{S}_n|$ is

$$2^{\lfloor n/2 \rfloor + \lfloor n/2^2 \rfloor + \lfloor n/2^3 \rfloor + \dots} < 2^n.$$

Hence $K > \mathbf{Z}(G)$, and so $K/\mathbf{Z}(G)$ is a nontrivial normal subgroup of $G/\mathbf{Z}(G)$. But $\bar{L} \cong R/\mathbf{Z}(R)$ is the unique minimal normal subgroup of $G/\mathbf{Z}(G)$, so we conclude that $K \geq R$. In particular, $R$ fixes each $V_i$ and induces a projective representation on $V_i$.

Let $X < \mathrm{PGL}(V_i)$ denote the image of $R$ in this projective representation. Note that $\mathbf{Z}(R)$ acts as scalars on $V_i$, so using (5.2.12.4) we see that $X$ is an elementary abelian 2-group. Recall that $g_0^3 \in K$. As $R \lhd K$, we see that $g_0^3$ normalizes $X$, and $g_0^3$ has odd order. By Lemma 5.2.11, $g_0^9$ centralizes $X$, i.e. $[g_0^9, x]$ acts as a scalar on $V_i$ for each $x \in R$. It follows that $[g_0^9, x]$ acts as a scalar on $V$, and so belongs to $\mathbf{Z}(G)$. Thus we can find

$$f : R \to \mathbf{Z}(G)$$

such that $g_0^9 x g_0^{-9} = x f(x)$ for all $x \in R$. Now for $x, y \in R$ we have

$$xyf(xy) = g_0^9 xy g_0^{-9} = g_0^9 x g_0^{-9} \cdot g_0^9 y g_0^{-9} = xf(x) \cdot yf(y) = xyf(x)f(y),$$

i.e. $f \in \mathrm{Hom}(R, \mathbf{Z}(G))$. In particular, if $2^a$ denotes the exponent of $R$, then $(f(x))^{2^a} = f(x^{2^a}) = 1$ for all $x \in R$. On the other hand, an induction on $j \geq 1$ shows that

$$g_0^{9j} x g_0^{-9j} = x(f(x))^j.$$

In particular, if $b$ denotes the odd order of $g_0^9$, then

$$x = g_0^{9b} x g_0^{-9b} = x(f(x))^b.$$

Thus $f(x)^b = f(x)^{2^a} = 1$, and so $f(x) = 1$ for all $x \in R$. We have shown that $g_0^9$ centralizes $R$. Hence, by Schur's lemma, $g_0^9$ acts as a scalar, and so $\bar{\mathsf{o}}(g_0)$ divides 9. But this contradicts Lemma 3.1.1, since $D \geq 16$. □

CHAPTER 6

# (Non-)existence results

## 6.1. Type $A$

We begin with an elementary fact and some lemmas about exotic behavior in low characteristic.

Lemma 6.1.1. *Let $Q < \mathrm{Sp}(V) \cong \mathrm{SL}_2(\mathbb{C})$ be a finite 2-subgroup which acts irreducibly on $V = \mathbb{C}^2$ and has only integer traces. Then $Q \cong Q_8$, the quaternion group of order 8.*

Proof. Certainly, $Q$ is non-abelian, and so $|Q| \geq 8$. Next, any involution $x \in Q$ acts on $V$ as $-\mathrm{Id}$, and thus is unique. Consider any $y \in Q$ of order $\geq 4$. Then $y$ acts as $\mathrm{diag}(\alpha, \alpha^{-1})$ with $\alpha \in \mathbb{C}^\times$ of 2-power order $\geq 4$ and $\alpha + \alpha^{-1} \in \mathbb{Z}$, hence $\{\alpha, \alpha^{-1}\} = \{1, -1\}$. Now, if $\varphi$ denotes the character of the $Q$-module $V$, then

$$|Q| = |Q| \cdot [\varphi, \varphi]_Q = \sum_{y \in Q} |\varphi(y)|^2 = 4 + 4,$$

i.e. $Q \cong D_8$ or $Q_8$. As $Q$ has a unique involution, we conclude that $Q \cong Q_8$. □

Lemma 6.1.2. *Suppose $p = 3$. Let $\mathcal{H}$ be a Kloosterman sheaf $\mathcal{K} := \mathcal{K}l_\psi(\chi, \overline{\chi})$ with $G_{\mathrm{geom}} = \mathrm{SL}_2$ (e.g., take $\chi = \mathbb{1}$, or take $\chi$ of prime order $> 5$). Then $\mathrm{Sym}^3(\mathcal{K})$ is a hypergeometric sheaf of type $(4, 2)$, whose $G_{\mathrm{geom}}$ is $\mathrm{SL}_2$ in its 4-dimensional irreducible representation.*

Proof. The $I(\infty)$-representation of any $\mathcal{K} := \mathcal{K}l_\psi(\chi, \overline{\chi})$ is independent of which $\chi$ we choose, cf. [**Ka-ESDE**, 8.6.4]. This allows us to compute the $I(\infty)$-representation by choosing a particular $\mathcal{K}$. We take the particular choice of

$$\mathcal{K}_0 := \mathcal{K}l_\psi(\xi_4, \xi_4^3) \cong \mathcal{L}_{\xi_4} \otimes \mathcal{K}l_\psi(\mathbb{1}, \xi_2),$$

which by [**Ka-GKM**, 5.6.2] is geometrically the Kummer direct image

$$[2]_\star(\mathcal{L}_{\xi_2} \otimes \mathcal{L}_{\psi(2x)}).$$

Thus the $I(\infty)$-representation of $[2]^\star(\mathcal{K})$ is the direct sum

$$\mathcal{L}_{\xi_2} \otimes (\mathcal{L}_{\psi(2x)} \oplus \mathcal{L}_{\psi(-2x)}).$$

So the $I(\infty)$-representation of $[2]^\star(\mathrm{Sym}^3(\mathcal{K})$ is

$$\mathcal{L}_{\xi_2} \otimes \big(\mathcal{L}_{\psi(6x)} \oplus \mathcal{L}_{\psi(2x)} \oplus \ \mathcal{L}_{\psi(-2x)} \oplus \mathcal{L}_{\psi(-6x)}\big).$$

Up to this point, the discussion has been valid in any odd characteristic. But when $p = 3$, the two characters $\mathcal{L}_{\psi(\pm 6x)}$ become trivial, so the $I(\infty)$-representation of $[2]^\star(\mathrm{Sym}^3(\mathcal{K}))$ is just

$$\mathcal{L}_{\xi_2} \otimes (\mathbb{1} \oplus \mathbb{1} \oplus \mathcal{L}_{\psi(2x)} \oplus \mathcal{L}_{\psi(-2x)}).$$

Therefore $\mathsf{Swan}_\infty\big([2]^\star(\mathrm{Sym}^3(\mathcal{K}))\big) = 2$, and hence $\mathsf{Swan}_\infty(\mathrm{Sym}^3(\mathcal{K})) = 1$. We also see that the $I(\infty)$-representation of any such $\mathcal{K}$ is the direct sum $\mathsf{Wild}_2 \oplus \mathsf{Tame}_2$.

Thus $\mathrm{Sym}^3(\mathcal{K}))$ is a lisse sheaf on $\mathbb{G}_m/\overline{\mathbb{F}_3}$ which is geometrically irreducible (its $G_{\mathrm{geom}}$ being $\mathrm{SL}_2$ in its 4-dimensional irreducible representation, which is tame at 0 because $\mathcal{K}$ is tame at 0) and with $\mathsf{Swan}_\infty = 1$. By [**Ka-ESDE**, 8.5.3], it follows that $\mathrm{Sym}^3(\mathcal{K})$ is hypergeometric of type $(4, 2)$. □

LEMMA 6.1.3. *Suppose $p = 2$. Let $\mathcal{H}$ be a Kloosterman sheaf $\mathcal{K} := \mathcal{K}l_\psi(\chi, \overline{\chi})$ with $G_{\mathrm{geom}} = \mathrm{SL}_2$ (e.g., take $\chi = \mathbb{1}$, or take $\chi$ of prime order $> 5$). Then $\mathrm{Sym}^4(\mathcal{K})$ is a hypergeometric sheaf of type $(5, 2)$, whose $G_{\mathrm{geom}}$ is the image of $\mathrm{SL}_2$ in its 5-dimensional irreducible representation.*

PROOF. One knows [**Ka-ESDE**, 8.6.4] that the $P(\infty)$-representation of $\mathcal{K}$ is independent of the choice of $\chi$. Take the particular choice of

$$\mathcal{K}_0 := \mathcal{K}l_\psi(\xi_3, \xi_3^2).$$

We now specialize to the case $p = 2$. Then $P(\infty)$ acts irreducibly, cf. [**Ka-GKM**, 1.15]. One knows that the Kummer pullback $]3]^\star(\mathcal{K}_0)$ on $\mathbb{G}_m/\mathbb{F}_4$ is geometrically isomorphic to the local system whose trace function at $t \in \mathbb{F}_{4^d}$ is $t \mapsto (1/2^d)\sum_x \psi(x^3 + tx)$. This local system has its $G_{\mathrm{geom}}$ a finite [**KT1**, 20.1] 2-group. All Frobenius traces are thus integers, and the representation is symplectic. Thus the image of $P(\infty)$ is a finite 2-group inside $\mathrm{SL}_2(\mathbb{C})$ which is irreducible and has traces in $\mathbb{Z}$. By Lemma 6.1.1, we see that the image of $P(\infty)$ is the quaternion group $Q_8$ in its irreducible 2-dimensional representation $\mathsf{std}_2$. From the character table of $Q_8$, one sees that $\mathrm{Sym}^4(\mathsf{std}_2)$ is the direct sum of 2 copies of $\mathbb{1}$ and each of the three linear characters of order 2. This shows that the $P(\infty)$ representation of $[3]^\star(\mathrm{Sym}^4(\mathcal{K}))$ is the direct sum of 2 copies of $\mathbb{1}$ and each of the three linear characters of order 2. Therefore the $I(\infty)$-representation of $\mathrm{Sym}^4(\mathcal{K})$ is the direct sum of a 2-dimensional tame part and a 3-dimensional wild part, say $\mathsf{Tame}_2 \oplus \mathsf{Wild}_3$. But $\mathrm{Sym}^4(\mathcal{K})$ has all $\infty$-slopes $\leq 1/2$, and hence has $\mathsf{Swan}_\infty \leq 3/2$. But Swan conductors are integers, so $\mathsf{Swan}_\infty$ is 0 or 1. It cannot be 0 since the wild part is nonzero. We now conclude exactly as in the proof of Lemma 6.1.2 above. □

LEMMA 6.1.4. *Suppose $p = 2$. Let $\mathcal{H}$ be the hypergeometric sheaf $\mathcal{H}yp_\psi(\mathbb{1}, \mathbb{1}; \rho)$ with $\rho \neq \mathbb{1}$. Then $\mathrm{Sym}^2(\mathcal{H})$ is geometrically isomorphic to the hypergeometric sheaf $\mathcal{H}yp_\psi(\mathbb{1}, \mathbb{1}, \mathbb{1}; \rho^2, \overline{\rho}^2)$ of type $(3, 2)$, whose $G_{\mathrm{geom}}$ is $\mathrm{O}_3$.*

PROOF. The $P(\infty)$ representation of $\mathcal{H}$ is $\mathbb{1} \oplus \mathcal{L}_\psi$. Hence the $P(\infty)$ representation of $\mathrm{Sym}^2(\mathcal{H})$ is $\mathbb{1} \oplus \mathbb{1} \oplus \mathcal{L}_\psi$. More precisely, let us consider the $I(\infty)$-representation of $\mathcal{H}$. By [**Ka-ESDE**, 8.12.2 (1)], $\det(\mathcal{H}) \cong \mathcal{L}_\psi$ geometrically. Therefore the $I(\infty)$-representation has $\det = \mathcal{L}_\psi$, and $\mathcal{L}_\rho$ is one summand. So the $I(\infty)$-representation is the direct sum $\mathcal{L}_\rho \bigoplus \mathcal{L}_{\overline{\rho}} \otimes \mathcal{L}_\psi$. Thus the $I(\infty)$-representation of $\mathrm{Sym}^2(\mathcal{H})$ is

$$\mathcal{L}_{\rho^2} \oplus \mathcal{L}_{\overline{\rho^2}} \oplus \mathcal{L}_{\overline{\rho}} \otimes \mathcal{L}_\psi.$$

Now $\mathcal{H}$ has $G^0_{\mathrm{geom}} = \mathrm{SL}_2$, because it is a semisimple subgroup of $\mathrm{SL}_2$ which contains a nonsemisimple element (namely local monodromy at 0, which is a unipotent Jordan block of size 2). Therefore $\mathrm{Sym}^2(\mathcal{H})$ has $G^0_{\mathrm{geom}} = \mathrm{SO}_3$. Thus $\mathrm{Sym}^2(\mathcal{H})$ is geometrically irreducible, lisse on $\mathbb{G}_m$, tame at 0 and has $\mathsf{Swan}_\infty = 1$. Thus $\mathrm{Sym}^2(\mathcal{H})$ is hypergeometric of type $(3, 2)$. From its local monodromies, it is a multiplicative translate [**Ka-ESDE**, 8.5,5] of

$\mathcal{H}yp_\psi(\mathbb{1},\mathbb{1},\mathbb{1};\rho^2,\overline{\rho}^2)$. This sheaf is orthogonally self-dual, cf. [**Ka-ESDE**, 8.8.1], but its determinant is $\mathcal{L}_\psi$, so its $G_{\rm geom}$ contains but cannot be $\mathrm{SO}_3$, so its $G_{\rm geom}$ is $\mathrm{O}_3$. In fact, there is no multiplicative translate, because its determinant, $\mathcal{L}_\psi$, detects multiplicative translates. □

THEOREM 6.1.5. *Let $\mathcal{H}$ be a hypergeometric sheaf in characteristic $p$, of type $(D,m)$ with $D>m$ and $D\geq 3$, such that $G^\circ_{\rm geom}$ is a simple algebraic group of type $A_1$ acting irreducibly on $\mathcal{H}$. Then $(D,m,p)=(5,2,2)$, $(4,2,3)$, $(3,1,p>2)$, $(3,0,2)$, or $(3,2,2)$. Conversely, all the listed cases do occur.*

PROOF. (i) Writing $G:=G_{\rm geom}$, we have $\mathbf{Z}(G^\circ)=\mathbf{Z}(G)\cap G^\circ$ by Schur's lemma, and $G=\mathbf{Z}(G)G^\circ$ since $G^\circ$ has no outer automorphisms. Hence $G/\mathbf{Z}(G)\cong G^\circ/\mathbf{Z}(G^\circ)\cong \mathrm{PGL}_2$ and so $G$ admits an irreducible representation $\Lambda: G\to \mathrm{GL}_3$. Set $e:=3$ if $p=2\nmid D$.

Assume in addition that $2|D$, so that $G^\circ=\mathrm{SL}_2$. If $m:=|\mathbf{Z}(G)|$ is odd, then $G=\mathbf{Z}(G)\times\mathrm{SL}_2$ admits an irreducible representation $\Lambda: G\to\mathrm{GL}_2$ with kernel $\mathbf{Z}(G)$; set $e=2$ in this case. If $2|m$, then $G=\mathbf{Z}(G)\circ\mathrm{SL}_2$ is a central product, with $\mathbf{Z}(G)\cap\mathrm{SL}_2=\langle \boldsymbol{z}^{m/2}\rangle$, where $\mathbf{Z}(G)=\langle\boldsymbol{z}\rangle$. In this case, $G$ admits a faithful irreducible representation $\Lambda: G\to\mathrm{GL}_2$, with $\mathrm{SL}_2$ acts via its natural representation and $\boldsymbol{z}$ acts as the scalar $\zeta_m$; again set $e:=2$.

Now consider the case $p>2$ and $2\nmid D$, so that $G^\circ=\mathrm{PSL}_2$ and $G=\mathbf{Z}(G)\times G^\circ$. Then $G=\Gamma/\langle\boldsymbol{j}\rangle$, where $\Gamma:=\mathbf{Z}(G)\times\mathrm{SL}_2$ and $\mathbf{Z}(\mathrm{SL}_2)=\langle\boldsymbol{j}\rangle\cong C_2$. Now $\Gamma$ admits an irreducible representation $\Lambda:\Gamma\to\mathrm{GL}_2$, with kernel $\mathbf{Z}(G)$ and with $\mathrm{SL}_2$ acting via its natural representation. Set $e:=2$ in this case.

Applying [**KT5**, Theorem 4.14] to $\Lambda$, we obtain

$$1\leq w:=D-m\leq e\leq 3. \tag{6.1.5.1}$$

Without any loss, we may assume that $G^\circ=\mathrm{SL}(W)\cong\mathrm{SL}_2$ acts on $\mathcal{H}$ via $\mathrm{Sym}^n(W)$, where $n=D-1$.

(ii) Now we consider any element $g\neq 1$ in the image $Q$ of $P(\infty)$ in $G$, and write $g=zh$ with $z\in\mathbf{Z}(G)$ and $h$ is conjugate to $\mathrm{diag}\big(\alpha,\alpha^{-1}\big)\in G^\circ$ for some $\alpha\in\mathbb{C}^\times$ and

$$\alpha^2\neq 1, \tag{6.1.5.2}$$

since $g\notin\mathbf{Z}(G)$. Then $z$ acts on $\mathcal{H}$ as a scalar $\beta\in\mathbb{C}^\times$, whereas $h$ acts on $\mathcal{H}$ as

$$\mathrm{diag}\big(\alpha^n,\alpha^{n-2},\dots,\alpha^{2-n},\alpha^{-n}\big), \tag{6.1.5.3}$$

and $D-w\geq n-2$ of these eigenvalues occur on $\mathsf{Tame}$ and so are all equal to $\beta^{-1}$ (as $g$ acts trivially on $\mathsf{Tame}$). On the other hand, no two consecutive eigenvalues $\alpha^j$ and $\alpha^{j-2}$ can be equal, because otherwise $\alpha^2=1$, contrary to (6.1.5.2). Now, if $D\geq 8$, then each of the four pairs $\{\alpha^j,\alpha^{j-2}\}$ with $j=n$, $n-4$, $n-8$, and $n-12\geq 2-n$, contains $\beta^{-1}$ at most once, forcing $m=\dim\mathsf{Tame}\leq D-4$, contrary to (6.1.5.1).

(iii) Assume now that $D=6$ or $7$. Again, each of the three pairs $\{\alpha^j,\alpha^{j-2}\}$ with $j=n$, $n-4$, $n-8\geq 2-n$, contains $\beta^{-1}$ at most once. But $\dim\mathsf{Tame}\geq D-3$ by (6.1.5.1), so each of them contains $\beta^{-1}$ exactly once, and furthermore $w=3$. Since $e=2$ when $2|D$, (6.1.5.1) implies that $D=7$. Thus either $\alpha^n=\alpha^{n-4}=\beta^{-1}$, or $\alpha^{n-2}=\alpha^{n-6}=\beta^{-1}$. In either case we have $\alpha^4=1$, and so we may assume that $\alpha=\zeta_4$ because of (6.1.5.2). Now $g$ acts as $\beta\cdot\mathrm{diag}(-1,1,-1,1,-1,1,-1)$. As 1 is an eigenvalue of multiplicity $\geq 4$ for $g$, we have $\beta=-1$, and $g$ acts on $\mathsf{Wild}$ as the scalar $-1$. We have therefore shown that each nontrivial element $g\in Q$ acts on $\mathsf{Wild}$ as the scalar $-1$. But this is impossible since we also have $w=3$.

(iv) Suppose $D = 5$. Then $h$ acts on $\mathcal{H}$ as $\mathrm{diag}(\alpha^4, \alpha^2, 1, \alpha^{-2}, \alpha^{-4})$, see (6.1.5.3), and 1 is an eigenvalue for $g$ with multiplicity $m \geq 2$. This implies that $\alpha^8$, or $\alpha^6$, or $\alpha^4 = 1$. Together with (6.1.5.2), we have one of the following three situations.

• $\alpha^8 = 1$ but $\alpha^4 \neq 1$. Then $\alpha^4 = -1$, and $g$ acts as $\beta \cdot \mathrm{diag}\big(-1, \zeta_4, 1, -\zeta_4, -1\big)$. As $m \geq 2$, we must have that $\beta = -1$, $g$ is a 2-element and hence $p = 2$, and $w = 3$. As $p \nmid w$, $Q$ is elementary abelian by [**KT5**, Proposition 4.10], and thus $g^2 = 1$, which is a contradiction as it has eigenvalue $\zeta_4$.

• $\alpha^6 = 1$ but $\alpha^2 \neq 1$. Then we may assume that $\alpha^2 = \zeta_3$, and so $g$ acts as $\beta \cdot \mathrm{diag}\big(\zeta_3^2, \zeta_3, 1, \zeta_3^2, \zeta_3\big)$. As $m \geq 2$, we must have that $\beta = \zeta_3$ or $\zeta_3^2$, $g$ is a 3-element and hence $p = 3$, and $w = 3$. But this contradicts (6.1.5.1), since $e = 2$ in this case.

• $\alpha^4 = 1$ but $\alpha^2 \neq 1$. Then $\alpha^2 = -1$, and $g$ acts as $\beta \cdot \mathrm{diag}\big(1, -1, 1, -1, 1\big)$. If $m \geq 3$, then $\beta = 1$, and $g$ acts on $\mathsf{Wild}$ as the scalar $-1$, a contradiction since $w = 2$. So $m = 2$, $w = 3$, $\beta = \pm 1$, $p = 2$, as stated.

(iv) Suppose $D = 4$. Then $h$ acts on $\mathcal{H}$ as $\mathrm{diag}(\alpha^3, \alpha, \alpha^{-1}, \alpha^{-3})$, see (6.1.5.3), and 1 is an eigenvalue for $g$ with multiplicity $m \geq 2$. This implies that $\alpha^4$, or $\alpha^6 = 1$. Together with (6.1.5.2), we have one of the following two situations.

• $\alpha^4 = 1$ but $\alpha^2 \neq 1$. Then we may assume that $\alpha = \zeta_4$, and $g$ acts as $\beta \cdot \mathrm{diag}\big(-\zeta_4, \zeta_4, -\zeta_4, \zeta_4\big)$. As $m \geq 2$, we must have that $\beta = \pm\zeta_4$, and $g$ acts on $\mathsf{Wild}$ as the scalar $-1$, a contradiction since $w = 2$.

• $\alpha^6 = 1$ but $\alpha^2 \neq 1$. Then we may assume that $\alpha = \pm\zeta_3$, and so $g$ acts as $\pm\beta \cdot \mathrm{diag}\big(1, \zeta_3, \zeta_3^2, 1\big)$. As $m \geq 2$, we must have that $\beta = \pm 1$, $g$ is a 3-element and hence $p = 3$, and $w = 2$, as stated.

(v) Now we consider the case $D = 3$. Assume first that $p > 2$. By (6.1.5.1), $1 \leq w \leq 2$. Assume in addition that $w = 1$. Now $h$ acts on $\mathcal{H}$ as $\mathrm{diag}(\alpha^2, 1, \alpha^{-2})$, see (6.1.5.3), and 1 is an eigenvalue for $g$ with multiplicity $m = 2$. This implies by (6.1.5.2) that $\alpha^2 = -1$, $\beta = -1$, and $g$ acts as $\mathrm{diag}(1, -1, 1)$, i.e. $p = 2$, a contradiction.

Assume now that $p = 2$ and $w = 2$. By [**KT5**, Proposition 4.8(iv)], $\mathbf{Z}(G)$ has odd order, and recall that $G = \mathbf{Z}(G) \times \mathrm{PSL}_2$. Hence, $\mathbf{Z}(G)$ acts on $\mathcal{H}$ via a linear character $\chi$ of odd order. Tensoring with $\mathcal{L}_{\overline{\chi}}$, we get a hypergeometric sheaf $\mathcal{H}'$ with $G_{\mathrm{geom}} = \mathrm{PSL}_2$, hence self-dual. Now the set $\{\chi_1, \chi_2, \chi_3\}$ of "upstairs" characters of $\mathcal{H}'$ is stable under complex conjugation, and so it contains $\mathbb{1}$. Similarly, the single "downstairs" character of $\mathcal{H}'$ is stable under complex conjugation, and so it equals to $\mathbb{1}$. But this violates the geometric irreducibility of $\mathcal{H}'$.

(vi) For the converse, as shown in Theorems 3.3 and 3.7 of [**Ka-CC**], there exist hypergeometric sheaves, of type $(3, 0)$ in characteristic $p = 2$ and of type $(3, 1)$ in any characteristic $p > 2$, with $G_{\mathrm{geom}}$ realizing $\mathrm{PSL}_2$ in its irreducible 3-dimensional representation. The cases $(D, m, p) = (5, 2, 2)$, $(4, 2, 3)$, and $(3, 2, 2)$ are shown in Lemmas 6.1.3, 6.1.2, and 6.1.4, to occur. □

To handle higher rank groups of type $A$, first we need a lifting lemma. For brevity, in what follows we use $\Sigma^k(V)$ to denote $\mathrm{Sym}^k(V)$ when $k \in \mathbb{Z}_{\geq 1}$ and $\Sigma = \mathrm{Sym}$, and $\wedge^k(V)$ when $\Sigma = \wedge$. In fact, we make the convention that *the notation* $\Sigma^k(V)$ *when* $\Sigma = \wedge$ *always implies that* $1 \leq k \leq \dim(V) - 1$. Slightly abusing the terminology, we will call a character of a finite group $Q$ *scalar*, if it is a multiple of a linear character of $Q$.

LEMMA 6.1.6. *Let $k \in \mathbb{Z}_{\geq 1}$, $V = \mathbb{C}^d$, and $\Sigma \in \{\mathrm{Sym}, \wedge\}$. Suppose $\mathcal{H} = \mathbb{C}^N$ and $G \leq \mathrm{GL}(\mathcal{H})$ is a reductive group with finite center $\mathbf{Z}(G)$, such that $G = \mathbf{Z}(G)G^\circ$ and $G^\circ$ acts on $\mathcal{H}$ as $\mathrm{SL}(V)$ acts on $\Sigma^k(V)$. Then we can find a reductive subgroup $H < \mathrm{GL}(V)$ with finite center $\mathbf{Z}(H)$ and a finite cyclic subgroup $Z \leq H \cap \mathbf{Z}(\mathrm{GL}(V))$ of order $k$, such that the following conditions hold:*

(a) *$H = \mathbf{Z}(H)\mathrm{SL}(V)$.*
(b) *Let $\Psi$ denote the natural action of $\mathrm{GL}(V)$ on $\Sigma^k(V)$. Then $Z$ is the kernel of $\Psi|_H$.*
(c) *There is a surjective homomorphism $\pi : H \twoheadrightarrow G$ with $\mathrm{Ker}(\pi) = Z$ and $\Psi|_H = \Phi \circ \pi$, where $\Phi$ denotes the representation of $G$ on $\mathcal{H}$.*

*In other words, $G$ acts on $\mathcal{H}$ as $H$ acts on $\Sigma^k(V)$.*

PROOF. Since $G^\circ$ is irreducible on $\mathcal{H}$, we have that $\mathbf{Z}(G) = \langle \boldsymbol{z} \rangle$, where $\boldsymbol{z} = \zeta_n \cdot \mathrm{Id}_{\mathcal{H}} \in \mathrm{GL}(\mathcal{H})$ for some $n \in \mathbb{Z}_{\geq 1}$. By assumption, $\mathbf{Z}(G^\circ) = \mathbf{Z}(G) \cap G^\circ$ is the image of $\mathbf{Z}(\mathrm{SL}(V)) = \langle \boldsymbol{j} \rangle \cong C_d$ acting on $\Sigma^k(V)$. Choosing $\boldsymbol{j} = \zeta_d \cdot \mathrm{Id}_V \in \mathrm{GL}(V)$, we have that $\boldsymbol{j}$ acts on $\mathcal{H}$ as $\zeta_d^k \cdot \mathrm{Id}_{\mathcal{H}}$. Since the latter belongs to $\mathbf{Z}(G)$, we have $1 = \zeta_d^{kn}$, i.e. $d|kn$. Set

$$\boldsymbol{t} := \zeta_{kn} \cdot \mathrm{Id}_V \in \mathrm{GL}(V),\ H := \langle \boldsymbol{t} \rangle \mathrm{SL}(V) < \mathrm{GL}(V),\ Z := \langle \boldsymbol{t}^n \rangle.$$

This ensures that (a) holds. Also, the kernel of $\mathrm{GL}(V)$ acting on $\Sigma^k(V)$ is precisely $\langle \zeta_k \cdot \mathrm{Id}_V \rangle = Z$; in particular, (b) holds. Next, $\boldsymbol{t}$ acts on $\Sigma^k(V)$ as the scalar $\zeta_{kn}^k = \zeta_n$, which is the same as the action of $\boldsymbol{z}$ on $\mathcal{H}$. Now we can define $\pi : H \to G$ by setting $\pi(\boldsymbol{t}) = \boldsymbol{z}$ and $\pi|_{\mathrm{SL}(V)}$ to be the natural projection $\mathrm{SL}(V) \twoheadrightarrow \mathrm{SL}(V)/(Z \cap \langle \mathrm{SL}(V))$. □

LEMMA 6.1.7. *Let $Q$ be a finite group, and let $\chi, \psi$ be complex characters of $Q$.*

(i) *Suppose that $\chi\psi$ is a multiple of some linear character $\tau$. Then $\chi = \chi(1)\alpha$ and $\psi = \psi(1)\beta$ for some linear characters $\alpha, \beta$ of $Q$ such that $\alpha\beta = \tau$.*
(ii) *Suppose that $\varphi = \varphi(1)\lambda$ for a linear character $\lambda$ of $Q$, where either $\varphi = \mathrm{Sym}^k(\chi)$ for some $k \geq 1$, or $\varphi = \wedge^k(\chi)$ for some $1 \leq k \leq d-1$. Then $\chi = \chi(1)\nu$, where $\nu$ is a linear character of $Q$ with $\nu^k = \lambda$.*
(iii) *Suppose that $\chi = \mathrm{Ind}_R^Q(\alpha)$ for some character $\alpha$ of a subgroup $R \leq Q$ and that $\chi$ is a multiple of a linear character $\lambda$ of $Q$. Then $R = Q$ and $\alpha = \chi$.*
(iv) *Suppose $Q$ acts on a finite non-empty set $\Omega$, and suppose for some $m$, $1 \leq m < |\Omega|$, $Q$ stabilizes every $m$-subset of $\Omega$. Then $Q$ acts trivially on $\Omega$.*

PROOF. (i) First we consider the case $\tau = 1_Q$. Write $\chi = \sum_{i=1}^m \chi_i$ and $\psi = \sum_{i=1}^n \psi_j$, with $\chi_i, \psi_j \in \mathrm{Irr}(Q)$. By assumption, $Q = \mathrm{Ker}(\chi_i\psi_j)$; in particular, $1 \leq [\chi_i\psi_j, 1_Q] = [\chi_i, \overline{\psi}_j]$. As $\chi_i$ and $\psi_j$ are irreducible, it follows that $\chi_i = \overline{\psi}_j$. If moreover $\chi_i(1) > 1$, then, as $1 = [[\chi_i, \overline{\psi}_j]$, we see that $\chi_i\psi_j$ must involve some nontrivial irreducible character of $Q$, a contradiction. We have shown that, for any pair $i, j$, $\chi_i = \overline{\psi}_j$ and has degree 1, whence the statement follows in this case.

The general case then follows, if we replace $\psi$ by $\psi' := \psi\overline{\tau}$ and apply the previous case to $\chi\psi'$.

(ii) It suffices to show that, in a representation $\Phi$ affording $\chi$, each $g \in Q$ acts as a scalar matrix. Assume the contrary, so that $d \geq 2$. We may assume that $\Phi(g) = \mathrm{diag}(\alpha_1, \alpha_2, \ldots, \alpha_{\chi(1)})$, but $\alpha_1 \neq \alpha_2$. Now, if $\Sigma = \mathrm{Sym}$, then $\Sigma^k(\Phi)(g)$ admits (at least) two distinct eigenvalues $\alpha_1^k$ and $\alpha_1^{k-1}\alpha_2$. If $1 \leq k \leq \chi(1) - 1$ and $\Sigma = \wedge$, then $\Sigma^k(\Phi)(g)$

admits (at least) two distinct eigenvalues $\alpha_1\alpha_3\alpha_4\ldots\alpha_{k+1}$ and $\alpha_2\alpha_3\alpha_4\ldots\alpha_{k+1}$. We reach a contradiction in both cases.

(iii) Assume the contrary: $Q > R$. By assumption, $\chi = \chi(1)\lambda$, so for any $g \in Q \smallsetminus R$ we have

$$\chi(1) = \left|\chi(g)\overline{\lambda(g)}\right| = \left|\frac{1}{|R|}\sum_{x\in Q,\ xgx^{-1}\in R}\alpha(xgx^{-1})\overline{\lambda(g)}\right| \leq \frac{(|Q|-1)\alpha(1)\lambda(1)}{|R|} < [Q:R]\alpha(1) = \chi(1),$$

a contradiction.

(iv) Assume the contrary: there exists some $\omega \in \Omega$ and $g \in Q$ such that $g(\omega) \neq \omega$. Then we can find an $m$-subset $\Delta \subseteq \Omega \smallsetminus \{g(\omega)\}$ that contains $\omega$. As $\omega \in \Delta$ but $g(\omega) \notin g(\Delta)$, $g(\Delta) \neq \Delta$, a contradiction. □

LEMMA 6.1.8. *Let* $\mathbb{C}^d = V = V_1 \oplus V_2 \oplus \ldots \oplus V_n$, *where* $\dim V_i = e = d/n$. *Let* $G := G_1 \rtimes \mathsf{S}_n$, *with* $G_1 = \prod_{i=1}^n \mathrm{GL}(V_i)$, *be the stabilizer of this decomposition in* $\mathrm{GL}(V)$. *If* $k \in \mathbb{Z}_{\geq 1}$ *and* $\Sigma \in \{\mathrm{Sym}, \wedge\}$, *then there is an isomorphism of* $G_1$*-modules*

$$\phi : \Sigma^k(V) \cong \bigoplus_{i_1,\ldots,i_n\in\mathbb{Z}_{\geq 0},\ i_1+i_2+\ldots+i_n=k} \Sigma^{i_1}(V_1)\otimes\Sigma^{i_2}(V_2)\otimes\ldots\otimes\Sigma^{i_n}(V_n), \tag{6.1.8.1}$$

*which is also an isomorphism of* $G$*-modules in the case* $\Sigma = \mathrm{Sym}$. *If* $\Sigma = \wedge$, *then* $\phi$ *needs not be* $G$*-equivariant, but* $\phi$ *has the property that the permutation actions of* $G$ *on the sets of subspaces* $\phi^{-1}\big(\Sigma^{i_1}(V_1)\otimes\Sigma^{i_2}(V_2)\otimes\ldots\otimes\Sigma^{i_n}(V_n)\big)$ *(on the left) and* $\Sigma^{i_1}(V_1)\otimes\Sigma^{i_2}(V_2)\otimes\ldots\otimes\Sigma^{i_n}(V_n)$ *(on the right) are the same.*

PROOF. The existence of a vector space isomorphism $\phi$ is well known, see [**FH**, (B.1), (B.2)]. Now assume $\Sigma = \mathrm{Sym}$. By viewing $V \cong (V^*)^*$, we may identify $\mathsf{S}^k(V)$ as the space of homogeneous polynomials of degree $k$ in $d = en$ variables $x_1, \ldots, x_d$, where $V_i$ is spanned by $x_{(i-1)e+1}, \ldots, x_{ie}$, and on which $\mathrm{GL}(V)$ acts via linear substitutions. Identifying each $\mathsf{S}^j(V_i)$ with the span of degree $j$ homogeneous polynomials in variables $x_{(i-1)e+1}, \ldots, x_{ie}$, we get a canonical isomorphism $\phi$ of $G$-modules.

Next assume that $\Sigma = \wedge$. Recall that $\wedge^k(V)$ is the quotient of $V^{\otimes k}$ by the subspace $X$ spanned by all $v_1\otimes\ldots\otimes v_k$ with two of the vectors equal. If $\pi$ denotes the natural projection, then $v_1\wedge\ldots\wedge v_k = \pi(v_1\otimes\ldots\otimes v_k)$. Furthermore, if $W$ is another $\mathbb{C}$-space, then there is a canonical linear map from $\wedge^a(V)\otimes\wedge^b(W)$ into $\wedge^{a+b}(V\oplus W)$, taking $(v_1\wedge\ldots\wedge v_a)\otimes(w_1\wedge\ldots\wedge w_b)$ to $v_1\wedge\ldots\wedge v_a\wedge w_1\wedge\ldots\wedge w_b$. This determines an isomorphism

$$\wedge^k(V\oplus W) \cong \bigoplus_{a+b=k} \wedge^a(V)\otimes\wedge^b(W), \tag{6.1.8.2}$$

see [**FH**, (B.1)], which can easily be seen to be an isomorphism of $\mathrm{GL}(V)\times\mathrm{GL}(W)$-modules. Assume in addition that $\dim(W) = \dim(V)$ and let $\tau \in \mathrm{GL}(V\oplus W)$ be the involution $e_i \leftrightarrow f_i$, for a fixed basis $(e_1, \ldots, e_d)$ of $V$ and a fixed basis $(f_1, \ldots, f_d)$ of $W$. With $v_i \in V$ and $w_j \in W$ as before, $\tau$ sends $v_1\wedge\ldots\wedge v_a\wedge w_1\wedge\ldots\wedge w_b$ to

$$\tau(v_1)\wedge\ldots\wedge\tau(v_a)\wedge\tau(w_1\wedge\ldots\wedge w_b) = \pm\tau(w_1)\wedge\ldots\wedge\tau(w_b)\wedge\tau(v_1)\wedge\ldots\wedge\tau(v_a)$$

on the left-hand-side of (6.1.8.2), and $(v_1\wedge\ldots\wedge v_a)\otimes(w_1\wedge\ldots\wedge w_b)$ to

$$(\tau(v_1)\wedge\ldots\wedge\tau(v_a))\otimes(\tau(w_1)\wedge\ldots\wedge\tau(w_b)) = (\tau(w_1)\wedge\ldots\wedge\tau(w_b))\otimes(\tau(v_1)\wedge\ldots\wedge\tau(v_a))$$

on the right-hand-side of (6.1.8.2). Taking $v_i$ among $e_1, \dots, e_d$ and $w_j$ among $f_1, \dots, f_d$, we see that the actions of $\sigma$ on the basis vectors of the two spaces in (6.1.8.2) agree with the indicated isomorphism *up to a sign*. This proves the case $n = 2$ for $\wedge^k$. The general case then follows by iterating the isomorphism in (6.1.8.2), noting that $\mathsf{S}_n$ is generated by transpositions. □

The heart of the proof for type $A$ groups relies on the analysis of the following situation:

HYPOTHESIS 6.1.9. Let $V = \mathbb{C}^d$ with $d \geq 3$, $k \in \mathbb{Z}_{\geq 2}$, $\Sigma \in \{\mathrm{Sym}, \wedge\}$, $p$ a prime, and $2 \leq k \leq d-2$ when $\Sigma = \wedge$. Let $J < \mathrm{GL}(V)$ be a finite subgroup with the following properties:

(a) $J = Q \rtimes C$, where $Q$ is a normal $p$-subgroup, and $C = \langle Z, \boldsymbol{\sigma} \rangle$ is a $p'$-subgroup for some $Z < \mathbf{Z}(\mathrm{GL}(V))$ and some $\boldsymbol{\sigma} \in J$;

(b) There exists a linear character $\gamma$ of $Q$ such that the character of the $J$-module $\Sigma^k(V)$ is
$$\varphi + \sum_{i=1}^{m} \theta_i,$$
where $\varphi \in \mathrm{Irr}(J)$, $\varphi(1) > 1$, and $[\varphi|_Q, \gamma]_Q = 0$. Furthermore, either $m = 0$, or $\theta_i \in \mathrm{Irr}(J)$ and $\theta_i|_Q = \theta_i(1)\gamma$ for all $1 \leq i \leq m$.

Note that in the case $\Sigma = \wedge$ we may, and will always, assume further that

$$2 \leq k \leq d/2. \tag{6.1.9.1}$$

Indeed, it is well known that $\wedge^{d-k}(\chi) = \overline{\wedge^k(\chi)}\det(\chi)$. Now, if $J$ satisfies 6.1.9 for $\wedge^k(V)$, then it also satisfies 6.1.9 for $\wedge^{d-k}(V)$, but with $\gamma$ replaced by $\overline{\gamma} \cdot \det(\chi)|_Q$. Replacing $k$ by $d-k$, we can therefore ensure (6.1.9.1).

PROPOSITION 6.1.10. *Assume Hypothesis 6.1.9, and assume in addition that $d \geq 5$ if $\Sigma = \wedge$. Then $J$ acts irreducibly on $V$.*

PROOF. (i) Assume the contrary: $J$ satisfies 6.1.9 but the $J$-character $\chi$ afforded by $V$ is reducible: $\chi = \alpha + \beta$ for some characters $\alpha$ and $\beta$ of $J$, where $a := \alpha(1) \geq \beta(1) =: b \geq 1$. In particular, $2a \geq a + b = d$. We note furthermore that

$$\varphi|_Q \text{ is not scalar.} \tag{6.1.10.1}$$

For, otherwise we would have $\varphi|_{QZ} = \varphi(1)\nu$ for some linear character $\nu$ of $QZ$ (since $Z$ acts via scalars on $\Sigma^k(V)$). Then $\nu$ is $J$-invariant. But $J/QZ$ is cyclic, so $\nu$ extends to $J$, and, by Gallagher's theorem [**Is**, (6.17)], any irreducible character of $J$ that lies above $\nu$ is of degree $\nu(1) = 1$. Thus $\varphi(1) = 1$, contradicting 6.1.9(b).

(ii) By Lemma 6.1.8 we can write

$$\varphi + \sum_{i=1}^{m} \theta_i = \Sigma^k(\alpha + \beta) = \sum_{l=0}^{k} \Sigma^{k-l}(\alpha)\Sigma^l(\beta). \tag{6.1.10.2}$$

Here, some summands $\Sigma^{k-l}(\alpha)\Sigma^l(\beta)$ may be zero in the case $\Sigma = \wedge$. We will call the summand $\Sigma^{k-l}(\alpha)\Sigma^l(\beta)$ *admissible*, if either $\Sigma = \mathrm{Sym}$, or $\Sigma^{k-l}(\alpha)\Sigma^l(\beta) \neq 0$ and $\Sigma = \wedge$. Since $\varphi \neq \theta_i$ by hypothesis, there always exists a unique $j$ such that $\varphi$ is a constituent of an admissible summand $\Sigma^{k-j}(\alpha)\Sigma^j(\beta)$ in (6.1.10.2). Moreover, any admissible $\Sigma^{k-l}(\alpha)\Sigma^l(\beta)$ with $l \neq j$ is a sum of some $\theta_i$ and hence is a multiple of $\gamma$ on restriction to $Q$.

Consider the case $j \neq 1$. By the above, $\bigl(\Sigma^{k-1}(\alpha)\beta\bigr)|_Q$ is a multiple of $\gamma$, and $1 \leq k-1 < d/2 \leq a$ in the case $\Sigma = \wedge$, see (6.1.9.1). By Lemma 6.1.7, both $\alpha|_Q$ and $\beta|_Q$ are scalars: $\alpha|_Q = a\lambda$ and $\beta|_Q = b\nu$ for some linear characters $\lambda, \nu$ of $Q$. In this case, $\bigl(\Sigma^{k-j}(\alpha)\Sigma^j(\beta)\bigr)|_Q$ is a multiple of $\lambda^{k-j}\nu^j$, and so is $\varphi|_Q$, contrary to (6.1.10.1).

(iii) We have shown that $j = 1$. In the case $\Sigma = \wedge$, $k \leq a$ by (6.1.9.1), hence $\Sigma^k(\alpha)$ is always admissible and so is scalar on $Q$. Assume in addition $b = 1$. If $\Sigma = \wedge$, (6.1.9.1) implies $4 \leq 2k \leq a+1$, and so $k \leq a-1$. Hence $\alpha|_Q = \alpha(1)\lambda$ is scalar by Lemma 6.1.7. It follows that $\bigl(\Sigma^{k-1}(\alpha)\beta\bigr)|_Q$ is a multiple of the linear character $\lambda^{k-1} \cdot \beta|_Q$, whence $\varphi|_Q$ is scalar, contradicting (6.1.10.1).

Next suppose $b = 2$. If $\Sigma = \wedge$, then $d \geq 5$ by assumption, whence $k < a$ by (6.1.9.1). Hence we can apply Lemma 6.1.7 to $\Sigma^k(\alpha)$ to see that $\alpha|_Q$ is scalar, and so, as $Z$ acts via scalars on $V$, $\alpha|_{QZ} = a\lambda$ for some linear $\lambda \in \mathrm{Irr}(QZ)$. It follows that $\bigl(\Sigma^{k-1}(\alpha)\beta\bigr)|_{QZ}$ is a multiple of $\lambda^{k-1} \cdot \beta|_{QZ}$. Consider the case $\beta|_{QZ} \in \mathrm{Irr}(QZ)$. Then $\varphi|_{QZ}$ is a multiple of the irreducible character $\lambda^{k-1} \cdot \beta|_{QZ}$, whence the latter is $J$-invariant, and so, $J/QZ$ being cyclic implies by Gallagher's theorem that $\varphi|_{QZ} = \lambda^{k-1} \cdot \beta|_{QZ}$. Note that $\Sigma^{k-1}(\alpha)(1) > 1$, so $\Sigma^{k-1}(\alpha)\beta - \varphi$ is a *true* character, whose restriction to $Q$ is still a multiple of $\lambda^{k-1} \cdot \beta|_Q$, contradicting (6.1.10.2). Assume now that $\beta|_{QZ}$ is reducible. Then $\bigl(\Sigma^{k-1}(\alpha)\beta\bigr)|_{QZ}$ is a multiple of $\lambda^{k-1} \cdot \beta|_{QZ} = \beta_1 + \beta_2$ with $\beta_i \in \mathrm{Irr}(QZ)$ of degree 1. Without loss, we may assume $\varphi|_{QZ}$ contains $\beta_1$. As $J/QZ$ is cyclic, $\mathrm{Stab}_J(\beta_1)$ is cyclic over $QZ$ and has index $\leq 2$ in $J$. Again by Gallagher's theorem, either $\varphi$ is of degree 1 and $\varphi|_{QZ} = \beta_1$, or $\varphi$ is of degree 2 and $\varphi|_{QZ} = \beta_1 + \beta_2$. However, as $\Sigma^{k-1}(\alpha)(1) > 1$, $\Sigma^{k-1}(\alpha)\beta - \varphi$ is again a true character, whose restriction to $Q$ contains $(\beta_1 + \beta_2)|_Q$, contradicting (6.1.10.2).

We have shown that $b \geq 3$. Consider the case $k \geq 3$. Then we can apply Lemma 6.1.7 to $\Sigma^{k-2}(\alpha)\Sigma^2(\beta)$ to see that $\alpha|_Q = a\lambda$ and $\beta|_Q = b\nu$ for some linear $\lambda, \nu \in \mathrm{Irr}(Q)$. In this case, $\bigl(\Sigma^{k-1}(\alpha)\beta\bigr)|_Q$ is a multiple of $\lambda^{k-1}\nu$, whence so is $\varphi|_Q$, contrary to (6.1.10.1). Finally, assume that $k = 2$. Applying Lemma 6.1.7 to $\Sigma^2(\alpha)$ and $\Sigma^2(\beta)$, we again see that $\alpha|_Q = a\lambda$ and $\beta|_Q = b\nu$ for some linear $\lambda, \nu \in \mathrm{Irr}(Q)$, and arrive at a contradiction as in the previous case. □

PROPOSITION 6.1.11. *Under Hypothesis 6.1.9, suppose that $J$ acts transitively on the summands of a decomposition $V = V_1 \oplus V_2 \oplus \ldots \oplus V_n$ with $\dim V_i =: t = d/n < d$. Then one of the following statements holds.*

(A) *$Q$ stabilizes each $V_i$.*

(B) *$\Sigma = \wedge$, $t = 1$, and one of the following possibilities occurs:*

  (a) *$p = 2$, $d = 4$, and $k = 2$.*

  (b) *$p = 3$, $d = 6$, and $k = 3$.*

  (c) *$p = 2$, $d = 8$, $k = 3$, $J$ is irreducible on $\wedge^3(V)$, and $\boldsymbol{\sigma}$ has at most 14 distinct eigenvalues on $\wedge^3(V)$.*

  (d) *$d = p^e$, $k = 2$, $J$ is irreducible on $\wedge^2(V)$, and $\boldsymbol{\sigma}$ has at most $\kappa(d-1)/2$ distinct eigenvalues on $\wedge^2(V)$, where either $\kappa = 4$, or $d \equiv 3(\mathrm{mod} 4)$ and $\kappa = 5$.*

PROOF. Let $\chi$ denote the character of $J$ acting on $V$, and $\epsilon := +$ or $-$ according as $\Sigma = \mathrm{Sym}$ or $\wedge$. Note that $J$ is contained in the stabilizer $\prod_{i=1}^n \mathrm{GL}(V_i) \rtimes \mathsf{S}_n$ of the decomposition.

Hence we can use Lemma 6.1.8 and the isomorphism $\phi$ in (6.1.8.1) to replace $\Sigma^k(V)$ by the direct sum in the right-hand-side of (6.1.8.1); in particular, we will identify each $\phi^{-1}\big(\Sigma^{i_1}(V_1)\otimes \Sigma^{i_2}(V_2)\otimes\ldots\otimes\Sigma^{i_n}(V_n)\big)$ with $\Sigma^{i_1}(V_1)\otimes\Sigma^{i_2}(V_2)\otimes\ldots\otimes\Sigma^{i_n}(V_n)$. We will assume that (A) does not hold, that is, $Q$ acts *nontrivially* on $\Omega := \{V_1, V_2, \ldots, V_n\}$, and let $D$ denote the kernel of the action of $J$ on $\Omega$.

(i) First we consider the case where either $\Sigma = \mathrm{Sym}$, or $\Sigma = \wedge$ but $k \leq t$. Then we use (6.1.8.1) to write $\Sigma^k(V) = A \oplus B$ as a direct sum of two $J$-submodules, where $A = \Sigma^k(V_1)\oplus\ldots\oplus\Sigma^k(V_n)$ and $B$ is the direct sum of all remaining summands.

Suppose that $\varphi$ is a constituent of the character of $B$. Then the character of the $Q$-module $A$ is scalar. Now, for any $Q$-orbit on $\Omega$, say $\{V_1, \ldots, V_m\}$, the submodule $\oplus_{i=1}^m \Sigma^k(V_i)$ of $A$ is an induced $Q$-module. It follows from Lemma 6.1.7(iii) that $m = 1$, and thus $Q$ acts trivially on $\Omega$.

We have shown that $\varphi$ is a constituent of the character of $A$, whence the character of the $Q$-module $B$ is scalar. Since $Q$ permutes the summands in $B$, applying Lemma 6.1.7(iii) as above, we see that $Q$ fixes each summand occurring in $B$. In particular, if $k \geq 3$, or if $k = 2$ but $n \geq 3$, then $Q$ must fix each of the summands $\Sigma^{k-1}(V_i)\otimes V_j$ with $1 \leq i \neq j \leq n$, and so it again acts trivially on $\Omega$. It follows that

$$k = n = 2,\ V = V_1 \oplus V_2,\ \Sigma^2(V) \cong \big(\Sigma^2(V_1)\oplus\Sigma^2(V_2)\big)\oplus V_1\otimes V_2.$$

As $Q$ acts nontrivially on $\Omega$, we have $Q = \langle Q_1, g\rangle$, where $Q_1$, of index 2 in $Q$, fixes each of $V_1$ and $V_2$, and $g : V_1 \leftrightarrow V_2$; in particular, $\chi(g) = 0$. Fix a basis $(e_1, \ldots, e_t)$ for $V_1$, so that $(f_i := g(e_i) \mid 1 \leq i \leq t)$ is a basis for $V_2$. As $Q_1 < G_1 = \mathrm{GL}(V_1)\times\mathrm{GL}(V_2)$, by Lemma 6.1.8 the $Q_1$-modules $B$ and $V_1 \otimes V_2$ are isomorphic. But $Q|_B$ is scalar, so $Q_1$ is scalar on both $V_1$ and $V_2$ by Lemma 6.1.7(i). As $g^2 \in Q_1$, it follows that

$$g^2 : e_i \mapsto \alpha e_i,\ f_i = g(e_i) \mapsto g^3(e_i) = g(g^2(e_i)) = g(\alpha e_i) = \alpha f_i,\ 1 \leq i \leq t \tag{6.1.11.1}$$

for some root of unity $\alpha \in \mathbb{C}^\times$. Also note that $g : \Sigma^2(V_1) \leftrightarrow \Sigma^2(V_2)$, so

$$\mathrm{Tr}(g|_B) = \mathrm{Tr}(g|_{\Sigma^2(V)}) = \Sigma^2(\chi)(g) = \frac{\chi(g)^2 + \epsilon\chi(g^2)}{2} = t\alpha$$

by (6.1.11.1). On the other hand, $\dim(B) = t^2$, and $t = d/2 > 1$. It follows that $g|_B$ is not a scalar, a contradiction.

(ii) We have shown that $\Sigma = \wedge$ and $k > t = \dim(V_i)$. Since $2 \leq k \leq d/2$, we can write $k = at + b$, with $a \leq n/2$ and $0 \leq b \leq t-1$. Here we consider the case $t \geq 2$. Write $\wedge^k(V) = A \oplus B$, where $A$ is the sum of summands $\wedge^{i_1}(V_1)\otimes\ldots\otimes\wedge^{i_n}(V_n)$ subject to the condition that exactly $a$ of the $i_j$ take value $t$, one of the remaining takes value $b$, and all the others equal 0; in particular, $A$ contains the summand $A_1 := \wedge^t(V_1)\otimes\wedge^t(V_2)\otimes\ldots\otimes\wedge^t(V_a)\otimes\wedge^b(V_{a+1})$.

Consider the case $\varphi$ is a constituent of $B$. Then $Q|_A$ is scalar. It follows from Lemma 6.1.7(iii) that $Q$ stabilizes every summand in $B$ (as any nontrivial $Q$-orbit would lead to a non-scalar imprimitive $Q$-module). Let $\Delta := \{V_1, \ldots, V_a\}$ if $b = 0$ and $\Delta := \{V_1, \ldots, V_a, V_{a+1}\}$ if $b > 0$. As $Q$ fixes $A_1$, $Q$ fixes $\Delta$. If $b = 0$, then $|\Delta| = a = k/t \leq d/2t = n/2 \leq n-1$. If $b > 0$, then $tn = d \geq 2k = 2at + 2b > 2at$, whence $n \geq 2a+1$ and $|\Delta| = a+1 \leq n-1$. Thus $\Delta \neq \Omega$. The same argument applied to any $\mathsf{S}_n$-conjugate of $\Delta$ shows that $Q$ fixes any $|\Delta|$-subset of $\Omega$. By Lemma 6.1.7(iv), $Q$ must act trivially on $\Omega$, i.e. (A) holds.

Next assume that $\varphi$ is a constituent of $A$. Then $Q|_B$ is scalar, and so, by Lemma 6.1.7(iii), $Q$ stabilizes every summand in $B$. Assume in addition that $0 \leq b \leq t-2$. Then $B$ contains the summand

$$B_1 := \wedge^t(V_1) \otimes \wedge^t(V_2) \otimes \ldots \otimes \wedge^t(V_{a-1}) \otimes \wedge^{t-1}(V_a) \otimes \wedge^{b+1}(V_{a+1}),$$

whence $Q$ fixes $\Delta_1 := \{V_1, V_2, \ldots, V_{a+1}\}$. If $a \leq n-2$, then $\Delta' \neq \Omega$. The same argument applied to any $(a+1)$-subset of $\Omega$, and so $Q$ acts trivially on $\Omega$ by Lemma 6.1.7(iv). So $n/2 \geq a \geq n-1$, whence $n = 2$, $a = 1$, and $b = 0$ as $k \leq d/2$. Hence $k = t$, which is impossible by (i).

Assume now that $b = t-1$. Then $tn = d \geq 2k = 2at + 2t - 2 \geq t(2a+1)$, i.e. $n \geq 2a+1 \geq a+2$. Suppose in addition that $a \leq n-3$. Then $B$ contains the summand

$$B_2 := \wedge^t(V_1) \otimes \wedge^t(V_2) \otimes \ldots \otimes \wedge^t(V_{a-1}) \otimes \wedge^{t-1}(V_a) \otimes \wedge^{t-1}(V_{a+1}) \otimes V_{a+2},$$

whence $Q$ fixes $\Delta_2 := \{V_1, V_2, \ldots, V_{a+1}, V_{a+2}\}$, a proper subset of $\Omega$. The same argument applied to any $(a+2)$-subset of $\Omega$, and so $Q$ acts trivially on $\Omega$ by Lemma 6.1.7(iv). So $a = n-2$, whence $a = 1$, $n = 3$, $3t = d \geq 2k = 2(2t-1)$, and so $t = 2$. In this case, $J$ acts transitively on $\Omega = \{V_1, V_2, V_3\}$, and the normal $p$-subgroup $Q$ acts nontrivially on it. It follows that $Q = \langle Q_2, h\rangle$, where $Q_2$, a normal subgroup of index 3 in $Q$, fixes each of $V_i$, and $h : V_1 \mapsto V_2 \mapsto V_3 \mapsto V_1$; in particular, $\chi(h) = 0$. Fix a basis $(u_1, u_2)$ for $V_1$, so that $(v_i := h(u_i) \mid i = 1, 2)$ is a basis for $V_2$, and $(w_i := h^2(u_i) \mid i = 1, 2)$ is a basis for $V_3$. As $Q_2 < G_1 = \mathrm{GL}(V_1) \times \mathrm{GL}(V_2) \times \mathrm{GL}(V_3)$, by Lemma 6.1.8 the $Q_2$-modules $B$ and $V_1 \otimes V_2 \otimes V_3$ are isomorphic. But $B|_Q$ is scalar, so $Q_2$ is scalar on each $V_i$ by Lemma 6.1.7(i). As $h^3 \in Q_2$, it follows that

(6.1.11.2)

$$h^3 : u_i \mapsto \beta u_i,\ v_i \mapsto h^4(u_i) = h(h^3(u_i)) = \beta v_i,\ w_i \mapsto h^5(u_i) = h^2(h^3(u_i)) = \beta w_i,\ i = 1, 2$$

for some root of unity $\beta \in \mathbb{C}^\times$. One can check that the trace of $h$ on $A$ is 0, so

$$\mathrm{Tr}(h|_B) = \mathrm{Tr}(h|_{\wedge^3(V)}) = \wedge^3(\chi)(h) = \frac{\chi(h)^3 - 3\chi(h^2)\chi(h) + 2\chi(h^3)}{6} = 2\beta$$

by (6.1.11.2). On the other hand, $\dim(B) = 8$, whence $h|_B$ is not a scalar, a contradiction.

(iii) It remains to handle the case $t = \dim(V_i) = 1$. Let $\Omega(k)$ denote the set of all $k$-subsets of $\Omega$. By Lemma 6.1.7(iii), any nontrivial $Q$-orbit on $\Omega(k)$ leads to a non-scalar $Q$-module. A $J$-orbit on $\Omega(k)$ will be called *$Q$-nontrivial* if $Q$ acts nontrivially on it. It follows from 6.1.9(b) that

(6.1.11.3) $J$ has at most one $Q$-nontrivial orbit on $\Omega(k)$.

Here we aim to show that $J$ acts *$k$-homogeneously* on $\Omega$, i.e.

(6.1.11.4) $J$ acts transitively on $\Omega(k)$.

Since $J$ acts transitively on $\Omega$ and $Q \lhd J$ acts nontrivially on $\Omega$, all $Q$-orbits on $\Omega$ have the same length $s > 1$. If $s \nmid k$, then any $\Delta \in \Omega(k)$ cannot be stabilized by $Q$, whence $Q$ acts nontrivially on the $J$-orbit of $\Delta$, and so this orbit is the entire $\Omega(k)$ by (6.1.11.3), and thus (6.1.11.4) holds. Hence, we may write $k = as$ for some $a \in \mathbb{Z}_{\geq 1}$. Since $Q$ acts nontrivially on $\Omega$, we may assume that $g(V_1) = V_2$ for some $g \in Q$. Also recall that $|\Omega| = n \geq 2k = 2as$. So we can find distinct $Q$-orbits $\Omega_1, \ldots, \Omega_a, \ldots, \Omega_{2a}$ (all of length $s$). We may assume $\Omega_a$ contains $V_1$, hence also $V_2 = g(V_1)$.

Consider the case $s \geq 3$. Then we may assume $V_3 \in \Omega_a$, and take the $k$-subset

$$X := \Omega_1 \sqcup \Omega_2 \sqcup \ldots \sqcup \Omega_{a-1} \sqcup (\Omega_a \smallsetminus \{V_2\}) \sqcup \{V_{i_0}\},$$

with $V_{i_0}$ contained in $\Omega_{a+1}$. As $g(V_1) = V_2 \notin X$, $g(X) \neq X$. Now if $n/s \geq a+2$, then we can find $V_{j_0}$ contained in $\Omega_{a+2}$, and set

$$Y := \Omega_1 \sqcup \Omega_2 \sqcup \ldots \sqcup \Omega_{a-1} \sqcup (\Omega_a \smallsetminus \{V_2, V_3\}) \sqcup \{V_{i_0}\} \sqcup \{V_{j_0}\}.$$

Again, $g(V_1) = V_2 \notin Y$, so $g(Y) \neq Y$. Thus the $J$-orbits of $X$ and of $Y$ are both $Q$-nontrivial. However, these two orbits are distinct (since $X$ intersects exactly $a+1$ $Q$-orbits and $Y$ intersects exactly $a+2$ $Q$-orbits), and this contradicts (6.1.11.3). If $n/s \leq a+1$, then in fact $(a,k,n) = (1,s,2s)$. Note that if $s = 3$, then $p = 3$ as $Q$ has orbits of length $s$, and we arrive at (B)(b). So we may assume $s \geq 4$ and choose a $k$-subset $Y_1$ of $\Omega = \Omega_1 \sqcup \Omega_2$ with $\{|Y_1 \cap \Omega_1|, |Y_1 \cap \Omega_2|\} = \{s-2, 2\}$. Clearly, $Y_1$ is not $Q$-invariant, so its $J$-orbit is again $Q$-nontrivial, and distinct from the $J$-orbit of $X$, since $\{|X \cap \Omega_1|, |X \cap \Omega_2|\} = \{s-1, 1\}$, again contradicting (6.1.11.3).

Next suppose that $s = 2$, so that $k = 2a$ and $p = 2$, but (B)(a) does not hold. Now we have $n = d \geq \max(5, 2k)$, and so $n/s \geq a+2$. Choose $X$ as before, and take a $k$-subset $Y_2$ of $\Omega$ with $Y_2 \supset \Omega_1 \sqcup \ldots \sqcup \Omega_{a-2}$ and $|Y_2 \cap \Omega_j| = 1$ for $a-1 \leq j \leq a+2$. Clearly, $Y_2$ is not $Q$-invariant, so its $J$-orbit is again $Q$-nontrivial, and distinct from the $J$-orbit of $X$ (since $X$ intersects exactly $a+1$ $Q$-orbits and $Y_2$ intersects exactly $a+2$ $Q$-orbits), again contradicting (6.1.11.3).

(iv) We may now assume that $J$ is $k$-homogeneous on $\Omega$, see (6.1.11.4). Let $\bar{J} = J/D \leq \mathsf{S}(\Omega)$ denote the permutation group induced by this action, and let $\bar{Q}$ denote the image of $Q$, which is a nontrivial $p$-subgroup by assumption. We claim that $\Omega$ can be identified with some $W = \mathbb{F}_p^e$, $e \in \mathbb{Z}_{\geq 1}$, such that the action of $\bar{J}$ on $\Omega$ is realized by a subgroup of the group

$$\mathrm{AGL}(W) = \bigl\{w \mapsto f(w) + v \mid f \in \mathrm{GL}(W),\ v \in W\bigr\} \cong \mathrm{AGL}_e(p)$$

of affine transformations of $W$. Since $\mathbf{O}_p(\bar{J}) \geq \bar{Q} > 1$, the claim follows if $\bar{J}$ is 2-transitive, see [**Cam**, Theorem 4.1]. Assume $\bar{J}$ is not 2-transitive. Then it cannot be $k$-transitive, and such groups are classified in [**Kan2**, Theorem 1]. As $\bar{J}$ is solvable, we can easily check that the claim holds in these cases as well; in fact, we can verify that $k = 2$ and $n \equiv 3 (\mathrm{mod}\ 4)$.

Note that in all cases, $\bar{J}$ is a primitive subgroup of $\mathsf{S}(\Omega)$. Now we can write $\bar{J} = \bar{W} \rtimes \bar{J}_0$, where $\bar{W}$ consists of translations $w \mapsto v + w$ and it is the unique minimal normal subgroup of $\bar{J}$, see [**Cam**, Theorem 4.1], and $\bar{J}_0 \leq \mathrm{GL}(W)$ is the stabilizer of 0 in $\bar{J}$. We can now write (6.1.11.5)

$$V = \bigoplus_{x \in W} V_x \text{ with } V_x = \langle e_x \rangle_{\mathbb{C}}, \quad \text{and } \forall h \in Q, \text{ there is } v \in W \text{ such that } h(e_x) \in V_{x+v}.$$

Next we aim to show that $k = 2$. Assume the contrary: $k \geq 3$. If $p > 2$, then $\bar{J}_0 \leq \mathrm{GL}(W)$ cannot act 2-transitively on $W \smallsetminus \{0\}$ (indeed, it acts imprimitively, preserving the sets of nonzero points on $\mathbb{F}_p$-lines of $W$), whence $\bar{J}$ is not $k$-transitive on $W$ with $k \geq 3$. The latter cannot happen by [**Kan2**, Theorem 1], since $n = p^e$ is odd and $\bar{J}$ is solvable.

If $p = 2$, then $n = 2^e \geq 8$, and $\bar{J}_0 \leq \mathrm{GL}(W)$ cannot act 3-transitively on $W \smallsetminus \{0\}$ (indeed, it acts on the sets of nonzero points $\{x, y, x+y\}$ on $\mathbb{F}_2$-planes of $W$), whence $\bar{J}$ is not $k$-transitive on $W$. If $k \geq 4$, then the latter cannot happen by [**Kan2**, Theorem 1], since

$\bar{J}$ is solvable. So assume $k = 3$. Again applying [**Kan2**, Theorem 1], we see that $\bar{J}$ is still 2-transitive, and thus $\bar{J}_0$ is transitive on $W \smallsetminus \{0\}$. As $\bar{J} \rhd \bar{Q} \neq 1$, we must have $\bar{W} \leq \bar{Q}$. Now, if $\bar{Q} > \bar{W}$, then $1 \neq \bar{Q}/\bar{W} \leq \mathbf{O}_p(\bar{J}_0)$, and so $\bar{J}_0$ fixes the $\mathbf{O}_p(\bar{J}_0)$-fixed point subspace in $W$, which is nonzero and proper, contradicting its transitivity on $W \smallsetminus \{0\}$. So $\bar{Q} = \bar{W}$, and so $\bar{J}_0 \cong \bar{J}/\bar{Q}$ is a cyclic $2'$-subgroup of $\mathrm{GL}(W)$. Any odd-order subgroup cannot be 2-transitive, so $\bar{J}$ is 3-homogeneous but not 3-transitive on $n = 2^e \geq 8$ points of $W$, with socle $\bar{W}$ and cyclic $\bar{J}_0$. Applying [**Kan2**, Theorem 1] once more, we conclude that $n = 8$ and $\bar{J} \cong \mathrm{AGL}_1(8) \cong 2^3 \rtimes 7$. In this case, consider the action of $h \in Q$ on the decomposition (6.1.11.5). For any three distinct $x, y, z \in W$,

$$h(e_x \wedge e_y \wedge e_z) \in \langle e_{x+v} \wedge e_{y+v} \wedge e_{z+v} \rangle_{\mathbb{C}}$$

can be a multiple of $e_x \wedge e_y \wedge e_z$ only when $\{x, y, z\} = \{x+v, y+v, z+v\}$, in which case $3v = 0$ and $v = 0$, i.e. $h \in D$. It follows that $Q$ acts on $\Omega(3)$ with 7 orbits, of length 8 each. Hence the restriction of $\wedge^3(\chi)$ to $Q$ is the sum of seven characters of the form $\mathrm{Ind}_{Q \cap D}^{Q}(\lambda)$, with $\lambda$ being linear. As $\gamma$ is linear,

$$[\mathrm{Ind}_{Q\cap D}^{Q}(\lambda), \gamma]_Q = [\lambda, \gamma|_{Q \cap D}]_{Q \cap D} \leq 1, \tag{6.1.11.6}$$

whence $[\wedge^3(\chi)|_Q, \gamma]_Q \leq 7$, and so $\varphi(1) \geq \wedge^3(\chi)(1) - 7 = 49$ by (6.1.9)(b). Since $D$ is an abelian normal subgroup of $J$, $\varphi(1)$ divides $|J/D| = 56$ by Ito's theorem [**Is**, (6.15)]. Thus $\varphi(1) = 56$, i.e. $J$ is irreducible on $\wedge^3(V)$. Next, $\boldsymbol{\sigma}$ induces a generator $\boldsymbol{t}$ of $\bar{J}_0 \cong C_7$ and so permutes cyclically the set $W \smallsetminus \{0\}$. Note that $\boldsymbol{\sigma}^7$ fixes each $V_x$ in the decomposition (6.1.11.5), and commutes with $\boldsymbol{\sigma}$ that permutes the 7 spaces $V_x$ with $x \neq 0$ cyclically. Hence we can find $\alpha, \beta \in \mathbb{C}^\times$ such that

$$\boldsymbol{\sigma}^7 : e_0 \mapsto \alpha e_0, \ e_x \mapsto \beta e_x, \ \forall x \neq 0.$$

Thus $\boldsymbol{\sigma}^7$ has only 2 eigenvalues $\alpha\beta^2, \beta^3$ on $\wedge^3(V)$, and so $\boldsymbol{\sigma}$ has at most 14 distinct eigenvalues on $\wedge^3(V)$, and we arrive at (B)(c).

(v) It remains to deal with $\Sigma^k(V) = \wedge^2(V)$. We now show that

$$d = p^e, \ \bar{Q} = \bar{W}, \ \text{and } |J/D| \in \{d(d-1), d(d-1)/2\}. \tag{6.1.11.7}$$

First, $d = p^e$ by (6.1.11.5). Next, as mentioned above, if $\bar{J}$ is 2-transitive, then $\bar{W} = \bar{Q}$, and so $\bar{J}_0 \cong \bar{J}/\bar{Q} \cong J/QD$ is a cyclic $p'$-subgroup of $\mathrm{GL}(W) \cong \mathrm{GL}_e(p)$. Any such subgroup is contained in a maximal torus of $\mathrm{GL}_e(p)$, hence has order $N \leq p^e - 1$. The transitivity of $\bar{J}_0$ on $W \smallsetminus \{0\}$ implies that $N = p^e - 1$, and so $|\bar{J}| = N \cdot |\bar{W}| = d(d-1)$. Next, $\boldsymbol{\sigma}$ induces a generator $\boldsymbol{t}$ of $\bar{J}_0$ and so permutes cyclically the set $W \smallsetminus \{0\}$. Note that $\boldsymbol{\sigma}^N$ fixes each $V_x$ in the decomposition (6.1.11.5), and commutes with $\boldsymbol{\sigma}$ that permutes the $N$ spaces $V_x$ with $x \neq 0$ cyclically. Hence we can find $\alpha, \beta \in \mathbb{C}^\times$ such that

$$\boldsymbol{\sigma}^N : e_0 \mapsto \alpha e_0, \ e_x \mapsto \beta e_x, \ \forall x \neq 0.$$

Thus $\boldsymbol{\sigma}^N$ has only 2 eigenvalues $\alpha\beta, \beta^2$ on $\wedge^2(V)$, and so $\boldsymbol{\sigma}$ has at most $2N = 2(d-1)$ distinct eigenvalues on $\wedge^2(V)$.

Suppose $\bar{J}$ is not 2-transitive, whence it has odd order and $d = n = p^e \equiv 3 (\mathrm{mod}\ 4)$. One can identify $W$ with the field $\mathbb{F}_{p^e}$ such that $\bar{J}_0$ has 2 orbits on $W \smallsetminus \{0\}$: the set $W_+$ of squares and the set $W_-$ of non-squares of $\mathbb{F}_{p^e}^\times$, and is contained in the subgroup $\Gamma L_1(p^e)$ of the semilinear transformations of $\mathbb{F}_{p^e}$, see [**Kan1**, Proposition 3.1]. If $\bar{W} < \bar{Q}$ in this case, then $\bar{J}_0$

would stabilize a nonzero proper subspace of $W$, hence a subset of size $2 \leq p^{e'}-1 < (p^e-1)/2$ of $W \smallsetminus \{0\}$, which is impossible. Thus we again have $\bar{Q} = \bar{W}$, and so $\bar{J}_0 \cong \bar{J}/\bar{Q}$ is a cyclic $p'$-subgroup of $\mathrm{GL}(W) \cong \mathrm{GL}_e(p)$, of order $N \leq p^e - 1$ as above. As $\bar{J}_0$ has two orbits of length $(p^e-1)/2$ on $W \smallsetminus \{0\}$, we must have that $N = d-1$ or $(d-1)/2$, and (6.1.11.7) is proved. Next, $\boldsymbol{\sigma}$ induces a generator $\boldsymbol{t}$ of $\bar{J}_0$ and so permutes cyclically each of the sets $W_+$ and $W_-$. Now $\boldsymbol{\sigma}^{(d-1)/2}$ fixes each $V_x$ in the decomposition (6.1.11.5), and commutes with $\boldsymbol{\sigma}$ that permutes the $(d-1)/2$ spaces $V_x$ with $x \in W_+$, respectively with $x \in V_-$, cyclically. Hence we can find $\alpha, \beta_+, \beta_- \in \mathbb{C}^\times$ such that

$$\boldsymbol{\sigma}^{(d-1)/2} : e_0 \mapsto \alpha e_0,\ e_x \mapsto \beta_+ e_x,\ \forall x \in W_+,\ e_y \mapsto \beta_- e_y,\ \forall y \in W_-.$$

Thus $\boldsymbol{\sigma}^{(d-1)/2}$ has only 5 eigenvalues $\alpha\beta_+, \alpha\beta_-, \beta_+^2, \beta_-^2, \beta_+\beta_-$ on $\wedge^2(V)$, and so $\boldsymbol{\sigma}$ has at most $5(d-1)/2$ distinct eigenvalues on $\wedge^2(V)$.

We again consider the action of any $h \in Q$ on the decomposition (6.1.11.5). For any $x \neq y \in W$, $h(e_x \wedge e_y) \in \langle e_{x+v} \wedge e_{y+v} \rangle_{\mathbb{C}}$ can be a multiple of $e_x \wedge e_y$ only when $\{x, y\} = \{x+v, y+v\}$. If $p > 2$, we then have $2v = 0$ and $v = 0$, i.e. $h \in D$. It follows that $Q$ acts on $\Omega(2)$ with $(d-1)/2$ orbits, of length $d$ each. Hence $\wedge^2(\chi)|_Q$ is the sum of $(d-1)/2$ characters of the form $\mathrm{Ind}_{Q \cap D}^{Q}(\lambda)$, with $\lambda$ being linear. Using (6.1.11.6), we see that $[\wedge^2(\chi)|_Q, \gamma]_Q \leq (d-1)/2$, and thus

$$\varphi(1) \geq \wedge^2(\chi)(1) - (d-1)/2 = (d-1)^2/2 \tag{6.1.11.8}$$

by (6.1.9)(b).

If $p = 2$, then we have either $v = 0$, or $v = x + y$. It follows that $Q$ acts on $\Omega(2)$ with $d-1$ orbits, of length $d/2$ each. Hence $\wedge^2(\chi)|_Q$ is the sum of $d-1$ characters of the form $\mathrm{Ind}_{Q_1}^{Q}(\lambda)$, with $\lambda$ being linear and $|Q_1/(Q \cap D)| = 2$. Again using (6.1.11.6), we see that $[\wedge^2(\chi)|_Q, \gamma]_Q \leq d-1$, and so

$$\varphi(1) \geq \wedge^2(\chi)(1) - (d-1)/2 = (d-1)(d-2)/2 \tag{6.1.11.9}$$

by (6.1.9)(b).

In both cases, $D$ is an abelian normal subgroup of $J$, so $\varphi(1)$ divides $|J/D|$ by Ito's theorem, and $|J/D|$ divides $d(d-1) = 2(\dim \wedge^2(V))$ by (6.1.11.7). Noting $2 = k \leq d/2$ and assuming (B)(a) does not hold, we conclude from (6.1.11.8) and (6.1.11.9) that $\varphi(1) = d(d-1)/2$, i.e. $J$ is irreducible on $\wedge^2(V)$, establishing (B)(d). □

PROPOSITION 6.1.12. *Under Hypothesis 6.1.9, suppose that $J$ acts irreducibly on $V$. Then either $Q$ acts irreducibly on $V$, or one of the following holds.*

(a) $\Sigma^k = \mathrm{Sym}^2$, *$d = 3$, and $V|_Q$ is a sum of* 3 *irreducible submodules of dimension* 1.
(b) $\Sigma = \wedge$, *$k = 2, 3$, $d = 6$, and $V|_Q$ is a sum of $d/k$ irreducible submodules of dimension $k$.*
(c) $\Sigma = \wedge$, *$k = 2, 3$, $d \leq 2k$, and $V|_Q$ is a sum of $d$ irreducible submodules of dimension* 1.

PROOF. Assume that $Q$ is reducible on $V$. Then $QZ$ is also reducible on $V$, and since $J/QZ$ is cyclic but $J$ is irreducible, we can decompose

$$V|_{QZ} = V_1 \oplus V_2 \oplus \ldots \oplus V_m,$$

where $V_i \in \mathrm{Irr}(QZ)$, $\dim V_i =: t = d/m$ and $m \geq 2$. Since $\boldsymbol{\sigma}$ generates $J/QZ$, we may also write

$$\boldsymbol{\sigma} : V_1 \mapsto V_2 \mapsto \ldots \mapsto V_m \mapsto V_1, \tag{6.1.12.1}$$

in particular, $R := \langle \boldsymbol{\sigma}^m, QZ \rangle$ fixes each $V_i$. Since $R \lhd J$, if a subspace $U \subseteq \Sigma^k(V)$ is $R$-stable, then so is $\boldsymbol{\sigma}^i(U)$, and $\langle \boldsymbol{\sigma} \rangle(U) = \sum_{i=0}^{m-1} \boldsymbol{\sigma}^i(U)$ is a $G$-submodule. In what follows, we will choose $U$ to be some summand in the decomposition (6.1.8.1).

(ii) First we consider the case $\Sigma = \mathrm{Sym}$. Using Lemma 6.1.8 we can write $\mathrm{Sym}^k(V) = A \oplus B$, where $A = \oplus_{i=1}^m \mathrm{Sym}^k(V_i)$ and $B$, the sum of the remaining summands, are both $J$-invariant. If the $J$-character of $A$ contains $\varphi$, then $Q$ is scalar on summands $\mathrm{Sym}^{k-1}(V_i) \otimes V_j$ (with $i \neq j$), and so $Q|_{V_i}$ is scalar by Lemma 6.1.7, say $V_i$ affords the $Q$-character $\lambda_i$. By (6.1.9)(b), $\lambda_i^{k-1}\lambda_j = \gamma$ for all $i \neq j$, and $n = d \geq 3$. It follows that $\lambda_i = \lambda_1$ and $\lambda_1^k = \gamma$. But in this case, $Q$ acts on $A$ via the character $\dim(A)\gamma$, and so $[\varphi|_Q, \gamma]_Q > 0$, violating (6.1.9)(b).

Hence the $J$-character of $B$ contains $\varphi$, and so $Q|_A$ is scalar and $Q|_{V_i}$ is again scalar by Lemma 6.1.7(ii). Again let $\lambda_i$ be the $Q$-character of $V_i$, and we also have $n = d \geq 3$ and $\lambda_i^k = \gamma$. Note that the $\lambda_i$ are pairwise distinct, since $J$ is irreducible on $V$. If $k \geq 3$, then $B$ contains the direct sum of two proper $J$-submodules $B_1 \oplus B_2$, where

$$\begin{aligned} B_1 &:= \mathrm{Sym}^{k-1}(V_1) \otimes V_2 \oplus \mathrm{Sym}^{k-1}(V_2) \otimes V_3 \oplus \ldots \oplus \mathrm{Sym}^{k-1}(V_m) \otimes V_1, \\ B_2 &:= V_1 \otimes \mathrm{Sym}^{k-1}(V_2) \oplus V_2 \otimes \mathrm{Sym}^{k-1}(V_3) \oplus \ldots \oplus V_n \otimes \mathrm{Sym}^{k-1}(V_m). \end{aligned}$$

If moreover the character of $B_2$ contains $\varphi$, then $Q|_{B_1}$ is scalar, and in fact $\lambda_1^{k-1}\lambda_2 = \gamma = \lambda_1^k$, whence $\lambda_1 = \lambda_2$, a contradiction. Otherwise $Q|_{B_2}$ is scalar, and in fact $\lambda_1\lambda_2^{k-1} = \gamma = \lambda_2^k$, whence $\lambda_1 = \lambda_2$, again a contradiction. If $k = 2$ and $d \geq 4$, then $B$ contains the direct sum of two proper $J$-submodules $B_1 \oplus B_3$, with

$$\begin{aligned} B_1 &:= \langle \boldsymbol{\sigma} \rangle(V_1 \otimes V_2) = V_1 \otimes V_2 \oplus V_2 \otimes V_3 \oplus \ldots \oplus V_{m-1} \otimes V_m \oplus V_m \otimes V_1, \\ B_3 &:= \langle \boldsymbol{\sigma} \rangle(V_1 \otimes V_3) = V_1 \otimes V_3 \oplus V_2 \otimes V_4 \oplus \ldots \oplus V_{m-1} \otimes V_1 \oplus V_m \otimes V_2. \end{aligned}$$

Now we can repeat the previous argument to reach a contradiction.

(ii) From now on we may assume $\Sigma = \wedge$ and $2 \leq k \leq d/2$, see (6.1.9.1). We also write

$$k = qt + r,$$

where $q, r \in \mathbb{Z}_{\geq 0}$ and $0 \leq r \leq t-1$. Here we consider the case $t \geq 3$.

First assume that $r \geq 2$. If $q = 0$, then $m \geq q + 2$. If $q \geq 1$, then $mt = d \geq 2k = 2qt + 2r > 2qt$, and so $m \geq 2q + 1 \geq q + 2$ as well. Hence, (6.1.12.1) implies that $\wedge^k(V)$ contains the direct sum $\langle \boldsymbol{\sigma} \rangle(X) \oplus \langle \boldsymbol{\sigma} \rangle(Y)$ of $G$-modules, where

$$X = \wedge^t(V_1) \otimes \wedge^t(V_2) \otimes \ldots \otimes \wedge^t(V_q) \otimes \wedge^r(V_{q+1}), \; Y = \wedge^t(V_1) \otimes \wedge^t(V_2) \otimes \ldots \otimes \wedge^t(V_q) \otimes \wedge^{r-1}(V_{q+1}) \otimes V_{q+2}.$$

By (6.1.9)(b), the character of at least one of them, say $\langle \boldsymbol{\sigma} \rangle(X)$, does not contain $\varphi$. It follows from Lemma 6.1.7 that $Q|_{V_{q+1}}$ is scalar, and so $1 = \dim(V_{q+1}) = t$ by irreducibility, a contradiction.

Next assume that $r = 1$. Then we still have $mt = d > 2qt$ and $m \geq q + 2$; also $q \geq 1$ as $2 \leq k = qt + 1$. Hence, (6.1.12.1) implies that $\wedge^k(V)$ contains the direct sum $\langle \boldsymbol{\sigma} \rangle(X) \oplus \langle \boldsymbol{\sigma} \rangle(Y_1)$ of $G$-modules, where $X$ is as above, and

$$Y_1 = \wedge^t(V_1) \otimes \wedge^t(V_2) \otimes \ldots \otimes \wedge^t(V_{q-1}) \otimes \wedge^{t-1}(V_q) \otimes \wedge^2(V_{q+1}).$$

By (6.1.9)(b), the character of at least one of them, say $\langle \boldsymbol{\sigma} \rangle(Y_1)$, does not contain $\varphi$. It follows from Lemma 6.1.7 that $Q|_{V_q}$ is scalar, and so $1 = \dim(V_q) = t$, again a contradiction.

Assume now that $r = 0$. Then $q \geq 1$ as $2 \leq k = qt$, and $mt = d \geq 2qt$ implies $m \geq q+1$. If moreover $(m,t) = (q+1,3)$, then $(d,k) = (6,3)$. Hence we may assume $m \geq q+2$ when $t = 3$. Now, (6.1.12.1) implies that $\wedge^k(V)$ contains the direct sum $\langle \boldsymbol{\sigma} \rangle(X_2) \oplus \langle \boldsymbol{\sigma} \rangle(Y_2)$ of $G$-modules, where

$$X_2 = \wedge^t(V_1) \otimes \wedge^t(V_2) \otimes \ldots \otimes \wedge^t(V_{q-1}) \otimes \wedge^{t-1}(V_q) \otimes V_{q+1},$$
$$Y_2 = \begin{cases} \wedge^t(V_1) \otimes \wedge^t(V_2) \otimes \ldots \otimes \wedge^t(V_{q-1}) \otimes \wedge^{t-2}(V_q) \otimes \wedge^2(V_{q+1}), & \text{if } t \geq 4, \\ \wedge^t(V_1) \otimes \wedge^t(V_2) \otimes \ldots \otimes \wedge^t(V_{q-1}) \otimes V_q \otimes V_{q+1} \otimes V_{q+2}, & \text{if } t = 3. \end{cases}$$

By (6.1.9)(b), the character of at least one of them, say $\langle \boldsymbol{\sigma} \rangle(X_2)$, does not contain $\varphi$. It follows from Lemma 6.1.7 that $Q|_{V_q}$ is scalar, and so $1 = \dim(V_q) = t$, again a contradiction.

(iii) Now we consider the case $t = 2$. We will use the same arguments as in (ii), by exhibiting a direct sum of two $G$-submodules $\langle \boldsymbol{\sigma} \rangle(X) \oplus \langle \boldsymbol{\sigma} \rangle(Y)$. Since at least one of them does not contain $\varphi$ in its character, Lemma 6.1.7 will imply that $Q$ is scalar on tensor factors of $X$ or $Y$, leading to the contradiction that $\dim(V_i) = t = 1$.

Suppose $k = 2q+1 \geq 3$. As $n = 2m \geq 2k$, we have $m \geq q+2$, and can choose

$$X = \wedge^2(V_1) \otimes \wedge^2(V_2) \otimes \ldots \otimes \wedge^2(V_q) \otimes V_{q+1},\ Y = \wedge^2(V_1) \otimes \wedge^2(V_2) \otimes \ldots \otimes \wedge^2(V_{q-1}) \otimes V_q \otimes V_{q+1} \otimes V_{q+2}.$$

Next, suppose that $k = 2q \geq 4$. As $n = 2m \geq 2k$, we have $m \geq q+2$, and can choose

$$X = \wedge^2(V_1) \otimes \wedge^2(V_2) \otimes \ldots \otimes \wedge^2(V_{q-1}) \otimes V_q \otimes V_{q+1},$$
$$Y = \wedge^2(V_1) \otimes \wedge^2(V_2) \otimes \ldots \otimes \wedge^2(V_{q-2}) \otimes V_{q-1} \otimes V_q \otimes V_{q+1} \otimes V_{q+2}.$$

If $k = 2$ and $d = 2m \geq 8$, then we choose $X = V_1 \otimes V_2$ ans $Y = V_1 \otimes V_3$, so that

$$\langle \boldsymbol{\sigma} \rangle(X) = V_1 \otimes V_2 \oplus V_2 \otimes V_3 \oplus \ldots V_m \otimes V_1,\ \langle \boldsymbol{\sigma} \rangle(Y) = V_1 \otimes V_3 \oplus V_2 \otimes V_4 \oplus \ldots,$$

(note that $\dim\langle \boldsymbol{\sigma} \rangle(X) = 2m$, $\dim\langle \boldsymbol{\sigma} \rangle(Y) = 2m$ if $2 \nmid m$ and $\dim\langle \boldsymbol{\sigma} \rangle(Y) = m$ if $2|m$).

(iv) Finally, we consider the case $t = 1$, so that $d = m$, and write $V_i = \langle e_i \rangle_{\mathbb{C}}$. Now, for any $k$-subset $\{i_1, \ldots, i_k\}$ of $\{1, 2, \ldots, d\}$, $\langle \boldsymbol{\sigma} \rangle(\langle e_{i_1} \wedge e_{i_2} \wedge \ldots \rangle_{\mathbb{C}})$ is a $J$-submodule of dimension $\leq d$, and $\wedge^k(V)$ is a direct sum of such submodules. By 6.1.9(b), one of them contains $\varphi$ in its character, in particular,

$$\varphi(1) \leq d, \tag{6.1.12.2}$$

and $Q$ acts via a multiple of $\gamma$ on all others. Let $\lambda_i$ denote the $Q$-character of $V_i$. Since $J/QZ$ is cyclic and $J$ is irreducible on $V$, the $d$ characters $\lambda_1, \lambda_2, \ldots, \lambda_d$ are pairwise distinct.

Suppose $k \geq 3$ and $d \geq 7$, and there exists a $(k-1)$-subset $S = \{j_1, \ldots, j_{k-1}\}$ of $\{3, 4, \ldots, d\}$ such that $Q$ acts on both $e_1 \wedge e_{j_1} \wedge e_{j_2} \wedge \ldots \wedge e_{j_{k-1}}$ and $e_2 \wedge e_{j_1} \wedge e_{j_2} \wedge \ldots \wedge e_{j_{k-1}}$ via the same character $\gamma$. It follows that $\gamma = \lambda_1 \prod_{i=1}^{k-1} \lambda_{j_i} = \lambda_2 \prod_{i=1}^{k-1} \lambda_{j_i}$, and so $\lambda_1 = \lambda_2$, a contradiction. Thus, for each such $S$, the character of $Q$ on at least one of $e_1 \wedge e_{j_1} \wedge e_{j_2} \wedge \ldots \wedge e_{j_{k-1}}$ and $e_2 \wedge e_{j_1} \wedge e_{j_2} \wedge \ldots \wedge e_{j_{k-1}}$ differs from $\varphi$. It follows that

$$\varphi(1) \geq \binom{d-2}{k-1} \geq \binom{d-2}{2} > d$$

(as $3 \leq k \leq d/2$ and $d \geq 7$), and this contradicts (6.1.12.2).

So we have $k = 2$ and $d \geq 5$. Suppose $\varphi$ is contained in the character of

$$M := \langle \boldsymbol{\sigma} \rangle(\langle e_1 \wedge e_2 \rangle_{\mathbb{C}}) = \langle e_1 \wedge e_2, e_2 \wedge e_3, \ldots, e_{d-1} \wedge e_d, e_d \wedge e_1 \rangle_{\mathbb{C}}.$$

In this case, $Q$ acts via $\gamma$ on $e_1 \wedge e_3$ and $e_1 \wedge e_4$, whence $\lambda_1\lambda_3 = \gamma = \lambda_1\lambda_4$, and so $\lambda_3 = \lambda_4$, again a contradiction. Hence $Q$ acts via the character $d\gamma$ on $M$, and so $\gamma = \lambda_1\lambda_2 = \lambda_2\lambda_3$, leading again to the contradiction that $\lambda_2 = \lambda_3$. □

LEMMA 6.1.13. *Let $\mathcal{H}$ be a hypergeometric sheaf of type $(6, m)$ with $m < 6$ in characteristic $p$. Suppose that $G^{\circ}_{\rm geom}$ realizes the image of $\mathrm{SL}_3$ on its representation $L(2\varpi_1)$. Then $p = 2$.*

PROOF. We will show that if $p > 2$, no such $\mathcal{H}$ exists. In view of Theorem 4.1.1, we know $w > 1$. Because $G^0_{\rm geom}$ has no nontrivial outer automorphism which preserves the given representation, Lemma 6.2.2 tells us that after replacing $\mathcal{H}$ by some $\mathcal{L}_\chi \otimes \mathcal{H}$, $\chi$ some tame character, we may assume that $G_{\rm geom} = \mathrm{SL}_3/\mu_2$. View $\mathcal{H}$ as giving a homomorphism $\Psi_0 : \pi_1^{\rm geom}(\mathbb{G}_m) \to \mathrm{SL}_3/\mu_2$, and use the vanishing of $H^2(\pi_1^{\rm geom}, \mu_2)$ to lift $\Psi_0$ to a homomorphism $\Psi : \pi_1^{\rm geom}(\mathbb{G}_m) \to \mathrm{SL}_3$. Then view $\Psi$ as giving a rank 3 lisse sheaf on $\mathbb{G}_m/\overline{\mathbb{F}_p}$ with $\mathrm{Sym}^2(\mathcal{F}) \cong \mathcal{H}$. Because $p \neq 2$, the fact that $\mathcal{H}$ is tame at 0 and has highest $\infty$-slope $1/w$ tells us that $\mathcal{F}$ is tame at 0 and has highest $\infty$-slope $1/w$. Then $w \leq 3$, because $\mathcal{F}$ is not tame at $\infty$ but has $\mathsf{Swan} \leq \mathrm{rank}(\mathcal{F})(1/w) = 3/2$.

Suppose first that $p \geq 5$. Then $w \neq 2$ by [**Ka-ESDE**, 7.2.7], applied to $\mathcal{H}$. [For $w = 2$, the only bad primes are $2, 3$, so if $w = 2$ then $\mathcal{H}$ would have its $G^{0,der}_{\rm geom}$ either $\mathrm{SL}_6$ or $\mathrm{SO}_6$ or $\mathrm{Sp}_6$.] Therefore $w = 3$. This in turn implies that $\mathcal{F}$ is Kloosterman of rank 3. So its $P(\infty)$ representation is the direct sum of three linear characters

$$\bigoplus_{\zeta \in \mu_3(\overline{\mathbb{F}_p})} \mathcal{L}_{\psi(3\zeta x)}.$$

If we arbitrarily label the three elements of $\mu_3(\overline{\mathbb{F}_p})$ as $\zeta_1, \zeta_2, \zeta_3$, then $\mathrm{Sym}^2(\mathcal{F})$ has $P(\infty)$ representation the direct sum of the six linear characters

$$\oplus_{i=1}^3 \mathcal{L}_{\psi(6\zeta_i x)} \bigoplus \oplus_{1 \leq i < j \leq 3} \mathcal{L}_{\psi(3(\zeta_i + \zeta_j)x)}.$$

Because $p \geq 5$, each of these characters of $P(\infty)$ is nontrivial (i.e. each of $\zeta_i$ and $\zeta_i + \zeta_j$ is nonzero in $\overline{\mathbb{F}_p}$), and thus $\mathrm{Sym}^2(\mathcal{F}) \cong \mathcal{H}$ is totally wild, contradicting the fact $\mathcal{H}$ has $w \leq 3$.

It remains to treat the case $p = 3$. If $w = 3$, then $\mathcal{F}$ is Kloosterman of rank 3, the image $Q$ of $P(\infty)$ is $3^{1+2}$ in one of its irreducible representations of dimension 3. So on $\mathcal{F}$, the center of $Q$ acts as $3\xi$ for some nontrivial character of the center, i.e. a nontrivial additive character of $C_3$. Then the center acts on $\mathrm{Sym}^2(\mathcal{F}) \cong \mathcal{H}$ as $6\xi^2$. Thus $\mathcal{H}$ is totally wild, contradicting the fact that $\mathcal{H}$ has $w \leq 3$. Suppose now $w = 2$. Then the $P(\infty)$ representation of $\mathcal{F}$ is $W_2 \oplus \mathbb{1}$, with $W_2$ the sum of two linear characters $\mathcal{L}_{\psi(x)} \oplus \mathcal{L}_{\psi(-x)}$. Then $\mathrm{Sym}^2(\mathcal{F}) \cong \mathcal{H}$ has $P(\infty)$ representation given by

$$\mathcal{L}_{\psi(2x)} \oplus \mathcal{L}_{\psi(-2x)} \oplus \mathbb{1} \oplus \mathbb{1} \oplus \mathcal{L}_{\psi(x)} \oplus \mathcal{L}_{\psi(-x)}.$$

Then $m = 2$, i.e. $\mathcal{H}$ has $w = 4$, contradiction. □

LEMMA 6.1.14. *Let $\mathcal{H}$ be a hypergeometric sheaf of type $(15, m)$ with $m < 15$ in characteristic $p$. Suppose that $G^{\circ}_{\rm geom}$ realizes the image of $\mathrm{SL}_6$ on its representation $L(\varpi_2)$. Then $p = 2$.*

PROOF. (i) We will show that if $p > 2$, then no such $\mathcal{H}$ exists. In view of Theorem 4.1.1, we know $w := 15 - m > 1$. Because $G^0_{\rm geom}$ has no nontrivial outer automorphism which preserves the given representation, Lemma 6.2.2 tells us that after replacing $\mathcal{H}$ by some $\mathcal{L}_\chi \otimes \mathcal{H}$, $\chi$ some tame character, we may assume that $G_{\rm geom} = {\rm SL}_6/\mu_2$. View $\mathcal{H}$ as giving a homomorphism $\Psi_0 : \pi_1^{\rm geom}(\mathbb{G}_m) \to {\rm SL}_6/\mu_2$, and use the vanishing of $H^2(\pi_1^{\rm geom}, \mu_2)$ to lift $\Psi_0$ to a homomorphism $\Psi : \pi_1^{\rm geom}(\mathbb{G}_m) \to {\rm SL}_6$. Then view $\Psi$ as giving a rank 6 lisse sheaf on $\mathbb{G}_m/\overline{\mathbb{F}_p}$ with $\wedge^2(\mathcal{F}) \cong \mathcal{H}$. Because $p \neq 2$, the fact that $\mathcal{H}$ is tame at 0 and has highest $\infty$-slope $1/w$ tells us that $\mathcal{F}$ is tame at 0 and has highest $\infty$-slope $1/w$. Now $\mathcal{F}$ cannot be tame at $\infty$ (simply because $\mathcal{H}$ is not). But $\mathsf{Swan}_\infty(\mathcal{F}) \leq ({\rm rank}(\mathcal{F}))(\text{highest slope}) = 6/w$ must be $\geq 1$ (otherwise $\mathcal{F}$ is tame at $\infty$), hence $w \leq 6$, i.e.

$$m \geq 9. \tag{6.1.14.1}$$

(i) Suppose first $p \nmid w$. Then $Q$, the image of $P(\infty)$ on $\mathcal{H}$, is an abelian group of exponent $p$ by [**KT5**, Proposition 4.10]. Because $p$ is odd, $Q$ lifts uniquely from ${\rm SL}_6/\mu_2$ to ${\rm SL}_6$. Thus $Q < {\rm SL}_6 = {\rm SL}(V)$; let $\sum_{i=1}^6 \alpha_i$ denote the $Q$-character of $V$, so that $Q$ acts on $\mathcal{H}$ with the character $\sum_{i<j} \alpha_i\alpha_j$. Consider first the case where the $\alpha_i$'s are pairwise distinct. Then each of the following five sets of characters $\{\alpha_1\alpha_2, \alpha_1\alpha_3, \alpha_1\alpha_4, \alpha_1\alpha_5, \alpha_1\alpha_6\}$, $\{\alpha_2\alpha_3, \alpha_2\alpha_4, \alpha_2\alpha_5, \alpha_2\alpha_6\}$, $\{\alpha_3\alpha_4, \alpha_3\alpha_5, \alpha_3\alpha_6\}$, $\{\alpha_4\alpha_5, \alpha_4\alpha_6\}$, $\{\alpha_5\alpha_6\}$ consists of pairwise distinct characters, and so $1_Q$ can occur at most five times, contradicting (6.1.14.1).

Suppose instead that $\alpha_1 = \alpha_2 =: \alpha$. Then for each $i \in \{3,4,5,6\}$, $\alpha_1\alpha_i = \alpha_2\alpha_i$. But $1_Q$ is the only character in $\mathcal{H}|_Q$ occurring more than once. Thus $\alpha_3 = \alpha_4 = \alpha_5 = \alpha_6 =: \beta$, and the character of $\mathcal{H}|_Q$ is $\alpha^2 + 8\alpha\beta + 6\beta^2$. Since only $1_Q$ occurs more than once, $\alpha\beta = \beta^2 = 1_Q$, whence $\alpha = \beta = 1_Q$ as $p > 2$, and so $Q$ acts trivially in $\mathcal{H}$, which is nonsense because $w > 0$.

(iii) It remains to treat the cases when $2 < p \mid w$. As $2 \leq w \leq 6$ by (6.1.14.1), the only cases of $(p, w)$ to consider are $(5,5), (3,3), (3,6)$. We first treat the case $p = 5 = w$, so $Q$ is non-abelian by [**KT5**, Proposition 4.10]. In this case, the $Q$-module $V$ decomposes as $X \oplus Y$ with $X, Y$ irreducible of dimension 5 and 1. Hence the $Q$-module $\mathcal{H}$ breaks as $\wedge^2(X) \oplus X \otimes Y$. Let $Q_X$ denote the kernel of $Q$ on $X$ and let $5\xi$ denote the character of $\mathbf{Z}(Q/Q_X)$ on $X$. Then $\mathbf{Z}(Q/Q_X)$ acts on $\wedge^2(X)$ with character $10\xi^2$; in particular $\wedge^2(X)$ is totally wild, contradicting $w = 5$.

In the case $p = 3$, the $Q$-module $V$ decomposes as $X \oplus Y$ with $X$ irreducible of dimension 3 and $Y$ either irreducible of dimension 3, or a sum of three irreducible submodules 1. In the latter case, the $Q$-module $\mathcal{H}$ breaks as $\wedge^2(X) \oplus X \otimes Y \oplus \wedge^2(Y)$, with $\wedge^2(X)$ totally wild (by a similar argument as in the case $p = 5$) and $X \otimes Y$ a sum of three irreducible modules each of dimension 3 and so totally wild as well, yielding the contradiction $w \geq 12$. In the former case, both $\wedge^2(X)$ and $\wedge^2(Y)$ are again totally wild, and so, as $w \leq 6$, $X \otimes Y$ must be tame. By Lemma 6.1.7(i), $Q$ acts via scalars on $X$, contradicting its irreducibility. □

LEMMA 6.1.15. *Let $\mathcal{H}$ be a hypergeometric sheaf of type $(20, m)$ with $m < 20$ in characteristic $p$. Suppose that $G^\circ_{\rm geom}$ realizes the image of ${\rm SL}_6$ on its representation $L(\varpi_3)$. Then $p \leq 3$.*

PROOF. (i) Arguing by contradiction, assume $p \geq 5$. Since ${\rm Out}({\rm SL}_6) \cong C_2$, the subgroup $G_1$ of $G := G_{\rm geom}$ that induces only inner automorphisms of $G^\circ$ has index $\leq 2$ in $G$. Moreover, since $G^\circ$ is irreducible on the underlying representation $V_{\mathcal{H}}$, $\mathbf{C}_G(G^\circ) = \mathbf{Z}(G)$, and $G_1 = \mathbf{Z}(G)G^\circ$. If $G = G_1$, set $\mathcal{H}_1 := \mathcal{H}$. In this case, $\mathcal{H}_1$ has largest $\infty$-slope $1/w$.

If $G > G_1$, then $G/G_1 \cong C_2$. The composite map

$$\pi_1^{\rm geom}(\mathbb{G}_m) \to G \to G/G_1 \cong C_2$$

is then trivialized by the unique (because $p \neq 2$) étale double covering of $G_m/\overline{\mathbb{F}_p}$, namely the Kummer double covering. Thus the Kummer pullback $\mathcal{H}_1 := [2]^\star\mathcal{H}$ has $G_1$ as its geometric monodromy group. In this case, $\mathcal{H}_1$ has largest $\infty$-slope $2/w$.

In both cases, $\mathcal{H}_1$ has $G_1$ as its geometric monodromy group and has largest $\infty$-slope $\leq 2/w$.

Applying Lemma 6.1.6, we obtain a reductive subgroup $H \leq \mathrm{GL}_6 = \mathrm{GL}(V)$ which admits a surjection $\sigma : H \twoheadrightarrow G_1$ with kernel $C_3$, and such that $G_1$ acts on $V_{\mathcal{H}}$ as $H$ acts on $\wedge^3(V)$. The homomorphism $\Psi_0 : \pi_1^{\mathrm{geom}} \to G_1$ given by $\mathcal{H}_1$ can be lifted to a homomorphism $\Psi : \pi_1^{\mathrm{geom}} \to H$ (by the vanishing of $H^2(\pi_1^{\mathrm{geom}}, C_3)$). We view $\Psi$ as giving us a rank 6 lisse sheaf $\mathcal{F}$ on $G_m/\overline{\mathbb{F}_p}$ with $\wedge^3(\mathcal{F}) \cong \mathcal{H}_1$. Because $p \neq 3$, $\mathcal{F}$ and $\mathcal{H}_1$ have the same highest $\infty$-slope, which is $\leq 2/w$. Thus $\mathcal{F}$ has $\mathsf{Swan}_\infty \leq \mathrm{rank}(\mathcal{F})(2/w) = 12/w$. As $\mathcal{F}$ is not tame at $\infty$, we must have $w \leq 12$, or equivalently

$$m \geq 8. \tag{6.1.15.1}$$

(ii) Let $Q$ denote the image of $P(\infty)$ in $G$. Since $p \neq 2$, $Q \leq G_1$. Next, since $p \neq 3$, $Q$ embeds in $H$ as a finite $p$-subgroup. Note that $Q$ acts on the tame part $\mathsf{Tame}_{\mathcal{H}}$ of $\mathcal{H}$ via the character $m \cdot 1_Q$ with $m \geq 8$, and the $Q$-module $\mathsf{Wild}_{\mathcal{H}}$ of $\mathcal{H}$ is multiplicity-free. Because $p \neq 2$, the action of $Q$ on $\mathsf{Wild}_{\mathcal{H}_1} = [2]^\star\mathsf{Wild}_{\mathcal{H}}$ is isomorphic to its action on $\mathsf{Wild}_{\mathcal{H}}$, so is multiplicity free, and its action on $\mathsf{Tame}_{\mathcal{H}_1}$ remains trivial of rank $m$. We now exploit the fact that $\wedge^3(\mathcal{F}) \cong \mathcal{H}_1$.

Assume first that $Q$ is abelian. Then $Q$ acts on $\mathcal{F}$ via a sum $\sum_{i=1}^6 \alpha_i$ of six linear characters, and acts on $\mathcal{H}_1$ via the character $\sum_{i<j<k} \alpha_i\alpha_j\alpha_k$. Suppose that $\alpha_i \neq \alpha_j$ whenever $i \neq j$. Then each of the 6 collections

$$\begin{array}{ll}\{\alpha_i\alpha_j\alpha_k \mid (i,j,k) = (123), (124), (125), (126)\}, & \{\alpha_i\alpha_j\alpha_k \mid (i,j,k) = (134), (135), (136)\}, \\ \{\alpha_i\alpha_j\alpha_k \mid (i,j,k) = (234), (235), (236)\}, & \{\alpha_i\alpha_j\alpha_k \mid (i,j,k) = (145), (245), (345)\}, \\ \{\alpha_i\alpha_j\alpha_k \mid (i,j,k) = (156), (256), (356), (456)\}, & \{\alpha_i\alpha_j\alpha_k \mid (i,j,k) = (146), (246), (346)\}\end{array}$$

contains $1_Q$ at most once, and thus $m \leq 6$, a contradiction. Hence we may assume $\alpha_1 = \alpha_2 =: \alpha$. Now, for each $3 \leq i < j \leq 6$, $\alpha_1\alpha_i\alpha_j$ and $\alpha_2\alpha_i\alpha_j$ coincide, hence cannot be among $Q$-characters on $\mathsf{Wild}$, and so $\alpha_1\alpha_i\alpha_j = \alpha_2\alpha_i\alpha_j$. It follows that $\alpha_3 = \alpha_4 = \alpha_5 = \alpha_6 =: \beta$. In this case, we see that the character of $Q$ on $\mathcal{H}_1$ is $12\alpha\beta^2 + 4\alpha^2\beta + 4\beta^3$. This contradicts the fact that every irreducible $Q$-character on $\mathsf{Wild}$ occurs exactly once in the $Q$-character of $\mathcal{H}_1$.

(iii) It remains to treat the case when $Q$ is non-abelian, whence $p|w$ by [**KT5**, Proposition 4.10]; moreover $Q \cap \mathbf{Z}(G) = 1$ by [**KT5**, Proposition 4.8(i)]. Since $p \neq 3 = |\mathrm{Ker}(\sigma)|$, $\sigma$ injects $Q \cap \mathbf{Z}(H)$ into $Q \cap \mathbf{Z}(G)$, hence $Q \cap \mathbf{Z}(H) = 1$. On the other hand, $Q \hookrightarrow H = \mathbf{Z}(H)\mathrm{SL}_6$, so $Q$ embeds in $H/\mathbf{Z}(H)$, a quotient of $\mathrm{SL}_6$ by $\mathbf{Z}(H) \cap \mathrm{SL}_6$ and so semisimple. By [**Bor**, E-44, II.5.16], $Q$ embeds in the normalizer of some maximal torus $\mathcal{T}$ of $H/\mathbf{Z}(H)$, which has Weyl group $\mathsf{S}_6$. Now, if $p \geq 7$, then $p \nmid |\mathsf{S}_6|$, and so $Q \hookrightarrow \mathcal{T}$ would be abelian. As $w \leq 12$ and $p \geq 5$, it therefore remains to consider the case $p = 5|w$, i.e. $w \in \{5, 10\}$. Now $\mathcal{F}_Q$ is a faithful module for the non-abelian 5-subgroup $Q$, so it decomposes as $X \oplus Y$ with $X, Y$ irreducible of dimension 5 and 1. Hence the $Q$-module $\mathcal{H}_1$ breaks as $\wedge^3(X) \oplus \wedge^2(X) \otimes Y$. Let $Q_X$ denote the kernel of $Q$ on $X$ and let $5\xi$ denote the character of $\mathbf{Z}(Q/Q_X)$ on $X$. Then $\mathbf{Z}(Q/Q_X)$ acts on $\wedge^3(X)$ with character $10\xi^3$; in particular $\wedge^3(X)$ is totally wild of dimension 10. As $w \leq 10$, this implies that $\wedge^2(X) \otimes Y$ is tame, whence $Q$ acts via scalars on $X$ by Lemma 6.1.7(ii), contradicting its irreducibility. □

Now we can prove the main result of this section:

THEOREM 6.1.16. *Suppose that $\mathcal{H}$ is a hypergeometric sheaf in characteristic $p$, of type $(D, m)$ with $D > m$, such that $G^\circ_{\mathrm{geom}}$ is a simple algebraic group of type $A_{d-1}$ for some $d \geq 3$ and acts irreducibly on $\mathcal{H}$. Then one of the following statements holds.*

(a) *$d = D$ and $\mathrm{SL}_D \lhd G_{\mathrm{geom}} < \mathrm{GL}_D$.*
(b) *$(p, d, D) = (2, 3, 6)$, and $G^\circ_{\mathrm{geom}}$ acts on $\mathcal{H}$ as $\mathrm{SL}_3 = \mathrm{SL}(V)$ acts on $\mathrm{Sym}^2(V)$ or $\mathrm{Sym}^2(V^*)$.*
(c) *$(d, D) = (3, 8)$, and $G^\circ_{\mathrm{geom}}$ acts on $\mathcal{H}$ as $\mathrm{SL}_3 = \mathrm{SL}(V)$ acts on the adjoint module.*
(d) *$d = 4, 6$, and $G^\circ_{\mathrm{geom}}$ acts on $\mathcal{H}$ as $\mathrm{SL}_d = \mathrm{SL}(V)$ acts on $\wedge^k(V)$ or $\wedge^k(V^*)$ for some $2 \leq k \leq d/2$. Moreover, if $d = 6$ then $p \leq k$.*

PROOF. (i) Recall that a (topological) generator $g_0$ of the image of $I(0)$ in $G := G_{\mathrm{geom}}$ has a regular spectrum on the representation $V_{\mathcal{H}}$ underlying $\mathcal{H}$. Staying aside from exceptions listed in (c) and (d), as well as the main case (a), we may apply Theorem 3.3.4 to conclude that $g_0 \in \mathbf{Z}(G)G^\circ$, and $G^\circ$ acts on $V_{\mathcal{H}}$ as $\mathrm{SL}(V) \cong \mathrm{SL}_d$ acts on $\Sigma^k(V)$ with $\Sigma = \mathrm{Sym}$ or $\wedge$, $k \geq 2$, and $2 \leq k \leq d-2$ if $\Sigma = \wedge$.

Let $G_0$ denote the Zariski closure of the normal closure of $\langle g_0 \rangle$ in $G$. Then $G_0 \leq \mathbf{Z}(G)G^\circ$. If $m \leq D-2$, then $G = G_0$ by Theorem 1.2.2. If $m = D-1$, then $G/G_0 \cong C_p$ by [**KRLT4**, Theorem 5.2]. Since $G^\circ$ is irreducible on $V_{\mathcal{H}}$, $G/\mathbf{Z}(G)G^\circ$ can only induce outer automorphisms of $G^\circ$, and we conclude that $G = \mathbf{Z}(G)G^\circ$ if $p > 2$. If $p = 2$, then by Theorem 4.1.5 we arrive at (a) or (d) (the latter being the case if $d = 4$ and $G^\circ = \mathrm{SO}_6$). We also note that, in the case of (d) with $d = 6$, the conclusion $p \leq k$ follows from Lemmas 6.1.14 and 6.1.15, and $p = 2$ in the case of (b) by Lemma 6.1.13.

(ii) From now, we will assume that none of (a)–(d) holds, and so $G = \mathbf{Z}(G)G^\circ$. By Lemma 6.1.6, there is a reductive subgroup $H \leq \mathrm{GL}(V)$ with finite center and a finite subgroup $Z \leq H \cap \mathbf{Z}(\mathrm{GL}(V))$, such that $G \cong H/Z$ and $G$ acts on $V_{\mathcal{H}}$ as $H$ acts on $\Sigma^k(V)$. Let $\Phi$ denote the representation of $I(\infty)$ on the wild part $\mathsf{Wild}$ of $V_{\mathcal{H}}$. Also, let $J_\infty$ denote the image of $I(\infty)$ in $G$, and let $Q_\infty$ denote the image of $P(\infty)$ in $G$. One knows by Proposition 2.4.2 that the $I(\infty)$-representation $\mathcal{H}$ is $\mathsf{Wild} \oplus \mathsf{Tame}$, and $\Phi(I(\infty))$ is a finite subgroup of $\mathrm{GL}(\mathsf{Wild})$, with $\Phi(P(\infty))$ as a normal subgroup with cyclic $p'$-quotient. Hence we can find an element $g_\infty \in J_\infty$ such that $\Phi(g_\infty)$ has finite $p'$-order and generates $\Phi(I(\infty))$ modulo $\Phi(P(\infty))$. Since $\mathsf{o}(\Phi(g_\infty))$ is finite, the unipotent part $u_\infty$ of $g_\infty$ acts trivially on $\mathsf{Wild}$, and $\Phi(g_\infty) = \Phi(s_\infty)$ for the semisimple part $s_\infty$ of $g_\infty$. The finite subgroup $Q_\infty$ is closed in $G$, and so is its normalizer $\mathbf{N}_G(Q_\infty)$, which must then act on $\mathsf{Tame}$, the fixed point subspace for $Q_\infty$ on $\mathcal{H}$. As $s_\infty$ belongs to the Zariski closure in $G$ of $J_\infty \leq \mathbf{N}_G(Q_\infty)$, $s_\infty$ also acts on $\mathsf{Tame}$ and normalizes $Q_\infty$. Recall that the "downstairs" characters of $\mathcal{H}$ determine the action of $\langle s_\infty \rangle$ on $\mathsf{Tame}$. It follows that $s_\infty$ is an element of finite $p'$-order in $G$, and by the construction, $\Phi(s_\infty)$ still generates $\Phi(I(\infty))$ modulo $\Phi(P(\infty))$.

Now we let $J$ be the full inverse image in $H$ of the finite subgroup $\langle Q_\infty, s_\infty \rangle$; in particular, $J < \mathrm{GL}(V)$ is finite. Then $R \lhd J$ for the full inverse image $R$ of $Q_\infty$ in $H$. Now $R/Z \cong Q_\infty$ is a finite $p$-group and $Z \leq \mathbf{Z}(J)$, so $R = Q \times \mathbf{O}_{p'}(Z)$ for a Sylow $p$-subgroup $Q$ of $R$, and $Q \lhd J$. Since $\langle Q_\infty, s_\infty \rangle / Q_\infty$ is a cyclic $p'$-group, by the Schur-Zassenhaus theorem [**KS**, 6.2.1] we can write $J = Q \rtimes C$ for a $p'$-subgroup $C$, and $C = \langle \mathbf{O}_{p'}(Z), \boldsymbol{\sigma} \rangle$ for some element $\boldsymbol{\sigma} \in J$. Since $J$ is solvable, by Hall's theorem [**KS**, 6.4.6] we can choose $\boldsymbol{\sigma}$ such that it projects onto $s_\infty$ under $H \twoheadrightarrow G$. The action of $\langle Q_\infty, s_\infty \rangle$ on $\mathsf{Wild}$, which is the same as the action of $I(\infty)$, is described in Propositions 4.8 and 4.9 of [**KRLT4**], and recall that $Z$ acts trivially on $\Sigma^k(V)$. Also, $Q$ acts trivially on $\mathsf{Tame}$. Switching from $\wedge^k(V)$ to $\wedge^{d-k}(V)$ to ensure (6.1.9.1) in the case $\Sigma^k = \wedge^k$ with $k > d/2$, we still have that the $Q$-character afforded by $\mathsf{Tame}$ is a multiple of a linear character $\gamma$. Hence Hypothesis 6.1.9 holds, with $\varphi$ being the $J$-character of $\mathsf{Wild}$. Again using Propositions 4.8 and 4.9 of [**KRLT4**], we note that

(6.1.16.1) $\boldsymbol{\sigma}$ has simple spectrum in a representation affording $\varphi$.

Indeed, write $\varphi(1) = \dim \mathsf{Wild} = D - m = p^a W_0$ with $p \nmid W_0$. If $a = 0$, then by [**KRLT4**, Proposition 4.8] the spectrum of $\boldsymbol{\sigma}$ on $\mathsf{Wild}$ consists of all $W_0^{\mathrm{th}}$ roots of some $\zeta \in \mathbb{C}^\times$. If $a > 0$, then by [**KRLT4**, Proposition 4.9] the spectrum of $\boldsymbol{\sigma}$ on $\mathsf{Wild}$ consists of all $W_0^{\mathrm{th}}$ roots of all elements in the set $\zeta \cdot (\mu_{p^a+1} \smallsetminus \{1\})$ for some $\zeta \in \mathbb{C}^\times$.

(iii) If $\Sigma = \wedge$, then $d \geq 4$ as $k \geq 2$. As (d) does not hold, we may assume $d > 4$ when $\Sigma = \wedge$. Hence, by Proposition 6.1.10, $J$ is irreducible on $V$. Now, since we are not in (b) nor in (d), we have by Proposition 6.1.12 that $Q$ is irreducible on $V$.

Let $A$ be any characteristic abelian subgroup of $Q$. Then $A \lhd J$, and so $J$ preserves a decomposition $V = V_1 \oplus V_2 \oplus \ldots \oplus V_n$ of $V$ into $A$-isotypic components. By irreducibility, $J$ acts transitively on its summands, and we can apply Proposition 6.1.11. Note that, in the cases (c) and (d) of 6.1.11(B), $\Sigma = \wedge$, and $\varphi(1) = D$ equals 56, respectively $d(d-1)/2$ with $d = p^e$, whereas $\boldsymbol{\sigma}$ has at most 14, respectively $\kappa(d-1)/2 < D = d(d-1)/2$ (note that $\kappa \leq 5$, and $\kappa = 4$ when $d = 5$). Hence (6.1.16.1) rules out these possibilities, and we conclude that $Q$ fixes each summand $V_i$. However, $Q$ is irreducible on $V$, so $n = 1$. As $A$ is abelian, it follows that $A$ acts via scalars on $V$, and so it is central.

We have shown that every characteristic abelian subgroup of $Q$ is central; also $Q < \mathrm{GL}(V)$ is irreducible on $V$; in particular, $d = p^m$. Hence Proposition 1.1.10 applies to $Q$. Consider the case $p \nmid k$. By Proposition 1.1.10(iii), the $Q$-character afforded by $W = \Sigma^k(V)$ is a multiple of a single irreducible character of degree $p^m = d$ of $Q$. Hypothesis 6.1.9 now implies that $\varphi(1) = D$, i.e. $\mathcal{H}$ is Kloosterman and $p|D$. Also, $\varphi|_Q$ is multiplicity-free by [**KRLT4**, Proposition 4.9], so $d = p^m = D \geq \binom{d}{2}$, a contradiction.

Finally, assume that $p|k$. By Proposition 1.1.10(iv), the $Q$-character afforded by $W = \Sigma^k(V)$ contains at least $N$ distinct linear characters of $Q$, where $N := p^{2m} - 1$ if $p > 2$, $N := 2^{m-1}(2^m + 1)$ if $p = 2$ and $\Sigma = \mathrm{Sym}$, and $N := 2^{m-1}(2^m - 1)$ if $p = 2$ and $\Sigma = \wedge$. Hypothesis 6.1.9 now implies that $\varphi|_Q$ contains at least $N - 1$ distinct linear characters of $Q$, and all these must be permuted transitively by $\boldsymbol{\sigma}$. On the other hand, by Proposition 1.1.10(ii), the order $M$ of the automorphism $f$ of $Q$ induced by $\boldsymbol{\sigma}$ is less than $p^{m+1}/(p-1)$. As $d = p^m \geq 3$, we arrive at the contradiction that $N - 1 > M$, unless $d = 4$. In the case $d = 4$, we may assume $\Sigma = \mathrm{Sym}$, whence $N = 10$, whereas $M \leq 8$ (in fact $M \leq 5$), again a contradiction. □

For later use, we will prove some more statements about case (d) of Theorem 6.1.16.

LEMMA 6.1.17. *In case* (d) *of Theorem 6.1.16, if* $d = 6$ *and* $p = k = 3$ *then* $m \neq 1$.

PROOF. Assume that $d = 6$ and $p = k = 3$ in Theorem 6.1.16(d), but $m = 1$, so that $w = 19$. By [**KRLT4**, Proposition 4.8], $Q$ is elementary abelian of order $3^{18}$, and it is normalized by a $3'$-element $g_\infty$ that permutes the 19 characters of $Q$ on $\mathsf{Wild}$ cyclically. Since $p \nmid D = 20$, $p \nmid |\mathbf{Z}(G)|$ by [**KT5**, Proposition 4.8(iv)]. So we have that $Q \leq G^\circ = \boldsymbol{G}/Z$, where

$G = G_{\mathrm{geom}}$ and $\boldsymbol{G} = \mathrm{SL}(V) \cong \mathrm{SL}_6$, $Z \cong C_3$; moreover, $g_\infty^2 \in \mathbf{Z}(G)G^\circ$ acts irreducibly on $Q$. Let $R$ be the full inverse image of $Q$ in $\boldsymbol{G}$, so that $\mathbf{Z}(R) \geq Z \geq [R,R]$. The irreducible action of $g_\infty^2$ on $R/Z$ shows that either $\mathbf{Z}(R) = R$, or $\mathbf{Z}(R) = Z$. Suppose we are in the former case. Then $R$ is abelian of exponent $\leq 9$ and order $3^{19}$. Hence $\Omega_1(R) := \{x \in R \mid x^3 = 1\}$ is an elementary abelian 3-subgroup of $\mathrm{SL}_6$ of order $\geq 3^{10}$, a contradiction. In the latter case, $[R,R] = Z = \mathbf{Z}(R)$ and the Frattini subgroup $\Phi(R)$ is also $Z$ since $\exp(Q) = 3$, whence $R$ is extraspecial 3-group $3_\pm^{1+18}$. In such a case, any complex representation of $R$ which is nontrivial on $Z$ must be of dimension $\geq 3^9$, too big for $\dim(V) = 6$. □

LEMMA 6.1.18. *In case* (d) *of Theorem 6.1.16, if* $(d,k) = (6,2)$ *then the set of "upstairs" characters cannot be* $\mu_{15}$.

PROOF. Assume that 6.1.16(d) occurs with $(d,k) = (6,2)$ and $\mu_{15}$ as the set of "upstairs" characters. Since $G = \mathbf{Z}(G)G^\circ$ with $G = G_{\mathrm{geom}}$ and $G^\circ = \mathrm{SL}_6/C_2$, we see that there exist $c \in \mathbb{C}^\times$ and $A \in \mathrm{SL}_6$ such that the spectrum of $g_0 = c \cdot \wedge^2(A)$ is $\mu_{15}$. It follows that $1 = \det(g_0) = c^{15}\det(\wedge^2(A)) = c^{15}$, i.e. $c \in \mu_{15}$ and so we can replace $g_0$ by $c^{-1}g_0$ to achieve $g_0 = \wedge^2(A)$. Since $\wedge^2$ maps $\mathrm{SL}_6$ into $\mathrm{SL}_{15}$ with kernel $C_2$ and $\mathsf{o}(g_0) = 15$, we can choose a unique $A$ of order 15. Now write $A = \mathrm{diag}(a_1, \ldots, a_6)$ with $a_i \in \mu_{15}$. The simple spectrum $\mu_{15}$ of $g_0$ shows that all $a_i$ are pairwise distinct. A computation on Mathematica shows however that no such $(a_1, \ldots, a_6)$ can yield the spectrum $\mu_{15}$ for $g_0$. □

## 6.2. Other types

We will now work with spin representations of $\mathrm{Spin}_N$. When $2 \nmid N = 2n+1 \geq 3$, $\mathrm{Spin}_N$ has center $C_2$ and a unique spin representation of degree $2^n$. When $N = 2n \geq 10$ is even, $\mathrm{Spin}_N$ has two half-spin representations, of degree $2^{n-1}$ and fused by any outer automorphism of $\mathrm{Spin}_N$. If $2 \nmid n$, then $\mathbf{Z}(\mathrm{Spin}_N) = \langle \boldsymbol{z} \rangle \cong C_4$, and the half-spin representations are faithful, see [**Lu**, Appendix A.2]. If $2|n$, then $\mathbf{Z}(\mathrm{Spin}_N) = \langle \boldsymbol{z}_1, \boldsymbol{z}_2 \rangle \cong C_2^2$ with $\mathrm{Spin}_N/\langle \boldsymbol{z}_1\boldsymbol{z}_2 \rangle \cong \mathrm{SO}_N$, and the two half-spin representations factor through the two half-spin groups $\mathrm{HSpin}_N = \mathrm{Spin}_N/\langle \boldsymbol{z}_i \rangle$ with $i = 1, 2$, again see [**Lu**, Appendix A.2].

LEMMA 6.2.1. *Let* $N \geq 9$, *and* $\mathcal{H}$ *a hypergeometric sheaf of type* $(D,m)$ *with* $D > m$ *in characteristic* $p$. *Consider the following three situations.*

(a) $N = 2n+1$ *is odd, and* $G_{\mathrm{geom}}^0$ *for* $\mathcal{H}$ *is* $\mathrm{Spin}_N$ *in its* $2^n$*-dimensional spin representation.*
(b) $N = 2n+2 \equiv 2(\bmod\ 4)$ *and* $G_{\mathrm{geom}}^0$ *for* $\mathcal{H}$ *is* $\mathrm{Spin}_N$ *in one of its* $2^n$*-dimensional half-spin representations.*
(c) $4|N = 2n+2$ *and* $G_{\mathrm{geom}}^0$ *for* $\mathcal{H}$ *is one of the two half-spin groups* $\mathrm{HSpin}_N$, *i.e. the image of* $\mathrm{Spin}_N$ *in one of its* $2^n$*-dimensional half-spin representations.*

*Then we have the following results.*

(i) *If* $N$ *is odd, then there exists a tame character* $\chi$ *such that* $G_{\mathrm{geom}}$ *for the hypergeometric sheaf* $\mathcal{L}_\chi \otimes \mathcal{H}$ *is* $\mathrm{Spin}_N$. *Moreover, if* $p > 2$ *then* $w := D - m$ *is even.*
(ii) *If* $N \equiv 2(\bmod\ 4)$, *then there exists a tame character* $\chi$ *such that* $G_{\mathrm{geom}}$ *for the hypergeometric sheaf* $\mathcal{L}_\chi \otimes \mathcal{H}$ *is* $\mathrm{Spin}_N$.
(iii) *If* $4|N$, *then there exists a tame character* $\chi$ *such that* $G_{\mathrm{geom}}$ *for the hypergeometric sheaf* $\mathcal{L}_\chi \otimes \mathcal{H}$ *is* $\mathrm{HSpin}_N$. *Moreover, if* $p > 2$ *then* $w := D - m$ *is even.*

Proof. When $N = 2n+1$ is odd or $N = 2n+2 \equiv 2 (\mathrm{mod}\ 4)$, the normalizer of $\mathrm{Spin}_N$ in the ambient $\mathrm{GL}_{2^n}$ is $\mathrm{GL}_1 * \mathrm{Spin}_N$, and hence $G_{\mathrm{geom}}$ is of the form (a finite group $\Lambda$ of scalars)$*\mathrm{Spin}_N$. The center of $\mathrm{Spin}_N$ is cyclic of order 2 when $N$ is odd, and cyclic of order 4 when $N \equiv 2 (\mathrm{mod}\ 4)$. When $4|N = 2n+2$, the normalizer of $\mathrm{HSpin}_N$ in the ambient $\mathrm{GL}_{2^n}$ is $\mathrm{GL}_1 * \mathrm{HSpin}_N$, and hence $G_{\mathrm{geom}}$ is of the form (a finite group $\Lambda$ of scalars)$*\mathrm{HSpin}_N$. When $4|N$, the center of $\mathrm{HSpin}_N$ is cyclic of order 2. To keep track of orders of centers, let us define

$$c(N) := 2 \text{ if } N \text{ is odd or if } 4|N, \quad c(N) := 4 \text{ if } N \equiv 2 (\mathrm{mod}\ 4).$$

Thus when we write any element $g \in G_{\mathrm{geom}}$ as $\lambda(g)h$ with $\lambda(g) \in \Lambda$ and $h \in \mathrm{Spin}_N$ (respectively in $\mathrm{HSpin}_N$), the map

$$g \mapsto \lambda(g)^{c(N)}$$

is a well-defined homomorphism from $G_{\mathrm{geom}}$ to $\Lambda$, so in particular a linear character of $G_{\mathrm{geom}}$, call it $\rho$. We claim that $\rho$ is a tame character. To see this, view $\rho$ as a character of $\pi_1^{\mathrm{geom}}$ which factors through the homomorphism to $G_{\mathrm{geom}}$ given by $\mathcal{H}$. Thus $\rho$ is tame at 0, and its $\infty$ slope is $\leq 1/w$. Admit for a moment that $w \geq 2$. Then $\rho$ is also tame at $\infty$ (because Swan conductors are integers, cf. [**Ka-GKM**, 1.9] or, for this linear case, [**Se**, Thm. (Hasse-Arf), p.82]). Whatever the characteristic $p$, a tame character always has a tame square root and a tame fourth root (the latter unique if $p = 2$, four in odd characteristic). Choose a tame $\chi$ so that $\chi^{c(N)} = 1/\rho$, and then we indeed have $G_{\mathrm{geom}}$ for $\mathcal{L}_\chi \otimes \mathcal{H}$ being $\mathrm{Spin}_N$ (respectively $\mathrm{HSpin}_N$).

To show that $w > 1$, we argue as follows. Because its $G_{\mathrm{geom}}$ is not finite, if $w = 1$ then by Theorems 4.1.1 and 4.1.5 its $G_{\mathrm{geom}}^0$ is either $\mathrm{SL}_{2^n}$ or $\mathrm{SO}_{2^n}$ (recall $D = 2^n$ is the rank of $\mathcal{H}$), and $2^n > N$ since $N \geq 9$.

We now turn to the discussion of $w$, which is unchanged when replacing $\mathcal{H}$ by $\mathcal{L}_\chi \otimes \mathcal{H}$. The key point is that when $N$ is odd, the spin representation is self-dual, and when $4|N$ each of the half-spin representations is self-dual (indeed, they have different kernels in $\mathrm{Spin}_N$). So in both these cases, once we replace $\mathcal{H}$ by $\mathcal{L}_\chi \otimes \mathcal{H}$ so that $G_{\mathrm{geom}}$ is $\mathrm{Spin}_N$, respectively $\mathrm{HSpin}_N$, our (new) $\mathcal{H}$ is self-dual. This autoduality forces $pw$ to be even, by [**Ka-ESDE**, 8.8.1]. [In the case when $N$ is even but is 2 mod 4, the half-spin representations are duals of each other.] □

For ease of later reference, we give a more general version of the above lemma.

Lemma 6.2.2. *Let $\mathcal{H}$ be a hypergeometric sheaf of type $(D, m)$ with $w := D - m \geq 2$ in characteristic $p$. Suppose that $\boldsymbol{G} := G^0_{\mathrm{geom},\mathcal{H}}$ is an irreducible subgroup of $\mathrm{GL}_D$ which has no nontrivial outer automorphism that preserves the given $D$-dimensional representation. Then there exists a tame character $\chi$ such that $\mathcal{L}_\chi \otimes \mathcal{H}$ has $G_{\mathrm{geom},\mathcal{L}_\chi\otimes\mathcal{H}} = \boldsymbol{G}$.*

Proof. The group $G_{\mathrm{geom},\mathcal{H}}$ normalizes its identity component, which is irreducible, hence $G_{\mathrm{geom},\mathcal{H}}$ lies in $\mathrm{GL}_1 * \boldsymbol{G}$. Thus $G_{\mathrm{geom},\mathcal{H}}$ is of the form (a finite group $\Lambda$ of scalars)$*\boldsymbol{G}$. Thus each element $g \in G_{\mathrm{geom},\mathcal{H}}$ can be written as $\lambda(g)h$ with $\lambda(g) \in \Lambda$ and $h \in \boldsymbol{G}$. For $c$ the order of the center, the map

$$g \mapsto \lambda(g)^c$$

is a well-defined homomorphism, call it $\rho$, from $G_{\mathrm{geom},\mathcal{H}}$ to $\Lambda$. Exactly as in the proof of Lemma 6.2.1, we view $\rho$ as a linear character of $\pi_1^{\mathrm{geom}}$, whose slope is $\geq 1/w$ for $w := D - m$.

Thus $\rho$ is tame because $w \geq 2$ by hypothesis. Then we take for $\chi$ any tame character with $\chi^c = \rho^{-1}$. □

REMARK 6.2.3. In the above Lemma 6.2.1 we take $N \geq 9$ because for $N \leq 8$ all the spin and half-spin groups are known to occur hypergeometrically. For $N = 3$, $\mathrm{Spin}_3 = \mathrm{SL}_2$, which occurs from $\mathcal{K}l(\mathbb{1}, \mathbb{1})$ in every characteristic $p$, cf. [**Ka-GKM**, 11.1]. For $N = 4$, the two half-spin groups are again $\mathrm{SL}_2$. For $N = 5$, the spin group is $\mathrm{Sp}_4$, which occurs from $\mathcal{K}l(\mathbb{1}, \mathbb{1}, \mathbb{1}, \mathbb{1})$ in every characteristic $p$, again by [**Ka-GKM**, 11.1]. For $N = 6$, the spin group is $\mathrm{SL}_4$, which occurs from $\mathcal{H}(\xi_2, \xi_2, \xi_2, \xi_2; \mathbb{1})$ in every odd characteristic $p$ (use [**Ka-GKM**, 11.6] and the fact that $w = 3$ is odd to rule out the other cases, all of which are self-dual). For $N = 7$, see [**Ka-ESDE**, 10.1.3] for examples in all sufficiently large characteristics. For $N = 8$, the half-spin groups are all isomorphic to $\mathrm{SO}_8$. Quite generally, we obtain $\mathrm{O}_D$ for any even $D \geq 4$ in characteristic $p = 2$ from hypergeometric sheaves of type $(D, D-1)$ with upstairs any collection of $D/2$ nontrivial characters and their inverses, and downstairs $\mathbb{1}$ repeated $D - 1$ times, cf. Theorem 4.1.5, the infinitude of $G_{\mathrm{geom}}$ from the unipotent block of size $D - 1$ given by the tame part of the $I(\infty)$-representation.

In characteristic $p \geq 5$, one can use [**Ka-ESDE**, 7.2.7] to show that, again with $D \geq 8$ even, the hypergeometric sheaf of type $(D, D-2)$ with upstairs characters $\xi_4$ repeated $D/2$ times and $\xi_4^3$ repeated $D/2$ times, and downstairs characters $\mathbb{1}$ repeated $D - 3$ times and $\xi_2$ repeated once will have $G_{\mathrm{geom}} = \mathrm{SO}_D$. To see this, let us admit for a moment that this sheaf $\mathcal{H}$ is Lie-irreducible. Then [**Ka-ESDE**, 7.2.7], applied with $b$ there our $w = 2$, for which the only excluded primes are $2, 3$, says that $G^0_{\mathrm{geom}}$ is one of $\mathrm{SL}_D$, $\mathrm{SO}_D$, $\mathrm{Sp}_D$. But by the duality recognition theorems [**Ka-ESDE**, 8.8.1-2], our $\mathcal{H}$ is orthogonally self-dual, and has trivial geometric determinant (because $w > 1$), and hence its $G_{\mathrm{geom}}$ must be $\mathrm{SO}_D$.

It remains to explain why this $\mathcal{H}$ is Lie-irreducible. After Kummer pullback by [4], the $I(0)$ representation is the sum of two unipotent blocks of size $D/2$. At the same time, the $I(\infty)$-representation of this pullback is the direct sum of a unipotent block of size $D-3 > D/2$ with a three dimensional piece. So if some further finite pullback of $[4]^\star\mathcal{H}$ were reducible, it would have to break into two irreducible pieces of dimension $D/2$, neither of which can contain the unipotent block of size $D - 3$.

LEMMA 6.2.4. *There is no hypergeometric sheaf $\mathcal{H}$ of type $(D, m)$ in characteristic $p > 2$ with $D = 2k + m$, $k \in \mathbb{Z}_{\geq 2}$, $m \in \mathbb{Z}_{\geq 1}$ in which every nontrivial element $g$ in the image $Q$ of $P(\infty)$ in $G_{\mathrm{geom}}$ acts on the underlying module $V_{\mathcal{H}}$ with Jordan canonical form* $\mathrm{diag}\big(\mathrm{Id}_m, \alpha \cdot \mathrm{Id}_k, \alpha^{-1} \cdot \mathrm{Id}_k\big)$*, for some $\alpha \in \mathbb{C}^\times$ depending on $g$.*

PROOF. Take $1 \neq z \in \mathbf{Z}(Q)$ of order $p$. Then $z$ acts on $W$ as $\mathrm{diag}\big(\zeta \cdot \mathrm{Id}_k, \zeta^{-1} \cdot \mathrm{Id}_k\big)$ for a $p^{\mathrm{th}}$ root of unity $\zeta \neq 1$. Then each $g \in Q \smallsetminus \{1, z^{-1}\}$ must act on $W_+ := \mathrm{Ker}(z|_W - \zeta \cdot \mathrm{Id})$ and on $W_- := \mathrm{Ker}(z|_W - \zeta^{-1} \cdot \mathrm{Id})$, and it acts on $W$ as $\mathrm{diag}\big(\alpha \cdot \mathrm{Id}_k, \alpha^{-1} \cdot \mathrm{Id}_k\big)$ for some $1 \neq \alpha \in \mathbb{C}^\times$, and the same holds for $gz \neq 1$. If $g$ affords both eigenvalues $\alpha$ and $\alpha^{-1}$ on $W_+$, then the two eigenvalues of $gz$ are $\zeta\alpha$ and $\zeta\alpha^{-1}$, forcing $1 = (\zeta\alpha)(\zeta\alpha^{-1}) = \zeta^2$, a contradiction as $p > 2$. Hence $g$ acts as a scalar on $W_+$. It follows that the $Q$-module $W_+$ is a sum of $k \geq 2$ copies of a simple module, contradicting [**KRLT4**, Proposition 4.8]. □

PROPOSITION 6.2.5. *There is no hypergeometric sheaf $\mathcal{H}$ of type $(16, m)$ in characteristic $p$, with $m = 8$ or $(m, p) = (7, 2)$, and with $G_{\mathrm{geom}}$ realizing $\boldsymbol{G} := \mathrm{Spin}_9$ in its spin representation.*

Proof. (i) Assume the contrary, and let $Q \neq 1$ be the (finite) image of $P(\infty)$ in $\boldsymbol{G}$. The first step of the proof is to find the spectrum of any element $1 \neq g \in Q$ on the underlying representation $V_{\mathcal{H}}$. We can embed $g$ in a maximal torus $\mathcal{T}$ of $\boldsymbol{G}$. Choose an orthonormal basis $(e_1, \dots, e_4)$ of $\mathbb{R}^4$ and realize the set of all $\mathcal{T}$-weights of the $\boldsymbol{G}$-module $V_{\mathcal{H}}$ as $\sum_{i=1}^4 a_i e_i/2$ with $a_i = \pm 1$ (written additively). In fact, we will write any such weight as

$$\mu = \mu_J = -\sum_{i=1}^{4} e_i/2 + \sum_{i \in J} e_i = \sum_{i \in J} e_i/2 - \sum_{i \in \Delta \smallsetminus J} e_i/2$$

with $J \subseteq \Delta := \{1, 2, 3, 4\}$. Let

$$\mathcal{F} = \mathcal{F}(g) := \{J \subseteq \Delta \mid \mu_J(g) = 1\},$$

(recall weights are elements of $\mathrm{Hom}(\mathcal{T}, \mathbb{C}^\times)$). Note that $\mu_J(g) \cdot \mu_{\Delta \smallsetminus J}(g) = 1$, so

$$J \in \mathcal{F} \text{ if and only if } (\Delta \smallsetminus J) \in \mathcal{F}, \tag{6.2.5.1}$$

in particular, $\#\mathcal{F}$ is even. But $m = \dim \mathsf{Tame}$ is 7 or 8, so we conclude that

$$\#\mathcal{F} \geq 8. \tag{6.2.5.2}$$

(ii) First we consider the case

$$e_i(g) \neq 1 \text{ for all } 1 \leq i \leq 4. \tag{6.2.5.3}$$

Suppose first that $\varnothing \in \mathcal{F}$, whence $\Delta := \{1, 2, 3, 4\} \in \mathcal{F}$ by (6.2.5.1). Then $\mu_{\{i\}}(g) = \mu_\varnothing(g) e_i(g) \neq 1$, so $\mathcal{F}$ contains no 1-subset, hence also no 3-subset, of $\Delta$. Now (6.2.5.2) implies that $\mathcal{F}$ consists of all even-size subsets of $\Delta$. In particular, $1 = \mu_{\{i,j\}}(g) = \mu_\varnothing(g) e_i(g) e_j(g)$ for all $i \neq j$. It follows that $e_i(g)$ has some constant value $\alpha$ for all $i$, and moreover $\alpha^2 = 1$. Condition (6.2.5.3) implies $\alpha = -1$, and evaluating all weights of $V_{\mathcal{H}}$ at $g$, we see that

$$g \text{ acts on } V_{\mathcal{H}} \text{ as } \mathrm{diag}\big(-\mathrm{Id}_8, \mathrm{Id}_8\big). \tag{6.2.5.4}$$

Suppose now that $\varnothing \notin \mathcal{F}$, so that $\Delta \notin \mathcal{F}$. Then (6.2.5.2) and (6.2.5.1) show that we may assume $\mathcal{F}$ contains some 1-subset, say $\{1\}$, hence $\{2, 3, 4\} \in \mathcal{F}$. Now (6.2.5.3) implies that none of $\{2, 3\}$, $\{2, 4\}$, and $\{3, 4\}$ belongs to $\mathcal{F}$, whence $\mathcal{F}$ contains none of $\{1, 4\}$, $\{1, 3\}$, and $\{1, 2\}$ as well. In this case, (6.2.5.2) shows that $\mathcal{F}$ consists of all odd-size subsets of $\Delta$. In particular, $\mu_{\{i\}}(g) = 1$, and $1 = \mu_{\{i,j,k\}}(g) = \mu_{\{i\}}(g) e_j(g) e_k(g)$ for all 3-set $\{i, j, k\}$. It follows that $e_i(g) = \alpha$ for all $i$, and $\alpha^2 = 1$. Condition (6.2.5.3) again implies $\alpha = -1$, and we again arrive at (6.2.5.4).

(iii) Next we consider the case

$$e_4(g) = 1, \text{ but } \beta := e_1(g) \neq 1. \tag{6.2.5.5}$$

Write $\alpha := \mu_\varnothing(g)$, $\gamma := e_2(g)$, $\delta := e_3(g)$. Condition (6.2.5.5) implies that $X \subseteq \{1, 2, 3\}$ belongs to $\mathcal{F}$ if and only $X \sqcup \{4\} \in \mathcal{F}$, but $\mathcal{F}$ cannot contain both $Y$ and $Y \sqcup \{1\}$ for any $Y \subseteq \{2, 3\}$. It follows from (6.2.5.2) that $\mathcal{F}$ contains exactly one subset from the four pairs $\{Y, Y \sqcup \{1\}\}$ with $Y \subseteq \{2, 3\}$. The corresponding weights take values

$$\{\alpha, \alpha\beta\}, \ \{\alpha\gamma, \alpha\beta\gamma\}, \ \{\alpha\delta, \alpha\beta\delta\}, \ \{\alpha\gamma\delta, \alpha\beta\gamma\delta\},$$

at $g$, respectively; and each pair (as a multi-set) contains 1 once.

Suppose $\gamma = \delta = 1$. Then each of $\alpha$ and $\alpha\beta$ is an eigenvalue for $g$ on $V_{\mathcal{H}}$ with multiplicity 8. Exactly one of them is 1 (because $m > 0$), and self-duality of $V$ implies that the other one is $-1$, whence (6.2.5.4) holds.

Suppose now that $\gamma \neq 1 = \delta$. Then exactly one among $\alpha, \alpha\beta$ and exactly one among $\alpha\gamma, \alpha\beta\gamma$ is 1. If $\alpha = 1$, then $1 \neq \alpha\gamma$ by assumption, hence $1 = \alpha\beta\gamma$, i.e. $\gamma = \beta^{-1}$. Evaluating the weights at $g$, we see that

$$g \text{ acts on } V_{\mathcal{H}} \text{ as } \operatorname{diag}\big(\mathrm{Id}_8, \beta \cdot \mathrm{Id}_4, \beta^{-1} \cdot \mathrm{Id}_4\big). \tag{6.2.5.6}$$

If $\alpha \neq 1$, then $\alpha\beta = 1$ and $1 \neq \alpha\beta\gamma$ by assumption, hence $1 = \alpha\gamma$, i.e. $\gamma = \beta = \alpha^{-1}$. Evaluating the weights at $g$, we see that (6.2.5.6) holds (with $\beta$ replaced by $\alpha$).

Next suppose that $\gamma \neq 1 \neq \delta$. First consider the case $\alpha = 1$. Then $\alpha\gamma, \alpha\delta \neq 1$ by assumption, hence $\alpha\beta\gamma = \alpha\beta\delta = 1$, i.e. $\gamma = \delta = \beta^{-1}$. Now $\{\alpha\gamma\delta, \alpha\beta\gamma\delta\} = \{\beta^{-2}, \beta^{-1}\}$ contains 1 once, whence $\beta = -1$, and we arrive at (6.2.5.4). Assume now that $\alpha \neq 1$, forcing $\alpha\beta = 1$. Then $\alpha\beta\gamma, \alpha\beta\delta \neq 1$ by assumption, hence $\alpha\gamma = \alpha\delta = 1$, i.e. $\beta = \gamma = \delta = \alpha^{-1}$. Now $\{\alpha\gamma\delta, \alpha\beta\gamma\delta\} = \{\alpha^{-1}, \alpha^{-2}\}$ contains 1 once, whence $\alpha = -1$, and we again arrive at (6.2.5.4).

(iv) Note that if $e_i(g) = 1$ for all $i$, then $g$ acts on $V_{\mathcal{H}}$ via the scalar $\mu_{\varnothing}(g)$, forcing $g = 1$ since $m > 0$. Thus we have shown that any $1 \neq g \in Q$ must act on $V$ as in (6.2.5.4) or (6.2.5.6).

Consider the case $p > 2$, so that $m = 8$ by assumption, and any $1 \neq g \in Q$ acts on $V_{\mathcal{H}}$ as $\operatorname{diag}\big(\mathrm{Id}_8, \beta \cdot \mathrm{Id}_4, \beta^{-1} \cdot \mathrm{Id}_4\big)$ for some $1 \neq \beta \in \mathbb{C}^\times$ by (6.2.5.6). This is impossible by Lemma 6.2.4.

We may now assume $p = 2$. First suppose $m = 7$. Then $W := \mathsf{Wild}$ has dimension 9, so $Q \cong 2^6$ by [**KRLT4**, Proposition 4.8]. Now (6.2.5.4) and (6.2.5.6), together with $\exp(Q) = 2$, imply that (6.2.5.4) holds for any $1 \neq g \in Q$, and that $g$ has trace 0 on $V_{\mathcal{H}}$. Counting the dimension of the fixed point subspace $\mathsf{Tame}$, we get $7 = 16/|Q|$, a contradiction.

(v) We may now assume $p = 2$ and $m = 8$. By [**KRLT4**, Proposition 4.9], $Q$ acts faithfully and irreducibly on $W := \mathsf{Wild}$ of dimension 8; in particular, $|Q| \geq 2^7$. By (6.2.5.4) and (6.2.5.6), any $1 \neq g \in Q$ acts on $W$ as $-\mathrm{Id}_8$ or $\operatorname{diag}\big(\beta \cdot \mathrm{Id}_4, \beta^{-1} \cdot \mathrm{Id}_4\big)$ for some $1 \neq \beta \in \mathbb{C}^\times$. In particular, $\mathbf{Z}(Q) = \langle z \rangle \cong C_2$, and $z$ is the unique involution in $Q$. Now $Q/\mathbf{Z}(Q)$ contains a central subgroup $C/\mathbf{Z}(Q) \cong C_2$, so that $R$ is (abelian) of order 4. But $z$ is the only involution in $Q$, so $C = \langle t \rangle \cong C_4$. It follows that $W = W_+ \oplus W_-$, where $t$ acts on $W_+$ via the scalar $\zeta_4$ and on $W_-$ via $\zeta_4^{-1}$. As $C \lhd Q$ and $Q$ is irreducible on $W$, $Q$ must permute $W_+$ and $W_-$, with kernel $R$ of index 2. Consider any $g \in R \smallsetminus \mathbf{Z}(Q)$, which then acts on $W$ as $\operatorname{diag}\big(\beta \cdot \mathrm{Id}_4, \beta^{-1} \cdot \mathrm{Id}_4\big)$ for some $\pm 1 \neq \beta \in \mathbb{C}^\times$. If $g$ affords both eigenvalues $\beta$ and $\beta^{-1}$, then $gt$ has distinct eigenvalues $\zeta_4\beta, \zeta_4\beta^{-1}$ on $W_+$, forcing $1 = (\zeta_4\beta)(\zeta_4\beta^{-1}) = \zeta_4^2 = -1$, a contradiction. Hence $R$ acts on $W_4$ via scalars. It is now easy to check that for any $0 \neq v \in W_+$ and $h \in Q \smallsetminus R$, $Q$ stabilizes the 2-dimensional subspace $\langle v, hv \rangle_{\mathbb{C}}$, contradicting its irreducibility on $W$. □

Lemma 6.2.6. *Suppose $\mathcal{H}$ is a hypergeometric sheaf of type $(16, m)$ with $m \in \{6, 7, 8\}$ in characteristic $p > 2$ whose $G_{\mathrm{geom}}$ is $\mathrm{Spin}_{10}$ in one of its half-spin representations. Then any element $\gamma$ of order $p$ in the image $Q$ of $P(\infty)$ in $G_{\mathrm{geom}}$ has a spectrum in the underlying representation $V_{\mathcal{H}}$ of the following form, where the superscript $[m]$ indicates that the multiplicity is $m$.*

(a) *$p = 3$, spectrum is $(1^{[8]}, \zeta_3^{[4]}, \bar{\zeta}_3^{[4]})$ or $(1^{[6]}, \zeta_3^{[5]}, \bar{\zeta}_3^{[5]})$.*

(b) $p \geq 5$, *spectrum is* $(1^{[8]}, \zeta_p^{[4]}, \bar{\zeta_p}^{[4]})$.

(c) $p \geq 5$, *spectrum is* $(1^{[6]}, \zeta_p^{[4]}, \bar{\zeta_p}^{[4]}, \zeta_p^2, \bar{\zeta_p}^2)$.

Proof. We first apply [**Ka-ESDE**, 7.2] to show that for any given imposed value of $w := D - m \in \{8, 9, 10\}$, there are only finitely many characteristics $p$ for which $G_{\mathrm{geom}}$ can fail to be one of $\mathrm{SL}_{16}$, $\mathrm{SO}_{16}$, $\mathrm{Sp}_{16}$. Let us explain this. Our $\mathcal{H}$ has its $G_{\mathrm{geom}}$ a connected semisimple group, irreducible inside $\mathrm{SL}_{16}$. Thus our $\mathcal{H}$ is Lie-irreducible, and is its own derived group. For each imposed value of $w$, the highest $\infty$ slope is $1/w$. According to [**Ka-ESDE**, 7.2], if $p$ does not divide the product denoted $2N_1(w)N_2(w)$ there, then any hypergeometric in characteristic $p$ of type $(16, 16 - w)$ has $G_{\mathrm{geom}}$ one of $\mathrm{SL}_{16}$, $\mathrm{SO}_{16}$, $\mathrm{Sp}_{16}$. The construction of $N_1(w)$ and $N_2(w)$, explained in [**Ka-ESDE**, 7.1.1] is to take

$$N_1(w) := \prod_{a,b,c,d \in \mu_w(\mathbb{C}) \text{ with } a-b-c+d \neq 0} (a - b - c + d), \; N_2(w) := \prod_{a,b,c \in \mu_w(\mathbb{C}) \text{ with } a-b-c \neq 0} (a - b - c),$$

Galois invariance shows that both $N_1(w)$ and $N_2(w)$ are (visibly nonzero) integers.

Somewhat surprisingly, the primes dividing $2N_1(w)N_2(w)$ for each $w \in \{8, 9, 10\}$ are not too large. Here they are.

$$\begin{aligned} w = 10: &\quad p = 2, 3, 5, 11, 31, 41, 61, \\ w = 9: &\quad p = 2, 3, 5, 7, 19, 37, 73, 109, 127, \\ w = 8: &\quad p = 2, 3, 5, 17, 41. \end{aligned} \tag{6.2.6.1}$$

Now we consider the 16 weights which occur in the half spin representation whose highest weight is $(1/2)(x_1 + x_2 + x_3 + x_4 - x_5)$. [The other half-spin representation is the dual of this one.] So the lowest weight is $-(1/2)\sum_{i=1}^5 x_i$, and the weights of the representation are

$$-(1/2)\sum_{i=1}^5 x_i + \text{sum of evenly many of the } x_i.$$

Now let $\gamma$ be an element of order $p$ in $\mathrm{Spin}_{10}$. It lies in a maximal torus, so its spectrum is the list of its images under the 16 weights of the representation. Each $x_i(\gamma)$ is some element of $\mu_p(\mathbb{C})$, and the lowest weight assigns to $\gamma$ the unique element of $\mu_p(\mathbb{C})$ whose square is $1/\prod_{i=1}^5 x_i(\gamma)$. We cannot assign all $x_i(\gamma) := 1$, for then $\gamma$ has order 1, not $p$. Renumbering the $x_i$, we may assume that $x_1(\gamma) = \zeta_p$, a primitive $p^{\mathrm{th}}$ root of unity. Thus we may write

$$x_i(\gamma) = \zeta_p^{a_i}, \quad a_i \in \mathbb{F}_p, \big(-\frac{1}{2}\sum_{i=1}^5 x_i\big)(\gamma) = \zeta_p^f, \quad f \in \mathbb{F}_p, f = \frac{p-1}{2}\sum_{i=1}^5 a_i.$$

The eigenvalues of $\gamma$ are then the following 16 powers of $\zeta_p$, where we write $a = 1, b, c, d, e$ for $a_1, a_2, a_3, a_4, a_5$, and where $f = ((p-1)/2)(a + b + c + d + e)$:

$$f, f+a+b, f+a+c, f+a+d, f+a+e, f+b+c, f+b+d, f+b+e, f+c+d, f+c+e, f+d+e,$$

$$-f - a, -f - b, -f - c, -f - d, -f - e.$$

From the assumption that the wild part has dimension $w \leq 10$, our element $\gamma$ must have at least 6 eigenvalues 1, or equivalently the number $0 \in \mathbb{F}_p$ must occur at least 6 times in the above list of length 16 of elements of $\mathbb{F}_p$.

For a given odd prime $p$, it is a simple matter to tabulate the lists of length 16 which arise having 0 at least 6 times. We did this calculation using the Magma program in Appendix A1 for each odd prime which divides $2N_1(w)N_2(w)$ for each of $w = 8, 9, 10$. In all cases, the spectrum was as asserted. $\square$

PROPOSITION 6.2.7. *Let $\mathcal{H}$ be a hypergeometric sheaf of type $(16, m)$ in characteristic $p$, with $6 \leq m \leq 15$ and with $G_{\mathrm{geom}}$ realizing $\boldsymbol{G} := \mathrm{Spin}_{10}$ in a half-spin representation. Then $p = 2$ and $6 \leq m \leq 8$.*

PROOF. (i) Let $Q$ be the (finite) image of $P(\infty)$ in $\boldsymbol{G}$. First we consider the case $m \geq 9$. By [**KT5**, Proposition 4.8], we can find $g \in Q \smallsetminus \mathbf{Z}(\boldsymbol{G})$, and embed $g$ in a maximal torus $\mathcal{T}$ of $\boldsymbol{G}$. Choose an orthonormal basis $(e_1, \ldots, e_5)$ of $\mathbb{R}^5$ and realize the set of all weights of the underlying module $V_{\mathcal{H}}$ as $\sum_{i=1}^{5} a_i e_i/2$ with $a_i = \pm 1$ and $\prod_{i=1}^{5} a_i = 1$. Again write any such weight as

$$\mu = \mu_J = -\sum_{i=1}^{5} e_i/2 + \sum_{i \in J} e_i$$

with $J \subseteq \Delta := \{1, 2, \ldots, 5\}$ of even size, and let

$$\mathcal{F} = \mathcal{F}(g) := \{J \subseteq \Delta \mid \mu_J(g) = 1\},\ \alpha := \mu_{\varnothing}(g).$$

Suppose that $(e_1 + \kappa e_2)(g) \neq 1$ for both $\kappa = +1$ and $\kappa = -1$. Then, for each choice of $\kappa$ and each choice of $(a_3, \ldots, a_5) \in \{\pm 1\}^3$ with $a_3 a_4 a_5 = \kappa$, at most one of the two weights $\sum_{i=3}^{5} a_i e_i/2 \pm (e_1 + \kappa e_2)/2$ can take value 1 at $g$. It follows that $m \leq \#\mathcal{F} \leq 2 \cdot 2^2 = 8$, a contradiction.

Repeating this argument, we see that for each pair $i \leq j$ there is exists some $\kappa_{ij} = \pm 1$ such that $(e_i + \kappa_{ij} e_j)(g) = 1$. Conjugating $g$ using the Weyl group, i.e. using an even number of sign changes on $e_i$, we may therefore assume that there is some $\kappa = \pm 1$ such that

$$\beta := e_1(g) = e_2(g) = e_3(g) = e_4(g) = e_5(g)^{\kappa}.$$

Consider the case $\kappa = +1$. Then $\mu_J(g) = \alpha\beta^{|J|}$ for any $J \subseteq \Delta$. So among the even-size subsets $J$ of $\Delta$, $\mu_J(g)$ yields $\alpha$, $\alpha\beta^2$, and $\alpha\beta^4$ with frequency 1, 10, and 5, respectively. Hence, if $\alpha\beta^2 \neq 1$ then $\#\mathcal{F} \leq 6 < m$, a contradiction. It follows that $\alpha\beta^2 = 1$. Also, note that $1 = \mu_{\varnothing}(g)\mu_{\Delta}(g) = \alpha^2\beta^5$. Hence $\alpha = \beta = 1$, i.e. $g = \mathrm{Id}$, again a contradiction.

Assume now that $\kappa = -1$. Then $\mu_K(g) = \alpha\beta^{|K|}$ and $\mu_{K \sqcup \{5\}}(g) = \alpha\beta^{|K|-1}$ for any $K \subseteq \{1, 2, 3, 4\}$. So among the even-size subsets $K$ of $\{1, 2, 3, 4\}$, $\mu_K(g)$ yields $\alpha$, $\alpha\beta^2$, and $\alpha\beta^4$ with frequency 1, 6, and 1, respectively. Among the odd-size subsets $K$ of $\{1, 2, 3, 4\}$, $\mu_{K \sqcup \{5\}}(g)$ yields $\alpha$ and $\alpha\beta^2$ with frequency 4 each. Thus the weights of $V_{\mathcal{H}}$ take values $\alpha$, $\alpha\beta^2$, and $\alpha\beta^4$ at $g$, with frequency 5, 10, and 1, respectively. Hence, if $\alpha\beta^2 \neq 1$, then $\#\mathcal{F} \leq 6 < m$, a contradiction. Thus $\alpha\beta^2 = 1$. Also, note that $1 = \mu_{\varnothing}(g)\mu_{\Delta}(g) = \alpha^2\beta^3$. Hence $\alpha = \beta = 1$, i.e. $g = \mathrm{Id}$, again a contradiction.

(ii) It remains to consider the case $6 \leq m \leq 8$ and $p > 2$; in particular, $Q \cap \mathbf{Z}(\boldsymbol{G}) = 1$. First suppose that $m = 8$, i.e. $w := D - m = 8$. By [**KRLT4**, Proposition 4.8], $Q$ is elementary abelian. Applying Lemma 6.2.6, we see that any element $1 \neq g \in Q$ acts on $V_{\mathcal{H}}$ as $\mathrm{diag}\big(\mathrm{Id}_8, \alpha \cdot \mathrm{Id}_4, \alpha^{-1} \cdot \mathrm{Id}_4\big)$ for some $\alpha \in \mathbb{C}^{\times}$ depending on $g$. But this is impossible by Lemma 6.2.4.

Suppose $m = 7$, so that $w = 9$. If $p = 3$, then $Q$ acts irreducibly and faithfully on $\mathsf{Wild}$ by [**KRLT4**, Proposition 4.9]. Hence any element $1 \neq z \in \mathbf{Z}(Q)$ of order 3 has an eigenvalue $\zeta \neq 1$ with multiplicity $\geq w = 9$, contradicting Lemma 6.2.6. Thus we may assume $p > 3$ in this case, and so $Q$ is elementary abelian by [**KRLT4**, Proposition 4.8]. By Lemma 6.2.6, any $g \in Q$ has real trace on $V_{\mathcal{H}}$, i.e. $\varphi(g) \in \mathbb{R}$ for the character $\varphi$ of $Q$ afforded by $V_{\mathcal{H}}$. In particular, for $1_Q \neq \nu \in \mathrm{Irr}(Q)$, $\nu$ and $\overline{\nu}$ have the same multiplicity in $\varphi$. This implies that $w$ must be even, a contradiction.

We may now assume that $m = 6$, i.e. $w = 10$. If $10|(p-1)$, then $Q$ is cyclic of order $p$ by [**KRLT4**, Proposition 4.8], but then Lemma 6.2.6 shows that the $Q$-module $\mathsf{Wild}$ is not multiplicity-free, a contradiction. Suppose $p = 3$. Then $Q$ is elementary abelian of order $3^4$ by [**KRLT4**, Proposition 4.8], and any $1 \neq g \in Q$ acts on $\mathcal{H}$ as $\mathrm{diag}\big(\mathrm{Id}_8, \zeta \cdot \mathrm{Id}_4, \bar{\zeta} \cdot \mathrm{Id}_4\big)$ (say with frequency $a$) and $\mathrm{diag}\big(\mathrm{Id}_6, \zeta \cdot \mathrm{Id}_5, \bar{\zeta} \cdot \mathrm{Id}_5\big)$ (with frequency $b$) for a cubic root $\zeta \neq 1$ of unity; in particular, $\varphi(g) = 4$ or 1, respectively. It follows that

$$6 = m = [\varphi, 1_Q]_Q = (16 + 4a + b \cdot 4)/81, \;\; a + b = 80,$$

yielding $(a, b) = (130, -50)$, a contradiction. The only remaining bad prime is $p = 5$, see (6.2.6.1). By [**KRLT4**, Proposition 4.9], the $Q$-module $\mathsf{Wild}$ is faithful and is a sum of two simple submodules of dimension 5 each. Hence, any $1 \neq z \in \mathbf{Z}(Q)$ of order 5 must have an eigenvalue $\zeta \neq 1$ with multiplicity at least 5, which is again impossible by Lemma 6.2.6. □

PROPOSITION 6.2.8. *There is no hypergeometric sheaf $\mathcal{H}$ of type $(32, m)$ in characteristic $p$ with $31 \geq m \geq 20$ and with $G_{\mathrm{geom}}$ realizing $\boldsymbol{G} := \mathrm{Spin}_{12}$ in a half-spin representation.*

PROOF. (i) Assume the contrary, and let $Q$ be the (finite) image of $P(\infty)$ in $\boldsymbol{G}$. By [**KT5**, Proposition 4.8], we can find $g \in Q \smallsetminus \mathbf{Z}(\boldsymbol{G})$, and embed $g$ in a maximal torus $\mathcal{T}$ of $\boldsymbol{G}$. Choose an orthonormal basis $(e_1, \ldots, e_6)$ of $\mathbb{R}^6$ and realize the set of all weights of the underlying module $V_{\mathcal{H}}$ as $\sum_{i=1}^{6} a_i e_i/2$ with $a_i = \pm 1$ and $\prod_{i=1}^{6} a_i = 1$. Write any such weight as

$$\mu = \mu_J = -\sum_{i=1}^{6} e_i/2 + \sum_{i \in J} e_i$$

with $J \subseteq \Delta := \{1, 2, \ldots, 6\}$ of even size, and let

$$\mathcal{F} = \mathcal{F}(g) := \{J \subseteq \Delta \mid \mu_J(g) = 1\}, \;\; \alpha := \mu_{\varnothing}(g).$$

Suppose that $(e_1 + \kappa e_2)(g) \neq 1$ for both $\kappa = +1$ and $\kappa = -1$. Then, for each choice of $\kappa$ and each choice of $(a_3, \ldots, a_6) \in \{\pm 1\}^4$ with $\prod_{i=3}^{6} a_i = \kappa$, at most one of the two weights $\sum_{i=3}^{6} a_i e_i/2 \pm (e_1 + \kappa e_2)/2$ can take value 1 at $g$. It follows that $m \leq \#\mathcal{F} \leq 2 \cdot 2^3 = 16$, a contradiction.

Repeating this argument, we see that for each pair $i \leq j$ there is exists some $\kappa_{ij} = \pm 1$ such that $(e_i + \kappa_{ij} e_j)(g) = 1$. Conjugating $g$ using the Weyl group, i.e. using an even number of sign changes on $e_i$, we may therefore assume that there is some $\kappa = \pm 1$ such that

$$\beta := e_1(g) = e_2(g) = \ldots = e_5(g) = e_6(g)^{\kappa}.$$

(ii) Consider the case $\kappa = +1$. Then $\mu_J(g) = \alpha\beta^{|J|}$ for any $J \subseteq \Delta$. So among the even-size subsets $J$ of $\Delta$, $\mu_J(g)$ yields $\alpha$, $\alpha\beta^2$, $\alpha\beta^4$, and $\alpha\beta^6$ with frequency 1, 15, 15, and 1, respectively. Hence, if $\alpha\beta^2 \neq 1$ or $\alpha\beta^4 \neq 1$, then $\#\mathcal{F} \leq 32 - 15 < 20 \leq m$, a contradiction.

It follows that $1 = \alpha\beta^2 = \alpha\beta^4$, i.e. $\beta^2 = 1$, and thus $g|_{V_{\mathcal{H}}} = \alpha \cdot \mathrm{Id}$, i.e. $g \in \mathbf{Z}(\boldsymbol{G})$, again a contradiction.

(iii) Finally, we consider the case $\kappa = -1$. Then $\mu_K(g) = \alpha\beta^{|K|}$ and $\mu_{K\sqcup\{6\}}(g) = \alpha\beta^{|K|-1}$ for any $K \subseteq \Delta \smallsetminus \{6\}$. So among the even-size subsets $K$ of $\Delta \smallsetminus \{6\}$, $\mu_K(g)$ yields $\alpha$, $\alpha\beta^2$, and $\alpha\beta^4$ with frequency 1, 10, and 5, respectively. Among the odd-size subsets $K$ of $\Delta \smallsetminus \{6\}$, $\mu_{K\sqcup\{6\}}(g)$ yields $\alpha$, $\alpha\beta^2$, and $\alpha\beta^4$ with frequency 5, 10, and 1, respectively. Thus the weights of $V_{\mathcal{H}}$ take values $\alpha$, $\alpha\beta^2$, and $\alpha\beta^4$ at $g$, with frequency 6, 20, and 6, respectively. Hence, if $\alpha\beta^2 \neq 1$, then $\#\mathcal{F} \leq 32 - 20 < 20 \leq m$, a contradiction. Thus $\alpha\beta^2 = 1$, i.e. $\alpha = \beta^{-2}$. Now, if $\beta^2 = 1$, then $g|_{V_{\mathcal{H}}} = \alpha \cdot \mathrm{Id}$ and $g \in \mathbf{Z}(\boldsymbol{G})$, again a contradiction.

Hence $\alpha \neq 1$, and $g|_{V_{\mathcal{H}}}$ has eigenvalues 1, $\alpha$, $\alpha^{-1}$ with multiplicity 20, 6, and 6, respectively. But $\dim \mathsf{Tame} = m \geq 20$, so $g$ acts on $W := \mathsf{Wild}$ as $\mathrm{diag}\big(\alpha \cdot \mathrm{Id}_6, \alpha^{-1} \cdot \mathrm{Id}_6\big)$ for any $1 \neq g \in Q$. This is impossible by Lemma 6.2.4. □

PROPOSITION 6.2.9. *There is no hypergeometric sheaf $\mathcal{H}$ of type $(512, m)$ in characteristic $p$ with $511 \geq m \geq 322$ and with $G_{\mathrm{geom}}$ realizing $\boldsymbol{G} := \mathrm{Spin}_{20}$ in a half-spin representation.*

PROOF. (i) Assume the contrary, and let $Q$ be the (finite) image of $P(\infty)$ in $\boldsymbol{G}$. By [**KT5**, Proposition 4.8], we can find $g \in Q \smallsetminus \mathbf{Z}(\boldsymbol{G})$, and embed $g$ in a maximal torus $\mathcal{T}$ of $\boldsymbol{G}$. Choose an orthonormal basis $(e_1, \ldots, e_{10})$ of $\mathbb{R}^{10}$ and realize the set of all weights of the underlying module $V_{\mathcal{H}}$ as $\sum_{i=1}^{10} a_i e_i/2$ with $a_i = \pm 1$ and $\prod_{i=1}^{10} a_i = 1$; in particular it has the lowest weight $-\sum_{i=1}^{10} e_i/2$. Write any such weight as

$$\mu = \mu_J = -\sum_{i=1}^{10} e_i/2 + \sum_{i \in J} e_i \tag{6.2.9.1}$$

with $J \subseteq \Delta := \{1, 2, \ldots, 10\}$ of even size, and let

$$\mathcal{F} = \mathcal{F}(g) := \{J \subseteq \Delta \mid \mu_J(g) = 1\}, \ \alpha := \mu_\varnothing(g).$$

Suppose that $(e_1 + \kappa e_2)(g) \neq 1$ for both $\kappa = +1$ and $\kappa = -1$. Then, for each choice of $\kappa$ and each choice of $(a_3, \ldots, a_{10}) \in \{\pm 1\}^8$ with $\prod_{i=3}^{10} a_i = \kappa$, at most one of the two weights $\sum_{i=3}^{10} a_i e_i/2 \pm (e_1 + \kappa e_2)/2$ can take value 1 at $g$. It follows that $m \leq \#\mathcal{F} \leq 2 \cdot 2^7 = 256$, a contradiction.

Repeating this argument, we see that for each pair $i \leq j$ there is exists some $\kappa_{ij} = \pm 1$ such that $(e_i + \kappa_{ij} e_j)(g) = 1$. Conjugating $g$ using the Weyl group, i.e. using an even number of sign changes on $e_i$, we may therefore assume that there is some $\kappa = \pm 1$ such that

$$\beta := e_1(g) = e_2(g) = \ldots = e_9(g) = e_{10}(g)^\kappa. \tag{6.2.9.2}$$

(ii) Consider the case $\kappa = +1$. Then $\mu_J(g) = \alpha\beta^{|J|}$ for any $J \subseteq \Delta$. So among the even-size subsets $J$ of $\Delta$, $\mu_J(g)$ yields $\alpha$, $\alpha\beta^2$, $\alpha\beta^4$, $\alpha\beta^6$, $\alpha\beta^8$, and $\alpha\beta^{10}$ with frequency 1, 45, 210, 210, 45, and 1, respectively. Hence, if $\alpha\beta^4 \neq 1$ or $\alpha\beta^6 \neq 1$, then $\#\mathcal{F} \leq 512 - 210 < 322 \leq m$, a contradiction. It follows that $1 = \alpha\beta^4 = \alpha\beta^6$, i.e. $\beta^2 = 1$, and thus $g|_{V_{\mathcal{H}}} = \alpha \cdot \mathrm{Id}$, i.e. $g \in \mathbf{Z}(\boldsymbol{G})$, again a contradiction.

Next we consider the case $\kappa = -1$. Then $\mu_K(g) = \alpha\beta^{|K|}$ and $\mu_{K\sqcup\{10\}}(g) = \alpha\beta^{|K|-1}$ for any $K \subseteq \Delta \smallsetminus \{10\}$. So among the even-size subsets $K$ of $\Delta \smallsetminus \{10\}$, $\mu_K(g)$ yields $\alpha$, $\alpha\beta^2$, $\alpha\beta^4$, $\alpha\beta^6$, and $\alpha\beta^8$ with frequency 1, 36, 126, 84, and 9, respectively. Among the odd-size subsets $K$ of $\Delta \smallsetminus \{10\}$, $\mu_{K\sqcup\{10\}}(g)$ yields $\alpha$, $\alpha\beta^2$, $\alpha\beta^4$, $\alpha\beta^6$, and $\alpha\beta^8$ with frequency 9, 84, 126, 36, and 1, respectively. Thus the weights of $V_{\mathcal{H}}$ take values $\alpha$, $\alpha\beta^2$, $\alpha\beta^4$, $\alpha\beta^6$, and $\alpha\beta^8$ at $g$, with frequency 10, 120, 252, 120, and 10, respectively. Hence, if $\alpha\beta^4 \neq 1$, then $\#\mathcal{F} \leq 512 - 252 < 322 \leq m$, a contradiction. Thus $\alpha\beta^4 = 1$. Now, if $\alpha\beta^2 \neq 1 \neq \alpha\beta^6$, then $\#\mathcal{F} \leq 512 - 240 < 322 \leq m$, again a contradiction. Hence either $\alpha\beta^2 = 1$ or $\alpha\beta^6 = 1$. We conclude that $\beta^2 = 1$, and thus $g|_{V_{\mathcal{H}}} = \alpha \cdot \mathrm{Id}$, i.e. $g \in \mathbf{Z}(\boldsymbol{G})$, again a contradiction. □

THEOREM 6.2.10. *Let $p$ be a prime and $N \geq 9$. Suppose that there exists a hypergeometric sheaf $\mathcal{H}$ in characteristic $p$, of type $(D, m)$ with $D > m$, such that $G^\circ_{\mathrm{geom}}$ realizes* $\mathrm{Spin}_N$ *with $2 \nmid N$ in its spin representation, or the image of* $\mathrm{Spin}_N$ *with $2|N$ in one of its half-spin representations. Then $p = 2$ and $N \in \{10, 12, 16\}$.*

PROOF. (i) Assume that such an $\mathcal{H}$ exists. By Lemma 6.2.1, we may assume that $G_{\mathrm{geom}}$ is $\boldsymbol{G} := \mathrm{Spin}_N$ when $4 \nmid N$ and $\boldsymbol{G} = \mathrm{HSpin}_N$ when $4|N$. Now we construct a group homomorphism $\Lambda : \boldsymbol{G} \to \mathrm{GL}_s$ with $\Lambda$ and $s$ as follows. First, if $2 \nmid N$, then we choose $s := N$ and $\Lambda$ to be the natural projection $\mathrm{Spin}_N \twoheadrightarrow \mathrm{SO}_N$, with kernel equal to $\mathbf{Z}(\boldsymbol{G}) \cong C_2$. If $2|N$ but $4 \nmid N$, then we choose $s := N$ and $\Lambda$ to be the natural projection $\mathrm{Spin}_N \twoheadrightarrow \mathrm{SO}_N$, with kernel equal to $\langle \boldsymbol{z}^2 \rangle \cong C_2$. Suppose $4|N$. Then $\mathrm{Spin}_N$ acts on $L(\varpi_2) = \wedge^2(L(\varpi_1))$ with kernel $\langle \boldsymbol{z}_1, \boldsymbol{z}_2 \rangle$; so we choose $s := \dim L(\varpi_2) = n(2n-1)$ and $\Lambda$ the action of $\boldsymbol{G}$ on $L(\varpi_2)$, with kernel equal to $\mathbf{Z}(\boldsymbol{G})$. Applying [**KT5**, Theorem 4.14], we obtain that $w \leq s$. It follows that

$$m = D - w \geq D - s. \tag{6.2.10.1}$$

In fact, we observe that if $p > 2$ and $4|N$ then (6.2.10.1) also holds with $s := N$. Indeed, in this case we may assume $\boldsymbol{G} = \hat{\boldsymbol{G}}/\langle \boldsymbol{z}_2 \rangle$, where $\hat{\boldsymbol{G}} := \mathrm{Spin}_N$. Consider the natural projections $\pi : \hat{\boldsymbol{G}} \twoheadrightarrow \boldsymbol{G}$ with kernel $\langle \boldsymbol{z}_2 \rangle$, and $\Theta : \hat{\boldsymbol{G}} \twoheadrightarrow \mathrm{SO}_N$ with kernel $\langle \boldsymbol{z}_1 \boldsymbol{z}_2 \rangle$. Now we can apply [**KT5**, Theorem 4.14] to conclude that $w \leq N$, as stated.

(ii) By [**KT5**, Proposition 4.8], the image $Q$ of $P(\infty)$ in $\boldsymbol{G} = G_{\mathrm{geom}}$ contains an element $g \notin \mathbf{Z}(\boldsymbol{G})$. We may put the semisimple element $g$ in a maximal torus $\mathcal{T}$ of $\boldsymbol{G}$. The condition (6.2.10.1) now implies that there is a subset $\mathcal{F}$ of weights of the module $V = \mathbb{C}^D$, of cardinality at least $D - s$, such that all weights $\mu \in \mathcal{F}$ take the same value 1 at $g$.

Consider the case $N = 2n + 1$. Then we can choose an orthonormal basis $(e_1, \ldots, e_n)$ of $\mathbb{R}^n$ and realize the set of all weights (written additively) of the $\boldsymbol{G}$-module $V$ as $\sum_{i=1}^n a_i e_i/2$ with $a_i = \pm 1$. Recall that $\mathbf{Z}(\boldsymbol{G})$ is the common kernel of all weights that belong to the root lattice $\langle e_1, \ldots, e_n \rangle_{\mathbb{Z}}$, and that $g \notin \mathbf{Z}(\boldsymbol{G})$. Hence we may assume that

$$e_1(g) \neq 1. \tag{6.2.10.2}$$

We can represent any $\mu \in \mathcal{F}$ as

$$\mu = \mu_J = -\sum_{i=1}^n e_i/2 + \sum_{i \in J} e_i \tag{6.2.10.3}$$

with $J \subseteq \{1, 2, \ldots, n\}$. Consider any subset $J' \subseteq \{2, 3, \ldots, n\}$. If both $\mu_{J'}$ and $\mu_{J' \cup \{1\}}$ belong to $\mathcal{F}$, then we get

$$1 = \mu_{J' \cup \{1\}}(g)/\mu_{J'}(g) = e_1(g),$$

contradicting (6.2.10.2). It follows that $\#\mathcal{F}$ is at most the number of subsets of $\{2, 3, \ldots, n\}$, and so

$$2^n - (2n+1) = D - s \leq \#\mathcal{F} \leq 2^{n-1},$$

a contradiction when $n \geq 5$. Assume $n = 4$. The previous inequality now shows $\#\mathcal{F} \leq 8$, and $\#\mathcal{F} \geq m \geq 7$ by (6.2.10.1), whence $m \in \{7, 8\}$. Moreover, if $p > 2$ then $2|m$ by Lemma 6.2.1. Applying Proposition 6.2.5, we arrive at a contradiction.

(iii) Now assume that $N = 2n$. Then we can choose an orthonormal basis $(e_1, \ldots, e_n)$ of $\mathbb{R}^n$ and realize the set of all weights of the $\boldsymbol{G}$-module $V$ as $\sum_{i=1}^n a_i e_i/2$ with $a_i = \pm 1$ and $\prod_{i=1}^n a_i = 1$; in particular it has the lowest weight $-\sum_{i=1}^n e_i/2$. Again recall that $\mathbf{Z}(\boldsymbol{G})$ is the common kernel of all weights that belong to the root lattice $\langle e_i \pm e_j \mid 1 \leq i \neq j \leq n \rangle_{\mathbb{Z}}$, and that $g \notin \mathbf{Z}(\boldsymbol{G})$. Hence, we may assume that $(e_1 + \kappa e_2)(g) \neq 1$ for some $\kappa = \pm 1$. Conjugating $g$ using some element in the Weyl group that fixes the weight $e_i$ with $i \neq 2, n$ and changes the sign of each $e_2$ and $e_n$, we may assume that

$$(e_1 + e_2)(g) \neq 1. \tag{6.2.10.4}$$

We can again represent $\mu = \mu_J$ as in (6.2.10.3), but with the additional proviso that $\#J$ is even. Consider any subset $J' \subseteq \{3, 4, \ldots, n\}$ of even size, and suppose that both weights $\mu_{J'}$ and $\mu_{J' \cup \{1,2\}}$ belong to $\mathcal{F}$. Then we get

$$1 = \mu_{J' \cup \{1,2\}}(g)/\mu_{J'}(g) = (e_1 + e_2)(g),$$

contradicting (6.2.10.4). It follows that $\mathcal{F}$ has to miss at least one of these two weights for each even-size subset $J' \subseteq \{3, 4, \ldots, n\}$, and so

$$2^{n-1} - s = D - s \leq \#\mathcal{F} \leq 2^{n-1} - 2^{n-3}.$$

This is a contradiction when $n \geq 7$ and either $2 \nmid n$ or $p > 2$ (since $s = 2n$ in these cases), and when $2|n \geq 12$ and $p = 2$ (since $s = n(2n-1)$).

If $N = 20$, then $m \geq 322$ by (6.2.10.1), and this case is ruled out by Proposition 6.2.9. If $N = 12$ and $p > 2$, then $m \geq 20$ by (6.2.10.1), and this case is ruled out by Proposition 6.2.8. If $N = 10$, then $m \geq 6$ by (6.2.10.1), and the subcase $p > 2$ is ruled out by Proposition 6.2.7. □

PROPOSITION 6.2.11. *There is no hypergeometric sheaf $\mathcal{H}$ of type $(14, m)$ in characteristic $p$, with $m < 14$ and with $G^\circ_{\rm geom}$ realizing $\boldsymbol{G} := \mathrm{Sp}_6$ in its representation $L(\varpi_3)$.*

PROOF. Assume the contrary that such a sheaf $\mathcal{H}$ exists. By Theorems 4.1.1 and 4.1.5 we have $m \leq 12$, and so, by Lemma 6.2.2, tensoring $\mathcal{H}$ with a suitable $\mathcal{L}_\chi$ we may assume that $G_{\rm geom} = \boldsymbol{G} = \mathrm{Sp}(V)$; in particular, $\mathcal{H}$ is symplectically self-dual. Applying [**KT5**, Theorem 4.14] to the natural representation of $\boldsymbol{G}$ on $V = \mathbb{C}^6$, we get $6 \geq w := 14 - m$, and thus $m \geq 8$.

Consider any element $1 \neq g$ in the image $Q$ of $P(\infty)$ in $\boldsymbol{G}$. Then $g \in \mathrm{Sp}(V)$ is conjugate to $\mathrm{diag}(a, b, c, a^{-1}, b^{-1}, c^{-1})$ for some $a, b, c \in \mathbb{C}^\times$. It is well known, see e.g. [**OV**, Table 5] that $\wedge^3(V) \cong V \oplus L(\varpi_3)$ as $\boldsymbol{G}$-modules. Hence the spectrum of $g$ on the underlying representation $V_\mathcal{H}$ is the (multi)set of $a^{\pm 1}$, $b^{\pm 1}$, $c^{\pm 1}$, and $a^{\pm 1}b^{\pm 1}c^{\pm 1}$, among which at least $m \geq 8$ are equal to 1. Suppose for instance $a^2 \neq 1$. Then 1 is not in $\{a, a^{-1}\}$, and each of the 4 pairs $\{ab^ic^j, a^{-1}b^ic^j\}$ with $i, j = \pm 1$ contains 1 at most once. It follows that $b = c = 1$, in which case no $a^kb^ic^j$ with $i, j, k = \pm 1$ can be 1, and thus 1 is an eigenvalue of $g$ on $V_\mathcal{H}$ of multiplicity 4 only, a contradiction. We have therefore shown that $a^2 = b^2 = c^2 = 1$ and so $g^2 = 1$. It follows that $Q$ is an elementary abelian 2-group, whence $p = 2$ and $2 \nmid w$ by

[**KRLT4**, Proposition 4.9]. But the oddness of $w$ contradicts the fact that, geometrically, $\mathcal{H}$ is symplectically self-dual, see [**Ka-ESDE**, 8.8.2]. $\square$

THEOREM 6.2.12. *Let $p$ be a prime, and suppose that there exists a hypergeometric sheaf $\mathcal{H}$ in characteristic $p$, of type $(56, m)$ with $D > m$, such that $\boldsymbol{G} := G^{\circ}_{\mathrm{geom}}$ is of type $E_7$. Then $p \le 3$. Moreover, $m \neq 1$.*

PROOF. (i) Theorems 4.1.1 and 4.1.5 show that $w := D - m \ge 2$. Since $\boldsymbol{G}$ has no outer automorphism, Lemma 6.2.2 allows us to assume that $G_{\mathrm{geom}} = \boldsymbol{G}$.

We argue by contradiction, relying on [**KT5**, Theorem 4.17]. Assume that either $p > 7$ (so $p$ is coprime to the order of the Weyl group $W(\boldsymbol{G})$), or $p \in \{5, 7\}$ (so $p$ is not a torsion prime for $\boldsymbol{G}$). Since $V_{\mathcal{H}}$ is self-dual, the $Q$-characters on $\mathsf{Wild}$ have to occur in pairs $(\theta, \overline{\theta})$ with equal multiplicity, hence $2|w$ in the latter case. Postponing the case where $p \in \{5, 7\}$ and $2p|w$ until (iv), we have that either $p > 7$, or $p \in \{5, 7\}$ and $p \nmid w$. Applying [**KT5**, Theorem 4.17], we see that $w$ divides the order of some element in $W(\boldsymbol{G}) = \mathrm{Sp}_6(2) \times 2$, hence either $w = 30$ or $w \le 18$, see [**CCNPW**]; also, its proof shows that $Q$ is abelian.

Suppose $w = 30$. We work with the finite group $\langle Q, \gamma_{\mathrm{ss}} \rangle$ of $\boldsymbol{G}$ constructed in [**KT5**, Proposition 4.11], where $Q$ is the image of $P(\infty)$ in $\boldsymbol{G}$. As shown in the proof of [**KT5**, Theorem 4.17], $\gamma_{\mathrm{ss}}$ has order 30 in $\mathbf{N}_{\mathcal{Q}}(Q)/\mathbf{C}_{\boldsymbol{G}}(Q)$, and transitively permutes the 30 distinct linear characters of $Q$ on $\mathsf{Wild}$. Furthermore, $Q$ is contained in a maximal torus $\mathcal{T}$ of $\boldsymbol{G}$, and we can find $c \in \mathbf{C}_{\boldsymbol{G}}(Q)$ such that $\gamma_{\mathrm{ss}}c$ normalizes $\mathcal{T}$ and induces an element $\omega \in W(\boldsymbol{G})$ of order divisible by 30. It follows that $\mathsf{o}(\omega) = 30$, $\omega$ is unique up to conjugacy in $W(\boldsymbol{G})$, and it has a unique orbit $\mathcal{O}$ of length 30 on the set $\Omega$ of 56 $\mathcal{T}$-weights of $V_{\mathcal{H}}$. Note that $\gamma_{\mathrm{ss}}$ and $\gamma_{\mathrm{ss}}c$ have the same action on the 30 $Q$-characters afforded by $\mathsf{Wild}$. As $Q \le \mathcal{T}$, it follows that these 30 characters are obtained by restricting the $\mathcal{T}$-weights in $\mathcal{O}$. A computer calculation done by F. Lübeck shows that if $t \in \mathcal{T}$ and $\alpha(t) = 1$ for all 26 weights $\alpha \in \Omega \smallsetminus \mathcal{O}$, then $t = 1$. As $Q$ acts trivially on $\mathsf{Tame}$ of dimension 26, we conclude that $Q = 1$, a contradiction.

(ii) Now we assume that $w \le 18$, and so $m = \dim \mathsf{Tame} \ge 38$. Consider any element $1 \neq g \in Q$ of order $p$, and we aim to find the spectrum of $g$ on $V_{\mathcal{H}}$. Let

$$\mathcal{F} := \mathcal{F}(g) := \{\alpha \in \Omega \mid \alpha(g) = 1\},$$

so that

$$\#\mathcal{F} \ge m \ge 38. \tag{6.2.12.1}$$

It is convenient for us to realize the set $\Omega$ as follows. Consider a 3-dimensional $\mathbb{F}_2$-vector space $U$ with basis $(a, b, c)$, and an orthogonal basis $(e_u \mid u \in U)$ of the Euclidean space $\mathbb{R}^8$ with $(e_u, e_u) = 1/2$. Then the root system of type $E_8$ can be realized as

$$\{\pm 2e_u, \pm e_x \pm e_y \pm e_z \pm e_t \mid x, y, z, t \in U, x + y + z + t = 0,\ x, y, z, t \text{ pairwise distinct}\}.$$

Imposing the condition $u \neq 0$ on the roots, one obtains the root system of type $E_7$, and moreover the set $\Omega$ of the 56 $\mathcal{T}$-weights of $V_{\mathcal{H}}$ is given by

$$\Omega := \{\pm e_x \pm e_y \pm e_z \mid x, y, z \in U, x + y + z = 0,\ x, y, z \text{ pairwise distinct}\}. \tag{6.2.12.2}$$

For brevity, we will label elements of $U$ by $\{\bar{0}, \bar{1}, \dots, \bar{7}\}$ as follows:

$$0 \mapsto \bar{0},\ a \mapsto \bar{1},\ b \mapsto \bar{2},\ a + b \mapsto \bar{3},\ c \mapsto \bar{4},\ a + c \mapsto \bar{5},\ b + c \mapsto \bar{6},\ a + b + c \mapsto \bar{7}.$$

Then the seven (unordered) triples $(x, y, z)$ occuring in (6.2.12.2) are

$$(\bar{1}, \bar{2}, \bar{3}),\ (\bar{1}, \bar{4}, \bar{5}),\ (\bar{1}, \bar{6}, \bar{7}),\ (\bar{2}, \bar{4}, \bar{6}),\ (\bar{2}, \bar{5}, \bar{7}),\ (\bar{3}, \bar{5}, \bar{6}),\ (\bar{3}, \bar{4}, \bar{7}).$$

(iii) Note that, since $p > 2$, the weight $2e_{\bar{i}}$ takes value 1 at $g$ if and only if $e_{\bar{i}}$ does. Suppose first that $e_{\bar{i}}(g) \neq 1$ for at least two different values of $i$, $1 \leq i \leq 7$. Since $\mathrm{SL}(U) \cong \mathrm{SL}_3(2)$ embeds in $W(\boldsymbol{G})$ and acts doubly transitively on $U \smallsetminus \{\bar{0}\}$, we may assume that $e_{\bar{1}}(g) \neq 1$ and $e_{\bar{2}}(g) \neq 1$. Then for each choice of $(\kappa_2, \kappa_3) = (\pm 1, \pm 1)$, each pair $\pm e_{\bar{1}} + \kappa_2 e_{\bar{2}} + \kappa_3 e_{\bar{3}}$ can contain at most one weight from $\mathcal{F}$, and thus the triple $(\bar{1}, \bar{2}, \bar{3})$ yields at most 4 weights in $\mathcal{F}$. The same is true for $(\bar{1}, \bar{4}, \bar{5})$ and $(\bar{1}, \bar{6}, \bar{7})$. Repeating the argument for $e_{\bar{2}}$, we see that the same holds for $(\bar{2}, \bar{4}, \bar{6})$ and $(\bar{2}, \bar{5}, \bar{7})$. Thus $\#\mathcal{F} \leq 4 \cdot 5 + 2 \cdot 8 = 36$, contradicting (6.2.12.1).

We may therefore assume that $e_{\bar{i}}(g) = 1$ for $1 \leq i \leq 6$. Setting $e_{\bar{7}}(g) = \beta$, we now see that the weights in (6.2.12.2) take values 1, $\beta$, and $\beta^{-1}$, at $g$, with frequency 32, 12, and 12. But then (6.2.12.1) implies that $\beta = 1$, and thus $g = 1$, a contradiction.

(iv) As promised, we now return to the case where $p \in \{5, 7\}$ and $2p|w$. By [**KRLT4**, Proposition 4.9], this implies that $Q$ is non-abelian. Since $Q$ is nilpotent, it is supersolvable and so embeds in $\mathbf{N}_{\boldsymbol{G}}(\mathcal{T})$ for some maximal torus $\mathcal{T}$ of $\boldsymbol{G}$, see [**Bor**, E-44, II.5.16]. Now the nontrivial $p$-group $Q/Q_{\mathcal{T}}$, with $Q_{\mathcal{T}} := Q \cap \mathcal{T}$, embeds in $W(\boldsymbol{G}) = \mathrm{Sp}_6(2) \times 2$, so in fact $Q/Q_{\mathcal{T}}$ has order $p$, and we may assume it is generated by an element $\eta$ of order $p$ in $W(\boldsymbol{G})$. If $\mathbf{Z}(Q) \not\leq Q_{\mathcal{T}}$, then $Q = \mathbf{Z}(Q)Q_{\mathcal{T}}$ would be abelian, a contradiction. Hence $1 \neq \mathbf{Z}(Q) \leq Q_{\mathcal{T}}$; in particular, $Q_{\mathcal{T}}$ contains an element $z \in \mathbf{Z}(Q)$ of order $p$. Note that if $\beta \neq 1$ is an arbitrary eigenvalue for $z$ on $V_{\mathcal{H}}$, then the corresponding eigenspace is a sum of wild simple $Q$-submodules, hence all of dimension divisible by $p$.

Suppose now that $p = 7$. The above condition on $z$ implies by [**CG**, Table 6] that 1 is not an eigenvalue for $z$ on $V_{\mathcal{H}}$. Thus $\mathsf{Tame} = 0$, i.e. $\mathcal{H}$ is Kloosterman of rank 56. By [**KRLT4**, Proposition 4.9], the $Q$-module $V_{\mathcal{H}}$ is the sum of 8 simple submodules, $V_l$, $1 \leq l \leq 7$, permuted transitively by $\gamma_{\mathrm{ss}}$. Next, $h := \gamma_{\mathrm{ss}}^8$ fixes each $V_l$, and the spectrum of $h$ on one, hence on every by $\gamma_{\mathrm{ss}}$-action, submodule $V_l$ is $\xi \cdot (\mu_8 \smallsetminus \{1\})$ for some root of unity $\xi \in \mathbb{C}^\times$. In particular, the trace of $h$ on $V_{\mathcal{H}}$ is $-8\xi$. As $V_{\mathcal{H}}$ is self-dual, we must have that $\xi = \pm 1$, which implies $\mathsf{o}(h) = 8$. Since the central involution $\boldsymbol{z}$ of $\boldsymbol{G}$ acts as $-\mathrm{Id}$ on $V_{\mathcal{H}}$, replacing $h$ by $\delta\boldsymbol{z}$, we may assume that $\xi = 1$, and thus $h$ is an element in $\boldsymbol{G}$ of order 8, whose eigenvalues on $V_{\mathcal{H}}$ are the 7 nontrivial 8th roots of unity, each with multiplicity 7. It follows that $h^2$ is an element of order 4 in $\boldsymbol{G}$ that has eigenvalues 1, $\zeta_4$, $-1$, and $\zeta_4^3$, with multiplicity 8, 16, 16, and 16, respectively. However, such an element does not exist in $\boldsymbol{G}$, see [**CG**, Table 6].

Suppose now that $p = 5$ and $10|w$. The above condition imposed in on $z$ implies by [**CG**, Table 6] that 1 is an eigenvalue of $z$ of multiplicity 6 or 16; in particular $m \leq 16$, and so $w = 50$ or $w = 40$. Since $Q/Q_{\mathcal{T}} = \langle \eta \rangle \cong C_5$ and $Q_{\mathcal{T}}$ is abelian, Ito's theorem [**Is**, (6.15)] implies that any simple $Q$-module has dimension dividing 5, ruling out the case $w = 50$. Consider the case $w = 40$, in which $z$ is an element of type $5J$ in [**CG**, Table 6], that is,
(6.2.12.3)

the multiplicity of $\zeta_5^j$ as an eigenvalue of $z$ on $V_{\mathcal{H}}$ is 16 if $j = 0$ and 10 if $1 \leq j \leq 4$.

Recall that $z \in \boldsymbol{G}$ is centralized by the element $\eta \in W(\boldsymbol{G})$ of order 5. It is now convenient to use yet another realization of the weight system of type $E_7$ given in [**OV**, Table 1]. Namely, in the Euclidean space $\mathbb{R}^8$ one can find $f_1, \ldots, f_8$ with $(f_i, f_j) = \delta_{i,j} - 1/8$ and

$$\sum_{i=1}^{8} f_i = 0, \tag{6.2.12.4}$$

so that $\Omega = \{\pm(f_i + f_j) \mid 1 \leq i < j \leq 8\}$. This construction exhibits the action of the natural subgroup $\mathsf{S}_8$ of $W(\boldsymbol{G})$ (permuting $f_1, \ldots, f_8$), and we may assume that $\eta$ permutes $f_1, \ldots, f_5$ cyclically and fixes each of $f_6, f_7, f_8$. Taking (6.2.12.4) and $\mathsf{o}(z) = 5$ into account, we now have

$$f_1(z) = f_2(z) = \ldots = f_5(z) = \alpha,\ f_6(z) = \beta,\ f_7(z) = \gamma,\ f_8(z) = \delta = (\beta\gamma)^{-1},$$

where $\alpha, \beta, \gamma \in \mathbb{C}^\times$ and $\alpha^5 = \beta^5 = \gamma^5 = 1$. Now, if $\alpha = 1$, then all 20 weights $\pm(f_i + f_j)$ with $1 \leq i < j \leq 5$ take value 1 at $z$, contradicting (6.2.12.3). Hence

$$\alpha \neq 1, \tag{6.2.12.5}$$

and $(f_i + f_j)(z)$ with $1 \leq i < j \leq 5$ yield $\alpha^2$ with frequency 10, and $(-f_i - f_j)(z)$ for these $i, j$ yield $\alpha^{-2}$ with frequency 10, and, by (6.2.12.3), the remaining 36 weights of $\Omega$ must take value 1 at $z$ 16 times. If, however, none of $\alpha\beta, \alpha\gamma, \alpha\delta$ is 1, then 1 can be achieved only by the 6 weights $\pm(f_i + f_j)(z)$, $6 \leq j \leq 8$, a contradiction. Using an element $(6, 7, 8) \in \mathsf{S}_8$ that centralizes $\eta$, we may assume $\alpha\beta = 1$. Now, if none of $\alpha\gamma, \alpha\delta$ is 1, then 1 can be achieved only by the 10 weights $\pm(f_i + f_6)$, $1 \leq i \leq 5$, and the 6 weights $\pm(f_6 + f_j)(z)$, $j = 7, 8$, and $\pm(f_7 + f_8)$. It follows from (6.2.12.3) that all the latter 6 weights take value 1 at $z$, i.e.

$$\beta\gamma = \beta\delta = \gamma\delta = 1,$$

yielding $\beta^2 = 1$, and so $\alpha = \beta^{-1} = 1$, contradicting (6.2.12.5). Using the action of $(7, 8) \in \mathsf{S}_8$ if needed, we may assume $\alpha\gamma = 1$. But then the 20 weights $\pm(f_i + f_6)$ and $\pm(f_i + f_7)$ with $1 \leq i \leq 5$ all take value 1 at $z$, again contradicting (6.2.12.3).

(v) Suppose now that $m = 1$, so that $w = 55$. By the above results, $p = 2$ or 3. Hence, [**KRLT4**, Proposition 4.8] implies that $Q$ is elementary abelian of order $2^{20}$ or $3^{10}$, which is impossible for subgroups in $\boldsymbol{G}$ by the main result of [**CS**]. □

Theorem 6.2.13. *Let $p$ be a prime, and suppose that there exists a hypergeometric sheaf $\mathcal{H}$ in characteristic $p$, of type $(27, m)$ with $D > m$, such that $\boldsymbol{G} := G^\circ_{\mathrm{geom}}$ is of type $E_6$. Then $p \leq 3$. Moreover, either $m > 1$, or $(m, p) = (0, 3)$.*

Proof. (i) Theorems 4.1.1 and 4.1.5 show that $w := D - m \geq 2$. Since any automorphism of $\boldsymbol{G}$ which preserves the isomorphism class of the underlying representation $V_{\mathcal{H}}$ for $\boldsymbol{G}$ is inner, Lemma 6.2.2 allows us to assume that $G_{\mathrm{geom}} = \boldsymbol{G}$.

We argue by contradiction, again relying on [**KT5**, Theorem 4.17]. Assume that either $p > 5$ (so $p$ is coprime to the order of the Weyl group $W(\boldsymbol{G})$), or $p = 5$ (so $p$ is not a torsion prime for $\boldsymbol{G}$). Postponing the case where $p = 5$ and $p|w$ until (v), we have that either $p > 5$, or $5 = p \nmid w$. Applying [**KT5**, Theorem 4.17], we see that $w$ divides the order of some element in $W(\boldsymbol{G}) = \mathrm{SU}_4(2) \rtimes 2$, hence $w \leq 12$, see [**CCNPW**]; also, its proof shows that $Q$ is contained in a maximal torus $\mathcal{T}$ and so is abelian. In particular, $m = \dim \mathsf{Tame} \geq 15$.

It is convenient to use the following realization of the weight system of type $E_6$ given in [**OV**, Table 1]. Namely, in the Euclidean space $\mathbb{R}^6$ one can find $f, e_1, \ldots, e_6$ with $(e_i, e_j) =$

$\delta_{i,j} - 1/6$, $(f, e_i) = 0$, $(f, f) = 1/2$, and

$$\sum_{i=1}^{6} e_i = 0, \tag{6.2.13.1}$$

so that the set $\Omega$ of 27 $\mathcal{T}$-weights of $V_{\mathcal{H}}$ is

$$\Omega = \{e_i \pm f, e_{ij} := -e_i - e_j \mid 1 \leq i < j \leq 6\}.$$

This construction exhibits the action of the natural subgroup $\mathsf{S}_6 \times C_2 \in W(\boldsymbol{G})$ (with $\mathsf{S}_6$ permuting $e_1, \ldots, e_6$ and fixing $f$ and $C_2$ fixing $e_1, \ldots, e_6$ and changing sign of $f$).

(ii) Consider any element $1 \neq g \in Q$ of order $p$. Note that, since $p > 3$, the weight $6e_i$ takes value 1 at $g$ if and only if $e_i$ does. Call a weight $\omega \in \Omega$ *good* (for $g$) if $\omega(g) = 1$, and *bad* otherwise. As $m \geq 15$, we have that

(6.2.13.2) the number of bad weights (for a fixed $g$) is at most 12.

We show that the action of $g$ on $V_{\mathcal{H}}$ is conjugate to

$$\operatorname{diag}\bigl(\mathrm{Id}_{15}, \zeta \cdot \mathrm{Id}_6, \zeta^{-1} \cdot \mathrm{Id}_6\bigr) \tag{6.2.13.3}$$

for a primitive $p^{\text{th}}$ root $\zeta$ of unity.

Here we consider the case $f(g) \neq 1$. Then each pair $e_i \pm f$, $1 \leq i \leq 6$, must contain at least one bad weight. Now, if $e_1(g) = e_2(g) = \ldots = e_6(g) =: \xi$, then (6.2.13.1) implies that $\xi^6 = 1$ and so $\xi = 1$, in which case (6.2.13.3) holds with $\zeta := f(g)$. So, using the $\mathsf{S}_6$-action, we may assume that $e_1(g) \neq e_2(g)$.

Suppose first that $e_3(g) \neq e_4(g)$. Then each of the 6 pairs $(e_{13}, e_{23})$, $(e_{14}, e_{24})$, $(e_{15}, e_{25})$, $(e_{16}, e_{26})$, $(e_{35}, e_{45})$, $(e_{36}, e_{46})$ also contains at least one bad weight from $\mathcal{F}$. Hence (6.2.13.2) implies that there are no more bad weights among the remaining 3 weights $e_{12}$, $e_{34}$, and $e_{56}$, and so

$$e_1(g) = \alpha,\ e_2(g) = \alpha^{-1},\ e_3(g) = \beta,\ e_4(g) = \beta^{-1},\ e_5(g) = \gamma,\ e_6(g) = \gamma^{-1}$$

for some $\alpha, \beta, \gamma \in \mathbb{C}^\times$. It also follows that each of the aforementioned 12 pairs contains exactly one bad weight and one good weight. Applying this to $(e_{13}, e_{23})$, we see that $1 = \alpha\beta$ or $1 = \alpha^{-1}\beta$. Conjugating by $(3, 4) \in \mathsf{S}_6$ if necessary, we may assume $\beta = \alpha$. Applying this argument to $(e_{15}, e_{25})$ and $e_1 \pm f$, we may also assume that $f(g) = \gamma = \alpha$. Thus, at $g$ the 27 weights in $\Omega$ take value 1, $\alpha^2$, and $\alpha^{-2}$, with frequency 15, 6 and 6, respectively, and thus (6.2.13.3) holds with $\zeta := \alpha^2$.

Now we consider the case $\alpha := e_1(g) \neq \beta := e_2(g)$ but $e_3(g) = e_4(g) = e_5(g) = e_6(g) =: \gamma$. Suppose in addition that $\gamma \neq 1$. Then all 6 weights $e_{ij}$, $3 \leq i < j \leq 6$ are bad. Hence (6.2.13.2) implies that the remaining weights are all good, including $e_{13}$, and $e_{23}$. In this case, $\alpha\gamma = 1 = \beta\gamma$, contradicting the assumption $\alpha \neq \beta$. Thus $\gamma = 1$. If in addition $\alpha \neq 1 \neq \beta$, then the 8 weights $e_{ij}$ with $i = 1, 2$ and $3 \leq j \leq 6$ are all bad, contradicting (6.2.13.2). Hence $1 \in \{\alpha, \beta\}$, which then implies by (6.2.13.1) that $\alpha = 1 = \beta$, again a contradiction.

(iii) Now we consider the case $f(g) = 1$. Suppose that $e_i(g) \neq 1$ for all $1 \leq i \leq 6$. Then the 12 weights $e_i \pm f$ are all bad, hence by (6.2.13.2), all the 15 weights $e_{ij}$ are good. It follows that $1 \neq e_1(g) = \ldots = e_6(g) =: \alpha$ but $\alpha^2 = 1$, a contradiction.

So we may assume that $e_1(g) = 1$. Suppose that $e_i(g) \neq 1$ for all $2 \leq i \leq 5$. Then the 12 weights $e_i \pm f$ and $e_{1i}$ with $2 \leq i \leq 5$ are all bad. Hence by (6.2.13.2), all the other 15 weights, including $e_{23}$, $e_{24}$, $e_{34}$, are good. It follows that $1 \neq e_2(g) = e_3(g) = e_4(g) =: \alpha$ but $\alpha^2 = 1$, again a contradiction.

Hence we may assume that $e_1(g) = e_2(g) = e_3(g) = 1$. If $e_i(g) \neq 1$ for all $4 \leq i \leq 6$, then the 15 weights $e_i \pm f$ and $e_{ij}$ with $4 \leq i \leq 6$, $1 \leq i \leq 3$ are all bad, contradicting (6.2.13.2). We may now assume that $e_1(g) = e_2(g) = e_3(g) = e_4(g) = 1$. In this case, (6.2.13.1) implies that $e_5(g) = \alpha$ and $e_6(g) = \alpha^{-1}$, showing that (6.2.13.3) holds for $\zeta := \alpha$.

(iv) Now that we have established (6.2.13.3), the condition $m \geq 15$ implies that in fact $m = 15$ and $w = 12$. As $5 \leq p \nmid w$, [**KRLT4**, Proposition 4.8] shows that $Q$ is elementary abelian of order $p^a$ for some $a \in \{1, 2\}$, and the $Q$-module $\mathsf{Wild}$ is multiplicifty-free. If $a = 1$, then (6.2.13.3) shows that $Q = \langle g \rangle$ has a simple submodule of dimension 1 with multiplicity 6 on $\mathsf{Wild}$, a contradiction. So we can write $Q = \langle g, h \rangle \cong C_p^2$. By (6.2.13.3), the $g$-module $\mathsf{Wild}$ is the sum of two $g$-eigenspaces $W_\zeta$ and $W_{\zeta^{-1}}$, each of dimension 6. The $Q$-module $\mathsf{Wild}$ being multiplicity-free forces $h$ to act on $W_\zeta$ with 6 distinct eigenvalues, and this contradicts (6.2.13.3) applied to $h$.

(v) As promised, we now return to the case where $5 = p|w$. By [**KRLT4**, Proposition 4.9], this implies that $Q$ is non-abelian. Since $Q$ is nilpotent, it is supersolvable and so embeds in $\mathbf{N}_{\boldsymbol{G}}(\mathcal{T})$ for some maximal torus $\mathcal{T}$ of $\boldsymbol{G}$, see [**Bor**, E-45, II.5.16]. Now the nontrivial $p$-group $Q/Q_\mathcal{T}$, with $Q_\mathcal{T} := Q \cap \mathcal{T}$, embeds in $W(\boldsymbol{G}) = \mathrm{SU}_4(2) \rtimes 2$, so in fact $Q/Q_\mathcal{T}$ has order 5, and we may assume it is generated by an element $\eta$ of order 5 in $W(\boldsymbol{G})$. If $\mathbf{Z}(Q) \not\leq Q_\mathcal{T}$, then $Q = \mathbf{Z}(Q)Q_\mathcal{T}$ would be abelian, a contradiction. Hence $1 \neq \mathbf{Z}(Q) \leq Q_\mathcal{T}$; in particular, $Q_\mathcal{T}$ contains an element $z \in \mathbf{Z}(Q)$ of order 5. Note that if $\beta \neq 1$ is an arbitrary eigenvalue for $z$ on $V_\mathcal{H}$, then the corresponding eigenspace is a sum of wild simple $Q$-submodules, hence all of dimension divisible by 5. This implies by [**CW**, Table 2] that 1 is an eigenvalue of $z$ of multiplicity 2 or 7; in particular $m \leq 7$, and so $w = 25$ or $w = 20$. Since $Q/Q_\mathcal{T} = \langle \eta \rangle \cong C_5$ and $Q_\mathcal{T}$ is abelian, Ito's theorem [**Is**, (6.15)] implies that any simple $Q$-module has dimension dividing 5, ruling out the case $w = 25$.

Consider the case $w = 20$, in which $z$ is an element of type $5E$ in [**CW**, Table 2], that is, (6.2.13.4)

the multiplicity of $\zeta_5^j$ as an eigenvalue of $z$ on $V_\mathcal{H}$ is 7 if $j = 0$ and 5 if $1 \leq j \leq 4$.

Recall that $z \in \boldsymbol{G}$ is centralized by the element $\eta \in W(\boldsymbol{G})$ of order 5, and we may assume that $\eta$ permutes $e_1, \ldots, e_5$ cyclically and fixes each of $e_6$ and $f$. Taking (6.2.13.1) and $\mathsf{o}(z) = 5$ into account, we now have

$$e_1(z) = e_2(z) = \ldots = e_5(z) = \alpha,\ e_6(z) = 1,\ f(z) = \beta,$$

where $\alpha, \beta \in \mathbb{C}^\times$ and $\alpha^5 = 1$. Now the 10 weights $e_{ij}$, $1 \leq i < j \leq 5$, all take value $\alpha^{-2}$ at $z$, violating (6.2.13.4).

(vi) Assume now that $m \leq 1$. By the previous results, we may now assume that $p = 2$ or 3. Suppose $m = 0$ but $p = 2$. As $w = 27$, by [**KRLT4**, Proposition 4.8], $Q$ is elementary abelian of order $2^{18}$, but $\boldsymbol{G}$ does not possess such a subgroup by the main result of [**CS**].

Suppose $m = 1$, so that $w = 26$. If $p = 3$, then [**KRLT4**, Proposition 4.8] implies that $g_\infty^{13}$ has spectrum $\big(1^{[13]}, (-1)^{[13]}\big)$ on $\mathsf{Wild}$. Then the 2-part $h$ of $g_\infty^{13}$ has the same spectrum on $\mathsf{Wild}$, and $\{\beta\}$ on $\mathsf{Tame}$ for some $\beta \in \mathbb{C}^\times$ of finite order $2^b$. If $b \leq 1$, then $h$ is an involution, and [**CW**, Theorem 3.1] shows that $\boldsymbol{G}$ cannot have an involution with such a spectrum. If $b \geq 2$, then $h^{2^{b-1}}$ has spectrum $\big(1^{[26]}, (-1)\big)$, which is again ruled out by [**CW**, Theorem 3.1].

If $p = 2$, then [**KRLT4**, Proposition 4.9] implies that $g_\infty^{13}$ has spectrum $\big(\xi^{[13]}, \xi\zeta_3^{[13]}\big)$ on $\mathsf{Wild}$, for some $\xi \in \mathbb{C}^\times$. Then the 3-part $h$ of $g_\infty^{13}$ has spectrum $\big(\alpha^{[13]}, \alpha\zeta_3^{[13]}\big)$ on $\mathsf{Wild}$ and $\{\beta\}$ on $\mathsf{Tame}$ for some $\alpha, \beta \in \mathbb{C}^\times$ of finite order $2^a$ and $2^b$. Replacing $\zeta_3$ by $\overline{\zeta}_3$ and $\alpha$ by $\alpha\zeta_3$, we may assume that $\mathsf{o}(\alpha) \geq \mathsf{o}(\alpha\zeta_3)$ and thus $a \geq 1$. Now, if $b > a$ or if $a > \max(b, 1)$, then $h^{\max(a,b)-1}$ is an element of order 3 with some $\zeta \in \mu_3$ as an eigenvalue of multiplicity 26, which contradicts [**CW**, Theorem 3.1]. If $a = 1 \geq b$, then two of $1, \zeta_3, \overline{\zeta}_3$ are eigenvalues of multiplicity $\geq 13$, which is again impossible by [**CW**, Theorem 3.1]. In the remaining case $a = b \geq 2$, $h^{3^{a-1}}$ acts as multiplication by $\alpha^{3^{a-1}} \in \mu_3 \smallsetminus \{1\}$ on $\mathsf{Wild}$ and $\beta^{3^{a-1}}$ on $\mathsf{Tame}$. Using [**CW**, Theorem 3.1], we see that $\beta^{3^{a-1}} = \alpha^{3^{a-1}}$. Replacing $h$ by $\alpha^{-1}h$, we see that $h$ has spectrum $\big(\zeta_3^{[13]}, 1^{[13]}\big)$ on $\mathsf{Wild}$ and an eigenvalue of order $3^{a-1} \geq 3$ on $\mathsf{Tame}$, which is ruled by the argument for the $b \geq a = 1$ case. □

Now we can formulate one of the main results of the book:

THEOREM 6.2.14. *Suppose $\mathcal{H}$ is a hypergeometric sheaf in characteristic $p$, of type $(D, m)$ with $D > m$ and $D \geq 2$ such that $G_{\rm geom}$ is primitive and infinite. If $D = 4, 8, 9$, suppose in addition that $\mathcal{H}$ satisfies* $(\mathbf{S}+)$. *Then $\boldsymbol{G} := G_{\rm geom}^\circ$ is a simple algebraic group that acts irreducibly on $\mathcal{H}$, and one of the following statements holds.*

(i) *$\boldsymbol{G}$ is $\mathrm{SL}_D$, $\mathrm{SO}_D$, or, $\mathrm{Sp}_D$ with even $D$, acting on $\mathcal{H}$ via the natural representation or its dual.*
(ii) *$D = 4$, $p = 3$, and $\boldsymbol{G}$ is the image of $\mathrm{SL}_2 = \mathrm{SL}(V)$ acting on $\mathrm{Sym}^3(V)$.*
(iii) *$D = 5$, $p = 2$, and $\boldsymbol{G}$ is the image of $\mathrm{SL}_2 = \mathrm{SL}(V)$ acting on $\mathrm{Sym}^4(V)$.*
(iv) *$D = 6$, $p = 2$, and $\boldsymbol{G} = \mathrm{SL}_3 = \mathrm{SL}(V)$ acting on $\mathcal{H}$ as on $\mathrm{Sym}^2(V)$ or $\mathrm{Sym}^2(V^*)$.*
(v) *$D = 7$ and $\boldsymbol{G}$ is $G_2$.*
(vi) *$D = 8$, and $\boldsymbol{G}$ acts on $\mathcal{H}$ as $\mathrm{SL}_3 = \mathrm{SL}(V)$ acts on the adjoint module.*
(vii) *$D = 8$, and $\boldsymbol{G}$ acts on $\mathcal{H}$ as $\mathrm{Spin}_7$ acts on its spin module.*
(viii) *$\boldsymbol{G}$ is the image of $\mathrm{SL}_6 = \mathrm{SL}(V)$ acting on $\wedge^k(V)$ or $\wedge^k(V^*)$ for $2 \leq k \leq 3$ and $2 \leq p \leq k$.*
(ix) *$p = 2$, $D = 2^{N/2-1}$ with $N \in \{10, 12, 16\}$, and $\boldsymbol{G} = \mathrm{HSpin}_N$.*
(x) *$2 \leq p \leq 3$, and $(D, \boldsymbol{G}) = (27, E_6)$ or $(56, E_7)$.*

*Moreover, if $w := D - m \geq 2$ in addition, then we have the following more precise information.*

(a) *In case* (i), *there exists a tame character $\chi$ such that the geometric monodromy group of $\mathcal{L}_\chi \otimes \mathcal{H}$ is either $\boldsymbol{G}$, or $\mathrm{O}_D$ with $2|D$.*
(b) *In cases* (ii)–(v), (ix), *and* (x), *there exists a tame character $\chi$ such that $\mathcal{L}_\chi \otimes \mathcal{H}$ has $G_{\rm geom} = \boldsymbol{G}$.*

PROOF. By Theorem 5.2.9, the primitivity of $\mathcal{H}$ implies $(\mathbf{S}+)$ when $D \neq 4, 8, 9$. Hence, $(\mathbf{S}+)$ holds in all cases, and so $\boldsymbol{G} = G_{\rm geom}^\circ$ is a simple algebraic group acting irreducibly in the underlying representation $V_{\mathcal{H}}$. Next, recall that a (topological) generator $g_0$ of the image of $I(0)$ in $G_{\rm geom}$ has a regular spectrum on $V_{\mathcal{H}}$, and so we can apply Theorem 3.3.4 to recognize $V_{\mathcal{H}}$. In the case $\boldsymbol{G}$ is of type $A_r$, the statement now follows from Theorem 6.1.5 when $r = 1$ (note that the image of $\mathrm{SL}_2 = \mathrm{SL}(V)$ on $\mathrm{Sym}^2(V)$ is just $\mathrm{SO}_3$ on its natural module), and Theorem 6.1.16 when $r > 1$ (again note the image of $\mathrm{SL}_4 = \mathrm{SL}(V)$ on $\wedge^2(V)$ is just $\mathrm{SO}_6$ on its natural module). If $\boldsymbol{G}$ is of type $C_r$, the statement follows from Proposition 6.2.11. For the remaining types $B_r, D_r$ and $E_6$, $E_7$, the statement follows from Theorems 6.2.10, 6.2.13, and 6.2.12.

The "moreover" statement results from Lemma 6.2.2, together with the fact that for $D > 4$ even, the normalizer of $\mathrm{SO}_D$ in $\mathrm{GL}_D$ is the central product $\mathrm{GL}_1 * \mathrm{O}_D$. □

Remark 6.2.15. The requirement that $w := D - m \geq 2$ in the "moreover" statement of Theorem 6.2.14 is essential. For if $w = 1$, then in any odd characteristic $p$, we have $G^0_{\mathrm{geom}} = \mathrm{SL}_D$, cf. Theorem 4.1.1, but (because $w = 1$) $\det(\mathcal{H})$ has order divisible by $p$. So we would need to twist by a character whose $D^{\mathrm{th}}$ power has order divisible by $p$, and no such character is tame. The best we could do is twist by a tame character so that the "upstairs" characters have product $\mathbb{1}$, in which case $G_{\mathrm{geom}}$ will be the group $\{g \in \mathrm{GL}_D | \det(g)^p = 1\}$.

CHAPTER 7

# Extraspecial normalizers and local systems in odd characteristics

## 7.1. A supersingularity result

Given an integer $n \geq 1$, and a power $q$ of $p$, consider the universal family of polynomials of the form

$$\sum_{i=0}^{n} s_i x^{1+q^i} + s_{-1}x$$

over the space $(\mathbb{G}_m \times \mathbb{A}^{n+1})/\mathbb{F}_p$, with coordinates $(s_n, s_{n-1}, \ldots, s_{-1})$. On $(\mathbb{G}_m \times \mathbb{A}^{n+1})/\mathbb{F}_p$, we have a local system $\mathcal{U}_{n,q}$ of rank $q^n$ whose trace function is as follows: for $k/\mathbb{F}_p$ a finite extension, and $(s_n, s_{n-1}, \ldots, s_{-1}) \in k^\times \times k^{n+1}$,

$$\mathrm{Trace}(\mathsf{Frob}_{(s_n,s_{n-1},\ldots,s_{-1}),k}|\mathcal{U}_{n,q}) = -\sum_{x\in k} \psi_k\big(\sum_{i=0}^{n} s_i x^{1+q^i} + s_{-1}x\big).$$

Theorem 7.1.1. *Over $\mathbb{F}_{p^2}$, the Tate twisted local system $\mathcal{U}_{n,q}(1/2)$ is geometricallly irreducible, and has finite arithmetic and geometric monodromy groups.*

Proof. To see the geometric irreducibility, notice that pulled back to the line $(1, 0, \ldots, 0, s_{-1})$ it is the Fourier transform of the lisse rank one sheaf $\mathcal{L}_{\psi(x^{1+q^n})}$, so already this pullback is geometrically irreducible. It is proven in [**Ka-MMP**, 3.8.6] that each curve

$$y^p - y = \sum_{i=0}^{n} s_i x^{1+q^i} + s_{-1}x$$

is supersingular. For such a curve over $\mathbb{F}_q/\mathbb{F}_{p^2}$, each Frobenius eigenvalue is of the form $q^{1/2}$ times a root of unity (where we write $q^{1/2} := p^{\deg(\mathbb{F}_q/\mathbb{F}_{p^2})}$). In particular, each eigenvalue of $\mathsf{Frob}_{k,(s_n,s_{n-1},\ldots,s_{-1})}|\mathcal{U}_n$ is of this form. Thus $\mathcal{U}_n(1/2)$ is pure of weight zero, and all of its Frobenius eigenvalues are roots of unity. This implies the asserted finiteness, cf. [**KRLT1**, 2.1]. □

Theorem 7.1.2. *For $k$ a finite extension of $\mathbb{F}_p$, $q$ a power of $p$, $n \geq 1$, and $(s_n, s_{n-1}, \ldots, s_0, s_{-1}) \in k^\times \times k^{n+1}$, define*

$$S(s_{-1}, s_0, \ldots, s_n; k) := \frac{-1}{\sqrt{\#k}} \sum_{x\in k} \psi_k\big(\sum_{i=0}^{n} s_i x^{1+q^i} + s_{-1}x\big).$$

*Then we have the following results.*

(a) *If $k$ is an extension of $\mathbb{F}_q$, then $|S(s_{-1}, s_0, \ldots, s_n; k)|^2$ is either $0$ or a power $q^\nu$ of $q$ with $0 \leq \nu \leq 2n$. If $s_{-1} = 0$ and $q$ is odd, the value $0$ does not occur.*

(b) *If $k$ is a subfield of $\mathbb{F}_q$ and $p$ is odd, then $|S(s_{-1}, s_0, \ldots, s_n; k)|^2$ is either $0$ or $1$ or $\#k$, and all three are attained as we range over all possible $(s_n, s_{n-1}, \ldots, s_0, s_{-1}) \in k^\times \times k^{n+1}$. If $s_{-1} = 0$ and $q$ is odd, the value $0$ does not occur.*

(c) *If $k$ is a subfield of $\mathbb{F}_q$ and $p = 2$, then $|S(s_{-1}, s_0, \ldots, s_n; k)|^2$ is either $0$ or $\#k$, and both are attained as we range over all possible $(s_n, s_{n-1}, \ldots, s_0, s_{-1}) \in k^\times \times k^{n+1}$.*

(d) *If $n$ is odd, and if $s_i = 0$ for all even $i$, and if $k$ is a finite extension of $\mathbb{F}_{q^2}$, then $|S(s_{-1}, s_0, \ldots, s_n; k)|$ is either $0$ or a power of $q$. If $s_{-1} = 0$ and $q$ is odd, the value $0$ does not occur.*

Proof. This is a variation of the argument of [**vdG-vdV**, Section 5].

We first prove (b). Suppose now $k$ is a subfield of $\mathbb{F}_q$. Then for $x \in k$ each term $s_i x^{1+q^i} = s_i x^2$, so our raw sum

$$-\sum_{x \in k} \psi_k\big(\sum_{i=0}^{n} s_i x^{1+q^i} + s_{-1}x\big) = -\sum_{x \in k} \psi_k\big((\sum_{i=0}^{n} s_i)x^2 + s_{-1}x\big)$$

is either 0 (if $\sum_{i=0}^n s_i = 0$ and $s_{-1} \neq 0$) or a quadratic Gauss sum over $k$ (if $(\sum_{i=0}^n s_i \neq 0)$ or $-\#k$ (if $\sum_{i=0}^n s_i = 0 = s_{-1}$).

For (c), we use the fact for $x \in k$, $s_i x^{1+q^i} = s_i x^2$ has the same $\mathrm{Tr}_{k/\mathbb{F}_p}$ as $s_i^{1/2}x$, and hence our raw sum is $\psi_k$ applied to a multiple of $x$ (the multiple being $s_{-1} + \sum_{i \geq 0} s_1^{1/2}$), so the raw sum is either 0 or $\#k$, and both are attained.

We now turn to the proof of (a). Denote by $R(x)$ the $q$-linear polynomial

$$R(x) := \sum_{i=0}^{n} s_i x^{q^i}.$$

Then the square absolute value of the sum in question is

$$\begin{aligned}
&(1/\#k) \sum_{x,y \in k} \psi_k\big(R(x)x + s_{-1}x - R(y)y - s_{-1}y\big) \\
&= (1/\#k) \sum_{x,y \in k} \psi_k\big(R(x+y)(x+y) - R(y)y + s_{-1}x\big) \\
&= (1/\#k) \sum_{x \in k} \psi_k\big(R(x)x + s_{-1}x\big) \sum_{y \in k} \psi_k\big(R(x)y + R(y)x\big).
\end{aligned}$$

The inner sum is $\psi$ applied to

$$\mathrm{Tr}_{k/\mathbb{F}_p}\big(R(x)y + R(y)x\big),$$

which is an $\mathbb{F}_p$-valued symmetric bilinear form on $k$, viewed as vector space over $\mathbb{F}_p$: let us denote it as

$$\langle x, y \rangle_R := \mathrm{Tr}_{k/\mathbb{F}_p}\big(R(x)y + R(y)x\big),$$

More precisely, we have

$$\begin{aligned}\mathrm{Tr}_{k/\mathbb{F}_p}\big(R(x)y+R(y)x\big) &= \mathrm{Tr}_{k/\mathbb{F}_p}\big(R(x)y+x\sum_{i=0}^{n}s_iy^{q^i}\big)\\ &= \mathrm{Tr}_{k/\mathbb{F}_p}(R(x)y+\sum_{i=0}^{n}(s_ix)^{1/q^i}y)\\ &= \mathrm{Tr}_{k/\mathbb{F}_p}\big(y(R(x)+\sum_{i=0}^{n}(s_ix)^{1/q^i})\big).\end{aligned}$$

So by nondegeneracy of the Trace, the inner sum over $y$ vanishes unless $x$ satisfies

$$R(x)+\sum_{i=0}^{n}(s_ix)^{1/q^i}=0,$$

i.e.

$$\sum_{i=0}^{n}s_ix^{q^i}+\sum_{i=0}^{n}(s_ix)^{1/q^i}=0,$$

or equivalently, applying the $q^n$ power map,

$$\sum_{i=0}^{n}s_i^{q^n}x^{q^{i+n}}+\sum_{i=0}^{n}(s_ix)^{q^{n-i}}=0,$$

in which case the inner sum is $\#k$. Let us denote by

$$W_R:=\left\{x\in k:\sum_{i=0}^{n}s_i^{q^n}x^{q^{i+n}}+\sum_{i=0}^{n}(s_ix)^{q^{n-i}}=0\right\}.$$

On the one hand, this is visibly an $\mathbb{F}_q$ vector space, of dimension $\leq 2n$. On the other hand, it is set of elements in $k$ which are orthogonal to every element $y\in k$ for $\langle x,y\rangle_R$. From this second interpretation, we see that the map

$$W_R\to\mathbb{F}_p: x\mapsto \mathrm{Tr}_{k/\mathbb{F}_p}(xR(x))$$

is additive. Indeed, for $x,y$ both in $W_R$, using the additivity of $x\mapsto R(x)$, we have

$$(x+y)R(x+y)=xR(x)+yR(y)+xR(y)+yR(x),$$

and we take $\mathrm{Tr}_{k/\mathbb{F}_p}$. Thus $x\mapsto \mathrm{Tr}_{k/\mathbb{F}_p}(xR(x)+s_{-1}x)$ is an additive map from $W_R$ to $\mathbb{F}_p$.

Recall that we have

$$|S(s_{-1},s_0,\ldots,s_n;k)|^2=\sum_{x\in W_R}\psi(\mathrm{Tr}_{k/\mathbb{F}_p}(xR(x)+s_{-1}x)).$$

If $x\mapsto \mathrm{Tr}_{k/\mathbb{F}_p}(xR(x)+s_{-1}x)$ is the zero map, then we get $|S(s_{-1},s_0,\ldots,s_n;k)|^2=\#W_R$. Otherwise we get 0. Because $W_R$ is an $\mathbb{F}_q$ vector space of $\mathbb{F}_q$-dimension $\leq 2n$, its cardinality is the asserted power of $q$.

To prove (d), we observe that if $n$ is odd and the only nonzero $s_i$ have $i$ odd, then in the equation defining $W_R$, only even powers of $q$ appear as exponents, so in this case $W_R$ is an $\mathbb{F}_{q^2}$ vector space. So its cardinality is a power of $q^2$, and hence $|S(s_{-1},s_0,\ldots,s_n;k)|$ itself is a power of $q$. □

Corollary 7.1.3. *Let $k$ be a subfield of $\mathbb{F}_q$, say $\#k = q_0$ and $q = q_0^f$ for some integer $f \geq 1$. Let $L/k$ be a finite extension. For $(s_n, s_{n-1}, \ldots, s_0, s_{-1}) \in L^\times \times L^{n+1}$, the square absolute value of*

$$(-1/\sqrt{\#L})\sum_{x\in L}\psi_L\big(\sum_{i=0}^{n} s_i x^{1+q^i} + s_{-1}x\big).$$

*is either $0$ or a power $q_0^\nu$ of $q_0$ with $0 \leq \nu \leq 2nf$. If $s_{-1} = 0$ and $q$ is odd, the value zero does not occur.*

Proof. View the situation as lying over $\mathbb{F}_{q_0}$, and apply Theorem 7.1.2. □

We will need the following, quite surprising, congruence result for certain trace functions:

Theorem 7.1.4. *Let $p$ be a prime, $\ell \neq p$, $\sqrt{p} \in \overline{\mathbb{Q}_\ell}$ a chosen square root of $p$, $q$ a power of $p$, $n \geq 2$ an integer, and let $a_1 > a_2 > \ldots > a_n > 0$ be odd integers. Consider the local system $\mathcal{G}$ on $\mathbb{G}_m \times \mathbb{A}^n$ over $\mathbb{F}_p$ whose trace function is*

$$(s_1, \ldots, s_n, t) \in k^\times \times k^n \mapsto \frac{-1}{\sqrt{\#k}}\sum_{x\in k}\psi_k\big(\sum_{i=1}^{n} s_i x^{q^{a_i}+1} + tx\big),$$

*in which we understand $\sqrt{\#k}$ to mean $\sqrt{p}^{\deg(k/\mathbb{F}_p)}$. Denote by $G_{\mathrm{arith}}$ the (finite, by Theorem 7.1.1) arithmetic monodromy group of $\mathcal{F}$.*

*If $p = 2$, let $k$ be a finite extension of $\mathbb{F}_{q^2}$. If $p$ is odd, let $k$ be a finite extension of $\mathbb{F}_{q^4}$. Given a point*

$$(s,t) := (s_1, \ldots, s_n, t) \in k^\times \times k^n,$$

*denote by $F_{(s,t),k}$ the image of $\mathsf{Frob}_{(s,t),k}$ in $G_{\mathrm{arith}}$. Let $K/k$ be a finite extension field whose degree $N$ is $1(\bmod\ p)$. Then the traces of $F_{(s,t),k}$ and of $\big(F_{(s,t),k}\big)^N = F_{(s,t),K}$ are related by the congruence*

$$\mathrm{Trace}\big((F_{(s,t),k})^N\big) \equiv \mathrm{Trace}(F_{(s,t),k}) \ (\mathrm{mod}\ (q+1)\mathbb{Z}[\zeta_p]).$$

Proof. We first remark that over extensions of $\mathbb{F}_{p^2}$, the "clearing factor" $\sqrt{\#k}$ is an integer, and hence over such extensions all Frobenius traces lie in $\mathbb{Z}[\zeta_p]$. We now turn to our particular $k$ containing $\mu_{q+1}$ (and containing $\mathbb{F}_{q^4}$ if $p$ is odd) and its extension $K/k$ of degree $N$ which is 1 (mod $p$). The first key point is that $p|(N-1)$ implies for all $y \in k$ that

$$\mathrm{Tr}_{K/k}(y) = Ny = y. \tag{7.1.4.1}$$

Thus every element $x \in K$ can be written uniquely in the form

$$x = y + z, \text{ with } y \in k,\ z \in K, \text{ and } \mathrm{Tr}_{K/k}(z) = 0. \tag{7.1.4.2}$$

Indeed, taking $y := \mathrm{Tr}_{K/k}(x) \in k$ and $z := x - y$, we have

$$\mathrm{Tr}_{K/k}(z) = \mathrm{Tr}_{K/k}(x) - \mathrm{Tr}_{K/k}(y) = 0,$$

giving such a writing. The writing is unique because $k \cap \mathrm{Ker}(\mathrm{Tr}_{K/k}) = \{0\}$.

Having fixed $(s_1, \ldots, s_n, t) \in k^\times \times k^n$, let us write

$$f(x) := \sum_{i=1}^{n} s_i x^{q^{a_i}+1} + tx.$$

Then, given (7.1.4.2), we readily compute

$$\begin{aligned} f(y+z) &= \sum_{i=1}^{n} s_i (y+z)^{q^{a_i}+1} + t(y+z) \\ &= t(y+z) + \sum_{i=1}^{n} s_i (y+z)(y^{q^{a_i}} + z^{q^{a_i}}) \\ &= f(y) + f(z) + \sum_{i=1}^{n} s_i (y z^{q^{a_i}} + y^{q^{a_i}} z). \end{aligned}$$

The second key point is that because $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ is abelian, $\mathrm{Ker}(\mathrm{Tr}_{K/k})$ is mapped to itself by any power of $\mathsf{Frob}_{\mathbb{F}_p}$. Therefore not only $z$ but each $z^{q^{a_i}}$ lies in $\mathrm{Ker}(\mathrm{Tr}_{K/k})$. By definition, $\psi_K = \psi_k \circ \mathrm{Tr}_{K/k}$, and hence

(7.1.4.3) $\psi_K\big(f(y+z)\big) = \psi_K\big(f(y) + f(z) + \text{elements with } \mathrm{Tr}_{K/k} = 0\big) = \psi_K\big(f(y) + f(z)\big).$

The clearing factor $\sqrt{\#k}$ is a power of $\pm q$ if $p = 2$, and a power of $q^2$ if $p$ is odd. As $N$ is odd for $p = 2$, the two clearing factors $\sqrt{\#k}$ and $\sqrt{\#k}^N$ are congruent to each other modulo $q+1$. For $p$ odd, each of the clearing factors is a power of $q^2$, so each is 1 modulo $q+1$. Thus it suffices to show the asserted congruence for the $\sum_x \psi$ sums without their clearing factors.

By (7.1.4.3), we have

$$\sum_{x\in K} \psi_K(f(x)) = \sum_{y\in k,\ z\in \mathrm{Ker}(\mathrm{Tr}_{K/k})} \psi_K(f(y)+f(z)) = \big(\sum_{y\in k} \psi_K(f(y))\big)\big(\sum_{z\in \mathrm{Ker}(\mathrm{Tr}_{K/k})} \psi_K(f(z))\big).$$

The first factor is

$$\sum_{y\in k} \psi_K(f(y)) = \sum_{y\in k} \psi_k(f(y)),$$

simply because $f(y)$ lies in $k$, so is its own $\mathrm{Tr}_{K/k}$, see (7.1.4.1). We write the second factor as

$$1 + \sum_{0\neq z\in \mathrm{Ker}(\mathrm{Tr}_{K/k})} \psi_K(f(z)).$$

So it suffices to show that

$$\Sigma := \sum_{0\neq z\in \mathrm{Ker}(\mathrm{Tr}_{K/k})} \psi_K(f(z)) \equiv 0 \ (\mathrm{mod}\ (q+1)\mathbb{Z}[\zeta_p]).$$

Because $k^\times$ contains $\mu_{q+1}$, the set $S := \mathrm{Ker}(\mathrm{Tr}_{K/k}) \smallsetminus \{0\}$ is stable by homothety by $\mu_{q+1}$. So if we pick a set of representatives $z_i \in S$ of the quotient space $S/\mu_{q+1}$, then

$$\sum_{0\neq z\in \mathrm{Ker}(\mathrm{Tr}_{K/k})} \psi_K(f(z)) = \sum_i \sum_{\zeta\in\mu_{q+1}} \psi_K(f(\zeta z_i)).$$

If we write $f(x) = g(x) + tx$ with $g(x) := \sum_{i=1}^n s_i x^{q^{a_i}+1}$, then $g(x)$ is a polynomial in $x^{q+1}$ (because the $a_i$ are odd). Hence $f(\zeta z_i) = g(z_i) + \zeta t z_i$, and our sum $\Sigma$ becomes

$$\sum_i \psi_K(g(z_i))\big(\sum_{\zeta\in\mu_{q+1}} \psi_K(\zeta t z_i)\big).$$

By the choice of $z_i$, $\mathrm{Tr}_{K/k}(\zeta t z_i) = 0$ for all $\zeta \in \mu_{q+1}$. Hence the inner sum is

$$\sum_{\zeta\in\mu_{q+1}} \psi_K(\zeta t z_i) = \sum_{\zeta\in\mu_{q+1}} \psi_k\big(\mathrm{Tr}_{K/k}(\zeta t z_i)\big) = \sum_{\zeta\in\mu_{q+1}} \psi_k(0) = q+1,$$

completing the proof. □

Corollary 7.1.5. *Hypotheses and notations as in Theorem 7.1.4 above, suppose $F_{(s,t),k} \in G_{\mathrm{arith}}$ is an element of order prime to $p$. Then every power $(F_{(s,t),k})^d$ of $F_{(s,t),k}$ has*

$$\mathrm{Trace}((F_{(s,t),k})^d) \equiv -1 \pmod{(q+1)\mathbb{Z}[\zeta_p]}.$$

Proof. If $(F_{(s,t),k})^M = \mathrm{Id}$ with $M$ prime to $p$, then after replacing $M$ by $N := M^{p-1}$, we have $(F_{(s,t),k})^N = \mathrm{Id}$ with $N \equiv 1 \pmod{p}$. Then

$$\mathrm{Trace}((F_{(s,t),k})^N) = \mathrm{Trace}(\mathrm{Id}) = q^{a_1} \equiv (-1)^{a_1} = -1(\mathrm{mod}\ (q+1)\mathbb{Z}[\zeta_p]).$$

So by Theorem 7.1.4, applied with $N$, we get $\mathrm{Trace}((F_{(s,t),k})) \equiv -1 \ (\mathrm{mod}(q+1)\mathbb{Z}[\zeta_p])$. But each power $(F_{(s,t),k})^d$ also has trivial $N^{\mathrm{th}}$ power, so this same argument gives the asserted congruence. □

## 7.2. Linear groups in characteristic $p > 2$

Let $p$ be a prime. Recall that an *extraspecial $p$-group* is any finite $p$-group $E$ such that $\mathbf{Z}(E) = [E,E] = \Phi(E)$ is cyclic of order $p$. Any such group has order $p^{1+2N}$ for some $N \in \mathbb{Z}_{\geq 1}$, in which case it has $p-1$ faithful, irreducible irreducible representations of degree $p^N$. For such a group $E$, the following statement is extracted from [**GT1**, Lemma 2.4] and its proof.

Lemma 7.2.1. *Let $p$ be a prime and let $E$ an extraspecial $p$-subgroup of order $p^{1+2N}$. Suppose $X$ is a finite group with a normal subgroup $R = \mathbf{Z}(R)E$. Suppose that $\psi$ is an irreducible complex character of $X$ of degree $p^N$ such that $\psi|_R \in \mathrm{Irr}(R)$. Then for any $g \in X$, $|\psi(g)|^2 = |\mathbf{C}_{R/\mathbf{Z}(R)}(g)|$ if $g$ acts trivially on the complete inverse image of $\mathbf{C}_{R/\mathbf{Z}(R)}(g)$ in $R$, and $\psi(g) = 0$ otherwise. In fact, for any $g \in X$, the coset $gR$ contains at least $p$ elements $h$ with $|\psi(h)|^2 = |\mathbf{C}_{R/\mathbf{Z}(R)}(g)|$.*

In the rest of this section, we fix an **odd** prime $p$ and prove some recognition results for finite subgroups of $\mathrm{GL}_{p^N}(\mathbb{C})$. We will consider the extraspecial $p$-group $E = p_+^{1+2N}$ with exponent $p$, embedded in $\mathrm{GL}_{p^N}(\mathbb{C})$ via one of its faithful irreducible representation $V = \mathbb{C}^{p^N}$ of degree $p^N$. It is well known, see e.g. [**Gr**], that this embedding extends to a larger group that induce all automorphisms of $E$ which are trivial on $\mathbf{Z}(E) \cong C_p$, and in fact

$$\Gamma(p,N) := \mathbf{N}_{\mathrm{GL}(V)}(E) = \mathbf{Z}(\mathrm{GL}(V))E \rtimes \mathrm{Sp}_{2N}(p),\ \Gamma(p,N)^{(\infty)} = E \rtimes \mathrm{Sp}_{2N}(p).$$

For any divisor $e$ of $N$, we have a standard subgroup $\mathrm{Sp}_{2N/e}(p^e) \rtimes C_e$ of $\mathrm{Sp}_{2N}(p)$, obtained by base change the natural module $\mathbb{F}_p^{2N}$ to $\mathbb{F}_{p^e}^{2N/e}$, see [**KT2**, §4].

Theorem 7.2.2. *Let $q = p^f$ be a power of a prime $p > 2$, $n \in \mathbb{Z}_{\geq 1}$, $N := nf$, and let $q^n \geq 11$. Let $G < \mathrm{GL}(V) \cong \mathrm{GL}_{p^N}(\mathbb{C})$ be a finite irreducible subgroup that contains a subgroup $G_1 \cong \mathrm{Sp}_{2n}(q)$. Then there exist an irreducible subgroup $E \cong p_+^{1+2N} < \mathrm{GL}(V)$,* *a divisor $e$ of $f$, a divisor $d$ of $e$, and a standard subgroup $L := \mathrm{Sp}_{2N/e}(p^e) \rtimes C_d$ inside $\mathrm{Sp}_{2N/e}(p^e) \rtimes C_e \leq \mathrm{Sp}_{2N}(p)$ such that*

$$G^{(\infty)} = E \rtimes \mathrm{Sp}_{2N/e}(p^e), \text{ and } \mathbf{Z}(\mathrm{GL}(V))G = \mathbf{Z}(\mathrm{GL}(V))(E \rtimes L).$$

*More precisely, any element in $G$ can be written as $\alpha h$ with $\alpha \in \mathbb{C}^\times$ a root of unity and $h \in E \rtimes L$, and vice versa, any element in $E \rtimes L$ can be written as $\beta g$ with $\beta \in \mathbb{C}^\times$ a root of unity and $g \in G$.*

PROOF. (i) By assumption, $G \geq G_1$ acts irreducibly on $V = \mathbb{C}^{p^N}$. Next, by [**TZ1**, Theorem 1.1], any nontrivial projective representation of $\mathrm{PSp}_{2n}(q)$ has degree at least $(p^N - 1)/2$. We also observe that $G_1$ cannot be irreducible on $V$. Indeed, if $n \geq 2$, then since $q^n \geq 11$, [**TZ1**, Theorem 5.2] implies that $G_1$ has no irreducible $\mathbb{C}$-representation of degree $q^n$. If $n = 1$ (and so $q \geq 11$), then the only irreducible $\mathbb{C}$-representation of $G_1 = \mathrm{SL}_2(q)$ of degree $q$ is the Steinberg representation, which is however trivial on $\mathbf{Z}(G_1) = \langle \boldsymbol{j} \rangle C_2$, and this contradicts the faithfulness of $G_1$ on $V$. Hence, the $G_1$-module $V$ is reducible, and each of its irreducible summands has dimension 1 or at least $(p^N - 1)/2$.

We also recall the fact that the smallest index $P(G_1)$ of proper subgroups of $G_1$ is at least $q^n = p^N$ (with equality only when $q^n = 11$), see [**KlL**, Table 5.2.A].

(ii) Suppose that $G$ fixes an imprimitive decomposition $V = \oplus_{i=1}^m V_i$ with $m > 1$. If $m < P(G_1)$, then $G_1$ has to fix each of the $V_i$'s. On the other hand, $\dim(V_i)$ is a proper divisor of $\dim(V) = p^N$, whence $\dim(V_i) \leq p^{N-1} < (p^N - 1)/2$. Given the shape described in (i) of the $G_1$-module $V$, this can happen only when $\dim(V_i) = 1$, which implies that $G_1$ acts trivially on $V$, a contradiction. Thus $m \geq P(G_1)$, and by (i) this is possible only when $q^n = 11$ and $\dim(V_i) = 1$. We have also shown that $G_1 = \mathrm{SL}_2(11)$ permutes the 11 subspaces $V_i$ transitively. Let $G_{11}$ denote the stabilizer of $V_1$ in $G_1$. According to [**CCNPW**], $G_{11}$ is a subgroup of type $2 \cdot \mathsf{A}_5$ in $G_1$. In fact, since $G_1$ has only one involution, namely the central involution $\boldsymbol{j}$, we must have that $G_{11} \cong \mathrm{SL}_2(5)$. Now the action of the perfect group $G_{11}$ on the 1-dimensional space $V_1$ must be trivial; in particular $\boldsymbol{j}$ acts trivially on $V_1$. As $G_1$ permutes the $V_i$'s transitively and $\boldsymbol{j} \in \mathbf{Z}(G_1)$, $\boldsymbol{j}$ acts trivially on every $V_i$ and so on $V$, contradicting the faithfulness.

We have shown that $G$ acts primitively on $V$. Suppose $G$ fixes a tensor decomposition $V = A \otimes_{\mathbb{C}} B$, that is, $G \leq \mathrm{GL}(A) \otimes \mathrm{GL}(B)$, with $1 < \dim(A), \dim(B)$. This induces projective representations of $G_1$ on $A$ and $B$, which have dimensions at most $p^N/3 < (p^N - 1)/2$. By (i), this is possible only when these projective representations are trivial, that is, $G_1$ acts via scalars on $A$ and on $B$. This implies that $G_1$ acts via scalars on $V$, whence this action is trivial since $G_1$ is perfect, again contradiction.

Assume now that $G$ fixes a tensor induced decomposition $V = U^{\otimes m}$ for some $m > 1$. Then $\dim(U) > 1$ is a power of $p$, whence $m \leq N < p^N = q^n \leq P(G_1)$. This shows that the action of $G_1$ on the $m$ tensor factors is trivial, and so $G_1$ fixes a tensor decomposition $V = U_1 \otimes U_2 \otimes \ldots \otimes U_m$ with $\dim(U_i) = \dim(U)$. But this is impossible by the preceding case.

(iii) We have shown that the finite group $G$ satisfies condition (**S**) of [**GT3**] and so can apply [**GT3**, Proposition 2.8] to conclude that either

(a) $G$ is almost quasisimple with $G^{(\infty)}$ acting irreducibly on $V$, or

(b) $E \lhd G < \mathbf{N}_{\mathrm{GL}(V)}(E)$ for some extraspecial $p$-group $E$ of order $p^{1+2N}$ acting irreducibly on $V$.

Here we consider the second possibility (b). First we note that

$$G_1 \cap \mathbf{Z}(\mathrm{GL}(V))E = 1. \tag{7.2.2.1}$$

Indeed, the quasisimple group $G_1$ normalizes the nilpotent subgroup $X := G_1 \cap \mathbf{Z}(\mathrm{GL}(V))E$, hence $X = 1$ or $X = \mathbf{Z}(G_1) = \langle \boldsymbol{j} \rangle$. In the latter case, if $\boldsymbol{j} \notin \mathbf{Z}(\mathrm{GL}(V))$, then it is a scalar multiple of a non-central element in $E$, whence it has trace 0 on $V$. On the other hand, the involution $\boldsymbol{j}$ has only eigenvalues 1 and $-1$ on $V = \mathbb{C}^{p^N}$ of odd dimension, and so its trace must be nonzero, a contradiction. So $\boldsymbol{j} \in \mathbf{Z}(\mathrm{GL}(V))$, whence it acts as scalar $-1$ and so has determinant $-1$ on $V$. This is again a contradiction, as $G_1$ is perfect and so lies in $\mathrm{SL}(V)$.

Next, we consider the conjugation action of $G_1$ on $E$. The kernel of this action is $G_1 \cap \mathbf{Z}(\mathrm{GL}(V)) = 1$ by (7.2.2.1), so the action embeds $G_1$ in the group $\mathrm{Aut}_1(E)$ of all automorphisms of $E$ that act trivially on $\mathbf{Z}(E)$, which is equal to $\mathbb{F}_p^{2N} \rtimes \mathrm{Sp}_{2N}(p)$ if $\exp(E) = p$ and $\mathbb{F}_p^{2N} \rtimes (p_+^{2N-1} \rtimes \mathrm{Sp}_{2N-2}(p))$ if $\exp(E) > p$, see [**Wi**, Theorem 1]. Now, if $N = 1$ then $|G_1| = |\mathrm{Sp}_{2N}(p)|$. If $N > 1$, using [**Zs**], we can find a primitive prime divisor $\ell = \mathrm{ppd}(p, 2N)$ of $p^{2N} - 1$ which then divides $|G_1|$. In either case, $G_1$ cannot embed in the subgroup $\mathbb{F}_p^{2N} \rtimes (p_+^{2N-1} \rtimes \mathrm{Sp}_{2N-2}(p))$ of $\mathrm{Aut}_1(E)$. This implies that $\exp(E) = p$, i.e. $E \cong p_+^{1+2N}$.

(iv) We have shown that $E \lhd G$ in the possibility (b). Now, if $f = 1$, then, by (7.2.2.1), $G_1 \cong \mathrm{Sp}_{2N}(p)$ embeds in $G/\mathbf{Z}(G)E \hookrightarrow \Gamma(p, N)/\mathbf{Z}(\mathrm{GL}(V))E \cong \mathrm{Sp}_{2N}(p)$, and so $\mathbf{Z}(\mathrm{GL}(V))G = \Gamma(p, N)$. In this case,

$$G \geq G^{(\infty)} = (\mathbf{Z}(\mathrm{GL}(V))G)^{(\infty)} = \Gamma(p, N)^{(\infty)} = E \rtimes \mathrm{Sp}_{2N}(p).$$

The statements now follow; indeed, if $X$ and $Y$ are two finite subgroups of $\mathrm{GL}(V)$ that agree modulo $\mathbf{Z}(\mathrm{GL}(V))$, then any element $x$ in $X$ can be written as $\alpha y$ with $\alpha \in \mathbb{C}^\times$ and $y \in Y$; taking determinants we see that $\alpha$ is a root of unity.

Consider the remaining case $f > 1$ and write $\Gamma(p, N) = E\Delta$, where $\Delta := \mathbf{Z}(\mathrm{GL}(V))\mathrm{Sp}_{2n}(p)$. [Here, we have chosen a fixed conjugate of $\mathrm{Sp}_{2n}(p)$ in $\Gamma(p, N)$, equivalently, a fixed central involution of $\mathrm{Sp}_{2n}(p)$.] As $G \geq E$, we can also write $G = EH$, and $G_1 \hookrightarrow H := G \cap \Delta$ by (7.2.2.1). Without loss, we will identify $G_1$ with a subgroup of $H$. Recall that $\mathrm{Sp}_{2n}(p)$ acts on $V$ with two irreducible summands $V_\epsilon$ of dimension $(p^N - \epsilon)/2$, $\epsilon = \pm$, each affording an irreducible Weil character with values in $\mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p})$ and having trivial determinant.

Assume now that $H^{(\infty)} \geq G_1$ acts reducibly on the summand $V_\epsilon$ of **even** dimension. Recall that any irreducible $\mathbb{C}$-representation of $\mathrm{Sp}_{2n}(q)$ has dimension at least $(q^n - 1)/2 = (p^N - 1)/2$ by [**TZ1**, Theorem 1.1]. First suppose that $p^N \equiv 3 (\mathrm{mod}\ 4)$. Then $V_+$ has odd dimension $(p^N - 1)/2 = (q^n - 1)/2$ and so the central involution $\boldsymbol{j}$ of $G_1$ acts trivially on $V_+$. As $G_1 \leq H^{(\infty)}$ acts reducibly on $V_-$, each of it irreducible summands on $V_-$ has dimension 1 or $(q^n - 1)/2$, which is always odd and so forces $\boldsymbol{j}$ to act trivially on all of them, i.e. $\boldsymbol{j}$ acts trivially on $V$, a contradiction. In the other case $p^N \equiv 1 (\mathrm{mod}\ 4)$, by assumption each irreducible $G_1$-summand on $V_+$ has dimension 1, so $\boldsymbol{j}$ acts trivially on $V_+$. If $G_1$ acts irreducibly on $V_-$ which now has odd dimension $(q^n + 1)/2$, then $\boldsymbol{j}$ acts trivially on it as well, a contradiction. Hence $G_1$ acts reducibly on $V_-$, and so $V_-$ splits off as a trivial module $V_0$, on which $\boldsymbol{j}$ is trivial, and another submodule $V'$ of dimension $(q^n - 1)/2$ on which $\boldsymbol{j}$ acts nontrivially. It follows that $V'$ is irreducible over $G_1$, and thus $\boldsymbol{j}$ acts as $-1$ on $V'$ and 1 on

$V_0$ and on $V_+$. On the other hand, the central involution $\boldsymbol{j}'$ of $\mathrm{Sp}_{2N}(p)$ acts as $-1$ on $V_+$ and $1$ on $V_- = V_0 \oplus V'$. Thus the involution $\boldsymbol{jj}'$ of $\Delta$ has trace $2 - p^N$ on $V$, and this contradicts Lemma 7.2.1 (applied to $E \rtimes \langle \boldsymbol{jj}' \rangle$).

We have shown that $H^{(\infty)} \leq \mathrm{Sp}_{2N}(p)$ acts irreducibly at least on the even-dimension summand $V_\epsilon$, and so the same holds for $H$; also, $\mathrm{Sp}_{2N}(p)$ acts faithfully on $V_\epsilon$. Now, applying Theorems 4.1 and 4.2 of [**KT2**] to the faithful action of $H^{(\infty)} \geq \mathrm{Sp}_{2n}(q)$ on $V_\epsilon$ we conclude that $H^{(\infty)}$ is a standard subgroup $\mathrm{Sp}_{2N/e}(p^e)$ for some divisor $e$ of $f$. Furthermore, $H \leq \Delta$ acting on $H^{(\infty)}$ can induce only a subgroup of

$$\mathbf{N}_{\mathrm{Sp}_{2N}(p)}(\mathrm{Sp}_{2N/e}(p^e)) = \mathrm{Sp}_{2N/e}(p^e) \rtimes C_e.$$

It follows that we can find a standard subgroup $L := \mathrm{Sp}_{2N/e}(p^e) \rtimes C_d$ inside $\mathrm{Sp}_{2N/e}(p^e) \rtimes C_e$, for some $d|e$, such that $\mathbf{Z}(\mathrm{GL}(V))H = \mathbf{Z}(\mathrm{GL}(V))L$. As $G = EH$, the statement follows.

(v) Now we handle the possibility (a), and recall that $L := G^{(\infty)}$ acts irreducibly on $V$. As $G$ is almost quasisimple, $L$ is a cover of a simple group $S$; furthermore, $L \geq G_1 = \mathrm{Sp}_{2n}(q)$ as $G_1$ is perfect.

First we consider the case $S = \mathsf{A}_m$ for some $m \geq 5$. Then $m \geq P(G_1) \geq q^n \geq 11$. Since $\dim(V) = p^N$, we can apply [**BBOO**, Theorem 2.4] to deduce that $m = p^N + 1$ and $L = \mathsf{A}_m$; in particular, $P(G_1) \leq q^n + 1$. This in turn implies by [**KlL**, Table 5.2.A] that $n = 1$. According to [**BHR**, Table 8.1], $G_1 = \mathrm{Sp}_2(q)$ has only conjugacy class of proper subgroups of index $\leq q + 1$, and any such subgroup contains the central involution $\boldsymbol{j}$. Thus $G_1$ cannot embed in $L = \mathsf{A}_m$, a contradiction.

From now on we may assume $S \neq \mathsf{A}_m$, and apply [**MZ**, Theorem 1.1]. We will rule out the arising possibilities case-by-case.

- $L = S$ is a simple group of Lie type in characteristic $p$, and $V|_L$ is the Steinberg representation. In this case $q^n = \dim(V)$ is the order of a Sylow $p$-subgroup $P$ of $S \geq G_1$. On the other hand, a Sylow $p$-subgroup of $G_1 = \mathrm{Sp}_{2n}(q)$ has order $q^{n^2}$, hence $n = 1$, and $P$ is elementary abelian of order $q$. As $S$ is of Lie type in characteristic $p$, this can happen only when $S$ is of (untwisted) Lie rank 1 and thus $S = \mathrm{PSL}_2(q)$. But then $G_1 = \mathrm{Sp}_2(q)$ cannot embed in $L = S$, a contradiction.
- $L$ is a cover of $\mathrm{PSL}_2(r)$ for some prime power $r$, and $q^n = \dim(V) \in \{r \pm 1, (r \pm 1)/2\}$. As $q^n \geq 11$, $L$ is a quotient of $\mathrm{SL}_2(r)$, and so $L$ admits a faithful irreducible representation of degree 2 or 3 over $\mathbb{F}_r$. But this contradicts the Landazuri-Seitz-Zalesskii bound [**KlL**, Table 5.3.A]

$$\mathfrak{d}(\mathrm{PSp}_{2n}(q)) \geq (q^n - 1)/2 \qquad (7.2.2.2)$$

for the smallest degree $\mathfrak{d}(\mathrm{PSp}_{2n}(q))$ of nontrivial projective representations of $\mathrm{PSp}_{2n}(q)$ over fields of characteristic $\neq p$.

- $(S, \dim(V))$ is $(\mathrm{PSL}_m(r), (r^m - 1)/(r - 1))$ or $(\mathrm{PSU}_m(r), (r^m + 1)/(r + 1))$ with $2 \nmid m > 2$, or $(\mathrm{PSp}_m(r), (r^{m/2} \pm 1)/2)$ with $2|m \geq 4$, and $r$ a prime power. In any of these cases, $S$ has a faithful projective representation of degree $m$ over $\overline{\mathbb{F}_r}$, hence $m \geq (q^n - 1)/2 \geq 5$ by (7.2.2.2). If $q^n > 13$, then this forces $\dim(V) \geq 2m + 2 \geq p^N + 1$, a contradiction. When $11 \leq q^n \leq 13$, the only possible cases are $(L, q^n) = (\mathrm{SU}_5(2), 11)$ or $(\mathrm{PSp}_6(3), 13)$, which are then ruled out for the reason that $G_1 = \mathrm{SL}_2(q)$ cannot embed in $L$ by [**CCNPW**].

- Either $\dim(V) = 11$ and $L = M_{11}, M_{12}$, or $\dim(V) = 23$ and $L = M_{24}, \mathsf{Co}_2, \mathsf{Co}_3$. By [**CCNPW**], $G_1 = \mathrm{SL}_2(11)$ cannot embed in $L$, a contradiction.
- $\dim(V) = 27$, and $L = \mathrm{Sp}_6(2)$, $3\cdot\Omega_7(3)$, $3\cdot G_2(3)$, ${}^2F_4(2)'$. By [**CCNPW**], $G_1 \geq \mathrm{SL}_2(27)$ cannot embed in $L$, a contradiction.
- Either $\dim(V) = 3^6$ and $L = 3\cdot\mathrm{PSU}_4(3), 3\cdot G_2(3)$, or $(\dim(V) = 3^9, 3\cdot\Omega_7(3))$. By [**CCNPW**], $G_1 \geq \mathrm{SL}_2(q^n)$ cannot embed in $L$, again a contradiction. □

## 7.3. Local systems in characteristic $p > 2$

Definition 7.3.1. Given any prime $p \geq 2$, any integers $A > B > 0$ coprime to $p$, a finite extension $k/\mathbb{F}_p$, and a character $\chi$ of $k^\times$, we denote by $\mathcal{F}(A, B, \chi)$ the arithmetically semisimple local system on $\mathbb{A}^1/k$ whose trace function is given as follows: for $L/k$ a finite extension and $s \in L$,

$$\mathrm{Trace}(\mathsf{Frob}_{s,L}|\mathcal{F}(A, B, \chi)) = -\sum_{x\in L}\psi_L(x^A + sx^B)\chi_L(x).$$

Its constant field twist by $(-\mathsf{Gauss}_k)^{-\deg/k}$ is denoted $\mathcal{G}(A, B, \chi)$:

$$\mathrm{Trace}(\mathsf{Frob}_{s,L}|\mathcal{G}(A, B, \chi)) = \frac{1}{\mathsf{Gauss}(\psi_L, \chi_2)}\sum_{x\in L}\psi_L(x^A + sx^B)\chi_L(x).$$

When $\gcd(A, B)$ is not explicitly assumed to be 1, these local systems will be denoted

$$\mathcal{F}_{nngcd}(A, B, \chi) \text{ and } \mathcal{G}_{nngcd}(A, B, \chi),$$

the subscript *nngcd* standing for ”not necessarily gcd = 1”.

Fix a prime $p > 2$ and $N \in \mathbb{Z}_{\geq 1}$. In this section, when $N \geq 2$ we will work with the local system

$$\mathcal{G}^{r,s,t} = \mathcal{G}(p^N + 1, p + 1, 2, 1, \mathbb{1}) \tag{7.3.1.1}$$

on $\mathbb{A}^3/\mathbb{F}_p$ whose trace function is given as follows: for $k/\mathbb{F}_p$ a finite extension, and $(r, s, t) \in k^3$,

$$(r, s, t) \mapsto \frac{1}{\mathsf{Gauss}(\psi_k, \chi_2)}\sum_{x\in k}\psi_k\big(x^{p^N+1} + rx^{p+1} + sx^2 + tx\big).$$

The notation $\mathcal{G}^{r,s,t}$ is included for convenience in working with various specializations. In particular, the specialization $r = t = 0$ is just $\mathcal{G}_{nngcd}(p^N + 1, 2, \mathbb{1})$:

$$\mathcal{G}^{0,s,0} = \mathcal{G}_{nngcd}(p^N + 1, 2, \mathbb{1}).$$

For completeness, for $N = 1$ we consider the local system

$$\mathcal{G}^{s,t} = \mathcal{G}(p + 1, 2, 1, \mathbb{1}) \tag{7.3.1.2}$$

on $\mathbb{A}^2/\mathbb{F}_p$ whose trace function is given as follows: for $k/\mathbb{F}_p$ a finite extension, and $(s, t) \in k^2$,

$$(s, t) \mapsto \frac{1}{\mathsf{Gauss}(\psi_k, \chi_2)}\sum_{x\in k}\psi_k\big(x^{p+1} + sx^2 + tx\big).$$

First we need some preliminary results.

Lemma 7.3.2. *Let $q \geq 5$ be a power of an odd prime $p$. Then the local system $\mathcal{G}_{nngcd}(q + 1, 2, \mathbb{1})$ in characteristic $p$ has $G_{\mathrm{geom}} = \mathrm{Sp}_2(q)$ in a total Weil representation.*

Proof. This system is the direct sum of the two systems, $\mathcal{G}_{\rm odd}$ with geometric monodromy group $\mathrm{PSp}_2(q)$, and $\mathcal{G}_{\rm even}$ with geometric monodromy group $\mathrm{Sp}_2(q)$, in respective irreducible constituents $\mathcal{W}_1$ and $\mathcal{W}_2$ of a total Weil representation $\mathcal{W}$ of degree $q$ of $\mathrm{Sp}_2(q)$, see [**KT1**, Theorem 17.2]. By Lemma 2.2.5, $G_{\rm geom}$ is a subgroup of $\mathrm{Sp}_2(q) \times \mathrm{PSp}_2(q)$ that maps onto each of the factors. Since $2 \nmid q > 3$, $\mathrm{Sp}_2(q)$ is quasisimple, with center $C_2$. So, by Goursat's lemma, $G_{\rm geom}$ is either $\mathrm{PSp}_2(q) \times \mathrm{Sp}_2(q)$ acting on $\mathcal{W}_1 \oplus \mathcal{W}_2$, or $G_{\rm geom} = \mathrm{Sp}_2(q)$ acting in a total Weil representation. In the former case, by Burnside's theorem we can find an element $g = (g_1, g_2)$ of $G_{\rm geom}$, with $g_1 \in \mathrm{PSp}_2(q)$ having trace 0 on $\mathcal{W}_1$ and $g_2 \in \mathrm{Sp}_2(q)$ having trace 0 on $\mathcal{W}_2$, whence $g$ has trace 0 in the underlying representation for $\mathcal{F}_{nngcd}(q+1, 2, \mathbb{1})$. However the squared absolute value of the trace of any element in $G_{\rm geom}$ is a power of $q$ by [**KT6**, Theorem 2.8(i)]. Hence we are in the latter case, and the statement follows. □

Lemma 7.3.3. *The local system $\mathcal{G}_{nngcd}(4, 2, \mathbb{1})$ in characteristic 3 has $G_{\rm geom} = \mathrm{Sp}_2(3)$ in a total Weil representation, with the convention that both the linear characters of order 3 are to be considered "Weil representations" of $\mathrm{Sp}_2(3) = 2^{1+2}_{-} \rtimes 3$.*

Proof. Its trace function is

$$t \in k/\mathbb{F}_3 \mapsto \frac{1}{\mathsf{Gauss}_k} \sum_{x \in k} \psi_k(x^4 + tx^2).$$

This is the direct sum of two local systems $\mathcal{G}(2, 1, \mathbb{1}) \oplus \mathcal{G}(2, 1, \chi_2)$, whose trace functions are respectively

$$t \in k/\mathbb{F}_3 \mapsto \frac{1}{\mathsf{Gauss}_k} \sum_{x \in k} \psi_k(x^2 + tx),\ t \in k/\mathbb{F}_3 \mapsto \frac{1}{\mathsf{Gauss}_k} \sum_{x \in k} \psi_k(x^2 + tx)\chi_2(x).$$

It is visible that for the first of these, namely $\mathcal{G}(2, 1, \mathbb{1})$, we have $G_{\rm geom,1} = G_{\rm arith,1} = \mu_3$. For the second, namely $\mathcal{G}(2, 1, \chi_2)$, it was proven in the first paragraph of the proof of Theorem 10.2.7 that $G_{\rm geom,2} = G_{\rm arith,2} = \mathrm{SL}_2(3) \cong \mathrm{Sp}_2(3)$. Thus $G_{\rm geom}$ of $\mathcal{G}_{nngcd}(4, 2, \mathbb{1})$ is a subgroup of $\mathrm{Sp}_2(3) \times \mu_3$ which maps onto each factor. Since it maps onto $\mathrm{Sp}_2(3)$, its order is divisible by $|\mathrm{Sp}_2(3)| = 24$, but as a subgroup of the product its order divides $3 \times 24 = 72$. So either the order is 24, and $G_{\rm geom}$ is $\mathrm{Sp}_2(3)$ in a total Weil representation, or its order is 72.

We now appeal to a Magma calculation, which shows that for $\mathcal{G}_{nngcd}(4, 2, \mathbb{1})$, over both $\mathbb{F}_{3^3}$ and $\mathbb{F}_{3^4}$ there are Frobenii with trace 3. So by Lemma 2.5.1, we conclude that for $\mathcal{G}_{nngcd}(4, 2, \mathbb{1})$, we have $G_{\rm geom} = G_{\rm arith}$. We now invoke Lemma 2.5.4, applied to $\mathcal{G}_{nngcd}(4, 2, \mathbb{1})$. Each of its two summands has $\mathsf{Swan}_\infty = 2$, so we may take $S_\infty = 2$ in that lemma. Then we have the inequality, for each finite extension $\mathbb{F}_q/\mathbb{F}_3$,

$$\left| \frac{\#\{x \in \mathbb{F}_q | \mathrm{Trace}(\mathsf{Frob}_{x,\mathbb{F}_q} | \mathcal{G}_{nngcd}(4, 2, \mathbb{1})) = 3\}}{q} - \frac{1}{|G_{\rm geom}|} \right| \le \frac{1}{\sqrt{q}}.$$

According to another Magma calculation, over $\mathbb{F}_{3^9}$ there are 820 Frobenii with trace 3. Thus

$$|820/3^9 - 1/|G_{\rm geom}|| \le 1/140.296,$$

hence

$$820/3^9 - 1/140.296 \le 1/|G_{\rm geom}| \le 820/3^9 + 1/140.296,$$

which is to say

$$0.0245 \le 1/|G_{\rm geom}| \le 0.0488,$$

which gives

$$20.49 \leq |G_{\mathrm{geom}}| \leq 40.82,$$

Since the only possible orders of $G_{\mathrm{geom}}$ are 24 or 72, we conclude that $|G_{\mathrm{geom}}| = 24$, and hence $G_{\mathrm{geom}} = \mathrm{Sp}_2(3)$ as asserted. □

THEOREM 7.3.4. *Suppose $p^N \geq 11$. If $N \geq 2$, then the geometric monodromy group $G^{r,s,t}_{\mathrm{geom}}$ of the local system $\mathcal{G}^{r,s,t}$ defined in* (7.3.1.1) *is isomorphic to the group*

$$\Gamma(p,N)^{(\infty)} = p_+^{1+2N} \rtimes \mathrm{Sp}_{2N}(p).$$

*When $N = 1$, the geometric monodromy group $G^{s,t}_{\mathrm{geom}}$ of the local system $\mathcal{G}^{s,t}$ defined in* (7.3.1.2) *is isomorphic to the group*

$$\Gamma(p,1)^{(\infty)} = p_+^{1+2} \rtimes \mathrm{Sp}_2(p).$$

PROOF. We can choose $k$ to contain $\mathbb{F}_{p^2}$, so that any element of $\mathbb{F}_p^\times$ is a square in $k$. In this case, $\mathsf{Gauss}(\psi_k, \chi_2) = \mathsf{Gauss}((\psi_a)_k, \chi_2)$ for any $\psi_a : t \mapsto \psi(at)$ with $a \in \mathbb{F}_p^\times$. First assume that $N \geq 2$. Then $\mathcal{G}^{r,s,0}$ is the local system $\mathcal{W}_{2\text{-param}}(\psi, N, p)$ introduced in [**KT3**, §4] when $2 \nmid N$ and in [**KT3**, §9] when $2|N$. Hence $\mathcal{G}^{r,s,0}$ has geometric monodromy group $G^{r,s,0}_{\mathrm{geom}} = L := \mathrm{Sp}_{2N}(p)$ by Theorem 4.3 and Theorem 10.3 of [**KT3**]. Similarly, when $2|N$, $\mathcal{G}^{r,0,0}$ has geometric monodromy group $G^{r,0,0}_{\mathrm{geom}} = L$ by [**KT3**, Theorem 10.6]. On the other hand, $\mathcal{G}^{0,0,t}$ is the Fourier transform of the lisse rank one sheaf $\mathcal{L}_{\psi(x^{1+p^N})}$, so is geometrically irreducible, hence its geometric monodromy group $G^{0,0,t}_{\mathrm{geom}}$ is irreducible and finite by Theorem 7.1.1. It follows that $G := G^{r,s,t}_{\mathrm{geom}}$ is a finite irreducible subgroup of $\mathrm{GL}_{p^N}(\mathbb{C})$ that contains $L = \mathrm{Sp}_{2N}(p)$.

Next we show that when $N = 1$, $G^{s,t}_{\mathrm{geom}}$ is also an irreducible subgroup of $\mathrm{GL}_p(\mathbb{C})$ that contains $L := \mathrm{Sp}_2(p)$. First, the irreducibility is established by the same argument as above, but applied to $\mathcal{G}^{0,t}$. Next, $\mathcal{G}^{s,0}$ is the direct sum of two irreducible local systems of rank $(p-\epsilon)/2$ and $(p+\epsilon)/2$, with $p \equiv \epsilon (\mathrm{mod}\ 4)$, which were shown in [**KT1**, Theorem 17.2] to have geometric monodromy groups $\mathrm{SL}_2(p)$, respectively $\mathrm{PSL}_2(p)$, when $p \geq 5$. Now the à la Goursat proof of [**KT2**, Proposition 6.6] can be repeated verbatim, see Lemma 7.3.2, to show that the geometric monodromy group $L$ of $\mathcal{G}^{s,0}$ is isomorphic to $\mathrm{SL}_2(p)$, again provided that $p \geq 5$. The same statement holds for $p = 3$, see Lemma 7.3.3.

In the rest of the proof, slightly abusing the notation, we use $\mathcal{G}^{r,s,t}$ and $G = G^{r,s,t}_{\mathrm{geom}}$ to denote $\mathcal{G}^{s,t}$ and $G^{s,t}_{\mathrm{geom}}$ when $N = 1$. By Theorem 7.1.1, $G$ is finite. Applying Theorem 7.2.2, we deduce that

$$G = \mathbf{Z}(G)\Gamma(p,N)^{(\infty)} \leq \Gamma(p,N).$$

Furthermore, the trace function takes values only in $\mathbb{Q}(\zeta_p)$. Hence $\mathbf{Z}(G) \geq \mathbf{Z}(E) \cong C_p$ can contain only scalars $\alpha \cdot \mathrm{Id}$, where $E = \mathbf{O}_p(\Gamma(p,N)^{(\infty)}) = p_+^{1+2N}$ and $\alpha \in \mathbb{Q}(\zeta_p)$ is a root of unity; in particular, $\alpha^{2p} = 1$ and $|\mathbf{Z}(G)|$ divides $2p$. Now, if $\mathbf{Z}(G) > \mathbf{Z}(E)$, then $\mathbf{Z}(G) = C_{2p}$ contains $-1 \cdot \mathrm{Id}$, and so $G \cong C_2 \times \Gamma(p,N)^{(\infty)}$ would have $C_2$ quotient, which is impossible since $H^1(\mathbb{A}^n/\overline{\mathbb{F}_p}, \mu_d) = 0$ if $p \nmid d$. It follows that $\mathbf{Z}(G) = \mathbf{Z}(E)$, and the statement is proved. □

Next we prove a full generalization of Theorem 7.3.4:

THEOREM 7.3.5. *Let $q = p^f$ be a power of an odd prime $p$, $n, l \in \mathbb{Z}_{\geq 1}$, and $q^n \geq 11$. Consider any sequence*

$$n > m_1 > m_2 > \ldots > m_l \geq 0$$

*with $l \geq 1$, $2|nm_1 \ldots m_l$, and $\gcd(n, m_1, \ldots, m_l) = 1$, and the local system*

$$\mathcal{G}^{s_1,\ldots,s_l,t} = \mathcal{G}(q^n + 1, q^{m_1} + 1, \ldots, q^{m_l} + 1, 1, \mathbb{1})$$

*on $\mathbb{A}^{l+1}/\mathbb{F}_p$ whose trace function is given as follows: for $k/\mathbb{F}_p$ a finite extension, and $(s_1, \ldots, s_l, t) \in k^{l+1}$,*

$$(s_1, \ldots, s_l, t) \mapsto \frac{1}{\mathsf{Gauss}(\psi_k, \chi_2)} \sum_{x \in k} \psi_k\big(x^{q^n+1} + s_1 x^{q^{m_1}+1} + \ldots + s_l q^{q^{m_l}+1} + tx\big).$$

(a) *Then the geometric monodromy group $G_{\mathrm{geom}}$ of $\mathcal{G}^{s_1,\ldots,s_l,t}$ is a standard subgroup $p_+^{1+2N} \rtimes \mathrm{Sp}_{2n}(q)$ of $\Gamma(p, N)^{(\infty)} = p_+^{1+2N} \rtimes \mathrm{Sp}_{2N}(p)$, where $N := nf$.*

(b) *For any $k$ a finite extension of $\mathbb{F}_p$, there exists a scalar subgroup $C_{\mathrm{arith},k}$ of order at most 2 such that the arithmetic monodromy group $G_{\mathrm{arith},k}$ of $\mathcal{G}^{s_1,\ldots,s_l,t}$ over $k$ is $C_{\mathrm{arith},k} \times G_{\mathrm{geom}}$ if $k \supseteq \mathbb{F}_q$, and $(C_{\mathrm{arith},k} \times G_{\mathrm{geom}}) \cdot \mathrm{Gal}(\mathbb{F}_q/k)$ if $k \subseteq \mathbb{F}_q$.*

PROOF. (i) First we aim to show that $G_{\mathrm{geom}}$ contains a subgroup isomorphic to $\mathrm{Sp}_{2N}(q)$ (acting on $\mathcal{G}^{s_1,\ldots,s_l,t}$ via a total Weil representation). When $N = 1$, $\mathcal{G}^{s_1,\ldots,s_l,t}$ is the system $\mathcal{G}^{s_1,t}$ considered in Theorem 7.3.4, hence $G_{\mathrm{geom}} = \Gamma(p, N)^{(\infty)}$. So we will assume $N > 1$. As explained in the proof of Theorem 7.3.4, specializing $s_1 = \ldots = s_l = 0$, we see that $G_{\mathrm{geom}}$ is a finite irreducible subgroup of $\mathrm{GL}_{p^N}(\mathbb{C})$. Furthermore, while working over extensions of $\mathbb{F}_{q^2}$, it does not matter what choice of Gauss sums is taken, and moreover

$$|\varphi(g)|^2 \text{ is either zero or a } q\text{-power} \tag{7.3.5.1}$$

by Theorem 7.1.2(a), if $\varphi(g)$ denotes the trace of any $g \in G_{\mathrm{geom}}$ (or even for any $g \in G_{\mathrm{arith},\mathbb{F}_q}$).

Consider the case where there exists an index $j$ such that $m := m_j$ is coprime to $n$ and $2|mn$. Then the system $\mathcal{G}^{s_1,\ldots,s_l,t}$, where all $s_i$ with $i \neq j$ and also $t$ are specialized to be 0, is the local system $\mathcal{W}(\psi, n, m, q)$ on $\mathbb{A}^1/\mathbb{F}_p$ defined in [**KT6**, (9.0.4)], whose geometric monodromy group is shown in [**KT6**, Theorem 9.2] to contain $\mathrm{Sp}_{2n}(q)$, as stated. (As shown in Theorem 7.3.11, the assumption $m < n/2$ in Theorems 9.2 and 10.2 of [**KT6**] is redundant.) In particular, we are done if $l = 1$. If $n = 2$ but $l > 1$, then $(m_1, m_2) = (1, 0)$ and so we are also done by taking $m := m_1$. So we may assume that $l > 1$ and $n \geq 3$. We may also assume that

$$(m_1, m_2) \neq (1, 0) \text{ when } (f, l) = (1, 2), \tag{7.3.5.2}$$

since the case $(f, l, m_1, m_2) = (1, 2, 1, 0)$ is precisely the one considered in Theorem 7.3.4.

(ii) For any $1 \leq j \leq l$, write $d_j := \gcd(n, m_j)$, so that $\gcd(n/d_j, m_j/d_j) = 1$. By assumption, $(q^{d_j})^{n/d_j} = q^n = p^N \geq 11$; also, if $m_j > 0$ then $d_j \leq n/2$ as $m_j < n$.

First suppose $2|(nm_j/d_j^2)$ for a given $j$. Then the system $\mathcal{G}^{s_1,\ldots,s_l,t}$, where all $s_i$ with $i \neq j$ and also $t$ are specialized to be 0, is the local system $\mathcal{W}(\psi, n/d_j, m_j/d_j, q^{d_j})$ on $\mathbb{A}^1/\mathbb{F}_p$ defined in [**KT6**, (9.0.4)], whose geometric monodromy group is shown in [**KT6**, Theorem 9.2] to contain $\mathrm{Sp}_{2n/d_j}(q^{d_j})$.

We also note that $2|(nm_{i_0}/d_{i_0}^2)$ for at least one $i_0$. (Indeed, assume $2 \nmid (nm_j/d_j^2)$ for all $j$. If $2|n$, then since $2 \nmid (n/d_j)$, we have that $2|d_j$ and so $2|m_j$ for all $j$ and thus

$2|\gcd(n,m_1,\ldots,m_l)$, a contradiction. So $2\nmid n$, forcing $2\nmid d_j$, and so, as $2\nmid(m_j/d_j)$, we have $2\nmid m_j$ for all $j$ and thus $2\nmid nm_1\ldots m_l$, again a contradiction.) As we explained above, this implies that $G_{\rm geom}$ contains $\mathrm{Sp}_{2n/d_{i_0}}(q^{d_{i_0}})$. By Theorem 7.2.2, modulo $\mathbf{Z}(\mathrm{GL}(V))$ the subgroup $G_{\rm geom}$ is $E\rtimes L$, with $E=p_+^{1+2N}$ and $\mathrm{Sp}_{2N/e'}(p^{e'})\lhd L\leq\mathrm{Sp}_{2N/e'}(p^{e'})\rtimes C_{e'}$ for some $e'|d_{i_0}f$, and $V$ is the underlying representation. Since $\mathrm{Sp}_{2N/e'}(p^{e'})$ is a standard subgroup of $\mathrm{Sp}_{2N}(p)$ acting in a total Weil representation, $|\varphi(h)|^2=p^{e'}$ for some $h\in\mathrm{Sp}_{2N/e'}(p^{e'})$ by [**KT3**, Theorem 3.5]. It follows from (7.3.5.1) that $e'=ef$ for some $e|d_{i_0}$.

If $e=1$, then we have $\mathrm{Sp}_{2n}(q)\hookrightarrow G_{\rm geom}$ as desired. So we will assume $e>1$. This argument also shows that

$$e|d_j \text{ whenever } 2|(nm_j/d_j^2). \tag{7.3.5.3}$$

Next we show that we may also assume that

$$e|d_j \text{ whenever } 2\nmid(nm_j/d_j^2). \tag{7.3.5.4}$$

Consider any such $j$; in particular $d_j\leq n/3$ (since $m_j\geq 1$). Then over $\mathbb{F}_{q^{2d_j}}$ the system $\mathcal{G}^{s_1,\ldots,s_l,t}$, where all $s_i$ with $i\neq j$ and also $t$ are specialized to be 0, is the pullback by the map $s_j\mapsto -s_j$ of the local system $\mathcal{W}^{n/d_j,m_j/d_j}$ defined in [**KT6**, §10], whose geometric monodromy group is shown in [**KT6**, Theorem 10.2] to contain $\mathrm{SU}_{n/d_j}(q^{d_j})$ (acting in the total Weil representation) and hence contains a maximal torus of order

$$(q^{d_j})^{n/d_j-1}-1=q^{n-d_j}-1=p^{f(n-d_j)}-1.$$

Note that $f(n-d_j)\geq 2N/3\geq 2$, with equality only when $(n,f)=(3,1)$ and $d_j=1$. In the latter case, by (7.3.5.2), we have $(f,l,m_1,m_2)\neq(1,2,1,0)$, so $m_{i'}=2$ for some $i'$ and we are done by (i). Hence we may assume that $f(n-d_j)\geq 3$, and so $p^{f(n-d_j)}-1$ admits a primitive prime divisor $\ell_j\geq f(n-d_j)+1\geq 2N/3+1$ by [**Zs**], and $G_{\rm geom}$ contains some non-scalar element $g_j$ of order $\ell_j$. As $g_j$ is non-scalar and of order coprime to $p$, $|g_j|=\ell_j$ divides $|L|$. We next note that $\ell_j$ in fact divides $|\mathrm{Sp}_{2n/e}(q^e)|$. (Indeed, if $\ell_j>2N/3$ divides $e'=ef$, then, as $e'|N$ we must have $\ell_j=e'=N$ is prime and so $d_j=1$, $e=e'$ (as $e>1$), and $f=1$. In this case, $\mathrm{PSU}_N(p)$ embeds in $\mathbf{Z}(\mathrm{GL}(V))EG_{\rm geom}/(\mathbf{Z}(\mathrm{GL}(V))E)\cong L\leq\mathrm{Sp}_2(p^N)\rtimes C_N$, which is impossible since $N\geq 3$.) It therefore follows that, there is some $1\leq c_j\leq n/e$ such that $\ell_j$ divides $q^{2ec_j}-1$. By the choice of $\ell_j$, we have that $(n-d_j)|2ec_j\leq 2n\leq 3(n-d_j)$. Hence,

$$\text{either } n-d_j=2ec_j,\text{ or } n-d_j=ec_j,\text{ or } 3n-3d_j=2ec_j=2n \text{ and } d_j=n/3=m_j.$$

Since $e|n$, (7.3.5.4) holds in the first two cases. So if $e\nmid d_j$, we must be in the third case. Then $\mathrm{PSU}_3(q^{n/3})$ embeds in $\mathbf{Z}(\mathrm{GL}(V))EG_{\rm geom}/(\mathbf{Z}(\mathrm{GL}(V))E)\cong L\leq\mathrm{Sp}_{2n/e}(q^e)\rtimes C_{e'}$. As mentioned above, a Sylow $\ell_j$-subgroup of $\mathrm{PSU}_3(q^{n/3})$ embeds in $\mathrm{Sp}_{2n/e}(q^e)$ for $\ell_j$ a primitive prime divisor of $p^{2N/3}-1=q^{2n/3}-1$, and this Sylow subgroup is non-cyclic. However, the Sylow $\ell_j$-subgroup of $C_{q^{2n}-1}$ is of course cyclic. So there exists another $1\leq c_j'<n/e=c_j$ such that $\ell_j$ divides $q^{2ec_j'}-1$. Using $e\nmid d_j$ and repeating the previous argument for $c_j'$ in place of $c_j$, we obtain that $3n-3d_j=2ec_j'=2n$ and thus $c_j'=n/e=c_j$, a contradiction.

We have therefore shown in (7.3.5.3) and (7.3.5.4) that $e|d_j$ for all $j$, and thus $e|m_j$ for all $j$. As $e>1$ and $e|n$, we get $\gcd(n,m_1,\ldots,m_l)>1$, a contradiction.

(iii) Thus $G_{\rm geom}$ contains $\mathrm{Sp}_{2n}(q)$. Again applying Theorem 7.2.2, we see that, modulo $\mathbf{Z}(\mathrm{GL}(V))$ the subgroup $G:=G_{\rm geom}$ is $E\rtimes L$, with $E=p_+^{1+2N}$ and $L=\mathrm{Sp}_{2N/c}(p^c)\rtimes C_d$ a standard subgroup of $\mathrm{Sp}_{2N}(p)$ for some $c|f$ and some $d|c$; moreover, $G^{(\infty)} = E \rtimes \mathrm{Sp}_{2N/c}(p^c)$. By [**KT3**, Theorem 3.5], $|\varphi(h')|^2 = p^{c/d}$ for some scalar multiple $h'$ of an element in $L$. It follows from (7.3.5.1) that $f$ divides $c/d$, and so $c = f$, $d = 1$ and thus $L = \mathrm{Sp}_{2n}(q) \le G^{(\infty)}$. It follows that $G = \mathbf{Z}(G)(E \rtimes L)$. Now, the same arguments as in the proof of Theorem 7.3.4 show that $G = E \rtimes L$.

The same arguments as in the proof of Theorem 7.3.4, but applied to $G_{\mathrm{arith},k}$, also show that $\mathbf{Z}(G_{\mathrm{arith},k}) = \mathbf{Z}(E) \times C_{\mathrm{arith},k}$ for some central scalar subgroup $C_{\mathrm{arith},k}$ of order $\le 2$, and moreover when $k \supseteq \mathbb{F}_q$ we have $G_{\mathrm{arith},k} = C_{\mathrm{arith},k} \times G_{\mathrm{geom}}$.

Consider the case $k = \mathbb{F}_{p^{f/r}} \subseteq \mathbb{F}_q$ for some $r|f$. We first observe that $\#k = q^{1/r}$ is attained as a value of $|\varphi(v)|^2$ for some $v \in G_{\mathrm{arith},k}$. One need simply take the image of Frobenius at the $k$-point $s_1 = -1$, other $s_i = 0$, $t = 0$, where the trace is

$$\frac{1}{\mathsf{Gauss}(\psi_k,\chi_2)}\sum_{x\in k}\psi_k\big(x^{q^n+1} - x^{q^{m_1}+1}\big) = \frac{1}{\mathsf{Gauss}(\psi_k,\chi_2)}\sum_{x\in k}\psi_k\big(x^2 - x^2\big) = \frac{\#k}{\mathsf{Gauss}(\psi_k,\chi_2)},$$

which indeed has the asserted square absolute value $\#k$, cf. the proof of Theorem 7.1.2. Together with Theorem 7.1.2(b), instead of (7.3.5.1) now we have that $|\varphi(v)|^2$ is 0 or a power of $q^{1/r}$, with $q^{1/r}$ attained. Using $H := G_{\mathrm{arith},k} \rhd G_{\mathrm{geom}}$ and applying Theorem 7.2.2, we have that

$$E \rtimes \mathrm{Sp}_{2n}(q) = G_{\mathrm{geom}} = H^{(\infty)},\ \mathbf{Z}(\mathrm{GL}(V))H = \mathbf{Z}(\mathrm{GL}(V))E \rtimes (\mathrm{Sp}_{2n}(q) \rtimes C_s)$$

for some $s|f$. Since $\mathrm{Sp}_{2n}(q) \rtimes C_s$ is a standard subgroup of $\mathrm{Sp}_{2ns}(q^{1/s}) \le \mathrm{Sp}_{2N}(p)$, by Lemma 7.2.1 applied to $E \rtimes \mathrm{Sp}_{2ns}(q^{1/s})$ we have that $|\varphi(g)|^2$ is either 0 or a power of $q^{1/s}$ for all $g \in G_{\mathrm{arith},k}$. As $q^{1/r}$ is attained, we have that $r|s$. On the other hand, [**KT3**, Theorem 3.5] shows that $|\varphi(u)|^2 = q^{1/s}$ for some $u \in \mathrm{Sp}_{2n}(q) \rtimes C_s$, showing $q^{1/s}$ is a power of $q^{1/r}$, i.e. $s|r$. We conclude that $s = r$, and the subgroup $C_s$ of field automorphisms of $\mathrm{Sp}_{2n}(q)$ can then be identified with $\mathrm{Gal}(\mathbb{F}_q/k)$, as stated. □

REMARK 7.3.6. In some cases, $C_{\mathrm{arith},k}$ in Theorem 7.3.5 can have order 2. For instance, if $2 \nmid n \ge 3$, $q = p \equiv 3(\mathrm{mod}\ 4)$, and $k \not\supseteq \mathbb{F}_{p^2}$, then $G_{\mathrm{arith},k}$ contains $-1 \cdot \mathrm{Id}$ by [**KT6**, Theorem 9.4(iii)], whence $C_{\mathrm{arith},k} \cong C_2$.

REMARK 7.3.7. In contrast to Theorems 7.3.4 and 7.3.5, it was shown in [**KT5**, Theorem 9.19] that the only **hypergeometric** sheaves $\mathcal{H}$ in odd prime-power dimension $r^n \ge 11$ that can have extraspecial normalizers as their geometric monodromy groups are the Pink-Sawin Kloosterman sheaves

$$\mathcal{H} = \mathcal{K}l(\mathsf{Char}(r^n + 1) \smallsetminus \{\mathbb{1}\})$$

in characteristic $p = r$, which has $G_{\mathrm{geom}} = r_+^{1+2n} \rtimes C_{r^n+1}$.

The situation when $r = 2$ is completely different, and will be addressed in the following chapters. We now improve some results of [**KT1**], [**KT3**, Theorem 5.2], and [**KT6**, Theorem 10.2] on arithmetic monodromy groups of local systems for $\mathrm{SU}_n(q)$ with $qn$ odd, as well as determine the arithmetic monodromy groups of the Pink-Sawin sheaves in any characteristic $p$.

We start with the Pink-Sawin sheaves:

THEOREM 7.3.8. *Let $q = p^f$ with $f \in \mathbb{Z}_{\geq 1}$, and consider the Pink-Sawin local system $\mathcal{G}$ on $\mathbb{A}^1/\mathbb{F}_p$ with trace function*

$$t \in k \mapsto \frac{-1}{\sqrt{\#k}} \sum_{x \in k} \psi_k(x^{q+1} + tx).$$

*Set $\kappa := 1$ if $p = 2$ and $\kappa := 2$ if $p > 2$. Then, over any finite extension $k$ of $\mathbb{F}_{q^{2\kappa}}$, $\mathcal{G}$ has arithmetic and geometric monodromy groups $G_{\mathrm{arith},k} = G_{\mathrm{geom}} = E$ where $E = p_+^{1+2f}$ is the extraspecial $p$-group of order $pq^2$ and exponent $p$ when $p > 2$, and $E = 2_-^{1+2f}$, the extraspecial 2-group of type $-$ and order $2q^2$ when $p = 2$. Over any subfield $k$ of $\mathbb{F}_{q^{2\kappa}}$, $\mathcal{G}$ has arithmetic monodromy group $G_{\mathrm{arith},k} = G_{\mathrm{geom}} \cdot \mathrm{Gal}(\mathbb{F}_{q^{2\kappa}}/k)$.*

PROOF. (i) Consider the images $h_i$ of $\mathsf{Frob}_{i,\mathbb{F}_p}$ for $i = 0, 1$ in $G := G_{\mathrm{arith},\mathbb{F}_p}$. First we show that

$$h_0^{2f} \neq \mathrm{Id} = h_0^{4f}. \tag{7.3.8.1}$$

Indeed, note that $\varphi(h_0^{2f}) = (-1/q) \sum_{x \in \mathbb{F}_{q^2}} \psi_{\mathbb{F}_{q^2}}(x^{q+1})$. Assume $p = 2$. Then for any $x \in \mathbb{F}_{q^2}$, we have $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(x^{q+1}) = x^{q+1} + x^{q^2+q} = 2x^{q+1} = 0$, so

$$\psi_{\mathbb{F}_{q^2}}(x^{q+1}) = \psi\big(\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_2}(x^{q+1})\big) = \psi\big(\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}\big(\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(x^{q+1})\big)\big) = \psi(0) = 1.$$

Hence $\varphi(h_0^{2f}) = -q$, yielding $h_0^{2f} = -\mathrm{Id}$ and $h_0^{4f} = \mathrm{Id}$.

Suppose $p > 2$. Then

$$\varphi(h_0^{2f}) = \frac{-1}{q} \sum_{x \in \mathbb{F}_{q^2}} \psi_{\mathbb{F}_{q^2}}(x^{q+1})) = \frac{-1}{q} \sum_{\mathbb{1} \neq \chi \in \mathrm{Char}(q+1)} \mathsf{Gauss}_{\mathbb{F}_{q^2}}(\psi, \chi).$$

By Stickelberger's theorem [**BEW**, 11.6.1], we have

$$\frac{1}{q}\mathsf{Gauss}_{\mathbb{F}_{q^2}}(\psi, \chi) = (-1)^{(q+1)/r} \text{ for } r \text{ the order of } \chi.$$

These signs are not all the same as $\chi$ varies: they are $-1$ when $r = q+1$, but are 1 if either $r$ is odd (always possible unless $q+1$ is a power of 2) or if $r = 2$ in this last case. So we have some cancellation, and hence $|\varphi(h_0^{2f})| < q$, i.e. $h_0^{2f} \neq \mathrm{Id}$, in fact,

$$h_0^{2f} \notin \mathbf{Z}(G). \tag{7.3.8.2}$$

On the other hand

$$\varphi(h_0^{4f}) = \frac{-1}{q^2} \sum_{x \in \mathbb{F}_{q^4}} \psi_{\mathbb{F}_{q^4}}(x^{q+1})) = \frac{-1}{q^2} \sum_{\mathbb{1} \neq \chi \in \mathrm{Char}(q+1)} \mathsf{Gauss}_{\mathbb{F}_{q^4}}(\psi, \chi).$$

But we have the identity

$$-\mathsf{Gauss}_{\mathbb{F}_{q^4}}(\psi, \chi) = (-\mathsf{Gauss}_{\mathbb{F}_{q^2}}(\psi, \chi))^2 = (\pm q)^2 = q^2,$$

and hence $\varphi(h_0^{4f}) = q$, i.e. $h_0^{4f} = \mathrm{Id}$, proving (7.3.8.1).

Now, for any divisor $j | 4f$ with $1 \leq j \leq 4f/3$,

$$|\varphi(h_0^j)| = \Big|\frac{-1}{p^{j/2}} \sum_{x \in \mathbb{F}_{p^j}} \psi_{\mathbb{F}_{p^j}}(x^{q+1})\Big| \leq p^{j/2} \leq p^{2f/3} < q,$$

showing $h_0^j \neq \mathrm{Id}$. Together with (7.3.8.1), this implies that

$$|h_0| = 4f. \tag{7.3.8.3}$$

(ii) Next we observe that $G := G_{\mathrm{geom}}$ is $G = 2_-^{1+2f}$ when $p = 2$ and $G = p_+^{1+2n}$ when $p > 2$. The case $p > 2$ is [**KT1**, Theorem 21.1]. Assume $p = 2$. Then $G$ is a 2-group and $G/\mathbf{Z}(G)$ is elementary abelian of order $q^2$ by [**KT1**, Corollary 20.3]; in particular, $\mathbf{Z}(G) \neq 1$. Next, $\mathcal{F}$ is of symplectic type [**Ka-MMP**, 3.10.1–3], implying $\mathbf{Z}(G) \cong C_2$. It follows that $\Phi(G) = [G, G] = \mathbf{Z}(G)$, and so $G$ is extraspecial. Finally, $\mathcal{F}$ being symplectic implies that $G \cong 2_-^{1+2f}$.

Now suppose that $k \supseteq \mathbb{F}_{q^{2\kappa}}$. Then the proofs of (7.3.8.1) and (7.3.8.3) shows that $h_0^{2\kappa f} \in E$. By [**KRLT4**, Lemma 4.1], $G_{\mathrm{arith}, \mathbb{F}_{p^{2\kappa f}}} = \langle E, h_0^{2\kappa f} \rangle = E$. It follows that $G_{\mathrm{geom}} = G_{\mathrm{arith},k}$.

We also show that

$$[G_{\mathrm{arith}, \mathbb{F}_{q^2}} : E] = 2 \text{ when } p > 2. \tag{7.3.8.4}$$

Indeed, (7.3.8.2) and (7.3.8.3) imply that $h_0^{2f}$ is a non-central involution, and there is no such element in $E$, so $G_{\mathrm{arith}, \mathbb{F}_{q^2}} > E = G_{\mathrm{arith}, \mathbb{F}_{q^4}}$.

(iii) By [**KRLT4**, Lemma 4.1] and the results of (ii), it suffices to show that $G/E \cong C_{2\kappa f}$, where $G = G_{\mathrm{arith}, \mathbb{F}_p}$ and $E = G_{\mathrm{arith}, \mathbb{F}_{q^{2\kappa}}}$. Denoting $m := |G/E|$, we have that $h_0^m \in E$. As $G/E \cong C_m$ embeds in $\mathrm{Gal}(\mathbb{F}_{q^{2\kappa f}}/\mathbb{F}_2) \cong C_{2\kappa f}$, we have that $m | 2\kappa f$.

Suppose that $p = 2$, so that $\kappa = 1$. Then any element in $E = 2_-^{1+2f}$ has order dividing 4. In particular, $h_0^{4m} = 1$. As $h_0$ has order $4f$ by (7.3.8.3), we must have that $f | m$. As $m | 2f$, we are done if $m > f$. Consider the remaining possibility $m = f$. In this case, $h_1^f \in E$, and so $|\varphi(h_1^f)| = 0$ or $q$. On the other hand, for any $x \in \mathbb{F}_q$, $x^{q+1} + x = x^2 + x$, and so $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(x^{q+1} + x) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(x^2 + x) = 0$, and thus $\psi_{\mathbb{F}_q}(x^{q+1} + x) = 1$. It follows that

$$\varphi(h_1^f) = \frac{-1}{q^{1/2}} \sum_{x \in \mathbb{F}_q} \psi_{\mathbb{F}_q}(x^{q+1} + x) = -q^{1/2},$$

a contradiction.

Assume now that $p > 2$, so that $\kappa = 2$. By (7.3.8.4), $E < G_{\mathrm{arith}, \mathbb{F}_{q^2}} = \langle E, h_0^{2f} \rangle$, whence $h_0^{2f} \notin E$ and $m \neq 2f$. To show that the divisor $m$ of $4f$ equals to $4f$, we must exclude the divisors of $4f/(2j-1)$ with $j \in \mathbb{Z}_{\geq 2}$. So assume that $h_0^{4f/(2j-1)} \in E$ for some $j \in \mathbb{Z}_{\geq 2}$ and set $r := p^{4f/(2j-1)} = s^4$ with $s := p^{f/(2j-1)}$. Then $r^j = p^{f+(2j-1)f/(2j+1)} = qs^{2j+1}$. Hence, for any $x \in \mathbb{F}_r$ we have

$$\psi_{\mathbb{F}_r}(x^{q+1}) = \psi\big(\mathrm{Tr}_{\mathbb{F}_r/\mathbb{F}_p}(x^{q+1}))\big) = \psi\big(\mathrm{Tr}_{\mathbb{F}_r/\mathbb{F}_p}\big(x^{(q+1)s^{2j+1}}\big)\big) = \psi\big(\mathrm{Tr}_{\mathbb{F}_r/\mathbb{F}_p}(x^{s^{2j+1}+1})\big) = \psi_{\mathbb{F}_r}(x^{s^{2j+1}+1}).$$

As $r = s^4$, applying Theorem 7.1.2(d) to $\sum_{x \in \mathbb{F}_r} \psi_{\mathbb{F}_r}(x^{s^{2j+1}+1})$, we see that $\varphi(h_0^{4f/(2j-1)}) \neq 0$, and so the element $h_0^{4f/(2j-1)} \in E$ must then belong to $\mathbf{Z}(E) \leq \mathbf{Z}(G)$. In such a case,

$$p^f = q = |\varphi(h_0^{4f/(2j-1)})| \leq r^{1/2} = p^{2f/(2j-1)},$$

i.e $2j - 1 \leq 2$, a contradiction as $j \geq 2$. □

LEMMA 7.3.9. *Let $q = p^f$ be any odd prime power, $n > m \geq 1$, $\gcd(n,m) = 1$, and $2 \nmid nm$. Consider the local system $\mathcal{G}$ on $\mathbb{A}^1/\mathbb{F}_q$ with trace function*

$$r \in k \mapsto \frac{1}{\mathsf{Gauss}(\psi_k, \chi_2)} \sum_{x \in k} \psi_k\big(x^{(q^n+1)/(q+1)} - rx^{(q^m+1)/(q+1)}\big)\chi_2(x)$$

*as introduced in* [**KT6**, §10]. *If $g$ denotes the image of $\mathsf{Frob}_{0,\mathbb{F}_q}$ in $G_{\mathrm{arith},\mathbb{F}_q}$, then $g^{2n} = \mathrm{Id}$ and $\mathrm{Trace}(g^n) = 1$. In fact, all odd powers of $g$ have $\mathrm{Trace} = 1$. If $(n,q) = (3,3)$ in addition, then $\mathrm{Trace}(g) = \mathrm{Trace}(g^2) = 1$.*

PROOF. For any integer $d \geq 1$, $g^d$ is the image of $\mathsf{Frob}_{0,\mathbb{F}_{q^d}}$ in $G_{\mathrm{arith},\mathbb{F}_q}$. Its trace is thus

$$\frac{1}{\mathsf{Gauss}(\psi_{\mathbb{F}_{q^d}}, \chi_2)} \sum_{x \in k} \psi_{\mathbb{F}_{q^d}}\big(x^{(q^n+1)/(q+1)}\big)\chi_2(x).$$

If $d$ is odd, we observe that the numerator is equal to the denominator, i.e. that as $x$ runs over $\mathbb{F}_{q^d}$, $x^{(q^n+1)/(q+1)}$ runs over $\mathbb{F}_{q^d}$, i.e. that

$$\gcd((q^n+1)/(q+1), q^d - 1) = 1.$$

To see this, compute it as

$$\gcd((q^n+1)/(q+1), q^n+1, q^d-1) = \gcd((q^n+1)/(q+1), \gcd(q^n+1, q^d-1)).$$

We first observe that $M := \gcd(q^n+1, q^d-1) = 2$. Indeed, it is obvious that 2 divides this $M$. In $\mathbb{Z}/M\mathbb{Z}$, we have $q^d = 1$, $q^n = -1$. Thus we have $q^{nd} = (-1)^d = -1$ (because $d$ is odd), and we also have $q^{nd} = (1)^n = 1$. Thus $1 = -1$ in $\mathbb{Z}/M\mathbb{Z}$, and hence $M$ divides 2. Thus $M = 2$. Thus $\gcd((q^n+1)/(q+1), q^d-1) = \gcd((q^n+1)/(q+1), 2) = 1$, the last equality because

$$(q^n+1)/(q+1) = 1 + q(q-1)(1 + q^2 + \ldots + q^{n-3})$$

is odd.

We next show that $g^{2n} = \mathrm{Id}$, or equivalently (because we are in a finite group) that $\mathrm{Trace}(g^{2n}) = (q^n+1)/(q+1)$. Once again, we examine the formula for this trace. It is

$$\frac{1}{\mathsf{Gauss}(\psi_{\mathbb{F}_{q^{2n}}}, \chi_2)} \sum_{x \in \mathbb{F}_{q^{2n}}} \psi_{\mathbb{F}_{q^{2n}}}\big(x^{(q^n+1)/(q+1)}\big)\chi_2(x).$$

Here we have

$$\gcd((q^n+1)/(q+1), q^{2n}-1) = ((q^n+1)/(q+1),$$

simply because $(q^n+1)/(q+1)$ divides $q^n+1$, which divides $q^{2n}-1$. Let us write

$$D := (q^n+1)/(q+1).$$

Because $D$ is odd, the numerator of the formula for $\mathrm{Trace}(g^{2n})$ is

$$\begin{aligned}\sum_{x\in\mathbb{F}_{q^{2n}}}\psi_{\mathbb{F}_{q^{2n}}}(x^D)\chi_2(x) &= \sum_{x\in\mathbb{F}_{q^{2n}}}\psi_{\mathbb{F}_{q^{2n}}}(x^D)\chi_2(x^D)\\ &= \sum_{u\in\mathbb{F}_{q^{2n}}^\times}\psi_{\mathbb{F}_{q^{2n}}}(u)\chi_2(u)(\#\{x\in\mathbb{F}_{q^D}, x^D=u\})\\ &= \sum_{u\in\mathbb{F}_{q^{2n}}^\times}\psi_{\mathbb{F}_{q^{2n}}}(u)\chi_2(u)\sum_{\rho\in\mathrm{char}(D)}\rho(u)\\ &= \sum_{\rho\in\mathrm{char}(D)}\mathsf{Gauss}(\psi_{\mathbb{F}_{q^{2n}}},\chi_2\rho).\end{aligned}$$

We now apply Stickelberger's theorem [**BEW**, 11.6.1], that for $Q$ a power of $p$ and $\Lambda$ a nontrivial character of order $m$ dividing $Q+1$, we have the identity

$$\mathsf{Gauss}(\psi_{\mathbb{F}_{Q^2}},\Lambda) = (-1)^{(Q+1)/m}Q.$$

We apply this with $Q := q^n$, and each of the characters $\chi_2\rho$. Each has order dividing $2D$, so dividing $q^n+1$, each is nontrivial because each $\rho$ has odd order, and the order of each is 2×odd. Thus the numerator is simply $(-1)^{(q^n+1)/2}Dq^n$, while the denominator is, again by Stickelberger, $(-1)^{(q^n+1)/2}q^n$.

The final assertion, that $\mathrm{Trace}(\mathsf{Frob}^2_{0,\mathbb{F}_3}) = 1$ when $q = n = 3$, holds because $\gcd(\frac{3^3+1}{3+1}, 3^2-1) = \gcd(7,8) = 1$. □

LEMMA 7.3.10. *Let $q = p^f$ be any odd prime power, $n > m \geq 1$, $\gcd(n,m) = 1$, and $2\nmid nm$. Consider the local system $\mathcal{W}^{n,m}$ on $\mathbb{A}^1/\mathbb{F}_p$ with trace function*

$$r\in k\mapsto \frac{1}{\mathsf{Gauss}(\psi_k,\chi_2)}\sum_{x\in k}\psi_k\big(x^{q^n+1}-rx^{q^m+1}\big),$$

*and its two summands $\mathcal{W}^{n,m,j(q+1)/2}$, $j\in\{0,1\}$, with trace functions*

$$r\in k\mapsto \frac{1}{\mathsf{Gauss}(\psi_k,\chi_2)}\sum_{x\in k}\psi_k\big(x^{(q^n+1)/(q+1)}-rx^{(q^m+1)/(q+1)}\big)\chi_2^j(x),$$

*as introduced in* [**KT6**, §10]. *Then we have the following results.*

(a) *For any subfield $k$ of $\mathbb{F}_q$, and any $a\in k$, $|\mathrm{Trace}(\mathsf{Frob}_{a,k}|\mathcal{W}^{n,m})|^2$ is a power of $\#k$.*
(b) *For any subfield $k$ of $\mathbb{F}_q$, $|\mathrm{Trace}(\mathsf{Frob}_{1,k}|\mathcal{W}^{n,m})|^2 = \#k$.*
(c) *For any subfield $k$ of $\mathbb{F}_q$, $|\mathrm{Trace}(\mathsf{Frob}_{1,k}|\mathcal{W}^{n,m,0})|^2 = \#k$ and $\mathrm{Trace}(\mathsf{Frob}_{1,k}|\mathcal{W}^{n,m,(q+1)/2}) = 0$.*

PROOF. The first statement was proven in Theorem 7.1.2. For the second, notice that for $k$ a subfield of $\mathbb{F}_q$ and $x\in k$, the summand $x^{q^n+1}-x^{q^m+1} = x^2-x^2$ vanishes, so the trace is just $\#k/\mathsf{Gauss}(\psi_k,\chi_2)$, which indeed has square absolute value $\#k$ as asserted. For the third, again notice that for $k$ a subfield of $\mathbb{F}_q$ and $x\in k$, the summand $x^{(q^n+1)/(q+1)}-x^{(q^m+1)/(q+1)} = x-x$ vanishes, so the first trace is $\#k/\mathsf{Gauss}(\psi_k,\chi_2)$, which has square absolute value $\#k$ as asserted, and the second trace is a multiple of $\sum_{x\in k}\chi_2(x) = 0$. □

More generally, we can consider the system $\mathcal{W}^{n,m}$, introduced in [**KT6**] for any two coprime integers $n > m$, which is also denoted by $\mathcal{F}_{nngcd}(q^n+1, q^m+1, \mathbb{1})$, see Definition 7.3.1.

THEOREM 7.3.11. *Let $p > 2$ be a prime, $q = p^f$, $n > m \geq 1$ be any two coprime integers, and let $q^n > 9$. Then Theorems 9.2–9.4 of* [**KT6**] *hold when $2|mn$, and Theorems 10.2, 10.3, and 10.5 of* [**KT6**] *hold when $2 \nmid nm$. In particular, the geometric monodromy group of*

$$\mathcal{W}^{n,m} = \mathcal{F}_{nngcd}(q^n+1, q^m+1, \mathbb{1})$$

*is*

(i) $\mathrm{Sp}_{2n}(q)$ *in its total Weil representation of degree $q^n$, if $2|nm$; and*
(ii) $\mathrm{SU}_n(q)$ *in its total Weil representation of degree $q^n$, if $2 \nmid nm$.*

PROOF. We first note that the treatment of unitary groups in [**KT6**, §10] does *not* need the assumption $m < n/2$ made in [**KT6**, (10.0.1)], and hence its main results Theorems 10.2, 10.3, and 10.5 all hold, implying our statement, whenever $2 \nmid nm$.

We next turn our attention to the case $2|nm$ and first show that Theorem 9.1 of [**KT6**] holds for $(n,m)$. The only place where the condition $m < n/2$ made in [**KT6**, (9.0.1)] was needed is to show that the parameter $d$ in [**KT6**, (9.1.5)] is 1 in the case $n \geq 4$, in part (iii) of the proof of [**KT6**, Theorem 9.1]. We now prove that the same conclusion holds if $2 \leq n/2 < m$. In the notation of that proof, consider a $p'$-generator $h$ of the image of $I(\delta)$ modulo the image of $P(\delta)$, and note that its spectrum on the tame part of $\mathcal{H}(n,m,\epsilon)$ with $\epsilon = \pm$ is a scalar multiple of $\mu_B$ or $\mu_B \smallsetminus \{1\}$, with $B := (q^m+1)/2$. Since $m \geq 3$, we have $B \geq 14$ and the central order of $h$ is divisible by $B$. Also, by [**Zs**], we can find a primitive prime divisor $\ell$ of $p^{2mf}-1$, which then divides $B$. Letting $h_0$ be the $\ell$-part of $h$, we have that $\ell|\bar{\mathsf{o}}(h_0)$ and $\ell \geq 2mf+1$.

Recall that the parameter $d$ in [**KT6**, (9.0.1)] satisfies $d|n$, and a scalar multiple of $h_0$ belongs to $\mathrm{Sp}_{2n/d}(q^d) \rtimes C_{df}$. Since $\ell > 2mf > nf \geq df$, in fact we have that $h_0 \in \mathrm{Sp}_{2n/d}(q^d)$. Hence there exists an integer $i$, $1 \leq i \leq n/d$, such that $\ell|(q^{2di}-1)$. By the primitivity of $\ell$, $2mf$ divides $2dif$, and so $mf$ divides $dif$, which is at most $d(n/d)f = nf < 2mf$. It follows that $dif = mf$ and thus $d$ divides both $m$ and $n$. Since $\gcd(m,n) = 1$ by hypothesis, we conclude that $d = 1$. Thus Theorem 9.1 of [**KT6**] holds for $(n,m)$.

The proofs of Theorems 9.2–9.4 of [**KT6**] rely only on Theorem 9.1 of [**KT6**] and again do *not* use the assumption $m < n/2$ made in [**KT6**, (9.0.1)]. □

LEMMA 7.3.12. *Let $q = p^f$ be an odd prime power, $2 \nmid n \geq 3$, and let $\theta$ denote the restriction $\zeta_{(q+1)/2,n}$ of the Weil character $\tilde{\zeta}_{(q+1)/2,n}$ of $\mathrm{GU}_n(q)$, as defined in* [**KT3**, (3.1.2)], *to $\mathrm{SU}_n(q)$. Let $G$ be a finite group containing $S = \mathrm{PSU}_n(q)$ as a normal subgroup of index $\leq 2$, and with an irreducible character $\varphi$ such that $\varphi|_S$ is equal to $\theta$ viewed as an $S$-character. Suppose that there exists an element $g \in G \smallsetminus S$ such that either*

(a) $(n,q) \neq (3,3)$, *$\varphi(g^n) = 1$ and $g^{2n} = \mathrm{Id}$, or*
(b) *$\varphi(g) = \varphi(g^2) = 1$, $g \notin S$, and $g^2$ is a $p$-element.*

*Then $G \cong S \rtimes \langle \tau \rangle \cong S \cdot 2$, where $\tau$ is the field automorphism of $S$ induced by the map $(x_{ij}) \mapsto (x_{ij}^q)$ on $\mathrm{SU}_n(q)$, and $g \notin S$.*

PROOF. Note that $\mathbf{Z}(\mathrm{SU}_n(q)) \cong C_{\gcd(n,q+1)}$ has odd order, so $\theta$ is trivial at $\mathbf{Z}(\mathrm{SU}_n(q))$ and so can indeed be viewed as an $H$-character.

First assume that either $\mathbf{C}_G(S) \neq 1$ or $g \in S$. Since $[G : H] \leq 2$, it follows in the former case that $\mathbf{C}_G(S) = \langle z \rangle \cong C_2$ and $G = \mathbf{C}_G(S) \times S$, where $z$ acts as the scalar $-1$ in a representation affording $\varphi$. In either case, we may write $g = z^j s$ with $s \in S$ and $j \in \{0, 1\}$.

In the case of (a) we have $(n, q) \neq (3, 3)$ and

$$\theta(s^n) = \varphi(z^j g^n) = (-1)^j = \pm 1. \tag{7.3.12.1}$$

In particular, $s^n \neq 1$, but $s^{2n} = g^{2n} = \mathrm{Id}$, so $|s^n| = 2$. We can therefore view $s^n$ as represented by

$$\mathrm{diag}\big(\underbrace{1, \ldots, 1}_{a}, \underbrace{-1, \ldots, -1}_{2b}\big)$$

in $\mathrm{SU}_n(q)$ with $a, b \in \mathbb{Z}_{\geq 1}$ and $a + 2b = n$. Using [**KT3**, (3.1.2)], we have that

$$\theta(s^n) = -\frac{((-q)^a - 1) + (-1)^{(q+1)^2/4}((-q)^{2b} - 1)}{q + 1} = \begin{cases} (q^a + q^{2b})/(q+1), & q \equiv 1(\mathrm{mod}\ 4), \\ -(q^{2b} - q^a - 2)/(q+1), & q \equiv 3(\mathrm{mod}\ 4). \end{cases}$$

Now, if $q \equiv 1(\mathrm{mod}\ 4)$, then $q | \theta(s^n)$, contradicting (7.3.12.1). Hence $q \equiv 3(\mathrm{mod}\ 4)$. If moreover $j = 0$, then $q^{2b} - q^a + q = 1$, again a contradiction. So $j = 1$ and $q^{2b} - q^a - 2 = q + 1$, whence $3 = q^{2b} - q^a - q$ is divisible by $q$ and so $q = 3$. Now $q + 3 = q^{2b} - q^a$ and $b \geq 1$, so comparing the 3-part we have that $a = 1$. Thus $2q + 3 = q^{2b}$, forcing $b = 1$ and $(n, q) = (3, 3)$, a contradiction.

In the case of (b), $j = 1$ as $g \notin S$, $g^2 = s^2$ is a $p$-element, and $\theta(s^2) = \varphi(g^2) = 1$. We will again view $s$ as an element in $\mathrm{SU}_n(q)$. Using [**KT3**, (3.1.2)], we have that

$$1 = \theta(s^2) = \frac{1 - (-q)^e}{q + 1}$$

where $e := \dim_{\mathbb{F}_{q^2}} \mathrm{Ker}(s^2 - 1)$. It follows that $e = 1$, i.e. $s^2$ is a regular unipotent element of $\mathrm{SU}_n(q)$. In particular, $\mathbf{C}_S(s^2)$ is a $p$-group, so $s \in \mathbf{C}_S(s^2)$ is also a $p$-element. Again using [**KT3**, (3.1.2)], we have that

$$1 = \varphi(g) = -\theta(s) = \frac{(-q)^{e'} - 1}{q + 1}$$

where $e' := \dim_{\mathbb{F}_{q^2}} \mathrm{Ker}(s - 1) \geq 1$. This is impossible, since $|(-q)^{e'} - 1| \geq q^2 - 1 > q + 1$ if $e' \geq 2$, and $((-q) - 1)/(q + 1) = -1$.

We have shown that $\mathbf{C}_G(S) = 1$ and $g \notin S$. Thus $G/S \cong C_2$, and it embeds in $\mathrm{Out}(S) = C_{\gcd(n,q+1)} \rtimes C_{2f}$. Since $2 \nmid n$, all subgroups of index 2 in $\mathrm{Out}(S)$ are conjugate to $\langle \tau \rangle$. It follows that $G$ is conjugate to $S \rtimes \langle \tau \rangle$ in $\mathrm{Aut}(S)$. □

PROPOSITION 7.3.13. *Let $q = p^f$ be any odd prime power, $n > m \geq 1$, $\gcd(n, m) = 1$, and $2 \nmid nm$. Consider the local system $\mathcal{W}^{(q+1)/2} := \mathcal{W}^{n,m,(q+1)/2}$ on $\mathbb{A}^1/\mathbb{F}_q$ with trace function*

$$r \in k \mapsto \frac{1}{\mathsf{Gauss}(\psi_k, \chi_2)} \sum_{x \in k} \psi_k\big(x^{(q^n+1)/(q+1)} - r x^{(q^m+1)/(q+1)}\big)\chi_2(x)$$

*as introduced in [**KT6**, §10]. Then the arithmetic monodromy group $G_{\mathrm{arith}, \mathbb{F}_q}$ of the system on $\mathbb{F}_q$ is isomorphic to $\mathrm{PSU}_n(q) \rtimes \langle \tau \rangle \cong \mathrm{PSU}_n(q) \cdot 2$, where $\tau$ is the field automorphism of $\mathrm{PSU}_n(q)$ induced by the map $(x_{ij}) \mapsto (x_{ij}^q)$ on $\mathrm{SU}_n(q)$.*

Proof. As shown in Theorem 7.3.11, Theorem 10.2 of [**KT6**] holds not only when $m < n/2$ but for any $m < n$; in particular, $\mathcal{W}^{(q+1)/2}$ has $G_{\mathrm{arith},\mathbb{F}_{q^4}} = G_{\mathrm{geom}} = S := \mathrm{PSU}_n(q)$, the image of $\mathrm{SU}_n(q)$ in the Weil representation with character $\zeta_{(q+1)/2,n}$. Moreover, if $m = 1$, then, as shown in [**KT3**, Theorem 5.2(b)], over $\mathbb{F}_{q^2}$ we have $G_{\mathrm{arith},\mathbb{F}_{q^2}} = S$ as well. Next, if $m = 1$ and $q \equiv 3 (\mathrm{mod}\ 4)$, then [**KT1**, Theorem 2.3(4)] shows that $\mathcal{W}^{(q+1)/2}$ has arithmetic determinant $(-1)^{\deg}$ over $\mathbb{F}_q$, and so $[G_{\mathrm{arith},\mathbb{F}_q} : S] = 2$.

For general $m < n$, [**KT6**, Theorem 10.2] shows that $S \lhd G_{\mathrm{arith},\mathbb{F}_{q^2}} \leq S \times \langle \boldsymbol{j} \rangle$ for some central involution $\boldsymbol{j}$ (which acts trivially on the Weil representation of $\mathrm{GU}_n(q)$ with character $\tilde{\chi}_2\tilde{\zeta}_{(q+1)/2,n}$). By [**KT6**, Corollary 5.8], over $\mathbb{F}_{q^2}$ the system $\mathcal{W}^{(q+1)/2}$ has trivial arithmetic determinant. Since $\mathcal{W}^{(q+1)/2}$ has odd rank, this implies that $\boldsymbol{j}$ acts trivially on $\mathcal{W}^{(q+1)/2}$ and thus $G_{\mathrm{arith},\mathbb{F}_{q^2}} = S$. In particular, $[G_{\mathrm{arith},\mathbb{F}_q} : S] \leq 2$.

Now we consider the element $g \in G_{\mathrm{arith},\mathbb{F}_q}$ constructed in Lemma 7.3.9. The above considerations imply that $g \notin S$ when $(n, q) = (3, 3)$. Applying Lemma 7.3.12, we conclude that $G_{\mathrm{arith},\mathbb{F}_q} \cong S \rtimes \langle \tau \rangle$. □

Theorem 7.3.14. *Let $q = p^f$ be any odd prime power, $n > m \geq 1$, $\gcd(n, m) = 1$, and $2 \nmid nm$. Consider the local system $\mathcal{W} := \mathcal{W}^{n,m}$ on $\mathbb{A}^1/\mathbb{F}_p$ with trace function*

$$r \in k \mapsto \frac{1}{\mathsf{Gauss}(\psi_k, \chi_2)} \sum_{x \in k} \psi_k\big(x^{q^n+1} - r x^{q^m+1}\big)$$

*as introduced in* [**KT6**, §10]. *Then, for any subfield $k \subseteq \mathbb{F}_{q^2}$, the arithmetic monodromy group $G_{\mathrm{arith},k}$ of the system on $k$ is isomorphic to $(C_2 \times \mathrm{SU}_n(q)) \cdot \mathrm{Gal}(\mathbb{F}_{q^2}/k)$, which induces the subgroup $\mathrm{PSU}_n(q) \rtimes \mathrm{Gal}(\mathbb{F}_{q^2}/k)$ of automorphisms of $\mathrm{SU}_n(q)$, and $C_2$ may be identified with the central subgroup of order $2$ of $\mathrm{GU}_n(q)$.*

Proof. (i) Consider $H := \mathrm{GU}_n(q)$, acting in its total Weil representation $\Phi = \oplus_{i=0}^{q} \Phi_i$ with character $\tilde{\zeta}_n$, see [**KT3**, Theorem 3.1], and let $\boldsymbol{z}$ denote a generator of $\mathbf{Z}(H)$, so that $\boldsymbol{z}$ acts as the scalar $\rho^i$ on $\Phi_i$ for some $(q+1)^{\mathrm{th}}$ root $\rho$ of unity. It is well known that $\Phi_{(q+1)/2}$ is orthogonal of dimension $D := (q^n + 1)/(q + 1)$, and $\Phi_0$ is symplectic of dimension $D - 1$, see [**KT3**, Lemma 3.2]. In fact, if $\sigma$ denotes the Galois automorphism $x \mapsto x^p$ of $\overline{\mathbb{F}_p}$, then we can embed $\mathrm{GU}_n(q) \rtimes \langle \sigma \rangle$ into $\mathrm{Sp}_{2n}(q) \rtimes \langle \sigma \rangle \leq \mathrm{Sp}_{2nf}(p)$, and extend $\Phi$ to a total Weil representation of $\mathrm{Sp}_{2nf}(p)$.

In the case $k = \mathbb{F}_{q^2}$, the statement also holds by [**KT6**, Theorem 10.2]: $G_{\mathrm{arith},\mathbb{F}_{q^2}} = C_2 \times L \leq H$, with $L := \mathrm{SU}_n(q)$ acting in its total Weil representation, and $C_2 = \langle \boldsymbol{j} \rangle = \langle \boldsymbol{z}^{(q+1)/2} \rangle$. Also recall [**KT6**, §10] that $\mathcal{W} = \oplus_{i=0}^{q} \mathcal{W}^i$, where $\mathcal{W}^i := \mathcal{W}^{n,m,i}$ is geometrically orthogonal of rank $D$ if and only if $i = (q+1)/2$, and $\mathcal{W}^i$ is geometrically symplectic of rank $D-1$ if and only if $i = 0$. It follows that $G_{\mathrm{arith},\mathbb{F}_{q^2}}$ and $L$ act on $\mathcal{W}^0$ via restrictions of $\Phi_0$, and on $\mathcal{W}^{(q+1)/2}$ via restrictions of $\Phi_{(q+1)/2}$. Moreover, since $L = [G_{\mathrm{arith},\mathbb{F}_{q^2}}, G_{\mathrm{arith},\mathbb{F}_{q^2}}] \lhd G_{\mathrm{arith},k}$, it follows from Clifford's theorem that $G_{\mathrm{arith},k}$ stabilizes each of $\mathcal{W}^0$ and $\mathcal{W}^{(q+1)/2}$ (but may permute the other subsheaves). Let $\Psi = \oplus_{i=0}^{q} \Psi^i$ denote the representation of $G := G_{\mathrm{arith},\mathbb{F}_p}$ on $\mathcal{W}$, with $\Psi^i$ denoting the resulting representation on $\mathcal{W}^i$. Then we have shown that $\Psi^i|_L = \Phi^i|_L$ for $i = 0$ and $i = (q+1)/2$.

(ii) Consider the case $k = \mathbb{F}_q$. Then $G_{\mathrm{arith},\mathbb{F}_q}$ contains $G_{\mathrm{arith},\mathbb{F}_{q^2}} = 2 \times L$ as a subgroup of index $\leq 2$. On the other hand, by Proposition 7.3.13, the arithmetic monodromy group

$\Psi^{(q+1)/2}(G_{\mathrm{arith},\mathbb{F}_q})$ of $\mathcal{W}^{(q+1)/2}$ is $\mathrm{PSU}_n(q) \rtimes \langle\tau\rangle$, and thus it contains $\Psi^{(q+1)/2}(2\times L) = \mathrm{PSU}_n(q)$ with index 2 (and induces the outer automorphism $\tau$ on the latter). It follows that $G_{\mathrm{arith},\mathbb{F}_q} = (2 \times L)\cdot\langle\tau\rangle$, and we can identify $\langle\tau\rangle$ with $\mathrm{Gal}(\mathbb{F}_{q^2}/k)$ in this case.

(iii) To prove the statement for any proper subfield $k$ of $\mathbb{F}_{q^2}$, it suffices to prove it for $k = \mathbb{F}_p$ (using the facts that $[G_{\mathrm{arith},k'} : G_{\mathrm{arith},\mathbb{F}_{q^2}}]$ divides $c = [\mathbb{F}_{q^2} : k']$, $[G_{\mathrm{arith},\mathbb{F}_p}] : G_{\mathrm{arith},k'}]$ divides $2f/c = [k' : \mathbb{F}_p]$ for any subfield $k' = \mathbb{F}_{p^{2f/c}}$ of $\mathbb{F}_{q^2}$, and that $\mathrm{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_p)$ is cyclic of order $2f$).

Let $g$ denote the image of $\mathsf{Frob}_{1,\mathbb{F}_p}$ in $G = G_{\mathrm{arith},\mathbb{F}_p}$. Then $g^f$ is the image of $\mathsf{Frob}_{1,\mathbb{F}_q}$ in $G$, and so it lies in $G_{\mathrm{arith},\mathbb{F}_q} = (2\times L)\cdot\langle\tau\rangle$, but not in its proper subgroup $G_{\mathrm{arith},\mathbb{F}_{q^2}}$. It follows that, modulo $\mathrm{Inn}(L) \cong S = \mathrm{PSU}_n(q)$, $g^f$ induces the outer automorphism $\tau$. Since $\mathrm{Inn}(L)$ is a normal subgroup of odd index $\gcd(n, q+1)$ in $\mathrm{Inndiag}(L) \cong \mathrm{PGU}_n(q)$, modulo $\mathrm{Inndiag}(L)$ the element $g^f$ still induces the involutive outer automorphism $\tau = \sigma^f$. Hence the order of $g$ in $\mathrm{Aut}(L)/\mathrm{Inndiag}(L) \cong \mathrm{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_p) \cong C_{2f}$ is some even integer $2f/j$ with $j|f$. In other words, we can find an element $h \in \mathrm{GU}_n(q) \rtimes \langle\sigma^j\rangle$ such that $g$ and $h$ induce the same action on $L$, and moreover $\langle g\rangle$, $\langle h\rangle$ and $\langle\sigma^j\rangle$ are all the same modulo $\mathrm{Inndiag}(L)$.

Recall that $\Phi|_L = \Psi|_L$ is a sum of pairwise inequivalent Weil representations. It follows that

$$\Phi(h)\Phi(x)\Phi(h)^{-1} = \Phi(hxh^{-1}) = \Psi(hxh^{-1}) = \Psi(gxg^{-1}) = \Psi(g)\Phi(x)\Psi(g)^{-1}$$

for all $x \in L$, and thus $\Phi(h)^{-1}\Psi(g)$ commutes with all $\Phi(x)$, $x \in L$. By Schur's lemma, $\Phi(h)^{-1}\Psi(g)$ fixes each of the summands $\mathcal{W}^i$ and in fact acts via some scalar $c_i$ on $\mathcal{W}^i$, with $c_i \in \mathbb{C}^\times$. As $g$ and $h$ both fix $\Phi^i|_L$ for $i = 0, (q+1)/2$, we have

$$\Psi^i(g) = c_i\Phi^i(h),\ i = 0, (q+1)/2, \tag{7.3.14.1}$$

where for $i = 0, (q+1)/2$, $\Phi^i(h)$ is the action of $\Phi(h)$ on the representation space of $\Phi^i|_L$ and similarly for $\Psi^i(g)$. Since both $g$ and $h$ have finite order, $\det(\Psi^i(g))$ and $\det(\Phi^i(h))$ have finite order, and so (7.3.14.1) implies that $c_0$ and $c_{(q+1)/2}$ are roots of unity.

We already noted that each $\Phi^i|_L = \Psi^i|_L$ is stable under $\mathrm{GU}_n(q)$, and that $g$ and $h$ both stabilize $\Phi^0|_L$ and $\Phi^{(q+1)/2}|_L$. On the other hand, $(\sigma^j)^{f/j} = \sigma^f = \tau$ acts as inversion on $\mathbf{Z}(H) = \langle \boldsymbol{z}\rangle$ and hence swaps $\Phi^i|_L$ and $\Phi^{q+1-i}|_L$ for $i \neq 0, (q+1)/2$. It follows that the traces of $\Phi(g)$ and $\Psi(h)$ on the representation space of $\oplus_{i\neq 0,(q+1)/2}\Phi^i|_L$ are both zero. Next, $\Psi^{(q+1)/2}(g)$ has trace 0 by Lemma 7.3.10(c), whence $\Phi^{(q+1)/2}(h)$ also has trace 0 by (7.3.14.1). It now follows from (7.3.14.1) that

$$|\mathrm{Trace}(\Psi(g))| = |\mathrm{Trace}(\Psi^0(g))| = |c_0\mathrm{Trace}(\Phi^0(h))| = |\mathrm{Trace}(\Phi^0(h))| = |\mathrm{Trace}(\Phi(h))|.$$

By Lemma 7.3.10(b), $|\mathrm{Trace}(\Psi(g))|^2 = p$. On the other hand, we already mentioned in (i) that the representation $\Phi$ of $\mathrm{GU}_n(q) \rtimes \langle\sigma^j\rangle$ is obtained by restricting a total Weil representation of $\mathrm{Sp}_{2n}(q) \rtimes \langle\sigma^j\rangle$. Applying [**KT3**, Theorem 3.5], we see that $|\mathrm{Trace}(\Phi(h))|^2$ is a power of $p^j$. It follows that $j = 1$.

We have shown that, modulo $\mathrm{Inndiag}(L) \cong \mathrm{PGU}_n(q)$, $g$ induces an outer automorphism of order $2f$. Recall that $g^f$, the image of $\mathsf{Frob}_{1,\mathbb{F}_q}$ in $G$, induces $\tau = \sigma^f$ modulo $\mathrm{Inn}(L)$. Clearly $g$ centralizes $g^f$, so the image of $g$ in $\mathrm{Out}(L) \cong C_{\gcd(n,q+1)} \rtimes C_{2f}$ is contained in the centralizer of $\tau$. Next, $\tau$ centralizes the subgroup $C_{2f} = \langle\sigma\rangle$ of $\mathrm{Out}(L)$, but acts as inversion on the odd-order subgroup $C_{\gcd(n,q+1)}$. It follows that the image of $g$ in $\mathrm{Out}(L)$ belongs to this subgroup $C_{2f}$ and so has order dividing $2f$. As the order of $g$ modulo $\mathrm{Inndiag}(L)$ is $2f$, we conclude that, modulo $\mathrm{Inn}(L)$, $g$ generates the subgroup $C_{2f} = \langle\sigma\rangle$. Since $G_{\mathrm{arith},\mathbb{F}_{q^2}} = 2 \times L$ has index dividing $2f$ in $G$, we have that $G = \langle 2\times L, g\rangle \cong (2\times L)\cdot \mathrm{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_p)$, as stated. □

Corollary 7.3.15. *Let $k$ be a subfield of $\mathbb{F}_{q^2}$. In the notation of Lemma 7.3.10, we have the following results.*

(a) *The arithmetic monodromy group of $\mathcal{W}^{n,m,0}$ is $(2 \times \mathrm{PSU}_n(q)) \cdot \mathrm{Gal}(\mathbb{F}_{q^2}/k)$ if $q \equiv 1 (\mathrm{mod}\ 4)$, and $\mathrm{PSU}_n(q) \rtimes \mathrm{Gal}(\mathbb{F}_{q^2}/k)$ if $q \equiv 3 (\mathrm{mod}\ 4)$.*

(b) *The arithmetic monodromy group of $\mathcal{W}^{n,m,(q+1)/2}$ is $\mathrm{PSU}_n(q) \rtimes \mathrm{Gal}(\mathbb{F}_{q^2}/k)$.*

(c) *If any other summand $\mathcal{W}^{n,m,i}$ of $\mathcal{W}^{n,m}$, with $i \neq 0, (q+1)/2$, is defined over $k$, then its arithmetic monodromy group $G_{\mathrm{arith},i,k}$ over $k$ is the image of $(2 \times \mathrm{SU}_n(q)) \cdot \mathrm{Gal}(\mathbb{F}_{q^2}/k)$ in a representation whose restriction to $\mathrm{SU}_n(q)$ affords a Weil character $\zeta_{i',n}$ for some $i' \neq 0, (q+1)/2$; in particular, it has the full index $[\mathbb{F}_{q^2} : k]$ over the arithmetic monodromy group $G_{\mathrm{arith},i,\mathbb{F}_{q^2}}$ over $\mathbb{F}_{q^2}$.*

Proof. We apply Theorem 7.3.14, and observe that the central involution $\boldsymbol{j} = \boldsymbol{z}^{(q+1)/2}$ in $2 \times \mathrm{SU}_n(q)$ acts as $(-1)^{(q+1)/2}$ on $\mathcal{W}^{n,m,0}$ and as 1 on $\mathcal{W}^{n,m,(q+1)/2}$, see [**KT3**, (3.2.1)]. The image of $(2 \times L)\cdot \mathrm{Gal}(\mathbb{F}_{q^2}/k)$ in $\mathrm{Aut}(L)$ is conjugate to $S \rtimes \mathrm{Gal}(\mathbb{F}_{q^2}/k)$, as shown in the proof of Theorem 7.3.14. It follows that the kernel of the action of $(2 \times L)\cdot \mathrm{Gal}(\mathbb{F}_{q^2}/k)$ on $\mathcal{W}^{n,m,i}$ is contained in $2 \times \mathbf{Z}(L)$ for any $i$, and contains $\mathbf{Z}(L)$ for $i = 0, (q+1)/2$. Hence the statements follow. □

CHAPTER 8

# Extraspecial normalizers and local systems in characteristic 2

## 8.1. Squared traces in characteristic 2

Fix a power $q$ of $p = 2$, and an integer $n \geq 2$. Fix a choice of $\alpha := \sqrt{2}$. For $K/\mathbb{F}_2$ a finite extension, define $\alpha_K := \alpha^{\deg(K/\mathbb{F}_2)}$. Denote by $\psi$ the unique nontrivial additive character of $\mathbb{F}_2$. For $K/\mathbb{F}_2$ a finite extension, define $\psi_K := \psi \circ \mathrm{Tr}_{K/\mathbb{F}_2}$. Given an integer $n \geq 1$, form the $n+1$-parameter local system (parameters $(r_0, \ldots, r_n)$) on $(\mathbb{A}^n \times \mathbb{G}_m)/\mathbb{F}_2$ whose trace function at a point $(r_0, \ldots, r_n) \in K^n \times K^\times$, $K/\mathbb{F}_2$ a finite extension, is

$$(r_0, \ldots, r_n) \mapsto (-1/\alpha_K) \sum_{x \in K} \psi\big(\sum_{i=0}^{n} r_i x^{1+q^i}\big).$$

Theorem 8.1.1. *For $K$ a finite extension of $\mathbb{F}_q$, and $(r_0, \ldots, r_n) \in K^n \times K^\times$, the square absolute value of*

$$(-1/\alpha_K) \sum_{x \in K} \psi\big(\sum_{i=0}^{n} r_i x^{1+q^i}\big)$$

*is either $0$ or a power $q^\nu$ of $q$ with $0 \leq \nu \leq 2n$. For $K$ a subfield of $\mathbb{F}_q$, the square absolute value is either $0$ or $\#K$.*

Proof. This is proven in [**vdG-vdV**, Section 5]. For the reader's convenience, we recall the proof. Fix $(r_0, \ldots, r_n) \in K^n \times K^\times$, and denote by $R(x)$ the $q$-linear polynomial

$$R(x) := \sum_{i=0}^{n} r_i x^{q^i}.$$

Then the square absolute value of the sum in question is

$$\begin{aligned}(1/\#K) \sum_{x,y \in K} \psi_K\big(R(x)x + R(y)y\big) &= (1/\#K) \sum_{x,y \in K} \psi_K\big(R(x+y)(x+y) + R(y)y\big) \\ &= (1/\#K) \sum_{x \in K} \psi_K\big(R(x)x\big) \sum_{y \in K} \psi_K\big(R(x)y + R(y)x\big).\end{aligned}$$

The inner sum is $\psi_{\mathbb{F}_q}$ applied to the $\mathrm{Tr}_{K/\mathbb{F}_q}$ of a sum of two products:

$$R(x)y + R(y)x = (\sum_{i=0}^{n} r_i x^{q^i})y + (\sum_{i=0}^{n} r_i y^{q^i})x.$$

Each term $r_i y^{q^i} x$ in the second product has the same trace to $\mathbb{F}_q$ as $(r_i x)^{q^{-i}} y$. So the inner sum is $\psi_K$ applied to

$$(\sum_{i=0}^{n} r_i x^{q^i} + \sum_{i=0}^{n} (r_i x)^{q^{-i}})y.$$

By orthogonality of characters, the inner sum vanishes unless $x \in K$ satisfies

$$\sum_{i=0}^{n} r_i x^{q^i} + \sum_{i=0}^{n} (r_i x)^{q^{-i}} = 0,$$

or equivalently, raising to the $q^n$ power,

$$\sum_{i=0}^{n} r_i^{q^n} x^{q^{i+n}} + \sum_{i=0}^{n} (r_i x)^{q^{n-i}} = 0,$$

in which case the inner sum is $\#K$. Denote by $W_R(K)$ the set of $x \in K$ for which

$$\sum_{i=0}^{n} r_i^{q^n} x^{q^{i+n}} + \sum_{i=0}^{n} (r_i x)^{q^{n-i}} = 0.$$

So the square absolute value of our sum is

$$\sum_{x \in W_R(K)} \psi_K\big(R(x)x\big).$$

The set $W_R(K)$ is an $\mathbb{F}_q$-vector space (under addition and scalar multiplication by $\mathbb{F}_q$), of dimension $\leq 2n$. But we can also describe $W_R(K)$ as the set of those $x \in K$ such that for any $y \in K$, we have

$$\mathrm{Tr}_{K/\mathbb{F}_q}\big(R(x)y + R(y)x\big) = 0.$$

We then infer that the function on $W_R(K)$ given by

$$x \in W_R(K) \mapsto \mathrm{Tr}_{K/\mathbb{F}_q}\big(R(x)x\big)$$

is additive on $W_R(K)$. Thus the function $x \in W_R(K) \mapsto \psi_K\big(R(x)x\big)$ is an additive character of the $\mathbb{F}_q$-space $W_R(K)$, with values in $\pm 1$. The sum

$$\sum_{x \in W_R(K)} \psi_K\big(R(x)x\big)$$

is thus the sum of an additive character of an $\mathbb{F}_q$-space over that space. If the character is nontrivial, the sum vanishes. If the character is trivial, the sum is $\#W_R(K) = q^{\dim_{\mathbb{F}_q} W_R(K)}$.

When $K$ is a subfield of $\mathbb{F}_q$, every term $x^{1+q^i}$ with $x \in K$ is equal to $x^2$, so the sum in question is

$$(-1/\alpha_K) \sum_{x \in K} \psi\big((\sum_{i=0}^{n} r_i)x^2\big).$$

If $\sum_{i=0}^{n} r_i = 0$, the sum is $\#K/\sqrt{\#K}$. If $\sum_{i=0}^{n} r_i \neq 0$, then the sum vanishes (simply because

$$\sum_{x \in K} \psi_K(ax^2) = \sum_{x \in K} \psi_K(a^{2^{-1}} x),$$

which vanishes if $a \neq 0$). □

Corollary 8.1.2. *For $K$ a finite extension of $\mathbb{F}_q$ of even (respectively odd) degree, and for any point $(r_0, \dots, r_n) \in K^n \times K^\times$, the square absolute value of*

$$(-1/\alpha_K)\sum_{x\in K}\psi\big(\sum_{i=0}^{n} r_i x^{1+q^i}\big)$$

*is either $0$ or an even (respectively odd) power of $q$.*

Proof. View $K$ as an $\mathbb{F}_q$-vector space. Because we are in characteristic 2, the $\mathbb{F}_q$-bilinear form

$$(x, y) := \mathrm{Tr}_{K/\mathbb{F}_q}\big(R(x)y + xR(y)\big)$$

has $(x, x) = 0$; in other words it is a symplectic form. The $\mathbb{F}_q$-space $W_R(K)$ is the kernel of this form: it is the set of vectors $y \in K$ such that $(x, y) = 0$ for all $x \in K$. One then knows that the dimensions over $\mathbb{F}_q$ of $W_R(K)$ and of $K$ have the same parity. [Recall the argument: pick any $\mathbb{F}_q$-subspace $U \subseteq K$ which is an $\mathbb{F}_q$-complement to $W_R(K)$. Then the restriction of the symplectic form to $U$ is non-degenerate, and hence $U$ has even $\mathbb{F}_q$ dimension.]

As explained in the proof of Theorem 8.1.1, the square absolute value of the trace is either $0$ or $\#W_R(K) = q^{\dim_{\mathbb{F}_q} W_R(K)}$; hence the statement follows. □

Remark 8.1.3. Because the character $\psi_K$ takes values $\pm 1$, and the clearing factor $\alpha_K$ is real, each "square absolute value" of a trace is just the square of that trace. Thus Corollary 8.1.2 could be restated as follows. For $K/\mathbb{F}_q$ an extension of even degree, each trace is either 0 or ±(a power of $q$). For $K/\mathbb{F}_q$ an extension of odd degree, each trace is either 0 or ±(an odd power of $\sqrt{q}$).

Corollary 8.1.4. *Let $K$ be a subfield of $\mathbb{F}_q$, say $\#K = q_0$ and $q = q_0^\nu$ for some integer $\nu \geq 1$. Let $L/K$ be a finite extension of even (respectively odd) degree, and and $(r_0, \dots, r_n) \in L^n \times L^\times$. Then the square absolute value of*

$$(-1/\alpha_L)\sum_{x\in L}\psi\big(\sum_{i=0}^{n} r_i x^{1+q^i}\big)$$

*is either $0$ or an even (respectively odd) power of $q_0$.*

Proof. View the situation as lying over $\mathbb{F}_{q_0}$, and apply the previous Corollary 8.1.2. □

Corollary 8.1.5. *If throughout we consider instead the $n + 2$ parameter system on $(\mathbb{A}^{n+1}\times\mathbb{G}_m)/\mathbb{F}_2$, parameters $(r_{-1}, r_0, \dots, r_n)$, whose trace function at a point $(r_{-1}, r_0, \dots, r_n) \in K^{n+1} \times K^\times$, $K/\mathbb{F}_2$ a finite extension, is*

$$(r_{-1}, r_0, \dots, r_n) \mapsto (-1/\alpha_K)\sum_{x\in K}\psi\big(\sum_{i=0}^{n} r_i x^{1+q^i} + r_{-1}x\big),$$

*then all of the results of this section, namely Theorem 8.1.1, Corollary 8.1.2, Remark 8.1.3 and Corollaty 8.1.4, remain valid as stated.*

Proof. Because we are in characteristic 2, the linear term $r_{-1}x$ is Artin-Schreier equivalent to

$$r_{-1}^2 x^2 = r_{-1}^2 x^{1+q^0}.$$

So the trace at $(r_{-1}, r_0, \dots, r_{n1})$ is simply the previous trace at $(r_0 + r_{-1}^2, \dots, r_n)$.

We can also give an alternative argument, along the lines of the proof of Theorem 7.1.2, as follows. With

$$R(x) := \sum_{i=0}^{n} r_i x^{q^i},$$

our sum is

$$(-1/\alpha_K) \sum_{x \in K} \psi\big(R(x)x + r_{-1}x\big).$$

The square absolute value of this sum is

$$= (1/\#K) \sum_{x,y \in K} \psi_K\big(R(x+y)(x+y) + R(y)y + r_{-1}x\big),$$

which, just as in the proof of Theorem 8.1.1, is equal to

$$\sum_{x \in W_R(K)} \psi_K\big(R(x)x + r_{-1}x\big).$$

As already noted,

$$x \in W_R(K) \mapsto \mathrm{Tr}_{K/\mathbb{F}_q}\big(R(x)x\big)$$

is an additive character on $W_R(K)$, and hence so also is

$$x \in W_R(K) \mapsto \mathrm{Tr}_{K/\mathbb{F}_q}\big(R(x)x + r_{-1}x\big).$$

The proof now concludes exactly as the proof of Theorem 8.1.1, the only difference being that a different additive character is being summed over $W_R(K)$. □

## 8.2. Traces of elements in normalizers of extraspecial 2-groups

In the case $p = 2$, there exist precisely two non-isomorphic extraspecial groups of order 8, namely the dihedral group $D_8 = 2_+^{1+2}$ and $Q_8 = 2_-^{1+2}$. More generally, for any $N \in \mathbb{Z}_{\geq 1}$, there exist precisely two non-isomorphic extraspecial groups of order $2^{1+2N}$, namely the central products

$$2_+^{1+2N} = \underbrace{D_8 * D_8 * \ldots * D_8}_{N \text{ times}}, \; 2_-^{1+2N} = \underbrace{D_8 * D_8 * \ldots * D_8}_{(N-1) \text{ times}} * Q_8.$$

Fixed $\epsilon = \pm$, $E = 2_\epsilon^{1+2N}$, and identify the elementary abelian $E/\mathbf{Z}(E)$ with $V := \mathbb{F}_2^{2N}$ and $\mathbf{Z}(E)$ with $\mathbb{F}_2$. Then the commutator map

$$(\cdot,\cdot) = (\cdot,\cdot)_1 : (x\mathbf{Z}(E), y\mathbf{Z}(E)) \mapsto [x,y] \in \mathbf{Z}(E)$$

defines a non-degenerate symplectic form on $V$, and the map

$$\mathsf{Q} = \mathsf{Q}_1 : x\mathbf{Z}(E) \mapsto x^2 \in \mathbf{Z}(E)$$

defines a quadratic form on $V$, associated to $(\cdot,\cdot)$ and of type $\epsilon$. Clearly, $\mathrm{Aut}(E)$ preserves $\mathsf{Q}$ and so one has a homomorphism $\mathrm{Aut}(E)/\mathrm{Inn}(E) \to \mathrm{O}(V) \cong \mathrm{O}_{2N}^\epsilon(2)$. When $N \geq 3$, the map is an isomorphism and $\mathrm{Aut}(E)$ is a non-split extension of $\mathrm{Inn}(E) \cong E/\mathbf{Z}(E)$ by $\mathrm{O}(V)$, see [**Gri**, Theorem 1]. Furthermore, the unique (up to isomorphism) complex irreducible representation of degree $2^N$ of $E$ gives rise to a non-split extension $2_\epsilon^{1+2N} \cdot \mathrm{O}_{2N}^\epsilon(2)$:

THEOREM 8.2.1. *Let $N \geq 3$ and $\epsilon = \pm$. There exists a finite irreducible subgroup*

$$\Gamma(2, N, \epsilon) := H_1^\epsilon < \mathrm{GL}_{2^N}(\mathbb{C})$$

*such that* $\mathbf{O}_2(H_1^\epsilon) = E \cong 2_\epsilon^{1+2N}$, $\mathbf{Z}(H_1^\epsilon) = \mathbf{Z}(E)$, $H_1^\epsilon/E \cong \mathrm{O}_{2N}^\epsilon(2)$, *and* $H_1^\epsilon/\mathbf{Z}(H_1^\epsilon) \cong \mathrm{Aut}(E)$. *Furthermore,* $H_1^+ < \mathfrak{G} := \mathrm{O}_{2^N}(\mathbb{C})$, *and* $H_1^- < \mathfrak{G} := \mathrm{Sp}_{2^N}(\mathbb{C})$. *In either case,* $H_1^\epsilon = \mathbf{N}_{\mathfrak{G}}(E)$.

PROOF. The first statement is [**Gri**, Theorem 5(a)]. If $\epsilon = +$, then an explicit construction of $H_1^\epsilon$ inside $\mathrm{O}_{2^N}(\mathbb{R})$ is given in [**NRS**, Theorem 2.2]. To show that $H_1^\epsilon$ preserves a non-degenerate symplectic form on $\mathbb{C}^{2^N}$ when $\epsilon = -$, first note that this is true for the subgroup $E$ of $H_1^-$. Next, we can embed a central product

$$H_1^- * Q_8 = 2_-^{1+2N} \cdot \mathrm{O}_{2N}^-(2) * 2_-^{1+2} \hookrightarrow \tilde{H}_1^+ := 2_+^{1+(2N+2)} \cdot \mathrm{O}_{2N+2}^+(2),$$

where $\tilde{H}_1^+ < \mathrm{O}_{2^{N+1}}(\mathbb{C})$ by the previous case. Now if $\varphi$ denotes the character of $\tilde{H}_1^+$ acting on the orthogonal module $\mathbb{C}^{2^{N+1}}$ and $\psi$ denotes the character of $H_1^-$ acting on $\mathbb{C}^{2^N}$, then $\varphi$ is real-valued and $\varphi|_H = 2\psi$. Thus $\psi$ is real-valued, but $\psi|_E$ is of type $-$, so $\psi$ is of type $-$ and $H_1^- \hookrightarrow \mathrm{Sp}_{2^N}(\mathbb{C})$.

For the third statement, first we note that $\mathbf{C}_{\mathfrak{G}}(E) = \mathbf{Z}(\mathfrak{G}) = \mathbf{Z}(E)$ by Schur's Lemma. Now consider any $x \in \mathbf{N}_{\mathfrak{G}}(E)$. Since $H_1^\epsilon/\mathbf{Z}(E) \cong \mathrm{Aut}(E)$, we can find $h \in H_1^\epsilon$ such that conjugations by $x$ and by $h$ induce the same automorphism of $E$. Thus $h^{-1}x \in \mathbf{C}_{\mathfrak{G}}(E) = \mathbf{Z}(E) < H_1^\epsilon$, and so $x \in H_1^\epsilon$. □

LEMMA 8.2.2. *In the notation of Theorem 8.2.1, consider a subgroup $P \rhd E$ of $H_1^\epsilon$, with $P/E$ a cyclic maximal torus of order $2^N - \epsilon$ of $\mathrm{O}_{2N}^\epsilon(2)$. Then $P = E \rtimes \langle c \rangle$ for some element $c$ of order $2^N - \epsilon$, and the action of $C := \langle c \rangle$ on $\mathbb{C}^{2^N}$ affords the character $\mathbf{reg}_C + \epsilon \cdot 1_C$.*

PROOF. Note that $E$ is a normal subgroup of $P$, of index coprime to its order. Hence, by the Schur-Zassenhaus theorem, $E$ has a complement $C$, with $C \cong P/E$, and so $C = \langle c \rangle \cong C_{2^N-\epsilon}$. The image of $c$ in $\mathrm{O}_{2N}^\epsilon(2)$ acts on $E/\mathbf{Z}(E) = \mathbb{F}_2^{2N}$ with eigenvalues $\zeta, \zeta^2, \ldots, \zeta^{2^{N-1}}, \zeta^{-1}, \zeta^{-2}, \ldots, \zeta^{-2^{N-1}}$, where $\zeta \in \overline{\mathbb{F}_2}^\times$ has order $2^N - \epsilon$. It follows that the image of $c^j$, with $1 \leq j < 2^N - \epsilon$, acts on $E/\mathbf{Z}(E)$ with no eigenvalue 1. Hence, if $\varphi$ denotes the character of $C$ acting on $\mathbb{C}^{2^N}$, then $|\varphi(c^j)| = 1$ by Lemma 7.2.1. On the other hand, $\varphi$ is real-valued by Theorem 8.2.1, hence $\varphi(c^j) = \pm 1$. It follows that $\Sigma := \sum_{j=1}^{2^N-\epsilon-1} \varphi(c^j)$ is an **even** integer of absolute value at most $2^N - \epsilon - 1$. Also note that

$$\mathbb{Z} \ni [\varphi|_C, 1_C]_C = (2^N + \Sigma)/(2^N - \epsilon),$$

whence $\Sigma + \epsilon$ is divisible by $2^N - \epsilon$.

Now, if $\epsilon = +$, then we must have that $\Sigma + 1 = 2^N - 1$, i.e. $\varphi(c^j) = 1$ for all $1 \leq j < 2^N - \epsilon$, and so $\varphi|_C = \mathbf{reg}_C + 1_C$. If $\epsilon = -$, then we must have that $\Sigma - 1 = -2^N - 1$, i.e. $\varphi(c^j) = -1$ for all $1 \leq j < 2^N - \epsilon$, and so $\varphi|_C = \mathbf{reg}_C - 1_C$. □

Now consider any 2-power $q = 2^f$ and $n \in \mathbb{Z}_{\geq 1}$ such that $N = nf \geq 3$. Also consider a $2n$-dimensional space $U := \mathbb{F}_q^{2n}$, endowed with a non-degenerate symplectic form $(\cdot, \cdot)_f : U \times U \to \mathbb{F}_q$ and a quadratic form $\mathsf{Q}_f : U \to \mathbb{F}_q$ of type $-$ associated to $(\cdot, \cdot)_f$. Then, choosing $E = 2_-^{1+2n}$, by base change we can identify the $\mathbb{F}_2$-space $U$ with $V$, $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}((\cdot, \cdot)_f)$

with $(\cdot,\cdot)_1$, and $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\mathsf{Q}_f)$ with $\mathsf{Q}_1$. This gives rise to an embedding of $\mathrm{O}(U) \cong \mathrm{O}^-_{2n}(q)$ into $\mathrm{O}(V) \cong \mathrm{O}^-_{2N}(2)$, and by Theorem 8.2.1 we obtain

(8.2.2.1)
$$H^-_f = E \cdot \mathrm{O}^-_{2n}(q) \leq H^-_1,\ H^\circ_f := [H^-_f, H^-_f] \cong E \cdot \Omega^-_{2n}(q), \quad \text{with } E := \mathbf{O}_2(H^-_f) \cong 2^{1+2nf}_-.$$

(Note that $H^\circ_f$ is perfect if $n \geq 2$. Indeed, the faithful irreducible action of the simple group $\Omega^-_{2n}(q)$ on $E/\mathbf{Z}(E)$ implies that $\mathbf{Z}(E)X = H^\circ_f$ for $X := (H^\circ_f)^{(\infty)}$, and thus $[H^\circ_f : X] \leq 2$. Hence, if $X < H^\circ_f$, then $H^\circ_f = X \times \mathbf{Z}(E)$ and so $E = \mathbf{Z}(E) \times (E \cap X)$ splits over $\mathbf{Z}(E)$, a contradiction.)

In what follows, by $H^-_f$ and $H^\circ_f$ we mean the subgroups as defined in (8.2.2.1), where the embedding $H^-_f/E \hookrightarrow H^-_1/E$ is obtained via base change as described above, and $H^-_1 = 2^{1+2nf}_- \cdot \mathrm{O}^-_{2nf}(2) < \mathrm{GL}_{2^{nf}}(\mathbb{C})$ is constructed in Theorem 8.2.1.

Proposition 8.2.3. *In the above notation, assume $n \geq 2$ and $nf \geq 3$. Then there is an element $\sigma \in \mathrm{O}(V) = \mathrm{O}^-_{2nf}(2)$ of order $2f$ such that the following statements hold:*

(i) *$\sigma$ induces an outer automorphism of order $2f$ of $\Omega(U) = \Omega^-_{2n}(2^f)$.*
(ii) *$\mathbf{N}_{\mathrm{O}(V)}(\Omega(U)) = \langle \Omega(U), \sigma\rangle \cong \mathrm{Aut}(\Omega(U)) \cong \Omega(U) \rtimes C_{2f} \cong \mathrm{O}(U) \cdot C_f$.*
(iii) *If $f = ab$ for some $a, b \in \mathbb{Z}_{\geq 1}$, then $\langle \Omega(U), \sigma^b\rangle \leq \mathrm{O}^-_{2na}(q^{1/a})$, $\langle \Omega(U), \sigma^{2b}\rangle \leq \Omega^-_{2na}(q^{1/a})$, and $|\mathbf{C}_V(\sigma^b)| = 2^{(2n-1)b}$. Furthermore, if $b > 1$ then there exists an element $\sigma' \in \langle \Omega(U), \sigma^b\rangle$ such that $|\mathbf{C}_V(\sigma')| = 2^{(2n-3)b}$. If $b = 1$ and $2 \nmid f$, then there exists an element $\sigma' \in \langle \Omega(U), \sigma^b\rangle$ such that $|\mathbf{C}_V(\sigma')| = 2^{(2n-2)b}$.*
(iv) *Suppose $f = ab$ for some $a, b \in \mathbb{Z}_{\geq 1}$ with $2 \nmid a \geq 3$. Then there exists an element $\tau \in \langle \Omega(U), \sigma^{2b}\rangle$ such that $|\mathbf{C}_V(\tau)| = 2^{2b}$ if $b > 1$ and $|\mathbf{C}_V(\tau)| = 2^{2n}$ if $b = 1$. If in addition $b = 1$ and $n \geq 3$, then there exists an element $\tau' \in \langle \Omega(U), \sigma^{2b}\rangle$ such that $|\mathbf{C}_V(\tau')| = 2^{2n-2}$.*

Proof. (a) We will follow the proof of [**KlL**, Proposition 2.8.2]. Fix an element $\zeta \in \mathbb{F}_q$ such that the polynomial $t^2 + t + \zeta \in \mathbb{F}_q[t]$ is irreducible over $\mathbb{F}_q$. Note that

$$\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\zeta) = 1. \tag{8.2.3.1}$$

(Indeed, the map $\pi : x \mapsto x^2 + x$ on $\mathbb{F}_q$ is $\mathbb{F}_2$-linear with kernel $\{0, 1\}$, hence $|\mathrm{Im}(\pi)| = q/2$. Next, if $y = x^2 + x \in \mathrm{Im}(\pi)$, then $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(y) = x + x^q = 0$. Since the equation $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(y) = 0$ can have at most $q/2$ roots in $\mathbb{F}_q$, we see that its roots are exactly the elements of $\mathrm{Im}(\pi)$. As $\zeta \notin \mathrm{Im}(\pi)$, (8.2.3.1) follows.)

Now we can choose a basis $(u_1, \ldots, u_n, v_1, \ldots, v_n)$ of $U = \mathbb{F}_q^{2n}$ in which $(\cdot,\cdot)_f$ has Gram matrix $\begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix}$ and furthermore

$$\mathsf{Q}_f(u_i) = \mathsf{Q}_f(v_i) = 0,\ 1 \leq i \leq n-1,\ \mathsf{Q}_f(u_n) = 1, \mathsf{Q}_f(v_n) = \zeta.$$

Define

$$\sigma : \sum_{i=1}^{n}(x_i u_i + y_i v_i) \mapsto \sum_{i=1}^{n-1}(x_i^2 u_i + y_i^2 v_i) + x_n^2 u_n + y_n^2(\zeta u_n + v_n),\ \forall x_i, y_i \in \mathbb{F}_q. \tag{8.2.3.2}$$

In particular, $\sigma$ is $\mathbb{F}_2$-linear, and

$$\mathsf{Q}_f(\sigma v) = \mathsf{Q}_f(v)^2,\ \forall v \in U. \tag{8.2.3.3}$$

It follows that $\sigma$ preserves $\mathsf{Q}_1$, whence $\sigma \in \mathrm{O}(V)$. Also, (8.2.3.3) implies that $\sigma$ normalizes $\mathrm{O}(U)$ and $\Omega(U)$, i.e. $\sigma \in \mathbf{N}_{\mathrm{O}(V)}(\Omega(U))$.

Suppose in addition that $f = ab$ for some $a, b \in \mathbb{Z}_{\geq 1}$. Then we can view $U$ as an $\mathbb{F}_{2^b}$-vector space, and endow it with the following non-degenerate symplectic form and associated quadratic form

$$(u,v)_b := \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{2^b}}((u,v)_f),\ \mathsf{Q}_b(v) := \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{2^b}}(\mathsf{Q}_f(v)).$$

Writing $r := 2^b$ and

(8.2.3.4) $$\eta := \zeta + \zeta^2 + \ldots + \zeta^{2^{b-1}},$$

from (8.2.3.2) we obtain that

(8.2.3.5) $$\sigma^b : \sum_{i=1}^{n}(x_i u_i + y_i v_i) \mapsto \sum_{i=1}^{n-1}(x_i^r u_i + y_i^r v_i) + x_n^r u_n + y_n^r(\eta u_n + v_n).$$

In particular, $\sigma^b$ is $\mathbb{F}_r$-linear, and, using (8.2.3.1) we see that

(8.2.3.6) $$\sigma^f(v) = v + (u_n, v)_f u_n,\ \forall v \in U,$$

that is, $\sigma^f$ is the reflection $\rho_{u_n}$ corresponding to $u_n$ and so $\langle \Omega(U), \sigma_f \rangle = \mathrm{O}(U)$. Furthermore, (8.2.3.3) shows that $\sigma^i \notin \mathrm{O}(U)$ when $1 \leq i \leq f-1$, and so

(8.2.3.7) $$\langle \Omega(U), \sigma \rangle \cong \Omega(U) \rtimes C_{2f}.$$

We also note from (8.2.3.3) that

$$\mathsf{Q}_b\big(\sigma^b(v)\big) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_r}\big(\mathsf{Q}_f(\sigma^b(v))\big) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_r}\big((\mathsf{Q}_f(v))^r\big) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_r}\big(\mathsf{Q}_f(v)\big) = \mathsf{Q}_b(v)$$

for all $v \in U$, i.e. $\sigma_b$ preserves $\mathsf{Q}_b$. Since the same obviously holds for $\Omega(U)$, we have shown that $\langle \Omega(U), \sigma^b \rangle \leq \mathrm{O}^-_{2na}(q^{1/a})$. As $\Omega(U) = \Omega^-_{2n}(q)$ is perfect and $\Omega^-_{2na}(q^{1/a})$ has index 2 in $\mathrm{O}^-_{2na}(q^{1/a})$, it follows that $\langle \Omega(U), \sigma^{2b} \rangle \leq \Omega^-_{2na}(q^{1/a})$.

(b) Note that $\Omega(U)$ acts irreducibly on $V = \mathbb{F}_2^{2N}$. Therefore $\mathbb{E} := \mathbf{C}_{\mathrm{End}(V)}(\Omega(U))$ is a division ring by Schur's lemma, hence a finite field by Wedderburn's theorem. Next, since $\Omega(U)$ is centralized by $\mathbf{Z}(\mathrm{GL}(U)) \cup \{0\}$, a field of size $q$, we have that $\mathbb{E}$ is an extension of $\mathbb{F}_q$, say of degree $e \geq 1$. Now, considered as $\Omega(U)$-module over $\mathbb{E}$, $V$ is absolutely irreducible, and $\dim_{\mathbb{E}} V = 2n/e$. When $n \geq 3$, applying [**KlL**, Proposition 5.4.11], we see that $e = 1$ and $\mathbb{E} \smallsetminus \{0\} = \mathbf{Z}(\mathrm{GL}(U))$. This also holds when $n = 2$, see [**KlL**, Proposition 2.9.1(v)]. It follows that $\mathbf{C}_{\mathrm{GL}(V)}(\Omega(U)) = \mathbf{Z}(\mathrm{GL}(U))$.

Next we show that $\mathbf{C}_{\mathrm{O}(V)}(\Omega(U)) = 1$. In fact we will show that

(8.2.3.8) $$\mathbf{C}_{\mathrm{Sp}(V)}(\Omega(U) = 1.$$

By the previous result, it suffices to show that if $\lambda \in \mathbb{F}_q^\times$ is such that $(\lambda u, \lambda v)_1 = (u,v)_1$ for all $u, v \in U$, then $\lambda = 1$. Assume the contrary: $\lambda \neq 1$. We apply the given identity to $(u,v) = (u_1, \zeta/(\lambda^2-1)v_1)$, so that $(u,v)_f = \zeta/(\lambda^2-1)$. For such $(u,v)$ we now have

$$(\lambda u, \lambda v)_1 - (u,v)_1 = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}\big((\lambda u, \lambda v)_f - (u,v)_f\big) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}\big((\lambda^2-1)(u,v)_f\big) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\zeta) = 1,$$

a contradiction.

We have shown that $\mathbf{N}_{\mathrm{O}(V)}(\Omega(U)) \hookrightarrow \mathrm{Aut}(\Omega(U))$, and the latter is isomorphic to $\Omega(U) \rtimes C_{2f}$ by [**GLS**, Theorem 2.5.12]. Together with (8.2.3.7), this implies that $\mathbf{N}_{\mathrm{O}(V)}(\Omega(U)) =$

$\langle \Omega(U), \sigma \rangle$ and that $\sigma$ is an outer automorphism of order $2s$ of $\Omega(U)$. As $\langle \Omega(U), \sigma^f \rangle = \mathrm{O}(U)$, we also obtain that $\langle \Omega(U), \sigma \rangle \cong \mathrm{O}(U) \cdot C_f$, the latter being a split extension only when $2 \nmid f$.

(c) To prove statement (iii), note that any $\sigma^b$-fixed point $v \in V$ is also $\sigma^f$-fixed, and so belongs to

$$u_n^\perp = \langle u_1, \dots, u_n, v_1, \dots, v_{n-1} \rangle_{\mathbb{F}_q}$$

by (8.2.3.6). Applying (8.2.3.5), we then see that

$$\mathbf{C}_V(\sigma^b) = \langle u_1, \dots, u_n, v_1, \dots, v_{n-1} \rangle_{\mathbb{F}_{2^b}},$$

and so $|\mathbf{C}_V(\sigma^b)| = 2^{(2n-1)b}$.

Assume $b > 1$. Then there exists $\beta \in \mathbb{F}_q \smallsetminus \{z^{2^b-1} \mid z \in \mathbb{F}_q\}$. Then we take $\sigma' := h\sigma^b$, where $h \in \mathrm{O}(\langle u_1, v_1 \rangle_{\mathbb{F}_q})$ sends $u_1$ to $\beta u_1$ and $v_1$ to $\beta^{-1} v_1$. The condition on $\beta$ implies that the system

$$x = \beta x^{2^b},\ y = \beta^{-1} y^{2^b},\ x, y \in \mathbb{F}_q$$

has only one solution $(0, 0)$. This means that $\sigma'$ fixes only the zero vector in $\langle u_1, v_1 \rangle_{\mathbb{F}_q}$. The previous case shows that $\sigma'$ fixes exactly $2^{(2n-3)b}$ vectors in $\langle u_2, \dots, u_n, v_2, \dots, v_n \rangle_{\mathbb{F}_q}$, and so $|\mathbf{C}_V(\sigma')| = 2^{(2n-3)b}$.

Next, consider the case $b = 1$ but $2 \nmid f$. Then we take $\sigma' := h\sigma$, where $h \in \mathrm{O}(\langle u_1, v_1 \rangle_{\mathbb{F}_q})$ sends $u_1$ to $v_1$ and $v_1$ to $u_1$. As $2 \nmid f$, the system

$$x = y^2,\ y = x^2,\ x, y \in \mathbb{F}_q$$

has exactly two solutions $x = y \in \mathbb{F}_2$. This means that $\sigma'$ fixes exactly 2 vectors in $\langle u_1, v_1 \rangle_{\mathbb{F}_q}$. As before, $\sigma'$ fixes exactly $2^{(2n-3)b}$ vectors in $\langle u_2, \dots, u_n, v_2, \dots, v_n \rangle_{\mathbb{F}_q}$. Hence $|\mathbf{C}_V(\sigma')| = 2^{(2n-2)b}$.

(d) Finally, we prove statement (iv). Again write $r := 2^b$, so that $q = r^a$, and choose $\zeta' \in \mathbb{F}_r$ such that $t^2 + t + \zeta' \in \mathbb{F}_r[t]$ is irreducible over $\mathbb{F}_r$. Then, for any root $\xi$ of $t^2 + t + \zeta'$ we have $\xi \in \mathbb{F}_{r^2} \smallsetminus \mathbb{F}_r$. But $a$ is odd, so $\xi \in \mathbb{F}_{q^2} \smallsetminus \mathbb{F}_q$, which means that $t^2 + t + \zeta' \in \mathbb{F}_q[t]$ is irreducible over $\mathbb{F}_q$. Hence, in what follows we may assume that the element $\zeta$ in (a) is chosen to be equal to $\zeta'$ and thus

$$\zeta \in \mathbb{F}_r.$$

For the element $\eta$ defined in (8.2.3.4), the proof of (8.2.3.1) now shows that

$$\eta = \zeta + \zeta^2 + \ldots + \zeta^{2^{b-1}} = \mathrm{Tr}_{\mathbb{F}_r/\mathbb{F}_2}(\zeta) = 1.$$

Together with (8.2.3.5), this implies that

$$\sigma^{2b} : \sum_{i=1}^{n} (x_i u_i + y_i v_i) \mapsto \sum_{i=1}^{n} (x_i^{r^2} u_i + y_i^{r^2} v_i). \tag{8.2.3.9}$$

We also note that

$$\gcd(r^2 - 1, q - 1) = \gcd(2^{2b} - 1, 2^{ab} - 1) = 2^b - 1 \tag{8.2.3.10}$$

since $a$ is odd.

Assume first that $b > 1$. Fix a generator $\gamma$ of $\mathbb{F}_q^\times$, of order $q - 1 = r^a - 1$, and consider

$$t \in \Omega(U) : u_i \mapsto \gamma u_i,\ v_i \mapsto \gamma^{-1} v_i,\ 1 \le i \le n-1,\ u_n \mapsto u_n,\ v_n \mapsto v_n.$$

We claim that $x = 0$ is the only solution of the equation $\gamma x^{r^2} = x$ over $\mathbb{F}_q$. (Indeed, if $x \in \mathbb{F}_q^\times$ is any such solution, then $\gamma = x^{1-r^2}$, and so

$$\gamma^{(q-1)/(r-1)} = x^{(-1-r)(q-1)} = 1.$$

Since $r - 1 = 2^b - 1 > 1$ and $(r-1)|(q-1)$, this contradicts the choice of $\gamma$.) Together with (8.2.3.9) and (8.2.3.10), this implies that $\sum_{i=1}^n (x_i u_i + y_i v_i) \in U$ can be fixed by $t\sigma^{2b}$ exactly when $x_n, y_n \in \mathbb{F}_r$ and $x_i = y_i = 0$ for $1 \le i \le n-1$, showing $|\mathbf{C}_V(t\sigma^{2b})| = 2^{2b}$. Thus we can take $\tau := t\sigma^{2b}$ in this case.

Assume now that $b = 1$. Then (8.2.3.9) and (8.2.3.10) show that $\sum_{i=1}^n (x_i u_i + y_i v_i) \in U$ can be fixed by $\sigma^{2b}$ exactly when $x_i, y_i \in \mathbb{F}_r$ for $1 \le i \le n$, yielding $|\mathbf{C}_V(\tau)| = 2^{2n}$ for $\tau := \sigma^{2b}$.

Finally, assume that $b = 1$ and $n \ge 3$. Then $U' := \langle u_1, u_2, v_1, v_2 \rangle_{\mathbb{F}_q}$ is a quadratic space of type $+$, and so $\Omega(U') \cong \Omega_4^+(q)$. Recalling that $q = 2^{ab} \ge 8$ and $\langle u_1, u_2 \rangle_{\mathbb{F}_q}$ is a totally singular plane in $U'$, we can find an element

$$t' := \mathrm{diag}\left( \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right) \in \mathrm{GL}_2(q) < \Omega(U')$$

(written in the basis $(u_1, u_2, v_1, v_2)$). Letting $t'$ acting trivially on $(U')^\perp$, we obtain an element in $\Omega(U)$ which we denote by the same letter $t'$.

We claim that $(x, y) = (0, 0), (1, 0)$ are the only two solutions of the system

$$x^4 + y^4 = x, \ y^4 = y$$

over $\mathbb{F}_q$. (Indeed, $y^4 = y$ implies that $y \in \mathbb{F}_4 \cap \mathbb{F}_{2^f} = \mathbb{F}_2$ (as $2 \nmid a = f$). If $y = 0$, then $x^4 = x$ implies that $x \in \mathbb{F}_4 \cap \mathbb{F}_{2^f} = \mathbb{F}_2$, giving rise to the two indicated solutions. Assume $y = 1$. Then

$$x^{16} = (x+1)^4 = x^4 + 1 = x,$$

and so $x \in \mathbb{F}_{16} \cap \mathbb{F}_{2^f} = \mathbb{F}_2$, for the same reason that $f$ is odd. But in this case, $x^4 + x = 0 \neq y^4$, a contradiction.) Together with (8.2.3.9) and (8.2.3.10), this implies that $\sum_{i=1}^n (x_i u_i + y_i v_i) \in U$ can be fixed by $\tau' := t'\sigma^{2b}$ exactly when

$$(x_1, x_2) \in \{(0,0), (1,0)\}, \ (y_1, y_2) \in \{(0,0), (0,1)\}, \ x_i, y_i \in \mathbb{F}_2, \ 3 \le i \le n.$$

Thus $|\mathbf{C}_V(\tau')| = 2^{2n-2}$, as stated. □

The next result is concerned with orthogonal groups of both types $+$ and $-$.

PROPOSITION 8.2.4. *Let $q = 2^f$, $n \ge 1$, and let $U = \mathbb{F}_q^{2n}$ be endowed with a non-degenerate $\mathbb{F}_q$-valued quadratic form $\mathsf{Q}_f$ of type $\epsilon = \pm$. View $U$ as a $2nf$-dimensional vector space $V = \mathbb{F}_2^{2nf}$, endowed with the $\mathbb{F}_2$-valued quadratic form $\mathsf{Q}_1(v) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\mathsf{Q}_f(v))$, which naturally embeds $\mathrm{O}(U)$ in $\mathrm{O}(V)$. Then the following statements hold.*

(i) *If $\epsilon = -$, then $\mathbf{N}_{\mathrm{O}(V)}(\Omega(U))$ contains a subgroup $A \cong \Omega(U) \rtimes C_{2f}$ and an element $\tau \in A$ such that $|\mathbf{C}_V(\tau)| = 2$.*

(ii) *Suppose $\epsilon = +$ and $2 \nmid f$. Then $\mathbf{N}_{\mathrm{O}(V)}(\Omega(U))$ contains a subgroup $A \cong \Omega(U) \rtimes C_{2f}$ and an element $\tau \in A$ such that $|\mathbf{C}_V(\tau)| = 2$ if $2 \nmid n$, $|\mathbf{C}_V(\tau)| = 4$ if $2|n$. In the latter case when $2|n$, $A$ also contains $\tau'$ such that $|\mathbf{C}_V(\tau')| = 2^{2n-1}$.*

(iii) *If $\epsilon = +$ and $2|f$, then $\mathbf{N}_{\Omega(V)}(\Omega(U))$ contains a subgroup $A \cong \Omega(U) \rtimes (C_2 \times C_f)$ and an element $\tau \in A$ such that $|\mathbf{C}_V(\tau)| = 4$. Furthermore, $|\mathbf{C}_V(g)|$ is a power of $4$ for all $g \in A$.*

Proof. (a) In the case $\epsilon = -$, part (a) of the proof of Proposition 8.2.3, which was formulated with the conditions $n \geq 2$ and $nf \geq 3$, also works for $n = 1$ and for $n = 2$, and we can take $A = \langle \Omega(U), \sigma \rangle$.

Consider the case $n = 1$. Then part (c) of the proof of Proposition 8.2.3 also works when $n = 1 = b$ and shows that $|\mathbf{C}_V(\sigma)| = 2$.

For the general case of any $n$, we apply the preceding remark to $\Omega_2^-(2^{nf}) = \Omega(\mathsf{Q}_{nf})$ to get

$$|\mathbf{C}_V(\sigma)| = 2, \tag{8.2.4.1}$$

where $\sigma$ is induced by the field automorphism $x \mapsto x^2$, and $\mathsf{Q}_{nf}$ is the quadratic form of type $-$ on $W := \mathbb{F}_{2^{nf}}^2$ specified in part (a) of the proof of Proposition 8.2.3. As mentioned there, $\sigma^f$ is then $\mathbb{F}_q$-linear. Now we view $W$ as $U = \mathbb{F}_q^{2n}$ with the $\mathbb{F}_q$-valued quadratic form

$$\mathsf{Q}'(v) = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\mathsf{Q}_{nf}(v)),$$

which is invariant under $\Omega(W)$ and $\sigma^f$. In particular, $\Omega(U_1) \cong C_{q^n+1}$ embeds in $\mathrm{O}(U)$. Furthermore, (8.2.3.3) applied to $W$ shows that

$$\mathsf{Q}_{nf}(\sigma(v)) = \mathsf{Q}_{nf}(v)^2$$

for all $v \in W$. Now, for any $g \in \mathrm{O}(U)$, writing $u := \sigma^{-1}(v)$ we have

$$\begin{aligned}
\mathsf{Q}'\big(\sigma g \sigma^{-1}(v)\big) &= \mathsf{Q}'\big(\sigma(g(u))\big) = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}\Big(\mathsf{Q}_{nf}\big(\sigma(g(u))\big)\Big) = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}\Big(\mathsf{Q}_{nf}\big(g(u)\big)^2\Big) \\
&= \Big(\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}\big(\mathsf{Q}_{nf}\big(g(u)\big)\big)\Big)^2 = \Big(\mathsf{Q}'\big(g(u)\big)\Big)^2 = \big(\mathsf{Q}'(u)\big)^2 \\
&= \Big(\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}\big(\mathsf{Q}_{nf}\big(\sigma^{-1}(v)\big)\big)\Big)^2 = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}\Big(\mathsf{Q}_{nf}\big(\sigma^{-1}(v)\big)^2\Big) \\
&= \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}\big(\mathsf{Q}_{nf}(v)\big) = \mathsf{Q}'(v)
\end{aligned} ,$$

showing that $\sigma$ normalizes $\mathrm{O}(U)$, and hence $\Omega(U) = [\mathrm{O}(U), \mathrm{O}(U)]$ as well.

Claim that $\mathrm{O}(U)$ has type $-$. It suffices to prove it for $n \geq 2$. If $(n, f) \neq (3, 1)$, then $2^{2nf} - 1$ admits a primitive prime divisor $\ell$ by [**Zs**], which divides $q^n + 1$ but not $|\mathrm{O}_{2n}^+(q)|$, whence the claim follows. If $(n, f) = (3, 1)$, then $\Omega(W) \cong C_9$, whereas $\mathrm{O}_6^+(2) \cong \mathsf{S}_8$ has no element of order 9, so we are also done.

Hence we can identify $\mathsf{Q}'$ with $\mathsf{Q}_f$. Now $\sigma$ fixes

$$\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_2}(\mathsf{Q}_{nf}) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\mathsf{Q}') = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\mathsf{Q}_f) = \mathsf{Q}_1,$$

and so $\sigma \in \mathrm{O}(V)$. We have shown above that $\sigma^f \in \mathrm{O}(U)$ and $\sigma \in \mathbf{N}_{\mathrm{O}(V)}(\Omega(U))$; furthermore, $\sigma$ is induced by the field automorphism $x \mapsto x^2$ (in a suitable basis of $U$). Hence (8.2.4.1) yields the desired property for the element $\sigma$ in $A$.

(b) Now assume that $\epsilon = +$. Then we consider $U = \mathbb{F}_q^{2n} = \langle u_1, \dots u_n, v_1, \dots, v_n \rangle_{\mathbb{F}_q}$ with the $\mathbb{F}_q$-valued quadratic form $\mathsf{Q}_f(\sum_i (x_i u_i + y_i v_i) = \sum_i x_i y_i$ of type $+$. Also consider the endomorphism

$$\sigma(\sum_i (x_i u_i + y_i v_i) = \sum_i (x_i^2 u_i + y_i^2 v_i) \tag{8.2.4.2}$$

of $U$, induced by the field automorphism $x \mapsto x^2$, and the involution

$$\boldsymbol{j} : u_1 \leftrightarrow v_1,\ u_i \mapsto u_i,\ v_i \mapsto v_i,\ \forall i \geq 2 \tag{8.2.4.3}$$

in $\mathrm{O}(U)$. Arguing as in (a), we see that $\sigma \in \mathrm{O}(V)$, $\sigma$ has order $f$ and normalizes $\Omega(U)$, and we can take $A := \Omega(U) \rtimes \langle \boldsymbol{j}, \sigma \rangle$. Note that $|\mathbf{C}_V(\sigma)| = 2^{2n}$, so $\sigma$ has quasideterminant 1 in $\mathrm{O}(V)$. Furthermore, $|\mathbf{C}_V(\boldsymbol{j})| = q^{2n-1}$. If $2|f$, then $\boldsymbol{j}$ has quasideterminant 1 in $\mathrm{O}(V)$, and so $A \leq \Omega(V)$; in particular, $|\mathbf{C}_V(g)|$ is a power of 4 for any $g \in A$. If $2 \nmid f$, then $\boldsymbol{j}$ has quasideterminant $-1$ in $\mathrm{O}(V)$.

Direct computation shows that $|\mathbf{C}_V(\sigma\boldsymbol{j})|$ equals $2^{2n-1}$ if $2 \nmid f$ and $2^{2n}$ if $2|f$. In particular, we are done if $n = 1$.

(c) Assume now that $\epsilon = +$ but $n > 1$. Then we consider $W = \mathbb{F}^2_{2^{nf}} = \langle u, v \rangle$ with the $\mathbb{F}_{q^n}$-valued quadratic form $\mathsf{Q}_{nf}(xu + yv) = xy$ of type $+$. Also consider the endomorphism

$$\sigma(xu + yv) = x^2u + y^2v$$

of $W$, induced by the field automorphism $x \mapsto x^2$, and the involution $\boldsymbol{j} : u \leftrightarrow v$ in $\mathrm{O}(W)$. Then $W$ can be considered as a $2n$-dimensional vector space $U = \mathbb{F}_q^{2n}$, endowed with the $\mathbb{F}_q$-quadratic form

$$\mathsf{Q}'(v) = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\mathsf{Q}_{nf}(v)).$$

In turn, $U$ can be considered as a $2nf$-dimensional vector space $V = \mathbb{F}_2^{2nf}$, endowed with the $\mathbb{F}_2$-quadratic form

$$\mathsf{Q}'_1(v) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\mathsf{Q}'(v)).$$

Under this identification, $\langle u \rangle_{\mathbb{F}_{q^n}}$ turns into a totally singular subspace of size $q^n$, showing that $\mathsf{Q}'$ and $\mathsf{Q}'_1$ are of type $+$. Hence we may assume $\mathsf{Q}_f = \mathsf{Q}'$ and $\mathsf{Q}_1 = \mathsf{Q}'_1$. The same computations as in part (a) then show that $\sigma^f, \boldsymbol{j} \in \mathrm{O}(U)$ and $\sigma, \boldsymbol{j} \in \mathbf{N}_{\mathrm{O}(V)}(\Omega(U))$. Furthermore, the last sentence in (b) applied to $\sigma\boldsymbol{j}$ then shows that $|\mathbf{C}_V(\sigma\boldsymbol{j})|$ equals 2 if $2 \nmid nf$ and 4 if $2|nf$. □

THEOREM 8.2.5. *In the notation of* (8.2.2.1), *the following statements hold when* $nf \geq 3$.

(i) *If* $g \in H_f^\circ := E \cdot \Omega_{2n}^-(q) < H_f^-$, *then* $|\mathrm{Trace}(g)|^2$ *is either* 0 *or a power of* $q^2 = 2^{2f}$.

(ii) *If* $g \in H_f^-$, *then* $|\mathrm{Trace}(g)|^2$ *is either* 0 *or a power of* $q = 2^f$. *Moreover, there exists some* $h \in H_f^-$ *such that* $|\mathrm{Trace}(h)|^2 = q$.

(iii) *Assume that* $n \geq 2$ *and embed* $H_1^-$ *in* $\mathfrak{G} := \mathrm{Sp}_{2^{nf}}(\mathbb{C})$. *Then there exists* $s \in \mathbf{N}_{H_1^-}(H_f^\circ)$ *such that* $sE$ *induces an outer automorphism of order* $2f$ *of* $H_f^\circ/E \cong \Omega_{2n}^-(q)$, $H_f^- = \langle H_f^\circ, s^f \rangle$, *and* $\mathbf{N}_{\mathfrak{G}}(H_f^\circ) = \langle H_f^\circ, s \rangle \cong H_f^\circ \cdot C_{2f}$. *Furthermore, if* $H_f^\circ \lhd X \leq \mathfrak{G}$ *and* $[X : H_f^\circ] = a_1$, *then we have the following.*

  (a) $a_1|2f$ *and* $X = \langle H_f^\circ, s^{2f/a_1} \rangle$.

  (b) *If* $a_1 = 2a$ *for some* $a|f$, *then* $X$ *contains elements* $t, t'$ *with* $|\mathrm{Trace}(t)|^2 = q^{(2n-1)/a}$, $|\mathrm{Trace}(t')|^2 = q^{(2n-3)/a}$ *if* $a < f$, *and* $|\mathrm{Trace}(t')|^2 = q^{(2n-2)/a}$ *if* $2 \nmid a = f$.

  (c) *If* $2 \nmid a_1$, *then* $X \leq H_{f/a_1}^\circ = E \cdot \Omega_{2na_1}^-(q^{1/a_1})$. *If* $2 \nmid a_1 \geq 3$, *then* $X$ *contains an element* $t$ *with* $|\mathrm{Trace}(t)|^2 = q^{2/a_1}$ *when* $a_1 < f$ *and* $|\mathrm{Trace}(t)|^2 = 2^{2n}$ *when* $a_1 = f$. *If* $2 \nmid a_1 = f \geq 3$ *and* $n \geq 3$, *then* $X$ *contains an element* $t'$ *with* $|\mathrm{Trace}(t')|^2 = 2^{2n-2}$.

PROOF. (i) It is well known, cf. [**GT1**, Lemma 5.8], that $\dim_{\mathbb{F}_q} \mathbf{C}_U(g)$ is even, i.e. $|\mathbf{C}_U(g)|$ is a power of $q^2$. Hence the statement follows from Lemma 7.2.1.

(ii) The first statement follows from Lemma 7.2.1 as in (i). For the second statement, consider an involution $j \in \mathrm{O}_2^+(q)$ and a regular semisimple element $x$ of order $q^{n-1} + 1$ in

$\mathrm{O}^-_{2n-2}(q)$ and set

$$\bar{y} := jx \in \mathrm{O}^+_2(q) \times \mathrm{O}^-_{2n-2}(q) < \mathrm{O}^-_{2n}(q).$$

Then it is straightforward to check that $|\mathbf{C}_U(\bar{y})| = q$. By Lemma 7.2.1, if $y$ is an inverse image of $\bar{y}$ in $H^-_f$, then $|\mathrm{Trace}(h)|^2 = q$ for some $h \in yE$.

(iii) We will choose $s \in H^-_1$ such that the coset $sE$ in $H^-_1/E \cong \mathrm{O}(V)$ corresponds to the element $\sigma$ constructed in Proposition 8.2.3. By its construction, $s \in \mathbf{N}_{H^-_1}(H^\circ_f)$, $sE$ induces an outer automorphism of order $2f$ of $H^\circ_f/E \cong \Omega^-_{2n}(q)$, $H^-_f = \langle H^\circ_f, s^f\rangle$, and $\mathbf{N}_{H^-_1}(H^\circ_f) \geq \langle H^\circ_f, s\rangle \cong H^\circ_f \cdot C_{2f}$. Next, since $E = \mathbf{O}_2(H^\circ_f)$, we have by Theorem 8.2.1 that

$$\mathbf{N}_{\mathfrak{G}}(H^\circ_f) \leq \mathbf{N}_{\mathfrak{G}}(E) = H^-_1.$$

It follows that $E \lhd \mathbf{N}_{\mathfrak{G}}(H^\circ_f)$, and so by Proposition 8.2.3(ii) we obtain

$$\mathbf{N}_{\mathfrak{G}}(H^\circ_f)/E = \mathbf{N}_{\mathrm{O}(V)}(\Omega(U)) = \langle \Omega(U), \sigma\rangle = \langle H^\circ_f, s\rangle/E,$$

yielding the equality $\mathbf{N}_{\mathfrak{G}}(H^\circ_f) = \langle H^\circ_f, s\rangle$.

Now consider any subgroup $X \leq \mathfrak{G}$ that contains $H^\circ_f$ as a normal subgroup. Then $X \leq \mathbf{N}_{\mathfrak{G}}(H^\circ_f)$, and as $\mathbf{N}_{\mathfrak{G}}(H^\circ_f) = \langle H^\circ_f, s\rangle \cong H^\circ_f \cdot C_{2f}$, we must have that $X/H^\circ_f \cong C_{a_1}$ for some $a_1|2f$ and $X = \langle H^\circ_f, s^{2f/a_1}\rangle$. Assume in addition that $a_1 = 2a$, so that $a|f$, and write $b := 2f/a_1 = f/a$. As $|\mathbf{C}_U(\sigma^b)| = q^{(2n-1)/a}$ by Proposition 8.2.3(iii), we can apply Lemma 7.2.1 to find an element $t \in X$ whose coset in $H^-_1/E$ corresponds to $\sigma^b$ and such that $|\mathrm{Trace}(t)|^2 = q^{(2n-1)/a}$. Next, by suitably choosing $t' \in X$ whose coset in $H^-_1/E$ corresponds to the element $\sigma'$ in Proposition 8.2.3(iii), we achieve that $|\mathrm{Trace}(t')|^2$ equals $q^{(2n-3)/a}$ when $a < f$, and equals $q^{(2n-2)/a}$ when $2 \nmid a = f$.

Assume now that $a_1$ is odd. Then $a_1|f$, and so by Proposition 8.2.3(iii) we have that

$$X/E = \langle \Omega(U), \sigma^{2(f/a_1)}\rangle \leq \Omega^-_{2na_1}(q^{1/a_1}) = H^\circ_{f/a_1}/E,$$

i.e. $X \leq H^\circ_{f/a_1}$. Assume in addition that $a_1 \geq 3$. Then we can choose $b := f/a_1$ and repeat the above arguments, but applying Proposition 8.2.3(iv). □

## 8.3. Linear groups in characteristic 2

First we prove the following group-theoretic result, which is a "$p = 2$" version of [**KT2**, Theorem 4.6]. Recall, see [**Zs**], that for any integer $m \geq 2$ and $m \neq 6$, $2^m - 1$ admits a *primitive prime divisor* $\mathrm{ppd}(2, m)$, that is, a prime divisor that does not divide $\prod_{i=1}^{m-1}(2^i - 1)$. Furthermore, if in addition $m \neq 2, 4, 10, 12, 18$, then $2^m - 1$ admits a *large primitive prime divisor*, i.e. a primitive prime divisor $\ell$ where either $\ell > m + 1$ (whence $\ell \geq 2m + 1$), or $\ell^2|(2^m - 1)$, see [**F2**].

THEOREM 8.3.1. *Let $q_0 = 2^f$ be a power of 2 and let $d \geq 2$. Assume in addition that*

$$df \neq 2, 4, 6, 10, 12, 18;$$

*in particular, $2^{df} - 1$ admits a large primitive prime divisor $\ell$, and we choose such an $\ell$ to maximize the $\ell$-part of $2^{df} - 1$. Let $W = \mathbb{F}^d_{q_0}$ and let $G$ be a subgroup of $\mathrm{GL}(W) \cong \mathrm{GL}_d(q_0)$ of order divisible by the $\ell$-part $Q := (q^d_0 - 1)_\ell$ of $q^d_0 - 1$. Then either $L := \mathbf{O}^{\ell'}(G)$ is a cyclic $\ell$-group of order $Q$, or there is a divisor $j < d$ of $d$ such that one of the following statements holds.*

(i) *$L = \mathrm{SL}(W_j) \cong \mathrm{SL}_{d/j}(q_0^j)$, $d/j \geq 3$, and $W_j$ is $W$ viewed as a $d/j$-dimensional vector space over $\mathbb{F}_{q_0^j}$. Furthermore, if $2|df \geq 4$ then $L$ does not fix any $\mathbb{F}_2$-valued non-degenerate quadratic form on $W$ viewed over $\mathbb{F}_2$. Moreover, $L$ does not fix any $\mathbb{F}_2$-valued non-degenerate alternating form on $W$ viewed over $\mathbb{F}_2$.*

(ii) *$2j|d$, $W_j$ is $W$ viewed as a $d/j$-dimensional vector space over $\mathbb{F}_{q_0^j}$ endowed with a non-degenerate symplectic form, and $L = \mathrm{Sp}(W_j) \cong \mathrm{Sp}_{d/j}(q_0^j)$. Furthermore, if $2|df \geq 4$ then $L$ does not fix any $\mathbb{F}_2$-valued non-degenerate quadratic form on $W$ viewed over $\mathbb{F}_2$.*

(iii) *$2|jf$, $2 \nmid (d/j)$, $W_j$ is $W$ viewed as a $d/j$-dimensional vector space over $\mathbb{F}_{q_0^j}$ endowed with a non-degenerate Hermitian form, and $L = \mathrm{SU}(W_j) \cong \mathrm{SU}_{d/j}(q_0^{j/2})$.*

(iv) *$2j|d$, $d/j \geq 4$, $W_j$ is $W$ viewed as a $d/j$-dimensional vector space over $\mathbb{F}_{q_0^j}$ endowed with a non-degenerate quadratic form of type $-$, and $L = \Omega(W_j) \cong \Omega^-_{d/j}(q_0^j)$.*

(v) *$(d, L) = (4j, {}^2B_2(q_0^j))$, $(6j, G_2(q_0^j))$ for some $j \in \mathbb{Z}_{\geq 1}$. Furthermore, if $jf > 1$ then $L$ does not fix any $\mathbb{F}_2$-valued non-degenerate quadratic form on $W$ viewed over $\mathbb{F}_2$.*

(vi) *$(d, q_0, \ell, L) = (8, 2, 17, \mathrm{PSL}_2(17))$, $(20, 2, 41, \mathrm{PSL}_2(41))$. In the former case, $L$ does not fix any $\mathbb{F}_2$-valued non-degenerate quadratic form on $W$.*

Proof. (a) We proceed by induction on $d \geq 2$. For the induction base $d = 2$, note that $L \leq G \cap \mathrm{SL}_2(q_0)$ and $\ell \geq 11$. The list of maximal subgroups of $\mathrm{SL}_2(q_0)$ is well known, see e.g. Tables 8.1 and 8.2 of [**BHR**]. Using this list, one easily checks that either $L \cong C_Q$, or (i) holds with $j = 1$.

(b) For the induction step $d \geq 3$, we will assume that $L \not\cong C_Q$, and apply the main result of [**GPPS**] to see that $G$ is one of the groups described in Examples 2.1–2.9 of [**GPPS**]. By assumption,

$$\text{Either } \ell \geq 2df + 1, \text{ or } Q = (q_0^d - 1)_\ell \geq \ell^2 \geq (df + 1)^2. \tag{8.3.1.1}$$

If $G$ is described in Example 2.1 of [**GPPS**], then $a_0 = 1$ since $\ell = \mathrm{ppd}(2, df)$. Furthermore, one of (i)–(iv) holds, with $j = 1$.

Next, as $\ell$ does not divide the order of any (maximal) parabolic subgroup of $\mathrm{GL}(W) \cong \mathrm{GL}_d(q_0)$, $G$ must act irreducibly on $W$, and so cannot be any of the groups in Example 2.2 of [**GPPS**]. Likewise, the condition $\ell||G|$ rules out all the groups listed in Example 2.3 of [**GPPS**]. Next, Example 2.5 of [**GPPS**] does not occur in characteristic 2, which is our case.

(c) Suppose $G$ is among the groups described in Example 2.4 of [**GPPS**]. Again, as $\ell > df$, $G$ can appear only in Example 2.4(b) of [**GPPS**]. Thus there is a divisor $1 < j|d$ and $W$ is endowed with the structure of a $d/j$-dimensional vector space $W_j$ over $\mathbb{F}_{q_0^j}$, and $G \leq \mathrm{GL}(W_j) \rtimes C_j$, where $C_j$ is the group of field automorphisms of $\mathbb{F}_{q_0^j}$ over $\mathbb{F}_q$. Note that $j \leq d \leq df < \ell$, so $L$ is contained in $\mathrm{GL}(W_j) \cong \mathrm{GL}_{d/j}(q_0^j)$ and has order divisible by $Q = ((q_0^j)^{d/j} - 1)_\ell = Q$. If $j = d$, then $L \cong C_Q$, contrary to our assumption. If $d/j = 2$, then the induction base implies that (i) holds with $j = d/2$. If $d/j \geq 3$, then the induction hypothesis then implies that one of (i)–(v) holds.

(d) In Examples 2.6–2.9 of [**GPPS**], $S \lhd G/(G \cap Z) \leq \mathrm{Aut}(S)$ for some non-abelian simple group $S$, where $Z := \mathbf{Z}(\mathrm{GL}_d(q_0)) \cong C_{q_0-1}$ and the full inverse image $N$ of $S$ in $G$ acts absolutely irreducibly on $W$. Moreover, $G \leq \mathrm{GL}_d(q_1) * Z$ for some root $q_1$ of $q_0$. If $q_1 < q_0$, then $|G|$ is not divisible by $\ell = \mathrm{ppd}(2, df)$. Hence $q_1 = q_0$, i.e. $\mathbb{F}_{q_0}$ is the smallest field over which $G$ is realizable modulo scalars (in the sense of [**GPPS**, p. 172]).

In Example 2.6 of [**GPPS**] we have $S = \mathsf{A}_n$; in particular, $\ell \leq n$. First, in Example 2.6(a) of [**GPPS**] we have $n-2 \leq d \leq n-1$, and so $\ell \geq d+1 \geq n-1 > n/2$, whence $\ell^2 \nmid |G|$. As $\ell$ is a large primitive prime divisor, we then have $\ell \geq 2d+1 > n$ and so $\ell \nmid |G|$, a contradiction. Example 2.6(b) of [**GPPS**] does not occur in characteristic 2. In Example 2.6(c) of [**GPPS**], we must have that $\ell = 7$ and $d = 4$, but then $\ell$ cannot be a primitive prime divisor of $2^{df} - 1$.

In Example 2.7 of [**GPPS**], $S$ is a sporadic simple group. With $\ell$ being a primitive prime divisor of $2^{df} - 1$, we are in one of the following cases:

$$(G', d, \ell) = (M_{11}, 10, 11),\ (M_{12}, 10, 11),\ (M_{22}, 10, 11),\ (Ru, 28, 29),$$
$$(M_{23}, 11, 23),\ (M_{24}, 11, 23),\ (3J_3, 9, 19).$$

In the first four cases, we have $\ell = d+1$ and $\ell^2 \nmid |G|$, contradicting the largeness of $\ell$. In the next two cases with $(d, \ell) = (11, 23)$, since $\ell^2 \nmid |G|$ and $\ell = 2d+1$, the largeness of $\ell$ implies that $f = 1$. But in this situation, we can choose 89 as a primitive prime divisor of $2^{df} - 1$, and this contradicts the maximality of $Q$. In the last case of $(3J_3, 9, 19)$, as $19^2 \nmid |G|$ and $3J_3 \not\hookrightarrow \mathrm{SL}_9(2)$, we must have that $f = 2$, giving $df = 18$.

In Example 2.8 of [**GPPS**], $S$ is a simple group of Lie type in the same characteristic 2. The condition $\ell = \mathrm{ppd}(2, df)$ leads to $(d, L) = (4, {}^2B_2(q_1))$, $(6, G_2(q_1))$ with $q_1 = q_0$, and we arrive at possibility (v) with $j = 1$.

In Example 2.9 of [**GPPS**], $S$ is a simple group of Lie type in characteristic $\neq 2$ and appears in Tables 7 and 8 of [**GPPS**]. The only case in Table 7 that occurs in characteristic 2 is $G_2(3)$ with $d = 14$ which however does not permit the primitive prime divisor $\ell$ to exist. Consider the case when $S$ appears in Table 8 of [**GPPS**]. Using the fact that $\ell$ is a large prime divisor of $2^{df} - 1$, we can again rule out all cases except for the case $(d, \ell, S) = ((\ell-1)/2, \ell, \mathrm{PSL}_2(\ell))$. In this case, $|G|_\ell = \ell = 2d+1$, and the largeness of $\ell$ forces $f = 1$. To handle this last case, we use a strengthening [**Tr**, Theorem 3.2.2] of the main result of [**F2**], proved by A. MacLaughlin and S. Trefethen. This result asserts that, $\ell$ can be chosen so that $(2^d - 1)_\ell > 2d + 1$, unless $d \in \{2, 3, 4, 6, 8, 10, 12, 18, 20\}$. Given our assumptions on $(d, f)$ and the fact that $\mathrm{PSL}_2(7) \cong \mathrm{SL}_3(2)$, we are left with the two last possibilities in (vi). Note that $\mathrm{PSL}_2(17)$ is a maximal subgroup of $\mathrm{Sp}_8(2)$ [**CCNPW**], so cannot embed in $\Omega_8^\pm(2)$.

Suppose now that $2|df \geq 4$ and $\mathsf{Q}$ is any $\mathbb{F}_2$-valued non-degenerate quadratic form. Then it takes both values 0 and 1 on $W \smallsetminus \{0\}$, and so any subgroup of $\mathrm{O}(\mathsf{Q})$ cannot act transitively on $W \smallsetminus \{0\}$. Since the group $L$ in (i) and (ii) are transitive on $W \smallsetminus \{0\}$, in none of these cases $G$ can fix $\mathsf{Q}$. The same applies to the case $L = G_2(q_0^j)$ in (v), see [**Li**, Appendix 1]. Consider the case $L = {}^2B_2(q_0^j)$ in (v), in which case $L$ has two orbits, of length $q_0^j(q_0^{2j}+1)(q_0^j-1)$ and $(q_0^{2j}+1)(q_0^j-1)$ on $W \smallsetminus \{0\}$, see [**Li**, Table 12]. These orbits must then match the sets of (nonzero) $\mathsf{Q}$-isotropic and $\mathsf{Q}$-anisotropic vectors on $W$, which are however of size $(q_0^{2j}+1)(q_0^{2j}/2-1)$ and $q_0^{2j}(q_0^{2j}+1)/2$, a contradiction.

Finally, suppose we are in case (i) and $L$ fixes a non-degenerate symplectic form on $\mathbb{F}_2^{df}$, which implies $L \hookrightarrow \mathrm{Sp}_{df}(2)$. Then we can find an element $g \in L$ of order $|g| = (q_0^d - 1)/(q_0^j - 1) = (2^{df}-1)/(q_0^j - 1)$ which is divisible by $\ell = \mathrm{ppd}(2, df)$. Such an element $g$ is irreducible on $\mathbb{F}_2^{df}$, hence $|g|$ divides $2^{df/2}+1$ by [**Hup**, Satz II.9.23], which is impossible since $j \leq d/3$. $\square$

The case $df = 6$ is a real exception in Theorem 8.3.1, since $2^6 - 1$ does not possess any primitive prime divisor. Before dealing with the remaining exceptions in Theorem 8.3.1, we record the following well-known facts:

LEMMA 8.3.2. *Let $\mathbb{F}$ be a finite field and $W$ a finite-dimensional vector space over $\mathbb{F}$. Let $G \leq \mathrm{GL}(W)$ be an irreducible subgroup. Then the following statements hold.*

(a) *$\mathbb{E} := \mathrm{End}_G(W)$ is a finite field containing $\mathbb{F}$. Moreover, $W$ is endowed with a structure of $\mathbb{E}G$-module structure $W_{\mathbb{E}}$, compatible with the action of $G$ on $W$, such that $W_{\mathbb{E}}$ is absolutely irreducible.*

(b) *Suppose that $W$ can be endowed with a structure of $\mathbb{L}G$-module structure $W_{\mathbb{L}}$, compatible with the action of $G$ on $W$, for some finite extension $\mathbb{L}$ of $\mathbb{F}$, and that $W_{\mathbb{L}}$ is absolutely irreducible. Then $\mathbb{E} \cong \mathbb{L}$; in fact, it is the set of scalar maps on $W_{\mathbb{L}}$.*

PROOF. (a) By Schur's lemma, $\mathbb{E}$ is a finite division ring, hence a field in which $\mathbb{F}$ embeds via $\alpha \mapsto \alpha \cdot \mathrm{id}_W$. Now for any $\beta \in \mathbb{E}$ we define

$$\beta \cdot v = \beta(v) \tag{8.3.2.1}$$

for all $v \in W$, and this turns $W$ into an $\mathbb{E}G$-module $W_{\mathbb{E}}$. If $W_1$ is any nonzero $\mathbb{E}G$-submodule of $W_{\mathbb{E}}$, then it is also a submodule of $W$, whence $W_1 = W_{\mathbb{E}}$ and thus $W_{\mathbb{E}}$ is irreducible. Next, $\mathbf{C}_{\mathrm{End}(W_{\mathbb{E}})}(G)$ contains $\mathbb{E}$ (by the definition of $W_{\mathbb{E}}$), and is contained in $\mathbf{C}_{\mathrm{End}(W)}(G) = \mathrm{End}_G(W) = \mathbb{E}$, so

$$\mathbf{C}_{\mathrm{End}(W_{\mathbb{E}})}(G) = \mathbb{E}. \tag{8.3.2.2}$$

The latter implies by [**Is**, Theorem 9.2] that $W_{\mathbb{E}}$ is absolutely irreducible.

(b) Since $W_{\mathbb{L}}$ is absolutely irreducible, $\mathbf{C}_{\mathrm{End}(W_{\mathbb{L}})}(G) \cong \mathbb{L}$ again by [**Is**, Theorem 9.2]. As $\mathrm{End}(W_{\mathbb{L}}) \subseteq \mathrm{End}(W)$, we have that $\mathbb{L} \subseteq \mathbb{E}$. Now $W_{\mathbb{E}}$ can be obtained from $W_{\mathbb{L}}$ via (8.3.2.1), and $\mathrm{End}(W_{\mathbb{E}}) \subseteq \mathrm{End}(W_{\mathbb{L}})$, so (8.3.2.2) implies that $\mathbb{E} \subseteq \mathbf{C}_{\mathrm{End}(W_{\mathbb{L}})}(G) = \mathbb{L}$. Thus $\mathbb{E} = \mathbb{L}$. □

PROPOSITION 8.3.3. *Let $q_0 = 2^f$ be a power of 2 and let $d \geq 2$. Assume in addition that*

$$df \in \{2, 4, 10, 12, 18\};$$

*in particular, $2^{df} - 1$ admits a primitive prime divisor $\ell$. Let $W = \mathbb{F}_{q_0}^d$ and let $G$ be a subgroup of $\mathrm{GL}(W) \cong \mathrm{GL}_d(q_0)$ of order divisible by the $\ell$-part $Q := (q_0^d - 1)_\ell$ of $q_0^d - 1$. Then either $L := \mathbf{O}^{\ell'}(G)$ is a cyclic $\ell$-group of order $Q$, or one of the following statements holds.*

(i) *There is a divisor $j < d$ of $d$ such that one of the conclusions* (i)–(v) *of Theorem 8.3.1 holds.*

(ii) *$(d, q_0, \ell) = (4, 2, 5)$ and $L \cong \mathsf{A}_6$ or $\mathsf{A}_7$.*

(iii) *$(d, q_0, \ell, L) = (5, 4, 11, \mathrm{PSL}_2(11))$.*

(iv) *$(d, q_0, \ell, L) = (6, 4, 13, \mathrm{PSL}_2(13))$.*

(v) *$(d, q_0, \ell) = (9, 4, 19)$, and $L \cong 3 \cdot \mathsf{J}_3$ or $\mathrm{PSL}_2(19)$.*

(vi) *$(d, q_0, \ell) = (10, 2, 11)$ and $L \in \{\mathrm{PSL}_2(11), M_{11}, M_{12}, M_{22}, \mathsf{A}_{11}, \mathsf{A}_{12}\}$.*

(vii) *$(d, q_0, \ell) = (12, 2, 13)$ and $L \in \{\mathrm{PSL}_2(13), \mathrm{PSL}_2(25), \mathrm{SL}_3(3), \mathsf{A}_{13}, \mathsf{A}_{14}\}$.*

(viii) *$(d, q_0, \ell) = (18, 2, 19)$ and $L \in \{3 \cdot \mathsf{J}_3, \mathrm{PSL}_2(19), \mathsf{A}_{19}, \mathsf{A}_{20}\}$.*

PROOF. The case $df = 2$ is obvious, and the case $df = 4$ can be checked using [**CCNPW**]. So we will assume that $df \geq 10$, so that $\ell \geq 11$, and that $L \not\cong C_Q$. We also assume that $L \neq \mathrm{SL}_d(q_0)$, as otherwise 8.3.1(i) holds with $j = 1$.

(a) We will argue by a partial induction on $d \geq 2$. First, part (a) of the proof of Theorem 8.3.1 already handles the case $d = 2$. Next assume that $d = 3$. As $q \geq 16$ in this case, $L \leq \mathbf{O}^{\ell'}(\mathrm{GL}_3(q_0)) = \mathrm{SL}_3(q_0)$. As $L \neq \mathrm{SL}_3(q_0)$, $L \leq M$ for some maximal subgroup $M$ of $\mathrm{SL}_3(q_0)$, whence $L \leq \mathbf{O}^{\ell'}(M)$. The list of maximal subgroups of $\mathrm{SL}_3(q_0)$ is given in Tables 8.3 and 8.4 of [**BHR**], and using the condition $\ell|\mathbf{O}^{\ell'}(M)|$ we see that $L \leq \mathrm{SU}_3(q_0^{1/2})$. Now we can apply the same argument and use the list of maximal subgroups of $\mathrm{SU}_3(q_0^{1/2})$ [**BHR**, Tables 8.5, 8.6] to conclude that $L = \mathrm{SU}_3(q_0^{1/2})$, i.e. 8.3.1(ii) holds with $j = 1$.

Next assume that $d = 4$, so that $df = 12$ and $q_0 = 8$. As above we have that $\mathrm{SL}_4(q_0) \neq L \leq \mathbf{O}^{\ell'}(\mathrm{GL}_4(q_0)) = \mathrm{SL}_4(q_0)$, and so $L \leq \mathbf{O}^{\ell'}(M)$ for some maximal subgroup $M$ of $\mathrm{SL}_4(q_0)$. Inspecting the list of maximal subgroups of $\mathrm{SL}_4(8)$ as given in [**BHR**, Tables 8.8, 8.9], we have $L$ is contained in (a natural subgroup) $\mathrm{SL}_2(q_0^2)$ or $\mathrm{Sp}_4(q_0)$. In the first case, the result of the case $d = 2$ implies that $L = \mathrm{SL}_2(q_0^2)$, i.e. 8.3.1(i) holds with $j = 2$. If $L = \mathrm{Sp}_4(q_0)$ then 8.3.1(ii) holds with $j = 1$. If not, $L \leq \mathbf{O}^{\ell'}(N)$ for some maximal subgroup $N$ of $\mathrm{Sp}_4(q_0)$, and using the list of maximal subgroups of $\mathrm{Sp}_4(q_0)$ [**BHR**, Table 8.14], we obtain $L$ is contained in (a natural subgroup) $\mathrm{Sp}_2(q_0^2)$, $\Omega_4^-(q_0)$, or ${}^2B_2(q_0)$. Now the results for $d = 2$ and the list of maximal subgroups of ${}^2B_2(q_0)$ [**BHR**, Table 8.16] shows that $L = \mathrm{Sp}_2(q_0^2)$, $\Omega_4^-(q_0)$, or ${}^2B_2(q_0)$, i.e. 8.3.1(ii), (iv), or (v) holds.

Consider the case $d = 5$, so that $df = 10$ and $q_0 = 4$. Then $L \leq \mathbf{O}^{\ell'}(\mathrm{GL}_5(q_0)) = \mathrm{SL}_5(q_0)$. As $L \neq \mathrm{SL}_5(q_0)$, $L \leq M$ for some maximal subgroup $M$ of $\mathrm{SL}_5(q_0)$, whence $L \leq \mathbf{O}^{\ell'}(M)$. The list of maximal subgroups of $\mathrm{SL}_5(q_0)$ is given in Tables 8.18 and 8.19 of [**BHR**], and using the condition $\ell|\mathbf{O}^{\ell'}(M)|$ we see that $L \leq \mathrm{SU}_5(2)$. Using the list of maximal subgroups of $\mathrm{SU}_5(2)$ and $\mathrm{PSL}_2(11)$ [**CCNPW**], we see that $L = \mathrm{SU}_5(2)$ or $\mathrm{PSL}_2(11)$, i.e. either 8.3.1(iii) holds or we arrive at (iii).

Now let $d = 6$, so that $df = 12$ or $18$, and $q_0 = 4$ or $8$. As above we have $\mathrm{SL}_6(q_0) \neq L \leq \mathbf{O}^{\ell'}(\mathrm{GL}_6(q_0)) = \mathrm{SL}_6(q_0)$, and so $L \leq \mathbf{O}^{\ell'}(M)$ for some maximal subgroup $M$ of $\mathrm{SL}_6(q_0)$. Inspecting the list of maximal subgroups of $\mathrm{SL}_6(q_0)$ as given in [**BHR**, Tables 8.24, 8.25], we have that $L$ is contained in (a natural subgroup) $\mathrm{SL}_2(q_0^3)$, $\mathrm{SL}_3(q_0^2)$, or $\mathrm{Sp}_6(q_0)$. In the first two cases, the results of the cases $d = 2$ and $d = 3$ imply that $L = \mathrm{SL}_2(q_0^3)$, $\mathrm{SL}_3(q_0^2)$, or $\mathrm{SU}_3(q_0)$, i.e. either 8.3.1(i) holds with $j = 2, 3$, or 8.3.1(iii) holds with $j = 2$. If $L = \mathrm{Sp}_6(q_0)$ then 8.3.1(ii) holds with $j = 1$. If not, $L \leq \mathbf{O}^{\ell'}(N)$ for some maximal subgroup $N$ of $\mathrm{Sp}_6(q_0)$, and using the list of maximal subgroups of $\mathrm{Sp}_6(q_0)$ [**BHR**, Tables 8.28, 8.29], we obtain $L$ is contained in (a natural subgroup) $\mathrm{Sp}_2(q_0^3)$, $\Omega_6^-(q_0)$, or $G_2(q_0)$. Now the results for $d = 2$ and the lists of maximal subgroups of $\Omega_6^-(q_0)$ and $G_2(q_0)$ [**BHR**, Tables 8.33, 8.34, 8.30] show that $L = \mathrm{Sp}_2(q_0^3)$, $\Omega_6^-(q_0)$, $G_2(q_0)$, $\mathrm{SU}_3(q_0)$, i.e. 8.3.1(ii), (iii), (iv), or (v) holds, or $q_0 = 4$ and $L = \mathrm{PSL}_2(13)$.

Next we consider the case $d = 9$ and $q_0 = 4$. Again, $\mathrm{SL}_9(4) \neq L \leq \mathbf{O}^{\ell'}(\mathrm{GL}_9(4)) = \mathrm{SL}_9(4)$, and so $L \leq \mathbf{O}^{\ell'}(M)$ for some maximal subgroup $M$ of $\mathrm{SL}_9(4)$. Inspecting the list of maximal subgroups of $\mathrm{SL}_9(4)$ as given in [**BHR**, Tables 8.54, 8.55], we have that $L$ is contained in (a natural subgroup) $\mathrm{SL}_3(q_0^3)$ or $\mathrm{SU}_9(2)$. In the first case, the result of the case $d = 3$ implies that $L = \mathrm{SL}_3(q_0^3)$, i.e. 8.3.1(i) holds with $j = 3$. If $L \leq \mathrm{SU}_9(2)$ then, using the list of maximal subgroups of $\mathrm{SU}_9(2)$ [**BHR**, Tables 8.56, 8.57], we see that $L = \mathrm{SU}_9(2)$, $\mathrm{SU}_3(8)$, i.e. 8.3.1(iii) holds with $j = 1, 3$, or $L = 3 \cdot J_3$ or $\mathrm{PSL}_2(19)$, i.e. we are in (v).

(b) It remains to consider the cases where $f = 1$ and $d \in \{10, 12, 18\}$. First we note that $L$ is irreducible on $W = \mathbb{F}_2^d$ since $|L|$ is disivible by $\ell = d + 1$. Now if the $L$-module $V$ is not absolutely irreducible, then $\mathbb{E} := \mathrm{End}_L(W)$ is a finite field of order $2^j$ for some $2 \leq j|d$, and $W$ becomes an absolutely irreducible $\mathbb{E}L$-module of dimension $d/j$ by Lemma 8.3.2(i). In this case, $L \leq \mathrm{GL}_{d/j}(2^j)$, and we are done by the results of (b). So we may assume $L$ is absolutely irreducible on $W$ but $L < \mathrm{SL}_d(2)$, and apply [**KlL**, Theorem 1.2.1] to $L$, to see that either $L = \mathbf{O}^{\ell'}(L)$ is simple, or $L \leq \mathrm{Sp}_d(2)$. In the first case, using [**HM**] we arrive at (vi)–(viii). Assuming $L$ is not simple, we then have $L < \mathrm{Sp}_d(2)$ (as otherwise 8.3.1(ii) holds). Applying [**KlL**, Theorem 1.2.1] we get $L \leq \Omega_d^-(2)$. Applying [**KlL**, Theorem 1.2.1] one more time, we obtain $L = \Omega_d^-(2)$, i.e. 8.3.1(iv) holds. □

Theorem 8.3.4. *Let $q = 2^f$ be a power of 2 and let $n > m \geq 1$ with $2|mn$, $\gcd(m, n) = 1$, and $nf \geq 4$. Let $W = \mathbb{F}_2^{2nf}$ and let $\mathsf{Q}$ be a non-degenerate $\mathbb{F}_2$-valued quadratic form on $W$. Suppose $G$ is a subgroup of $\mathrm{GL}(W) \cong \mathrm{GL}_{2nf}(2)$ of order divisible by $\mathrm{lcm}(q^n + 1, q^m + 1, q^{n-m} - 1)$ that fixes $\mathsf{Q}$. Then, with $\ell$ as chosen in Theorem 8.3.1 and Proposition 8.3.3, $L := \mathbf{O}^{\ell'}(G)$ is not cyclic.*

*Suppose in addition that the action of $L$ on $W$ carries an $\mathbb{F}_q$-structure. Then one of the following statements holds.*

(a) *$L = \Omega(W_f) \cong \Omega_{2n}^-(q)$, where $W_f$ is $W$ viewed as a $2n$-dimensional vector space over $\mathbb{F}_q$ endowed with a non-degenerate quadratic form $\mathsf{Q}_f$ of type $-$. Moreover, there is $\alpha \in \mathbb{F}_q^\times$ such that $\mathsf{Q}(u) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\alpha \cdot \mathsf{Q}_f(u))$ for all $u \in W_f$.*

(b) *$(n, m, q) = (5, 2, 2)$ and $L \in \{\mathsf{A}_{11}, \mathsf{A}_{12}\}$.*

Proof. (i) First we note that $2|mn$ and $\gcd(m, n) = 1$ imply by Lemma 10.3.2 that

$$\gcd(q^n + 1, q^m + 1) = \gcd(q^n + 1, q^{n-m} - 1) = \gcd(q^m + 1, q^{n-m} - 1) = 1, \tag{8.3.4.1}$$

and so $|G|$ is divisible by $(q^n + 1)(q^m + 1)(q^{n-m} - 1)$. By assumption, $2^{2nf} - 1$ admits a primitive prime divisor $\ell$ [**Zs**], which we can choose to be a large primitive prime divisor when $nf \neq 5, 6, 9$ [**F2**]. Among such $\ell$, choose $\ell$ to maximize the $\ell$-part of $2^{2nf} - 1$. Again by hypothesis, $|G|$ is divisible by $Q := (q^{2n} - 1)_\ell$, hence we can apply Theorem 8.3.1 and Proposition 8.3.3, with $q_0 = 2$, to the $\mathbb{F}_2$-vector space $W$ to determine $L$. By the choice of $\ell$, any element of order $\ell$ in $\mathrm{O}(\mathsf{Q})$ acts irreducibly on $W$, and is contained in a conjugate of a fixed cyclic maximal torus $T$ of order $q^n + 1$ with normalizer $T \cdot C_{2nf}$ in $\mathrm{O}(\mathsf{Q})$.

Suppose $L \cong C_Q$. Then we may assume $L$ is the unique $C_Q$-subgroup of $T$, whence $G \leq T \cdot C_{2nf}$ and so $(q^m + 1)(q^{n-m} - 1)$ divides $nf$. Note that $2^a - 1 > 2a$ whenever $a \in \mathbb{Z}_{\geq 3}$ and $2^a + 1 > 2a$ whenever $a \in \mathbb{Z}_{\geq 1}$. Now, if $m < n/2$, then since $2 \nmid (n - m)$ we have $n - m \geq 3$, whence $q^{n-m} - 1 > 2(n - m)f > nf$, a contradiction. Now, if $m \geq n/2$, then $q^m + 1 > 2mf \geq nf$, again a contradiction.

We have shown that $L \not\cong C_Q$. As mentioned above, any element of order $\ell$ in $L$ is regular semisimple in $\mathrm{O}(\mathsf{Q})$ and has centralizer conjugate to $T \cong C_{q^n+1}$. Hence, (8.3.4.1) implies that the order of $\mathbf{C}_G(L) \leq \mathbf{C}_{\mathrm{O}(\mathsf{Q})}(L)$ is coprime to $(q^m + 1)(q^{n-m} - 1)$. As $L \lhd G$, it follows that

$$(q^m + 1)(q^{n-m} - 1) \text{ divides } |\mathrm{Aut}(L)|. \tag{8.3.4.2}$$

Note that $Q$ divides $|L|$. By Theorem 8.3.1 and Proposition 8.3.3, but now applied to $W$ viewed as an $\mathbb{F}_qL$-module, we have one of the following cases.

(ii) There is some divisor $j \in \mathbb{Z}_{\geq 1}$ of $n$ such that $j < n$, $2 \nmid n/j$, and $L = \mathrm{SU}(W_j) \cong \mathrm{SU}_{n/j}(q^j)$, where $W_j$ is $W$ viewed as an $n/j$-dimensional vector space over $\mathbb{F}_{q^{2j}}$ endowed with a non-degenerate Hermitian form. Note that $m \neq n/2$, because otherwise we have $(n, m, j) = (2, 1, 1)$ and so $2|(n/j)$.

First consider the case $m < n/2$. Then $2 \nmid (n-m) \geq 3$. Assume in addition that $(n-m)f \neq 6$. Then by [**Zs**] we can find a primitive prime divisor $\ell_1$ of $2^{(n-m)f} - 1$ which certainly divides $q^{n-m} - 1$ and is at least $(n-m)f + 1 \geq \max(3f+1, n/2+1)$. On the other hand, $|\mathrm{Aut}(L)| = |\mathrm{PGU}_{n/j}(q^j)| \cdot 2jf$, with $j \leq n/3$. So (8.3.4.2) implies that $\ell_1$ divides $|\mathrm{PGU}_{n/j}(q^j)|$, and so there exists some $i \leq n/j$ such that $\ell_1|(q^{ij} - (-1)^i)$. Hence $\ell_1|(q^{2ij} - 1)$, and the primitivity of $\ell_1$ implies that $(n-m)|2ij$. As $2 \nmid (n-m)$, we have $(n-m)|ij$. But $ij \leq n < 2(n-m)$, so $ij = n-m$ and thus $2 \nmid i$, in which case $\ell_1$ divides $q^{ij} - (-1)^i = q^{n-m} + 1$, a contradiction. Suppose now that $(n-m)f = 6$, i.e. $(n-m, q) = (3, 4)$. Then we have $(n, m) = (4, 1)$ or $(5, 2)$. Now we can take $\ell_1 = 7$, which is a primitive prime divisor for $q^{n-m} - 1$, and repeat the preceding argument.

We have shown that $m > n/2$. Assume in addition that $mf \neq 3$. Then by [**Zs**] we can find a primitive prime divisor $\ell_2$ of $2^{2mf} - 1$ which then divides $q^m + 1$ and is at least $2mf + 1 > nf + 1$. As $j \leq n/3$, (8.3.4.2) implies that $\ell_2$ divides $|\mathrm{PGU}_{n/j}(q^j)|$, and so there exists some $i \leq n/j$ such that $\ell_2|(q^{ij} - (-1)^i)$. Hence $\ell_2|(q^{2ij} - 1)$, and the primitivity of $\ell_2$ implies that $m|ij \leq n < 2m$, and so $ij = m$. Now if $2 \nmid n$, then $2 \nmid j$ and $2|m$, so $2|i$, and $\ell_2$ divides $q^{ij} - (-1)^i = q^m - 1$, a contradiction. If $2|n$, then $2 \nmid m$, whence $2 \nmid j$ and so $2|n/j$, again a contradiction. Suppose now that $mf = 3$, i.e. $(m, q) = (3, 2)$. As $2|n < 2m$, we have $n = 4$, in which case there is no divisor $j < n$ of $n$ with $2 \nmid (n/j)$.

(iii) There is some divisor $j \leq n/2$ of $n$ such that $L = \Omega(W_{jf}) \cong \Omega^-_{2n/j}(q^j)$, where $W_{jf}$ is $W$ viewed as a $2n/j$-dimensional vector space over $\mathbb{F}_{q^j}$ endowed with a non-degenerate quadratic form $\mathsf{Q}_{jf}$ of type $-$. In this case, $\mathrm{Aut}(L) \cong \mathrm{O}^-_{2n/j}(q^j) \cdot C_{jf}$. We will show that

$$j = 1. \tag{8.3.4.3}$$

First, if $m = n/2$, then $(n, m) = (2, 1)$ and so $j = 1$. Next we consider the case $m < n/2$. Then $2 \nmid (n-m) \geq 3$. Assume in addition that $(n-m)f \neq 6$. Then by [**Zs**] we can find a primitive prime divisor $\ell_1$ of $2^{(n-m)f} - 1$ which then divides $q^{n-m} - 1$ and is at least $(n-m)f + 1 \geq \max(3f+1, n/2+1)$. As $j \leq n/2$, (8.3.4.2) implies that $\ell_1$ divides $|\mathrm{O}^-_{2n/j}(q^j)|$, and so there exists some $i \leq n/j$ such that $\ell_1|(q^{2ij} - 1)$. Hence the primitivity of $\ell_1$ implies that $(n-m)|2ij$. As $2 \nmid (n-m)$, we have $(n-m)|ij$. But $ij \leq n < 2(n-m)$, so $ij = n-m$. It follows that $j$ divides both $n$ and $m$, and hence $j = 1$, as stated in (8.3.4.3). Suppose now that $(n-m)f = 6$, i.e. $(n-m, q) = (3, 4)$. Then we have $(n, m) = (4, 1)$ or $(5, 2)$. Now we can take $\ell_1 = 7$, which is a primitive prime divisor for $q^{n-m} - 1$, and repeat the preceding argument.

Now suppose that $m > n/2$. Assume in addition that $mf \neq 3$. Then by [**Zs**] we can find a primitive prime divisor $\ell_2$ of $2^{2mf} - 1$ which then divides $q^m + 1$ and is at least $2mf + 1 > nf + 1$. As $j \leq n/3$, (8.3.4.2) implies that $\ell_2$ divides $|\mathrm{O}^-_{2n/j}(q^j)|$, and so there exists some $i \leq n/j$ such that $\ell_2|(q^{2ij} - 1)$. Hence the primitivity of $\ell_2$ implies that $m|ij \leq n < 2m$, and so $ij = m$. It follows that $j|\gcd(n, m) = 1$, as desired in (8.3.4.3). Suppose now that $mf = 3$, i.e. $(m, q) = (3, 2)$, but $j > 1$. As $2|n < 2m$, we have $n = 4$ and $j = 2$. In this case, the order of $\mathrm{Aut}(L) = \mathrm{Aut}(\Omega_4^-(q^2)) = \mathrm{Aut}(\mathrm{SL}_2(16)) \cong \mathrm{SL}_2(16) \cdot 4$ is not divisible by $9 = q^3 + 1$, contrary to (8.3.4.2).

With (8.3.4.3) established, consider the non-degenerate $L$-invariant $\mathbb{F}_q$-valued alternating form $(\cdot|\cdot)_f$ on $W_f$ associated to $\mathsf{Q}_f$, which leads to the non-degenerate $L$-invariant $\mathbb{F}_2$-valued alternating form $(u|v)_1 := \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}\big((u|v)_f\big)$. Fix a basis of $W$ as $\mathbb{F}_2$-vector space, and consider the Gram matrices of $(\cdot|\cdot)_1$ and of the form $(\cdot|\cdot)$ associated to $\mathsf{Q}$ relative to this basis:

$$(u|v)_1 = {}^t\!uJ_1v,\ \ (u|v) = {}^t\!uJv$$

for any $u, v \in W$ written as coordinate vectors in $\mathbb{F}_2^{2nf}$ with respect to this basis. For any element of $L$ written as a matrix $X$ in this basis, the $L$-equivariance of the two forms implies that

$$({}^tX)^{-1} = JXJ^{-1} = J_1XJ_1^{-1},$$

hence $J_1^{-1}J \in \mathrm{GL}(W)$ commutes with all $X \in L$ and thus $J_1^{-1}J \in \mathrm{End}_L(W) \cong \mathbb{F}_q$ by Lemma 8.3.2(ii). It follows that there is a scalar $\alpha \in \mathbb{F}_q^\times$ such that $J = J_1T_\alpha$, where $T_\alpha$ is the matrix of the transformation $x \mapsto \alpha x$ on $W$ written in the chosen basis, and so

$$(u|v) = {}^t\!uJv = {}^t\!uJ_1T_\alpha v = (u|T_\alpha v)_1.$$

Back to viewing $u, v$ as vectors in $W$, we now have

$$(u|v) = (u|\alpha v)_1 = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}\big(\alpha(u|v)_f\big).$$

Rescaling $(\cdot|\cdot)_f$ by $\alpha$, we may therefore assume that $(u|v) = (u|v)_1$. Now $L$ fixes quadratic forms $\mathsf{Q}$ and $\mathsf{Q}_1 := \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\mathsf{Q}_f)$, which are both associated to $(\cdot|\cdot)$. Hence $L$ fixes $\mathsf{Q} - \mathsf{Q}_1$, a map in $\mathrm{Hom}_{\mathbb{F}_2}(W, \mathbb{F}_2)$, which can be identified with $W$ using $(\cdot|\cdot)$. Since $L$ has no nonzero fixed point on $W$, it follows that $\mathsf{Q} = \mathsf{Q}_1$, and we arrive at (a).

(iv) $(2n, q, L) = (8, 2, \mathrm{PSL}_2(17))$, $(20, 2, \mathrm{PSL}_2(41))$. Here, (8.3.4.2) implies that $(2^m + 1)(2^{n-m} - 1)$ divides 9, respectively $5 \cdot 21$, a contradiction.

(v) $(2n, q) = (18, 2)$ and $L \in \{3 \cdot J_3, \mathrm{PSL}_2(19), \mathsf{A}_{19}, \mathsf{A}_{20}\}$. Here, $m = 2$, 4, or 8, hence $(2^m + 1)(2^{n-m} - 1)$ is divisible by 127, 31, or 257, respectively, and so cannot divide $|\mathrm{Aut}(L)|$, contrary to (8.3.4.2).

(vi) $(2n, q) = (12, 2)$ and $L \in \{\mathrm{PSL}_2(13), \mathrm{PSL}_2(25), \mathrm{SL}_3(3), \mathsf{A}_{13}, \mathsf{A}_{14}\}$. Here, $m = 1$ or 5, hence $(2^m + 1)(2^{n-m} - 1)$ is divisible by 31 or 11, respectively, and so cannot divide $|\mathrm{Aut}(L)|$, contrary to (8.3.4.2).

(vii) $(2n, q, \ell) = (10, 2, 11)$ and $L \in \{\mathrm{PSL}_2(11), M_{11}, M_{12}, M_{22}, \mathsf{A}_{11}, \mathsf{A}_{12}\}$. Here, if $m = 4$, then $(2^m + 1)(2^{n-m} - 1)$ is divisible by 17, and so cannot divide $|\mathrm{Aut}(L)|$, contrary to (8.3.4.2). Thus $m = 2$, and (8.3.4.2) rules out $L = \mathrm{PSL}_2(11)$, $M_{11}$, and $M_{12}$. Since $M_{22}$ cannot embed in $\Omega_{10}^-(2)$, we arrive at (b).

(viii) Since $nf \geq 4$, we are left with one case $(2n, q, L) = (6, 4, \mathrm{PSL}_2(13))$. In this case, $m = 2$, $(4^m + 1)(4^{n-m} - 1)$ is divisible by 17, and so cannot divide $|\mathrm{Aut}(L)|$, contrary to (8.3.4.2). □

We will also need to classify another kind of linear groups in characteristic 2.

THEOREM 8.3.5. *Let $q_0 = 2^{f_0}$ be a power of 2 and let $a, b, f \in \mathbb{Z}_{\geq 1}$ and $d \in \mathbb{Z}_{\geq 2}$ be such that*

$$\gcd(a, b) = 1,\ \ 2|ab,\ \ a > b,\ \ df_0 = 2(a + b)f,\ \ af \neq 3,\ \ (a + b)f \neq 3, 6.$$

*Let $\ell_1 = \mathrm{ppd}(2, 2af)$ and $\ell_2 = \mathrm{ppd}(2,(a+b)f)$ be primitive prime divisors of $2^{2af}-1$ and $2^{(a+b)f}-1$, which exist by* [**Zs**]. *Let $W = \mathbb{F}_{q_0}^d$ and let $G$ be a subgroup of $\mathrm{GL}(W) \cong \mathrm{GL}_d(q_0)$ that contains elements $h_1$ of order $Q_1 := (2^{af}+1)_{\ell_1}$, and $h_2$ of order $Q_2 := (2^{(a+b)f}-1)_{\ell_2}$ with $\mathbf{C}_W(h_2) = 0$. Then there exists a divisor $j \leq d/3$ of $d$ such that one of the following statements holds for $L := G^{\{\ell_1,\ell_2\}'}$, the normal subgroup of $G$ generated by Sylow $\ell_1$-subgroups and Sylow $\ell_2$-subgroups of $G$.*

(i) *$L = \mathrm{SL}(W_j) \cong \mathrm{SL}_{d/j}(q_0^j)$, and $W_j$ is $W$ viewed as a $d/j$-dimensional vector space over $\mathbb{F}_{q_0^j}$. Moreover, $G$ does not fix any $\mathbb{F}_2$-valued non-degenerate quadratic form on $W$ viewed over $\mathbb{F}_2$.*

(ii) *$2j|d$, $L = \mathrm{Sp}(W_j) \cong \mathrm{Sp}_{d/j}(q_0^j)$, and $W_j$ is $W$ viewed as a $d/j$-dimensional vector space over $\mathbb{F}_{q_0^j}$ endowed with a non-degenerate symplectic form. Furthermore, $G$ does not fix any $\mathbb{F}_2$-valued non-degenerate quadratic form on $W$ viewed over $\mathbb{F}_2$.*

(iii) *$2|jf_0$, $L = \mathrm{SU}(W_j) \cong \mathrm{SU}_{d/j}(q_0^{j/2})$, and $W_j$ is $W$ viewed as a $d/j$-dimensional vector space over $\mathbb{F}_{q_0^j}$ endowed with a non-degenerate Hermitian form.*

(iv) *$2j|d$, $d/j \geq 4$, $L = \Omega(W_j) \cong \Omega^\epsilon_{d/j}(q_0^j)$, and $W_j$ is $W$ viewed as a $d/j$-dimensional vector space over $\mathbb{F}_{q_0^j}$ endowed with a non-degenerate quadratic form of type $\epsilon = \pm$.*

(v) *$(d, q_0, a, b, f, \ell_1, \ell_2, L) = (20, 2, 3, 2, 2, 13, 11, \mathsf{A}_{22})$. Moreover, $G$ does not fix any $\mathbb{F}_2$-valued non-degenerate quadratic form on $W$.*

Proof. (a) Since $\mathbf{C}_W(h_2) = 0$ and

$$\mathsf{o}(h_2) = \ell_2 = \mathrm{ppd}(2, df_0/2) \geq df_0/2 + 1, \tag{8.3.5.1}$$

the semisimple $\langle h_2\rangle$-module $W$ is the direct sum of two simple modules, both of dimension $d/2$. Hence, if $0 \neq U \neq W$ is a simple $L$-submodule, then as $h_2$ acts on both $U$ and $W/U$, we have $\dim U = \dim(W/U) = d/2 < 2af/f_0$. However, using

$$\mathsf{o}(h_1) = \ell_1 = \mathrm{ppd}(2, 2af) \geq 2af + 1 \geq df_0/2 + 2, \tag{8.3.5.2}$$

we can see that the semisimple $\langle g_1\rangle$-module $W$ contains a simple submodule of dimension $2af/f_0$, a contradiction. Thus $L$ is irreducible on $W$. For future reference we note that

$$af \geq 4, \;\; \ell_1 \geq 11. \tag{8.3.5.3}$$

(Indeed, $af \geq 2$ and $af \neq 3$ by hypothesis. If $af = 2$, then $(a, f, b) = (2, 1, 1)$ and so $(a+b)f = 3$, a contradiction. So $2af \geq 8$ and $\ell_1 = \mathrm{ppd}(2, 2af) \geq 11$.)

Suppose $L$ is imprimitive: $G$ permutes transitively $t$ summands of a decomposition $W = \oplus_{i=1}^t W_i$ with $1 < t|d$. If $t = d$ and $q_0 = 2$, then $\dim_{\mathbb{F}_2} W_i = 1$, so $L$ permutes transitively an $\mathbb{F}_2$-basis of $W$ and so is reducible, a contradiction. Hence either $2 \leq t \leq d/2$, or $t = d$ but $f_0 \geq 2$. In either case, we have $df_0/t \leq df_0/2 < 2af$ and $t \leq df_0/2 < 2af$. It follows that the order of $\mathrm{GL}_{d/t}(q_0) \wr \mathsf{S}_t \geq G$ is not divisible by $\ell_2 > 2af$, a contradiction. Thus $L$ is irreducible and primitive on $W$.

(b) We proceed by induction on $d \geq 2$. For the induction base $d = 2$, note from (8.3.5.2) that $\ell_1 \nmid (q_0 - 1)$. Hence $\ell_1 | (q_0 + 1)$, and so $2af | 2f_0$ by primitivity of $\ell_1$, whence (8.3.5.2) implies that $2af = 2f_0 = 2(a+b)f$, i.e. $b = 0$, a contradiction.

For the induction step $d \geq 3$, we will apply the main result of [**GPPS**] to the prime $\ell_1$ to see that $G$ is one of the groups described in Examples 2.1–2.9 of [**GPPS**]. The choices of $\ell_{1,2}$ imply that $\ell_1, \ell_2 \nmid (q_0 - 1)$.

Suppose $G$ is described in Example 2.1 of [**GPPS**], in which $\ell_1$ is a primitive prime divisor of $q_0^{e/a_0} - 1$ for some $e \leq d$ and $a_0 | f_0$, whence $2af$ divides $ef_0/a_0 \leq df_0/a_0 \leq df_0$. If $a_0 > 1$, then $df_0/a_0 \leq df_0/2 < 2af$ by (8.3.5.2), a contradiction. Hence $a_0 = 1$, and we arrive at (i)–(iv) with $j = 1$.

Next, the primitivity of $G$ on $V$ rules out the groups in Examples 2.2 and 2.3 of [**GPPS**]; also, Example 2.5 of [**GPPS**] does not occur in characteristic 2, which is our case.

Suppose $G$ is among the groups described in Example 2.4 of [**GPPS**]. Thus for a divisor $1 < j | d$, $W$ is endowed with the structure of a $d/j$-dimensional vector space $W_j$ over $\mathbb{F}_{q_0^j}$, and $G \leq \mathrm{GL}(W_j) \rtimes C_j$, where $C_j$ is the group of field automorphisms of $\mathbb{F}_{q_0^j}$ over $\mathbb{F}_{q_0}$. Suppose $j = d$, i.e. $G \leq \mathrm{GL}_1(q_0^d) \rtimes C_d$. If $\ell_1 | d$, then (8.3.5.2) implies that $f_0 = 1$ and $\ell_1 = d = 2(a+b)f$, a contradiction. So $\ell_1 | (q_0^d - 1)$, which implies by primitivity of $\ell_1$ that $2af > df_0/2$ divides $df_0$, whence $2af = df_0 = 2(a+b)f$, i.e. $b = 0$, a contradiction. Hence $2 \leq j \leq d/2$, in which case $j \leq df_0/2 < \min(\ell_1, \ell_2)$ by (8.3.5.1) and (8.3.5.2). It follows that $L$ is contained in $\mathrm{GL}(W_j) \cong \mathrm{GL}_{d/j}(q^j)$. Since $h_1, h_2 \in L$, we can apply the induction base and the induction hypothesis to see that one of (i)–(iv) holds.

(c) In Examples 2.6–2.9 of [**GPPS**], $S \lhd G/(G \cap Z) \leq \mathrm{Aut}(S)$ for some non-abelian simple group $S$, where $Z := \mathbf{Z}(\mathrm{GL}_d(q_0)) \cong C_{q_0-1}$ and the full inverse image $N$ of $S$ in $G$ acts absolutely irreducibly on $W$. Moreover, $G \leq \mathrm{GL}_d(q_1) * Z$ for some root $q_1 = 2^{f_1}$ of $q_0$. If $q_1 < q_0$, then, since $2af > df_0/2 \geq df_1$, $|G|$ is not divisible by $\ell_1 = \mathrm{ppd}(2, 2af)$. Hence $q_1 = q_0$, i.e. $\mathbb{F}_{q_0}$ is the smallest field over which $G$ is realizable modulo scalars (in the sense of [**GPPS**, p. 172]). As $\ell_i \nmid (q_0 - 1)$, we have that $\mathrm{Aut}(S)$ contains elements of order $Q_1$ and $Q_2$.

In Example 2.6 of [**GPPS**] we have $S = \mathsf{A}_n$ with $n \geq 5$; in particular, $\ell_1, \ell_2 \leq n$. First, in Example 2.6(a) of [**GPPS**] we have $n - 2 \leq d \leq n - 1$, and so (8.3.5.2) implies that $\ell_1 \geq d/2 + 2 \geq n/2 + 1$, whence $\ell_1^2 \nmid |G|$. In fact, if $f_0 \geq 2$ then we have $\ell_1 \geq d + 2 \geq n$, whence $n = \ell_1$ is odd, in which case $d = n - 1$ and $\ell_1 > n$, a contradiction. So $f_0 = 1$. If moreover $2af \notin \{10, 12, 18\}$, then by [**F2**] we can choose $\ell_1$ to be a large primitive prime divisor of $2^{2af} - 1$, for which we have $\ell_1 \geq 4af + 1 \geq d + 3 > n$ and so $\ell \nmid |G|$, a contradiction. Hence

$$af \in \{5, 6, 9\}. \tag{8.3.5.4}$$

Suppose $(a+b)f \notin \{8, 10, 12, 18, 20\}$. By [**Tr**, Theorem 3.2.2] we can choose $\ell_2$ to be a "very large" primitive prime divisor of $2^{(a+b)f} - 1$, for which we either have $\ell_2 \geq 3(a+b)f + 1 \geq 3d/2 + 1 > n$, or $\ell_2 = (a+b)f + 1 = d/2 + 1 \geq n/2$ but $Q_2 \geq \ell_2^2$. The former case is impossible, and in the latter case $\mathrm{Aut}(\mathsf{A}_n)$ cannot contain elements of order $Q_2$. Hence

$$(a+b)f \in \{8, 10, 12, 18, 20\}. \tag{8.3.5.5}$$

By hypothesis, $2 \nmid a + b \geq 3$. Now if $(a+b)f \in \{8, 12, 20\}$, then $4 | f$, contrary to (8.3.5.4). If $(a+b)f = 18$, then $2 | f$, so $af = 6$ and $(a, f) = (3, 2)$ by (8.3.5.4), but then $a + b = 9$ and $b = 6 > a$, a contradiction. Hence $(a+b)f = 10$, $f = 2$, $a = 3$, $b = 2$, $\ell_1 = 13$, $\ell_2 = 11$, $d = 20$, and $n \in \{21, 22\}$. If $n = 21$, then elements of order $Q_2 = 11$ have nonzero fixed points on $W = \mathbb{F}_2^{20}$, again a contradiction. So $n = 22$, and we arrive at (v). Note that $W$ can support a non-degenerate $L$-invariant alternating, but not quadratic, form, because $22 \equiv 2 (\mathrm{mod}\ 4)$, see [**Ben**, Lemma 6.2].

Example 2.6(b) of [**GPPS**] does not occur in characteristic 2. In Example 2.6(c) of [**GPPS**], we have $\ell_1 \in \{5, 7\}$, contrary to (8.3.5.3).

Example 2.7 of [**GPPS**] lists 11 cases with $S$ being a sporadic simple group. In six cases, we have $d \geq 10$ and $\ell_1 = \mathrm{ppd}(2, d)$. It follows that $df_0/2 < 2af = d$, so $f_0 = 1$, but then $d = df_0 = 2(a + b)f > 2af$, a contradiction. In another case we have $d = 20$ and $\ell_1 = \mathrm{ppd}(2, d - 2) = 19$. It follows that $df_0/2 < 2af = d - 2$, so $f_0 = 1$, whence $d = df_0 = 2(a + b)f$, whence $(af, bf) = (9, 1)$ and $2 \nmid ab$, again a contradiction. In two cases we have $d = 11$ and $\ell_1 = \mathrm{ppd}(2, d - 1) = 11$. It follows that $df_0/2 < 2af = d - 1$, so $f_0 = 1$, but then $d = df_0 = 2(a + b)f$ is even, a contradiction. In another case we have $(d, L) = (9, 3\mathsf{J}_3)$, $2|f_0$, and $\ell_1 = \mathrm{ppd}(2, 2d) = 19$. It follows that $df_0/2 < 2af = 2d$, so $f_0 = 2$, whence $2d = df_0 = 2(a + b)f$ and $b = 0$, again a contradiction. In the final case we have $(d, L) = (6, 3\mathsf{M}_{22})$, $2|f_0$, and $\ell_1 = \mathrm{ppd}(2, 10) = 11$. It follows that $3f_0 < 2af = 10$, so $f_0 = 2$, whence $12 = df_0 = 2(a + b)f$, $(af, bf) = (5, 1)$, and $2 \nmid ab$, a contradiction.

Example 2.8 of [**GPPS**] lists six examples with $S$ a simple group of Lie type in the same characteristic 2. In two of them, with $(d, L) = (4, {}^2B_2(q_0))$, $(6, G_2(q_0))$, $\ell_1$ is a primitive prime divisor of $2^{df_0} - 1$, so we get $2af = df_0 = 2(a + b)f$ and thus $b = 0$, a contradiction. In three of them, we have $d = 8$ and $\ell_1$ is a primitive prime divisor of both $2^{6f_0} - 1$. Hence $af = 3f_0$, and $8f_0 = 2(a + b)f$, i.e. $bf = f_0$. It follows that $f = \gcd(af, bf) = \gcd(3f_0, f_0) = f_0$, so $(a, b) = (3, 1)$ and thus $2 \nmid ab$, a contradiction. In the remaining case, we have $d = 9$, $L$ is a quotient of $\mathrm{SL}_3(q_0^2)$, and $\ell_1$ is a primitive prime divisor of $2^{6f_0} - 1$. Hence $af = 3f_0$, and $9f_0 = 2(a + b)f$, i.e. $2bf = 3f_0$. It follows that $2f = \gcd(2af, 2bf) = \gcd(6f_0, 3f_0) = 3f_0$, so $2f = 3f_0$ and $(a, b) = (2, 1)$. But now we can check that $\ell_2 = \mathrm{ppd}(2, (a+b)f) = \mathrm{ppd}(2, 9f_0/2)$ does not divide $|L|$, again a contradiction.

In Example 2.9 of [**GPPS**], $S$ is a simple group of Lie type in characteristic $\neq 2$ and appears in Tables 7 and 8 of [**GPPS**]. The only case in Table 7 that occurs in characteristic 2 is $G_2(3)$ with $(d, \ell_1) = (14, 13)$, in which case $12 = 2af > df_0/2$, whence $f_0 = 1$, $(af, bf) = (6, 1)$, but then $\ell_2 = \mathrm{ppd}(2, 7) = 127$ does not divide $|G|$. In all but one example appearing in Table 8 of [**GPPS**], we have $d - 1 \leq \ell_1 \leq d + 1$, $|S|_{\ell_1} = \ell_1$, $\ell_1$ is coprime to the order of $\mathrm{Out}(S)$ and of the Schur multiplier of $S$. It follows that

$$\ell_1^2 \nmid |G|. \tag{8.3.5.6}$$

Moreover, $\ell_1$ is a primitive prime divisor $\mathrm{ppd}(q_0, \ell_1 - 1)$ of $q_0^{\ell_1 - 1} - 1$. As $\ell_1$ divides $2^{2af} - 1$ and $(q_0^{2af} - 1)$, we have $(\ell_1 - 1)|2af$ and so $2af \geq d - 2$. If $f_0 \geq 2$, then $\ell_1 \geq d + 2$ by (8.3.5.2), a contradiction. So $f_0 = 1$, $d = 2af + 2bf$, and therefore $(af, bf) = (d/2 - 1, 1)$, $f = b = 1$, and $\ell_1 = d - 1 = 2af + 1$. The latter conclusion, together with (8.3.5.6) implies that $2^{2af} - 1$ does not possess large primitive prime divisors. Applying [**F2**, Theorem A] and (8.3.5.3), we obtain $af \in \{5, 6, 9\}$. As $2|ab = a$, it follows that $af = 6$ and thus $\ell_1 = 13$. Using the information from [**GPPS**, Table 8], we have $S = \mathrm{PSp}_{2m}(s)$ for some odd prime power $s$, and either $V$ comes from a Weil representation of degree $(s^m + 1)/2$, which is impossible in characteristic 2, or $s = \ell_1$ and $m = 1$. Thus $S = \mathrm{PSL}_2(13)$. But then $\ell_2 = \mathrm{ppd}(2, 7) = 127$ does not divide $|G|$, a contradiction.

In the remaining case of [**GPPS**, Table 8], $(d, S) = ((\ell_1 - 1)/2, \mathrm{PSL}_2(\ell_1))$, and $\ell_1$ is a primitive prime divisor $\mathrm{ppd}(q_0, d)$ of $q_0^d - 1$. As $\ell_1$ divides $2^{2af} - 1$ and $q_0^{2af} - 1$, we have $d|2af$. Also, $2d + 1 = \ell_1 \geq df_0/2 + 2$ by (8.3.5.2), so $f_0 \leq 3$. On the other hand, $df_0 = 2(a + b)f > 2af \geq d$, we have $f_0 > 1$. If $f_0 = 2$, then $2d = 2(a + b)f > 2af$, whence $2af = d = 2bf$ and $a = b$, a contradiction. So $f_0 = 3$, $3d = 2af + 2bf > 2af$ and $3d/2 < 2af$, whence $(2af, 2bf) = (2d, d)$. In this case, we have $2f = \gcd(2af, 2bf) = \gcd(2d, d)$, so $d = 2f$ and $(a, b) = (2, 1)$. But then $\ell_2 = \mathrm{ppd}(2, 3f) = \mathrm{ppd}(2, 3(\ell_1 - 1)/4) \geq (3\ell_1 + 1)/4 > 8$ (as $\ell_1 \geq 11$ by (8.3.5.3)) cannot divide $q_0 - 1 = 7$ and $|\mathrm{Aut}(S)| = |\mathrm{PGL}_2(\ell_1)|$ and thus $\ell_2 \nmid |G|$, a contradiction.

Finally, suppose $2|df \geq 4$ and $\mathsf{Q}$ is any $\mathbb{F}_2$-valued non-degenerate quadratic form. Then it takes both values 0 and 1 on $W \smallsetminus \{0\}$, and so any subgroup of $\mathrm{O}(\mathsf{Q})$ cannot act transitively on $W \smallsetminus \{0\}$. Since the group $L$ in (i) and (ii) are transitive on $W \smallsetminus \{0\}$, in none of these cases $G$ can fix $\mathsf{Q}$. □

THEOREM 8.3.6. *Let $a, b, f \in \mathbb{Z}_{\geq 1}$ be such that $\gcd(a, b) = 1$, $2|ab$, $a > b$. Set $d := 2(a + b)f$ and let $W := \mathbb{F}_2^d$ be endowed with a non-degenerate $\mathbb{F}_2$-valued symplectic form $\mathsf{Q}$ of type $+$. Assume $G$ is subgroup of $\mathrm{O}(W) \cong \mathrm{O}_d^+(2)$ that contains an element $g_1$, a generator of a maximal torus $C_{2^{af}+1} \times C_{2^{bf}+1}$, and an element $g_2$ of order $2^{(a+b)f} - 1$ with $\mathbf{C}_W(g_2) = 0$, of $\mathrm{O}(W)$. Then there exists a divisor $j \leq d/4$ of $d/2$ such that $L := G^{(\infty)} = \Omega(W_j) \cong \Omega_{d/j}^+(2^j)$, where $W_j$ is $W$ viewed as a $d/j$-dimensional vector space over $\mathbb{F}_{2^j}$ endowed with a non-degenerate quadratic form $\mathsf{Q}_j$ of type $+$. Moreover, there is $\alpha \in \mathbb{F}_{2^j}^\times$ such that $\mathsf{Q}(u) = \mathrm{Tr}_{\mathbb{F}_{2^j}/\mathbb{F}_2}(\alpha \cdot \mathsf{Q}_j(u))$ for all $u \in W_j$.*

PROOF. (a) First we consider the case $(a+b)f = 3$, i.e. $W = \mathbb{F}_2^6$, but $G \not\geq \Omega(W)$. In this case, $(a, b, f) = (2, 1, 1)$, $\mathsf{o}(g_1) = 15$, and $\mathsf{o}(g_2) = 7$. Then $G \cap \Omega(W)$ is a proper subgroup of $\Omega_6^+(2) \cong \mathsf{A}_8$ that contains both $g_1$ and $g_2$. Checking maximal subgroups of $\mathsf{A}_8$ listed in [**CCNPW**], we see that $G \cap \Omega_6^+(2)$ is contained in $\mathsf{A}_7$, which is a contradiction since $\mathsf{A}_7$ contains no elements of order 15.

Next we consider the case $d = 10$, $W = \mathbb{F}_2^{10}$, but $G \not\geq \Omega(W)$. In this case, $\mathsf{o}(g_1) = 45$ or 51, and $\mathsf{o}(g_2) = 31$. Then $G \cap \Omega(W)$ is a proper subgroup of $\Omega_{10}^+(2)$ that contains both $g_1$ and $g_2$, and this contradicts the list of maximal subgroups of $\Omega_{10}^+(2)$ [**CCNPW**]. We also note that if $af = 3$, then $(a, f, b) = (3, 1, 2)$ and so $d = 10$.

Note that $a+b \geq 3$ is odd. In what follows we may assume that $(a+b)f \geq 6$ and $af \neq 3$. Hence $2^{2af} - 1$ has a primitive prime divisor $\ell_1 = \mathrm{ppd}(2, 2af)$ [**Zs**], and $Q_1 := (2^{2af} - 1)_{\ell_1}$ divides $\mathsf{o}(g_1)$. Next we consider the case $(a + b)f = 6$. As $2 \nmid (a + b) \geq 3$, we have that $(a, b, f) = (2, 1, 2)$. In this case, $\mathsf{o}(g_1) = 85$ and $\mathsf{o}(g_2) = 63$. Assuming $G \not\geq \Omega(W)$, and using the list of maximal subgroups of $\Omega_{12}^+(2)$ [**BHR**, Table 8.83], we must then have $G \cap \Omega(W) \leq \Omega_6^+(4) \cdot 4$. Again using the list of maximal subgroups of $\Omega_6^+(4) \cong \mathrm{SL}_4(4)$ [**BHR**, Table 8.8], we arrive at the conclusion with $j = 2$.

(b) From now on we may assume $(a+b)f \neq 6$, whence $2^{(a+b)f} - 1$ admits a primitive prime divisor $\ell_2 = \mathrm{ppd}(2, (a + b)f)$ [**Zs**], and $Q_2 := (2^{(a+b)f} - 1)_{\ell_2}$ divides $\mathsf{o}(g_2)$. Since $\mathbf{C}_W(g_2) = 0$, we can apply Theorem 8.3.5 to $G$. Since $G$ fixes $\mathsf{Q}$, cases (i), (ii), and (v) of Theorem 8.3.5.

Suppose we are in the case of 8.3.5(iii). If $2 \nmid d/j$, then $|L|$, and hence $|\Omega_{2(a+b)f}^+(2)|$, is divisible by $(2^{j/2})^{d/j} + 1 = 2^{(a+b)f} + 1$, which can be seen impossible by using a primitive prime divisor $\mathrm{ppd}(2, 2(a+b)f)$ [**Zs**]. Hence $2j|d$, and so

$$j|(a+b)f. \tag{8.3.6.1}$$

As $L$ acts absolutely irreducibly on $W_j$, $\mathrm{End}_L(W) \cong \mathbb{F}_{2^j}$ and thus $\mathbf{C}_G(L) \hookrightarrow C_{2^j-1}$. Now (8.3.6.1) implies that $j < 2af$, so $\ell_1 \nmid |\mathbf{C}_G(L)|$. It follows that $\ell_1$ divides $|G/\mathbf{C}_G(L)|$ and $\mathrm{Aut}(L) \cong \mathrm{PGU}_{d/j}(2^{j/2}) \cdot C_j$. As $\ell_1 \geq 2af+1 > j$, we can find $1 \leq i \leq d/j$ such that $\ell_1$ divides $2^{ij/2} - (-1)^i$. In particular, $\ell_1|(2^{ij}-1)$, and the primitivity of $\ell_1$ implies that $2af|ij$. Now $2af > d/2$ and $ij \leq d$, so $ij = 2af$. As $\ell_1 \nmid (2^{af}-1)$ by primitivity, we have that $2 \nmid i$, and so $j$ is divisible by the 2-part of $2af$. But this contradicts (8.3.6.1), since $2 \nmid (a+b)$.

Hence we are in the case of 8.3.5(iv). If $\epsilon = -$, then $|L|$, and hence $|\Omega^+_{2(a+b)f}(2)|$, is divisible by $(2^j)^{d/2j}+1 = 2^{(a+b)f}+1$, which is impossible as mentioned above. Hence $\epsilon = +$. To link the quadratic form for $L$ on $W_j$ to $\mathsf{Q}$, we can argue as in part (iii) of the proof of Theorem 8.3.4. □

## 8.4. Unitary-type subgroups

Let $q = p^f$ be any power of a prime $p$ and $n \geq 2$. Throughout this and all the subsequent sections, we will assume that $(n,q) \neq (2,2), (3,2)$, so that $G := \mathrm{SU}_n(q)$ is perfect.

It is well known, see e.g. [**Ge**, Theorem 4.9.2], that the function

$$\tilde{\zeta}_{n,q} = \tilde{\zeta}_n : g \mapsto (-1)^n(-q)^{\dim_{\mathbb{F}_{q^2}} \mathrm{Ker}(g-1_W)} \tag{8.4.0.1}$$

defines a complex character, called the (reducible) *Weil character*, of the general unitary group $\tilde{G} := \mathrm{GU}(W) \cong \mathrm{GU}_n(q)$, where $W = \mathbb{F}_{q^2}^n$ is a non-degenerate Hermitian space with Hermitian product $\circ$. Fix some $\theta \in \mathbb{F}_{q^2}^\times$ with $\theta^{q-1} = -1$; if $p = 2$ we will take $\theta = 1$. Then the $\mathbb{F}_q$-bilinear form

$$(u|v)_f := \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\theta u \circ v)$$

on $W$, viewed as an $\mathbb{F}_q$-vector space $U_f$, is non-degenerate alternating. This leads to an embedding

$$\tilde{G} = \mathrm{GU}(W) \hookrightarrow \mathrm{Sp}(U_f) \cong \mathrm{Sp}_{2n}(q).$$

Similarly, the $\mathbb{F}_p$-bilinear form

$$(u|v)_1 := \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}\big((u|v)_f\big) = \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_p}(\theta u \circ v) \tag{8.4.0.2}$$

on $W$, viewed as an $\mathbb{F}_p$-vector space $U_1$, is also non-degenerate alternating, and this leads to an embedding

$$\tilde{G} = \mathrm{GU}(W) \hookrightarrow \mathrm{Sp}(U_1) \cong \mathrm{Sp}_{2nf}(p).$$

If $p = 2$, then $\tilde{G}$ preserves the quadratic form $\mathsf{Q}_f(u) = u \circ u$ on $U_f$, and, since $[\tilde{G}, \tilde{G}] = \mathrm{SU}(W) = G$ has odd index $q+1$ in $\tilde{G}$, this leads to an embedding

$$\tilde{G} = \mathrm{GU}(W) \hookrightarrow \Omega(U_f) \cong \Omega^-_{2n}(q).$$

In general, $\tilde{G}$ preserves the $\mathbb{F}_2$-valued quadratic form

$$\mathsf{Q}_1 = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(u \circ u) \tag{8.4.0.3}$$

on $U_1$. When $n$ is odd, the type of the quadratic form $\mathsf{Q}_f$ is $-$, as one can see using the fact that $q^n+1$ divides both $|\tilde{G}|$ and $|\Omega(U_f)|$, and this justifies the use of the same notation $\mathsf{Q}_f$

for this quadratic form on $U_f$, cf. §8.2. Moreover, $\tilde{G}$, being embedded in $\Omega(U_1)$, acts on the extraspecial 2-group $E = 2_-^{1+2nf} = \mathbf{O}_2(H_f^-)$, with $H_f^-$ constructed in (8.2.2.1). We also fix the generator $z = \rho \cdot 1_W$ of $\mathbf{Z}(\tilde{G}) \cong C_{q+1}$.

We start with a general fact for any prime $p$:

PROPOSITION 8.4.1. *Given the above notation for any prime $p$ and any $n \geq 3$ with $(n,q) \neq (3,2)$, the following statements hold.*

(a) *Let $G_1$ be any subgroup of $\mathrm{Sp}(U_f) = \mathrm{Sp}_{2n}(q)$. Assume that $G_1$ is isomorphic to $\mathrm{SU}_n(q)$. Then $U_f = \mathbb{F}_q^{2n}$ can be endowed with an $\mathbb{F}_{q^2}$-vector space structure $W_1$ (compatible with $\mathbb{F}_q$-vector space structure on $U_f$) such that $G_1 = \mathrm{SU}(W_1)$.*

(b) *Let $G_1$ be any subgroup of $\mathrm{Sp}(U_1) = \mathrm{Sp}_{2nf}(p)$. Assume that $U_1 = \mathbb{F}_p^{2nf}$ can be endowed with an $\mathbb{F}_{q^2}$-vector space structure $W_1$ (compatible with $\mathbb{F}_p$-vector space structure on $U_1$) such that $G_1 = \mathrm{SU}(W_1)$. Then the following statements hold.*

(b1) *There is some $\alpha \in \mathbb{F}_q^\times$ such that the symplectic form $(\cdot|\cdot)$ on $U_1$ and the Hermitian form $\circ$ on $W_1$ satisfy $(u|v) = \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_p}(\alpha\theta u \circ v)$ for all $u, v \in W_1$.*

(b2) *Assume in addition that $p = 2$ and $G_1$ preserves a quadratic form $\mathsf{Q}$ on $U_1$ that is associated to the symplectic form $(\cdot|\cdot)$. Then $\mathsf{Q}(u) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\alpha u \circ u)$, with $\alpha$ chosen in* (b1). *Moreover, if $nf \geq 4$ then $\mathbf{N}_{\mathrm{O}(\mathsf{Q})}(G_1) \cong \mathrm{GU}(W_1) \rtimes \mathrm{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_2)$.*

PROOF. (a) By assumption, $p^{2nf} - 1$ admits a primitive prime divisor $\ell$ [**Zs**], and $G_1$ contains an element of order $\ell$. Any such element acts irreducibly on $U_f$ (in fact also on $U_1$), so the $2n$-dimensional $\mathbb{F}_q$-representation of $G_1$ on $U_f$ is irreducible. This representation becomes absolutely irreducible (and still nontrivial) over $\mathbb{E} := \mathrm{End}_{G_1}(U_f) \supseteq \mathbb{F}_q$, of dimension dividing $2n \leq n(n+1)/2$. By [**KlL**, Proposition 5.4.11], up to an isomorphism of $G_1$ and taking the dual when $n = 3$ if necessary, the $\mathbb{E}$-representation is just the natural $n$-dimensional representation of $G_1$ and $\mathbb{E} \cong \mathbb{F}_{q^2}$, giving the desired structure of $W_1$.

(b1) As shown in (a), the $\mathbb{F}_p$-representation of $G_1$ on $U_1$ is irreducible, so $\mathbb{E} := \mathrm{End}_{G_1}(U_1)$ is a finite field. By assumption,

$$\mathbb{E} = \mathrm{End}_{G_1}(W_1) = \mathbb{F}_{q^2}. \tag{8.4.1.1}$$

Now using the $G_1$-invariant Hermitian form $\circ$ on $W_1$, we can define a non-degenerate $G_1$-invariant alternating form $(\cdot|\cdot)_1$ as in (8.4.0.2). Fix a basis of $U_1$ as $\mathbb{F}_p$-vector space, and consider the Gram matrices of $(\cdot|\cdot)$ and $(\cdot|\cdot)_1$ relative to this basis:

$$(u|v) = {}^t\!uJv, \ (u|v)_1 = {}^t\!uJ_1v$$

for any $u, v \in U_1$ written as coordinate vectors in $\mathbb{F}_p^{2nf}$ with respect to this basis. For any element of $G_1$ written as a matrix $X$ in this basis, the invariance of the two forms implies that $({}^tX)^{-1} = JXJ^{-1} = J_1XJ_1^{-1}$, hence $J_1^{-1}J \in \mathrm{GL}(U_1)$ commutes with all $X \in G_1$ and thus $J_1^{-1}J \in \mathbb{E}$. It follows from (8.4.1.1) that there is a scalar $\alpha \in \mathbb{F}_{q^2}^\times$ such that $J = J_1T_\alpha$, where $T_\alpha$ is the matrix of the transformation $x \mapsto \alpha x$ on $W_1$ written in the chosen basis, and so

$$(u|v) = {}^t\!uJv = {}^t\!uJ_1T_\alpha v = (u|T_\alpha v)_1.$$

Back to viewing $u, v$ as vectors in $W_1$ and using (8.4.0.2), we now have

$$(u|v) = (u|\alpha v)_1 = \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_p}(\theta u \circ \alpha v).$$

Recalling that $(\cdot|\cdot)$ is alternating and $u \circ u \in \mathbb{F}_q$, we have

$$0 = (u|u) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}\big((\theta\alpha^q + \theta^q\alpha)(u \circ u)\big) \tag{8.4.1.2}$$

for all $u \in W_1$. Since $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}$ maps $\mathbb{F}_q$ onto $\mathbb{F}_p$, we can find $\lambda \in \mathbb{F}_q$ with $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\lambda) = 1$. Now, if $\theta\alpha^q + \theta^q\alpha \neq 0$, then we can find $u \in W_1$ with $u \circ u = (\theta\alpha^q + \theta^q\alpha)^{-1}\lambda$, and (8.4.1.2) shows that $(u|u) = 1$, a contradiction. Thus $\theta\alpha^q + \theta^q\alpha = 0$, and so, since $\theta^{q-1} = -1$, we get $\alpha \in \mathbb{F}_q$, proving the statement.

(b2) Applying (b1) and changing $u \circ v$ to $\alpha u \circ v$ on $W_1$, we may assume that $(\cdot|\cdot) = (\cdot|\cdot)_1$. Thus both $\mathsf{Q}$ and $\mathsf{Q}_1$ are $G_1$-invariant, and associated to the same symplectic form $(\cdot|\cdot)$. It follows that $G_1$ stabilizes $\mathsf{Q} - \mathsf{Q}_1$, a map in $\mathrm{Hom}_{\mathbb{F}_2}(U_1, \mathbb{F}_2)$, which can be identified with $U_1$ using $(\cdot|\cdot)$. Since $G_1$ acts irreducibly on $U_1$, we conclude that $\mathsf{Q} = \mathsf{Q}_1$.

The Hermitian $\mathbb{F}_{q^2}$-structure on $W_1$ shows that $\mathbf{N}_{\mathrm{O}(\mathsf{Q})}(G_1)$ contains $\mathrm{GU}(W_1) \rtimes \mathrm{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_2)$. Under the assumptions $nf \geq 4$ and $n \geq 3$, the latter group induces (via conjugation) the full automorphism group of $G_1 = \mathrm{SU}(W_1)$. So, to prove the last statement in (b2), it suffices to show that $\mathbf{C}_{\mathrm{O}(\mathsf{Q})}(G_1) \leq \mathbf{Z}(\mathrm{GU}(W_1)) \cong C_{q+1}$. In fact we will show the stronger statement

$$\mathbf{C}_{\mathrm{Sp}(U_1)}(\mathrm{SU}(W_1)) = \mathbf{Z}(\mathrm{GU}(W_1)) \cong C_{q+1}. \tag{8.4.1.3}$$

Assume the contrary. As $\mathbb{F}_{q^2}^\times = \mu_{q+1}\mathbb{F}_q^\times$ for $p = 2$, it then follows from (8.4.1.1) that $\mathbf{C}_{\mathrm{Sp}(U_1)}(G_1)$ contains a scalar map $z := u \mapsto \lambda u$ on $W_1$ for some $1 \neq \lambda \in \mathbb{F}_q^\times$. The inclusion $z \in \mathrm{Sp}(U_1)$ implies that

$$\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_2}(\lambda u \circ \lambda v) = (\lambda u|\lambda v) = (u|v) = \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_2}(u \circ v),$$

i.e. $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}\big((\lambda^2 - 1)(u \circ v + v \circ u)\big) = 0$, for all $u, v \in W_1$. Since $u \circ v + v \circ u$ covers $\mathbb{F}_q$, this identity shows that $\lambda^2 = 1$, i.e. $\lambda = 1$, a contradiction. □

From now on, we will assume $p = 2$.

Proposition 8.4.2. *Assume $n \geq 3$ is odd, $p = 2$, and $(n, q) \neq (3, 2)$. Let $\hat{z}$ be an inverse image of odd order of a generator $z$ of the center of $\tilde{G} < \Omega(U_f)$ in $H_f^- \leq H_1^-$. Then $\mathbf{C}_{H_1^-}(\hat{z}) = \mathbf{C}_{H_f^-}(\hat{z}) \cong \tilde{G} \times C_2$, where $C_2$ can be identified with $\mathbf{Z}(E)$. Furthermore, if*

$$\psi(x) := \mathrm{Trace}(x)$$

*for any $x \in H_f^- < \mathrm{GL}_{q^n}(\mathbb{C})$, then the restriction of $\psi$ to $\tilde{G} \cong \mathrm{GU}_n(q)$ is the total Weil character $\tilde{\zeta}_n$ in (8.4.0.1), if we identify $\tilde{G}$ with $\tilde{G}_1 := \mathbf{O}^2(\mathbf{C}_{H_f^-}(\hat{z}))$. Moreover, if $G$ is a subgroup of $H_1^-$ that centralizes $z$ modulo $E$ and $G \cong \mathrm{SU}_n(q)$, then $G$ is conjugate in $E\tilde{G}_1$ to $[\tilde{G}_1, \tilde{G}_1]$.*

Proof. Clearly, $|\hat{z}| = q + 1$ as $E$ is a 2-group. Thus the coset $E\hat{z}$ contains elements $\hat{z}$ of order $q + 1$, and $\boldsymbol{j}\hat{z}$ of order $2(q + 1)$, where $\mathbf{Z}(E) = \langle \boldsymbol{j} \rangle$. Next, $z$ fixes no no-identify element in $E/\mathbf{Z}(E)$, and so

$$\mathbf{C}_E(\hat{z}) = \mathbf{Z}(E). \tag{8.4.2.1}$$

It follows that exactly half of $E\hat{z}$ is $E$-conjugate to $\hat{z}$, and the other half is $E$-conjugate to $\boldsymbol{j}\hat{z}$. (Indeed, note that $x\hat{z}x^{-1} \in E\hat{z}$ as $E \lhd H_f^-$. Next, when $x, y \in E$, then $x\hat{z}x^{-1} = y\hat{z}y^{-1}$ if and only if $y^{-1}x \in \mathbf{C}_E(\hat{z}) = \mathbf{Z}(E)$. It follows that $\hat{z}$ has exactly $|E|/|\mathbf{Z}(E)| = |E|/2$ $E$-conjugates in $E\hat{z}$.)

Now note that $\mathbf{C}_{\mathrm{O}^-_{2nf}(2)}(z) = \tilde{G} = \mathbf{C}_{\mathrm{O}(U_f)}(z)$, whence the full inverse image $X$ of $\tilde{G}$ in $H_1^-$ fixes $E\hat{z}$ and contains $C := \mathbf{C}_{H_1^-}(\hat{z})$. Hence $\hat{z}^X = \hat{z}^X \cap E\hat{z} = \hat{z}^E$, it follows from the above result that

$$|C| = |\mathbf{C}_X(\hat{z})| = \frac{|X|}{|\hat{z}^X|} = \frac{|X|}{|\hat{z}^E|} = \frac{|X|}{|E|/2} = 2 \cdot |\tilde{G}|.$$

Since $C \cap E = \mathbf{Z}(E)$ by (8.4.2.1), this implies that

$$X/\mathbf{Z}(E) = (E/\mathbf{Z}(E)) \rtimes (C/\mathbf{Z}(E)),$$

and so

$$C/\mathbf{Z}(E) \cong X/E \cong \tilde{G}. \tag{8.4.2.2}$$

The same arguments show that (8.4.2.2) also for $\mathbf{C}_{H_f^-}(\hat{z})$, whence $C = \mathbf{C}_{H_f^-}(\hat{z})$. Next, the assumptions on $(n,q)$ imply by [**KlL**, Theorem 5.1.4] that $\mathrm{SU}_n(q)$ is perfect and has trivial Schur multiplier. Hence we see from (8.4.2.2) that the last term $D := C^{(\infty)}$ of the derived series of $C$ satisfies

$$D/(D \cap \mathbf{Z}(E)) \cong D\mathbf{Z}(E)/\mathbf{Z}(E) = (C/\mathbf{Z}(E))^{(\infty)} \cong G \cong \mathrm{SU}_n(q),$$

whence $D \cap \mathbf{Z}(E) = 1$ and $D \cong \mathrm{SU}_n(q)$. As $\tilde{G}/G \cong C_{q+1}$, (8.4.2.2) now implies that $C/D\mathbf{Z}(E) \cong C_{q+1}$ and $C/D \cong C_2 \rtimes C_{q+1} = C_2 \times C_{q+1}$. Since $D$ is perfect, it follows that $\mathbf{O}^2(C)$ contains $D$ and has index 2 in $C$, and in fact $C = \mathbf{Z}(E) \times \mathbf{O}^2(C)$. Now, $\mathbf{O}^2(C) \cong C/\mathbf{Z}(E) \cong \tilde{G}$ by (8.4.2.2), and so we can identify $\tilde{G}$ with $\tilde{G}_1 := \mathbf{O}^2(C)$.

The statement about $\psi|_{\tilde{G}_1}$ follows from Theorems 3.3 and 4.9.2 of [**Ge**].

To prove the last statement, note that $G \leq E\tilde{G}_1$ since $\mathbf{C}_{H_1^-/E}(z) = E\tilde{G}_1/E$. First we work in $\bar{X} := X/\mathbf{Z}(E) = (E/\mathbf{Z}(E)) \rtimes \tilde{G}$ and recall that $E/\mathbf{Z}(E)$ can be identified with the natural module for $\tilde{G} = \mathrm{GU}_n(q)$. Since $G$ is perfect and $\mathbf{O}_2(G) = 1$, $G$ embeds in $[\bar{X},\bar{X}] \cong \mathbb{F}_{q^2}^n \rtimes \mathrm{SU}_n(q)$, and in fact we have $(E/\mathbf{Z}(E)) \rtimes G = (E/\mathbf{Z}(E)) \rtimes [\tilde{G},\tilde{G}]$. Since $H^1(\mathrm{SU}_n(q), \mathbb{F}_{q^2}^n) = 0$, see [**CPS**, Table 4.3], $G$ is conjugate to $[\tilde{G},\tilde{G}]$ in $\bar{X}$. Conjugating $G$ in $E$ suitably, we may assume that $G\mathbf{Z}(E) = [\tilde{G}_1,\tilde{G}_1]\mathbf{Z}(E)$. Taking the derived subgroup, we obtain $G = [\tilde{G}_1,\tilde{G}_1]$. □

In view of Proposition 8.4.2, we will now fix a subgroup $C := \mathbf{C}_{H_f^-}(\hat{z}) = \tilde{G} \times \mathbf{Z}(E)$ in $H_f^-$. Fix a generator $\sigma$ of $\mathbb{F}_{q^2}^\times$ and set $\rho := \sigma^{q-1}$. We also fix a primitive $(q^2-1)^{\text{th}}$ root of unity $\boldsymbol{\sigma} \in \mathbb{C}^\times$ and let $\boldsymbol{\rho} = \boldsymbol{\sigma}^{q-1}$. By [**TZ2**, Lemma 4.1],

$$\tilde{\zeta}_n = \sum_{i=0}^{q} \tilde{\zeta}_{i,n} \tag{8.4.2.3}$$

decomposes as the sum of $q+1$ characters of $\tilde{G}$, where

$$\tilde{\zeta}_{i,n}(g) = \frac{(-1)^n}{q+1} \sum_{l=0}^{q} \boldsymbol{\rho}^{il}(-q)^{\dim \mathrm{Ker}(g - \rho^l \cdot 1_W)}. \tag{8.4.2.4}$$

In particular, $\tilde{\zeta}_{i,n}$ has degree $(q^n - (-1)^n)/(q+1)$ if $i > 0$ and $(q^n + (-1)^n q)/(q+1)$ if $i = 0$.

We will let $\zeta_{i,n}$ denote the restriction of $\tilde{\zeta}_{i,n}$ to $G = \mathrm{SU}_n(q)$, for $0 \leq i \leq q$. By [**TZ2**, Lemma 4.7], these $q+1$ characters are all irreducible and distinct. Formula (7.2.1) implies that Weil characters $\zeta_{i,n}$ enjoy the following branching rule while restricting to the natural subgroup $H := \mathrm{Stab}_G(w) \cong \mathrm{SU}_{n-1}(q)$ ($w \in W$ any anisotropic vector):

$$\zeta_{i,n}|_H = \sum_{j=0,\ j \neq i}^{q} \zeta_{j,n-1}. \tag{8.4.2.5}$$

Furthermore, complex conjugation fixes $\tilde{\zeta}_{0,n}$ and sends $\tilde{\zeta}_{j,n}$ to $\tilde{\zeta}_{q+1-j,n}$ when $1 \leq j \leq q$. As $n \geq 3$ is odd, it is also known that $\tilde{\zeta}_{0,n}$ is of symplectic type. Let

$$\Psi_0 : C \to \mathrm{Sp}(V)$$

be a complex representation affording this character on restriction to $\tilde{G}$ and being faithful on $\mathbf{Z}(E)$. For the remaining $1 \leq i \leq q$, also let

$$\Psi_i : C \to \mathrm{GL}(V)$$

be a complex representation affording the character $\tilde{\zeta}_{i,n}$ on restriction to $\tilde{G}$ and again being faithful on $\mathbf{Z}(E)$.

LEMMA 8.4.3. *Assume $n \geq 3$ is odd and $(n, q) \neq (3, 2)$.*

(i) $\Psi_0(\mathrm{GU}_n(q)) \cong \mathrm{PGU}_n(q)$ *is contained in* $\mathrm{Sp}(V)$ *and contains* $\Psi_0(\mathrm{SU}_n(q)) \cong \mathrm{PSU}_n(q)$ *with index $d$, where $d := \gcd(n, q+1)$.*

(ii) *If $1 \leq i \leq q$, then* $\mathrm{Ker}(\Psi_i)$ *is a central subgroup of order* $\gcd(i, q+1)$, *and* $\mathrm{Ker}(\Psi_i|_{\mathrm{SU}_n(q)})$ *is a central subgroup of order* $\gcd(i, n, q+1)$. *Furthermore,* $\Psi_i(\mathrm{GU}_n(q)) \cap \mathrm{SL}(V)$ *contains* $\Psi_i(\mathrm{SU}_n(q))$ *with index* $\gcd(i, n, q+1)$.

(iii) *Suppose $H \leq \mathrm{GU}_n(q)$. Then $\Psi_i(H) \leq \mathrm{SL}(V)$ for all $0 \leq i \leq q$ if and only if $H \leq \mathrm{SU}_n(q)$.*

(iv) *Suppose $H \leq C = \tilde{G} \times \mathbf{Z}(E)$. Then $\Psi_i(H) \leq \mathrm{SL}(V)$ for all $0 \leq i \leq q$ if and only if $H \leq \mathrm{SU}_n(q)$.*

PROOF. According to [**TZ2**, §4], one can label $\Psi_i$ in such a way that

$$\Psi_i(z) = \boldsymbol{\rho}^i \cdot 1_V \tag{8.4.3.1}$$

for the generator $z = \rho \cdot 1_W$ of $\mathbf{Z}(\tilde{G})$. In particular, $\mathrm{Ker}(\Psi_0) \cap \mathbf{Z}(\tilde{G}) = \langle z \rangle$, and (i) follows.

Now we can assume $1 \leq i \leq q$. By (8.4.3.1), $z^j \in \mathrm{Ker}(\Psi_i)$ if and only if $j$ is divisible by $(q+1)/\gcd(i, q+1)$. Furthermore, $z^{j(q+1)/d} \in \mathrm{Ker}(\Psi_i|_{\mathrm{SU}_n(q)})$ if and only if $j$ is divisible by $d/\gcd(i, d) = d/\gcd(i, n, q+1)$ for $d = \gcd(n, q+1)$, equivalently, if $j(q+1)/d$ is divisible by $(q+1)/\gcd(i, n, q+1)$. Hence (ii) follows.

Consider the element $g := \mathrm{diag}(\rho, 1, 1, \ldots, 1) \in \tilde{G}$; note that $\tilde{G} = \langle G, g \rangle$. Then (8.4.2.4) implies that

$$\tilde{\zeta}_{i,n}(g^k) = -\frac{q^{n-1} - 1}{q+1} + \boldsymbol{\rho}^{ik}$$

when $1 \leq k \leq q$. It follows that $\Psi_i(g)$ has eigenvalues $\boldsymbol{\rho}^j$, $1 \leq j \leq q$, with multiplicity $(q^{n-1} - 1)/(q+1)$ if $j \neq i$ and $1 + (q^{n-1} - 1)/(q+1)$ if $j = i$, and so

$$\det(\Psi_i(g)) = \boldsymbol{\rho}^i.$$

In particular, $\Psi_i(g^j) \in \mathrm{SL}(V)$ if and only if $j$ is divisible by $(q+1)/\gcd(i, q+1)$. Since $\mathrm{SU}_n(q)$ is perfect, (ii) and the "if" directions of (iii), (iv) follow.

For the "only if" direction of (iii), assume that $\Psi_1(H) \leq \mathrm{SL}(V)$, and consider any $h \in H$. If $\det(h) = \rho^j$ for $0 \leq j \leq q$, then $hg^{-j} \in \mathrm{SU}_n(q)$ and so $\Psi_1(hg^{-j}) \in \mathrm{SL}(V)$ by the previous statement. It follows that

$$1 = \det(\Psi_1(h)) = \det(\Psi_1(hg^{-j}))\det(\Psi_1(g^j)) = \det(\Psi_1(g^j)) = \boldsymbol{\rho}^j,$$

whence $j = 0$ and $\det(h) = 1$, as stated.

For the "only if" direction of (iv), again assume that $\Psi_1(H) \leq \mathrm{SL}(V)$. If $H \leq \tilde{G} = \mathrm{GU}_n(q)$, then we are done by (iii). Suppose $H \not\leq \tilde{G}$, and consider any $h \in H \smallsetminus \tilde{G}$. Then $h^{q+1} = \boldsymbol{j}h_1$ for some $h_1 \in \mathrm{SU}_n(q)$. Since $\Psi_1(\boldsymbol{j}) = -1_V$ and $\dim V$ is odd, we have that

$$\det(\Psi_1(h))^{q+1} = \det(\Psi_1(\boldsymbol{j}))\det(\Psi_1(h_1)) = -1,$$

a contradiction. □

The first main result of this section is the following theorem:

THEOREM 8.4.4. *Let $q = 2^f$ and let $n \geq 3$ be an odd integer, with $(n,q) \neq (3,2)$. Consider the subgroup $H_1^- = 2_-^{1+2nf} \cdot \mathrm{O}_{2nf}^-(2) < \mathrm{GL}_{2^{nf}}(\mathbb{C})$ constructed in Theorem 8.2.1 and its natural representation $\Phi$ on $V := \mathbb{C}^{2^{nf}}$. Suppose that $G \leq H_1^-$ is a subgroup such that $\Phi|_G = \oplus_{j=0}^{q}\Phi_j$ is a sum of $q+1$ irreducible summands, $\Phi_0$ of degree $(q^n - q)/(q+1)$ and $\Phi_j$ of degree $(q^n+1)/(q+1)$ for $1 \leq j \leq q$. Then $G$ is conjugate to a subgroup of $C_2 \times \tilde{G} \cong C_2 \times \mathrm{GU}_n(q)$ identified in Proposition 8.4.2, where $\mathrm{GU}_n(q)$ is acting on $V$ via the total Weil representation with character $\tilde{\zeta}_n$ in* (8.4.0.1). *Moreover, $\mathrm{SU}_n(q) \lhd G \leq C_2 \times \mathrm{GU}_n(q)$, with one exception $G \rhd L_1 \in \{\mathrm{PSL}_2(11), \mathrm{SL}_2(11)\}$ when $(n,q) = (5,2)$.*

PROOF. (a) The assumption $n \geq 3$ and $(n,q) \neq (3,2)$ implies that $2^{2nf} - 1$ admits a primitive prime divisor $\ell_1$. Furthermore, since $\Phi_1$ is irreducible of degree $(q^n+1)/(q+1)$, $\ell$ divides $|G|$, and so $G$ admits an element $g$ of order $\ell_1$. Next, $G$ normalizes $E := 2_-^{1+2nf}$ and $U_1 := E/\mathbf{Z}(E) \cong \mathbb{F}_2^{2nf}$, and $\mathbf{C}_{H_1^-}(E/\mathbf{Z}(E)) = E$, so $G$ acts faithfully on $E/\mathbf{Z}(E)$; in particular, $g$ induces an element of order $\ell_1$ in $H_1^-/E$. The choice of $\ell_1$ ensures that any such element acts irreducibly on $E/\mathbf{Z}(E)$. Hence, if $\mathbf{Z}(E)G \cap E \neq \mathbf{Z}(E)$, then $\mathbf{Z}(E)G \geq E$, and so $\mathbf{Z}(E)G$ acts irreducibly on $V$. Since $\mathbf{Z}(E)$ acts via scalars on $V$, this contradicts the reducible action of $G$ on $V$. We have shown that $\mathbf{Z}(E)G \cap E = \mathbf{Z}(E)$, and so

$$\bar{G} := \mathbf{Z}(E)G/\mathbf{Z}(E) \cong G/(G \cap \mathbf{Z}(E)) \cong G/(G \cap E)$$

embeds in $H_1^-/E = \mathrm{O}(U_1) \cong \mathrm{O}_{2nf}^-(2)$. The main bulk of the proof is to identify this subgroup $\bar{G}$ inside $\mathrm{O}(U_1) < \mathrm{GL}(U_1)$.

(b) First we assume that $nf \neq 5, 6, 9$; in particular,

$$nf \geq 7,$$

so that $2^{2nf} - 1$ admits a large primitive prime divisor $\ell$, in which case we choose such an $\ell$ to maximize the $\ell$-part of $2^{2nf} - 1$. Note the assumptions imply that $|\bar{G}|$ is divisible by both $(q^n - q)/(q+1)$ and $(q^n+1)/(q+1)$. In particular, $\bar{G} < \mathrm{GL}(U_1)$ has order divisible by

$$qQ := q(2^{2nf} - 1)_\ell. \tag{8.4.4.1}$$

Let $L := \mathbf{O}^{\ell'}(\bar{G})$, $M$ denote the full inverse image of $L$ in $G$ so that

$$\text{(8.4.4.2)} \qquad \text{either } M = L, \text{ or } \mathbf{Z}(G) \geq \mathbf{Z}(E) = C_2 \text{ and } M/\mathbf{Z}(E) = L,$$

and let $d(L)$ denote the smallest degree of nontrivial complex projective irreducible representations of $L$. Note that

$$\text{(8.4.4.3)} \qquad d(L) \leq (q^n+1)/(q+1) \leq (q^n+1)/3.$$

(Otherwise $\Phi_1$ induces a trivial projective representation of $L$. Then $\Phi_1(M)$ is a scalar, hence cyclic central subgroup of $\Phi_1(G)$, and $\Phi_1(G)/\Phi_1(M)$ has order dividing $2|\bar{G}/L|$, a prime to $\ell$ integer. It follows from Ito's theorem [**Is**, (6.15)] that $\deg(\Phi_1)$ is also coprime to $\ell$, a contradiction.) Similarly, if $L$ is cyclic of order $Q$, then $M = C \times M_1$, where $M_1$ is cyclic of order $Q$ and $|C| \leq 2$. In this case, again by Ito's theorem, the degree of any irreducible character of $G$ divides $|G/M_1|$, an integer prime to $\ell$, and so again $G$ cannot be irreducible on $\Phi_1$. Now we can apply Theorem 8.3.1 with $(q_0, d) = (2, 2nf)$ to arrive at one of the following cases (note that 8.3.1(i), (ii) cannot occur since $\bar{G}$ fixes $\mathsf{Q}_1$).

(b1) $L \cong \Omega^-_{2nf/j}(2^j)$ for some divisor $1 \leq j \leq nf/2$ of $nf$. If $j \leq nf/3$, then by [**TZ1**, Theorem 1.1] we have $d(L) > (q^n+1)/3$, contradicting (8.4.4.3). If $j = nf/2$, then $L \cong \mathrm{SL}_2(q^n)$ with $q^n \geq 2^7$, and so by [**TZ1**, Theorem 1.1] we have $d(L) = q^n - 1 > (q^n+1)/3$, again contradicting (8.4.4.3).

(b2) There is some even divisor $j = 2k$ of $2nf$ with $k|nf$ and $2 \nmid nf/k > 1$, such that $U_1 = \mathbb{F}_2^{2nf}$ can be viewed as a $nf/k$-dimensional vector space over $\mathbb{F}_{q^j}$ endowed with a non-degenerate Hermitian form and $L = \mathrm{SU}(U_1) \cong \mathrm{SU}_{nf/k}(2^k)$. Now if $k \leq f-1$, then by [**TZ1**, Theorem 1.1] we have

$$d(L) > (2^k)^{nf/k-1}/2 = q^n/2^{k+1} \geq q^{n-1} > (q^n+1)/(q+1),$$

contradicting (8.4.4.3). Suppose $k > f$, and let $\psi$ be an irreducible constituent of the $M$-character afforded by $\Phi_0$, so that $\psi(1)|(q^n-q)/(q+1)$. By [**TZ1**, Theorem 4.1],

$$\psi(1) \in \left\{1, \frac{q^n+1}{2^k+1}, \frac{q^n-2^k}{2^k+1}\right\}.$$

Note that $\psi(1) \neq (q^n-2^k)/(2^k+1)$ as $k > f$. The possibility $\psi(1) = (q^n+1)/(2^k+1)$ is also ruled out since $\ell \nmid \dim \Phi_0$. Hence $\psi(1) = 1$. Note that $L$ contains an element of order $\ell$, and so by (8.4.4.2), this has an inverse image $h \in M$ of same order $\ell$ which then acts trivially in $\Phi_0$. As $|G/M|$ is coprime to $\ell$, each irreducible constituent of $(\Phi_i)|_M$ with $i > 0$ has $\ell$-defect 0 and so $h$ has trace 0 on it. It follows that $\mathrm{Trace}(\Phi(h)) = \dim \Phi_0 = (q^n-q)/(q+1) > 1$, which is a contradiction since $h$ has no nonzero fixed point on $U_1$ and so $|\mathrm{Trace}(\Phi(h))| \leq 1$ by Lemma 7.2.1. [We take this opportunity to mention that this same argument shows that $\psi(1) \neq 1$ in part (iii) of the proof of [**KT3**, Theorem 3.4], fixing an inaccuracy therein.]

We have shown that $k = f$, i.e. $L = \mathrm{SU}(U_1) \cong \mathrm{SU}_n(q)$. As $2 \nmid n \geq 3$ and $(n,q) \neq (3,2)$, $\mathrm{SU}_n(q)$ has trivial Schur multiplier, whence $M = C \times L_1$ with $C \leq C_2$ and $L_1 \cong L$. Also, $U_1$ carries the structure of the natural module $W_1 = \mathbb{F}_{q^2}^n$ for $L$, and $L < \mathrm{O}^-_{2nf}(2)$ preserves the $\mathbb{F}_2$-valued quadratic form $\mathsf{Q}_1$ on $U_1$. Hence $L$ satisfies the hypothesis of Proposition 8.4.1(b), and so, after a suitable rescaling of the Hermitian form $\circ$ on $W_1$, $\mathsf{Q}_1$ is obtained from $\circ$ via (8.4.0.3), i.e $\mathsf{Q}_1(u) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(u \circ u)$ and $L = \mathrm{SU}(W_1) < \Omega(U_f) \leq \Omega(U_1)$. In particular, $L$ centralizes a generator $z$ of the center of $\mathrm{GU}(W_1) \cong \mathrm{GU}_n(q)$. Applying Proposition 8.4.2, we conclude that $L_1 = [\tilde{G}_1, \tilde{G}_1] \cong \mathrm{SU}_n(q)$ after a suitable conjugation in $H_1^-$ (where $\tilde{G}_1 \cong \mathrm{GU}_n(q)$ is constructed in Proposition 8.4.2). We also know that the restriction of $\Phi$ to $\tilde{G}_1$ is a total Weil representation of $\tilde{G}_1$, and so the restriction $\Phi|_{L_1}$ is the total Weil representation of $L_1$. As $L \lhd \bar{G}$,

$$\bar{G} \leq \mathbf{N}_{H_1^-/E}(L) \cong \mathrm{GU}(W_1) \rtimes \langle \sigma \rangle,$$

where $\sigma$ is an involutive automorphism of $\mathrm{GU}(W_1)$ that sends $z$ to $z^{-1}$. Recall the decomposition $\Phi|_{\tilde{G}_1} = \oplus_{i=0}^{q} \Psi_i$, where $\Psi_0$ of degree $(q^n - q)/(q+1)$ and $\Psi_i$ of degree $(q^n+1)/(q+1)$ for $1 \leq i \leq q$, and $\Psi_i(\hat{z})$ is the multiplication by $\xi^i$ for a primitive $(q+1)^{\mathrm{th}}$ root of unity $\xi \in \mathbb{C}^\times$. In particular, $\sigma$ fuses $\Psi_1$ and $\Psi_q$. Since $L_1 = [M, M] \lhd G$, the assumption on $\Phi|_G$ now implies that $\bar{G} \leq \mathrm{GU}(W_1)$, and so $L_1 \lhd G \leq \mathbf{C}_{H_1^-}(\hat{z}) = \mathbf{Z}(E) \times \tilde{G}_1$, as stated.

(b3) $(2nf, L) = (6j, G_2(r))$ with $r = 2^{nf/3} = q^{n/3}$, or $(2nf, L) = (6j, {}^2B_2(r))$ with $r = 2^{nf/2} = q^{n/2}$. In the former case, $d(L) \geq r(r^2-1) > q^n/2$ (see e.g [**TZ1**, Table 1]), contradicting (8.4.4.3). In the latter case, let $\psi$ be an irreducible constituent of the $M$-character afforded by $\Phi_0$, so that $\psi(1) | (q^n - q)/(q+1) < r^2/2$. It follows from [**Bur**] that $\psi(1) = 1$ or $\psi(1) = \sqrt{r/2}(r-1)$. The same arguments as in (b2) rules out the possibility $\psi(1) = 1$. So $\psi(1) = \sqrt{r/2}(r-1)$, and so, by comparing 2-parts, we have $r \leq 2q^2$ and so either $n = 3$ or $(n, q) = (5, 4)$. Now, if $n = 3$ then $r - 1 = q^{3/2} - 1$ does not divide $(\dim \Phi_0)/q = q - 1$, and if $(n, q) = (5, 4)$ then $r - 1 = q^{5/2} - 1 = 31$ does not divide $(\dim \Phi_0)/q = 51$, a contradiction.

(b4) $(f, nf, L) = (1, 10, \mathrm{PSL}_2(41))$ or $(1, 8, \mathrm{PSL}_2(17))$. These cases are excluded since $2 \nmid n$.

(c) It remains to consider the cases $nf = 5, 6, 9$. Then, aside from cases already handled in (b), by Proposition 8.3.3 we need to consider the following possibilities.

(c1) $(f, nf) = (1, 6)$. This case is excluded since $2 \nmid n$.

(c2) $(f, nf) = (1, 9)$ and $L$ is one of $3\mathsf{J}_3$, $\mathsf{A}_{19}$, $\mathsf{A}_{20}$, or $\mathrm{PSL}_2(19)$. In all these cases, $L$ acts irreducibly on $U_1 = \mathbb{F}_2^{18}$, and so $\mathbf{C}_{\mathrm{O}(U_1)}(L)$ embeds in a finite extension of $\mathbb{F}_2$, hence a cyclic group of odd order. Next, $|\mathrm{Out}(L)| \leq 2$ and $L \lhd \bar{G}$, so we see that $\bar{G}$ has index at most 2 over $\mathbf{C}_{\bar{G}}(L)L$. It follows that $L_1 \lhd G \leq (AL_1) \cdot 2$, where $L_1$ is a cover of $L$ and $M = AL_1$ and $A$ an abelian group centralizing $L_1$, see (8.4.4.2). Restricting $\Phi_i$ to $L_1$, we see that $L_1$ admits irreducible representations of degree 171, and also either 85 or 170. This rules out the last three cases, see [**GAP**]. Note that $3\mathsf{J}_3 < \mathrm{SU}_9(2)$, see [**BHR**, Table 8.57]. However, $3\mathsf{J}_3$ does not have an irreducible representation of degree 170, and $3\mathsf{J}_3 \cdot 2$ does not have an irreducible representation of degree 171, see [**GAP**].

(c3) $(f, nf) = (1, 5)$ and $L$ is one of $\mathsf{M}_{11}$, $\mathsf{M}_{12}$, $\mathsf{M}_{22}$, $\mathsf{A}_{11}$, $\mathsf{A}_{12}$, or $\mathrm{PSL}_2(11)$. In all these cases, $L$ acts irreducibly on $U_1 = \mathbb{F}_2^{10}$, and so $\mathbf{C}_{\mathrm{O}(U_1)}(L)$ embeds in a finite extension of $\mathbb{F}_2$, hence a cyclic group of odd order. Next, $|\mathrm{Out}(L)| \leq 2$ and $L \lhd \bar{G}$, so we see that $\bar{G}$ has index at most 2 over $\mathbf{C}_{\bar{G}}(L)L$. It follows that $L_1 \lhd G \leq (AL_1) \cdot 2$, where $L_1$ is a cover of $L$ and $M = AL_1$ with $A$ an abelian group centralizing $L_1$ of order at most 2, see (8.4.4.2). Restricting $\Phi_i$ to $L_1$, we see that $L_1$ admits irreducible representations of degree 11, and also either 5 or 10. This rules out the cases $L = \mathsf{M}_{22}$, $\mathsf{A}_{11}$ and $\mathsf{A}_{12}$, see [**GAP**]. In the case $L = \mathsf{M}_{11}$ or $\mathsf{M}_{12}$, we see that $\mathrm{Trace}(\Phi_i(g))$ equals 1 for $i = 0$ and 2 for $i = 1, 2$, if $g$ belongs to class $3a$ in [**GAP**], and thus $\mathrm{Trace}(\Phi(g)) = 5$, contradicting Lemma 7.2.1. [Note that $\mathrm{PSL}_2(11) < \mathrm{SU}_5(2)$, see [**CCNPW**].] □

The next result will be used frequently in "going-up" situations:

THEOREM 8.4.5. *Let $N \geq 4$ be an integer and consider the subgroup $H_1^- = 2_-^{1+2N} \cdot \mathrm{O}_{2N}^-(2)$ of $\mathrm{Sp}_{2^N}(\mathbb{C})$ constructed in Theorem 8.2.1.*

(a) *Let $G < \mathrm{GL}(V) \cong \mathrm{GL}_{2^N}(\mathbb{C})$ be a finite subgroup that satisfies $(\mathbf{S}+)$ and contains an* $\mathsf{ssp}$*-element of central order $2^N + 1$. Then either $G$ is in the extraspecial normalizer case of* [**KT5**, Lemma 1.1]*, or $\mathrm{PSL}_2(q) \leq G \leq \mathrm{Aut}(\mathrm{PSL}_2(q))$ for some prime power $2^N \leq q \leq 2^{N+1} + 1$. Suppose in addition that $G < \mathrm{Sp}(V) \cong \mathrm{Sp}_{2^N}(\mathbb{C})$. Then one of the following statements holds.*
  ($\alpha$) *Up to conjugation, $\mathbf{O}_2(H_1^-) \lhd G \leq H_1^-$.*
  ($\beta$) *$q := 2^{N+1} + 1$ is a Fermat prime and $G = \mathrm{SL}_2(q)$.*

(b) *Let $G < \mathrm{GL}(V) \cong \mathrm{GL}_{2^N}(\mathbb{C})$ be any finite irreducible subgroup that contains a subgroup $G_1 \cong \mathrm{SU}_n(q)$ with $q^n = N$ and $2 \nmid n \geq 3$. Suppose $G_1$ acts on $V = \mathbb{C}^{2^N}$ via its total Weil representation. Then $G$ satisfies $(\mathbf{S}+)$ on $V$.*

(c) *If $2 \nmid N$, then $H_1^-$ is a maximal finite subgroup of $\mathrm{Sp}_{2^N}(\mathbb{C})$. If $2|N$ and $H_1^-$ satisfies $(\mathbf{S}+)$, then $H_1^-$ is a maximal finite subgroup of $\mathrm{Sp}_{2^N}(\mathbb{C})$.* [It will be shown in Theorem 8.5.5 that $H_1^-$ always satisfies $(\mathbf{S}+)$.]

PROOF. (a) Since $G$ satisfies $(\mathbf{S}+)$, we can apply [**KT5**, Lemma 1.1] to $G$. First suppose that $G$ is almost quasisimple, and let $S$ be the unique non-abelian composition factor of $G$. By [**KT5**, Lemma 1.4], $V$ is irreducible over $L := G^{(\infty)}$, a cover of $S$. By hypothesis, $V$ is an irreducible $\mathbb{C}G$-module of dimension $2^N \geq 16$ and $G$ admits an $\mathsf{ssp}$-element $g$ of central order $\bar{\mathsf{o}}(g) = 2^N + 1$. This excludes the case $S = \mathsf{A}_n$ with $n \geq 8$ by [**KT5**, Theorem 6.2]. The cases $S = \mathsf{A}_n$ with $5 \leq n \leq 7$ are also excluded because $G/\mathbf{Z}(G) \hookrightarrow \mathrm{Aut}(S)$ would contain elements of central order only $\leq 12$ [**GAP**]. Next, the cases where $S$ is a sporadic group are excluded by [**KT5**, Theorem 6.4]. This leaves only the case $S$ is a simple group of Lie type in characteristic $p$. Now we can apply [**KT5**, Theorem 6.6] to see that either

(a1) $V$ comes from a Weil module of a finite classical group $G$ with $S = \mathrm{PSL}_n(q)$ with $n \geq 3$, $\mathrm{PSU}_n(q)$ with $n \geq 3$, or $\mathrm{PSp}_{2n}(q)$ with $n \geq 2$, or

(a2) $S = \mathrm{PSL}_2(q)$ and $\dim(V) \leq \bar{\mathsf{o}}(g) \leq q + 1$.

If $S = \mathrm{PSL}_n(q)$ with $n \geq 3$, then since $\dim(V) + 1 = \bar{\mathsf{o}}(g)$, by [**KT5**, Theorem 8.1] we must have that $2^N = \dim(V) = q(q^{n-1} - 1)/(q - 1)$, which is impossible. If $S = \mathrm{PSp}_n(q)$ with $n \geq 2$, then since $\dim(V) + 1 = \bar{\mathsf{o}}(g)$, by [**KT5**, Theorem 8.2] we must have that

$$2^N = \dim(V) = (q^n - 1)/2, \tag{8.4.5.1}$$

i.e. $q^n - 1 = 2^{N+1}$. This implies that $n$ is a 2-power (otherwise $q^n - 1$ would have an odd divisor $> 1$), and in fact $n = 2$ (otherwise $(q^{n/2} + 1)/2 > 1$ is again an odd divisor of $q^n - 1$), in which case $q = 3$ and $2^{N+1} = 8$ (otherwise one of $(q - 1)/2 > 1$ and $(q + 1)/2 > 1$ is odd), again a contradiction. Suppose $S = \mathrm{PSU}_n(q)$ with $n \geq 3$. Since $\dim(V) + 1 = \bar{\mathsf{o}}(g)$, checking the cases

$$(n, q) = (3, 3),\ (3, 4),\ (4, 2),\ (4, 3),\ (5, 2),\ (6, 2)$$

directly using [**GAP**], we may apply [**KT5**, Theorem 8.1] to see that $2 \nmid n$ and $2^N = \dim(V) = q(q^{n-1} - 1)/(q + 1)$, which is again impossible.

Thus we must be in (a2). Then $2^N = \dim(V) = \bar{\mathsf{o}}(g) - 1 \leq q$. Thus $S = \mathrm{PSL}_2(q)$ and $q \geq 17$, and so $2^N = \dim(V) \geq (q-1)/2$, i.e. $q \leq 2^{N+1}+1$.

Assume in addition that $G < \mathrm{Sp}(V)$. Then $V$ is irreducible over $L$, a cover of $S$, so the symplectic type of $V$ rules out the case $2^N = q$. Since $2^N \geq 16$, this leaves only $2^N = (q \pm 1)/2$. If $2^N = (q+1)/2$, and thus $G/\mathbf{Z}(G) \hookrightarrow \mathrm{Aut}(\mathrm{PSL}_2(q))$ admits an element of odd order $(q+3)/2 \geq 17$, a contradiction. So $2^N = (q-1)/2$, and so, the analysis of (8.4.5.1) shows that $q = 2^{N+1}+1$ is a Fermat prime. It is easy to see in this case that $L = \mathrm{SL}_2(q)$, $\mathbf{C}_{\mathrm{Sp}(V)}(L) = \mathbf{Z}(L)$, and so $G = L$, leading to possibility $(\beta)$.

The remaining case is that $G$ is an extraspecial normalizer. Applying [**KT5**, Theorem 8.5], we see that $G \rhd R$, where $R = \mathbf{Z}(R)E$ with $E = 2^{1+2N}_{\epsilon}$ and $\mathbf{Z}(R) \hookrightarrow C_4$. Assuming $G < \mathrm{Sp}(V)$, we then have $\mathbf{Z}(R) = \mathbf{Z}(E)$, $R = E$, and $\epsilon = -$. Up to conjugation, we now have $E = \mathbf{O}_2(H_1^-)$ and $G \leq H_1^-$, as stated in $(\alpha)$.

(b) Since $N \geq 4$ and $q^n = 2^N$ with $2 \nmid n \geq 3$, we either have $n \geq 5$, or $n = 3$ or $q \geq 4$. Hence, if $P(G_1)$ denotes the smallest index of proper subgroups of $G_1$, then

$$P(G_1) > q^n, \tag{8.4.5.2}$$

see [**KlL**, Table 5.2.A]. By assumption, $G$ is irreducible on $V$. Suppose the $G$-module $V$ is imprimitive: $G$ permutes transitively the $t > 1$ summands of some decomposition $V = \oplus_{i=1}^{t} V_i$. Since $t \leq \dim(V) = q^n$, (8.4.5.2) implies that $G_1$ fixes every summand $V_i$, and hence each $V_i$ is a direct sum of some irreducible Weil modules of $G_1$. As $V|_{G_1}$ is a total Weil module, we may assume that

$$\frac{q^n - q}{q+1} + a\frac{q^n+1}{q+1} = \dim(V_1) = \dim(V_2) = b\frac{q^n+1}{q+1}$$

for some integers $a \geq 0$ and $b \geq 1$, whence $(a+1-b)(q^n+1)/(q+1) = 1$, a contradiction. Hence $V$ is primitive.

Suppose the action of $G_1$ on $V$ preserves some tensor decomposition $V = A \otimes_{\mathbb{C}} B$ with $\dim(A) \geq \dim(B) > 1$. Then $B$ yields a projective $G_1$-representation of dimension $\leq q^{n/2}$ (see part (i) of the proof of [**KRLT3**, Theorem 2.4]). Since $G_1$ is perfect and the dimension of any nontrivial irreducible projective representation of $G_1$ is at least $(q^n - q)/(q+1)$, cf. [**TZ1**, Theorem 1.1], the action of $G_1$ is linearized as a trivial representation, whence the projective action of $G_1$ on $A$ is actually linear. Thus the $G_1$-module $V$ is a direct sum of $\dim(B)$ copies of the $G_1$-module $A$, contradicting the prescribed action of $G_1$ on $V$. In particular, $G$ does not fix any tensor decomposition structure on $V$.

Finally, suppose that the action of $G$ on $V$ preserves some tensor induced decomposition $V = V_1^{\otimes t}$ with $t > 1$. Then $t \leq \log_2 q^n < q^n$. As $G_1$ permutes the $t$ tensor factors of this decomposition, (8.4.5.2) now implies that this permutation action is trivial, i.e. $G_1$ preserves a tensor decomposition $V = V_1 \otimes \ldots \otimes V_t$ with $V_i \cong V_1$. This however contradicts the preceding conclusion. Hence $(G, V)$ satisfies ($\mathbf{S}$+).

(c) Suppose $H_1^- \leq G < \mathrm{Sp}_{2^N}(\mathbb{C})$ for some finite subgroup $G$. If $2 \nmid N$, then by Proposition 8.4.2, $H_1^-$ contains a subgroup $G_1 \cong \mathrm{GU}_N(2)$ that acts on $V$ via a total Weil representation. It follow from (b) that $G$ satisfies ($\mathbf{S}$+) on $V$. So we may now assume that $H_1^-$ satisfies ($\mathbf{S}$+) for all $N$. Next, any generator of a cyclic maximal torus $C_{2^N+1}$ of $\Omega_{2N}^-(2)$ gives rise to an $\mathsf{ssp}$-element on $V$ of central order $2^N + 1$, cf. Lemma 8.2.2. By (a), $G$ must either satisfy $(\alpha)$ or $(\beta)$. In the former case, $|G| \leq |H_1^-|$, and so $G = H_1^-$. In the latter case, $\mathrm{SL}_2(2^{N+1}+1) = G \geq H_1^- = 2_-^{1+2N} \cdot \mathrm{O}_{2N}^-(2)$, a contradiction. □

Note that it was shown in [**NRS**, Theorem 5.6] that $\Gamma(2,N,+) = H_1^+$ is a maximal finite subgroup of $\mathrm{GL}_{2^N}(\mathbb{R})$ if $N \geq 2$. Also, it will be shown in Theorem 8.5.5 that $\Gamma(2,N,-) = H_1^-$ satisfies (**S**+) when $2|N$.

## 8.5. Local systems in characteristic $p = 2$

In this section, we fix a power $q = 2^f$, and work with the local system

$$\mathcal{G}(n, m_1, \dots, m_r; q) = \mathcal{G}(q^n+1, q^{m_1}+1, \dots, q^{m_{r-1}}+1, \kappa, \mathbb{1}) \tag{8.5.0.1}$$

on $\mathbb{A}^r/\mathbb{F}_2$ whose trace function is given as follows: for $k/\mathbb{F}_2$ a finite extension, and $(s_1, \dots, s_r) \in k^r$,

$$(s_1, \dots, s_r) \mapsto \frac{-1}{\sqrt{\#k}} \sum_{x \in k} \psi_k\big(x^{q^n+1} + s_1 x^{q^{m_1}+1} + \ldots + s_{r-1} x^{q^{m_{r-1}}+1} + s_r x^{\kappa}\big),$$

where $r \geq 1$ and $n > m_1 > \ldots > m_r \geq 0$; furthermore, $\kappa := q^{m_r}+1$ if $m_r \geq 1$ and $\kappa := 1$ if $m_r = 0$. [The first notation in (8.5.0.1) is chosen for brevity, whereas the second follows our general notational scheme in the book.]

For future reference, we state the following general fact:

LEMMA 8.5.1. *Let $p$ be a prime, $k \geq 1$, and let $A > B_1 > \ldots > B_k \geq 1$ be integers with $p \nmid AB_1 \ldots B_k$. Consider the local system $\mathcal{F} = \mathcal{F}(A, B_1, \dots, B_k, \theta)$ over $\mathbb{A}^k$ with trace function for any finite extension $L/\mathbb{F}_p$*

$$(t_1, \dots, t_k) \in L^k \mapsto -\sum_x \psi_L\big(x^A + t_1 x^{B_1} + \ldots + t_k x^{B_k}\big)\theta(x),$$

*and the local system $\mathcal{F}^\sharp = \mathcal{F}^\sharp(A, B_1, \dots, B_k, \theta)$ over $\mathbb{G}_m \times \mathbb{A}^k$ with trace function*

$$(s, t_1, \dots, t_k) \in L^\times \times L^k \mapsto -\sum_x \psi_L\big(s x^A + t_1 x^{B_1} + \ldots + t_k x^{B_k}\big)\theta(x),$$

*Denote by $N$ the order of $\theta$. Then the geometric monodromy group $H$ of $\mathcal{F}^\sharp$ contains the geometric monodromy group $G$ of $\mathcal{F}$ as a normal subgroup, with cyclic quotient of order dividing $AN$.*

PROOF. Consider the local system $\mathcal{F}^*$ over $\mathbb{G}_m \times \mathbb{A}^k$ with trace function

$$(s, t_1, \dots, t_k) \mapsto -\sum_x \psi_L\big(s^{AN} x^A + t_1 x^{B_1} + \ldots + t_k x^{B_k}\big)\theta(x)$$

and geometric monodromy group $K$. Then $\mathcal{F}^*$ is the $[s \mapsto s^{AN}] \times \mathrm{Id}_{\mathbb{A}^k}$ partial Kummer pullback of $\mathcal{F}^\sharp$, so $H$ contains the geometric monodromy group $K$ of $\mathcal{F}^*$ as a normal subgroup, with cyclic quotient of order dividing $AN$. Next, the change of variable $x \mapsto x/s^N$, followed by the reparameterization $s \mapsto s, t_i \mapsto t_i s^{NB_i}$ makes $\mathcal{F}^*$ geometrically isomorphic to the tensor product of the constant sheaf on $\mathbb{G}_m$ and $\mathcal{F}$, whence $K \cong G$. □

We also consider the local system

$$\mathcal{G}^\sharp(n, m_1, \ldots, m_r; q) = \mathcal{G}^\sharp(q^n + 1, q^{m_1} + 1, \ldots, q^{m_{r-1}} + 1, \kappa, \mathbb{1}) \tag{8.5.1.1}$$

on $(\mathbb{G}_m \times \mathbb{A}^r)/\mathbb{F}_2$ whose trace function is given as follows: for $k/\mathbb{F}_2$ a finite extension, and any point $(s_0, s_1, \ldots, s_r) \in k^\times \times k^r$,

$$(s_0, s_1, \ldots, s_r) \mapsto \frac{-1}{\sqrt{\#k}} \sum_{x \in k} \psi_k\big(s_0 x^{q^n+1} + s_1 x^{q^{m_1}+1} + \ldots + s_{r-1} x^{q^{m_{r-1}}+1} + s_r x^\kappa\big),$$

with $\kappa$ as defined above. One knows [**Ka-MMP**, Theorem 3.10.6] that both the local systems $\mathcal{G}(n, m_1, \ldots, m_r; q)$ and $\mathcal{G}^\sharp(n, m_1, \ldots, m_r; q)$ are symplectically self-dual. Furthermore, by Lemma 8.5.1, the geometric monodromy group $G$ of $\mathcal{G}(n, m_1, \ldots, m_r; q)$ is a normal subgroup of the geometric monodromy group $G^\sharp$ of $\mathcal{G}^\sharp(n, m_1, \ldots, m_r; q)$, with $G^\sharp/G \hookrightarrow C_{q^n+1}$.

For later use, we record the following lemma.

LEMMA 8.5.2. *For $k$ a subfield of $\mathbb{F}_q$,*

$$\mathrm{Trace}\big(\mathsf{Frob}_{(0,\ldots,0,1),k} | \mathcal{G}(n, m_1, \ldots, m_{r-1}, m_r; q)\big) = -\sqrt{\#k}.$$

PROOF. Without the clearing factor $\frac{-1}{\sqrt{\#k}}$, the "raw trace" is the sum over $x \in k$ of $\psi_k(x^{1+q^n} + x^j)$, where $j = 1$ if $m_r = 0$ and $j = q^{m_r} + 1$ otherwise. But for $k \subseteq \mathbb{F}_q$, each $x \in k$ satisfies $x^{1+q^l} = x^2$ for any $l \in \mathbb{Z}_{\geq 1}$. Also, $x$ is Artin-Schreier equivalent to $x^2$ (because of the characteristic $p = 2$). So each summand is $\psi_k(x^2 + x^2) = \psi_k(0) = 1$. Thus the "raw trace" is $\#k$, and hence the trace is $-\sqrt{\#k}$. □

We next give some technical lemmas.

LEMMA 8.5.3. *Let $n \geq 2$ and $q = 2^f$ be a power of $2$ such that $nf \geq 4$. Let $2^N = q^n$, $E = 2^{1+2N}_\epsilon$ an extraspecial $2$-group of type $\epsilon = \pm$, $R = \mathbf{Z}(R)E$ a finite $2$-group, embedded as a normal irreducible subgroup of a finite subgroup $G$ of $\mathrm{GL}(V) \cong \mathrm{GL}_{2^N}(\mathbb{C})$. Set $q_0 := 2$, $d := 2N$, and suppose that $L := \mathbf{O}^{\ell'}(G/\mathbf{Z}(G)R)$ is perfect and satisfies one of the conclusions* (i)–(v) *of Theorem 8.3.1, or* (i)–(iii), (vi) *of Proposition 8.3.3. Suppose that*

(a) *$|\mathrm{Trace}(g)|^2$ is $0$ or a power of $q$ for any $g \in G$.*

(b) *In the cases* (iii), (iv) *of Theorem 8.3.1, $|\mathrm{Trace}(g)|$ is $0$ or a power of $q$ for any $g \in G$.*

*Then $W := R/\mathbf{Z}(R)$ carries an $\mathbb{F}_q L$-module structure.*

PROOF. It suffices to prove the statement for $q = 2^f \geq 4$.

In the case of 8.3.1(i), there is a proper divisor $j$ of $d = 2nf$ such that $3 \leq 2nf/j$ and $L = \mathrm{SL}(W_j) \cong \mathrm{SL}_{d/j}(2^j)$, where $W_j$ is $W = \mathbb{F}_2^d$ viewed as a $d/j$-dimensional vector space over $\mathbb{F}_{2^j}$. Here, $L$ is perfect. We consider an $R$-coset in $G$ which corresponds to a regular unipotent element in $L$, whose fixed point subspace in $W$ has size $2^j$. By Lemma 7.2.1, this coset contains an element $h$ with $|\mathrm{Trace}(h)|^2 = 2^j$. By hypothesis, $2^j$ is a power of $q$.

In the case of 8.3.1(ii), there is a divisor $j$ of $d/2 = nf$ such that $L = \mathrm{Sp}(W_j) \cong \mathrm{Sp}_{d/j}(2^j)$, where $W_j$ is $W = \mathbb{F}_2^d$ viewed as a $d/j$-dimensional symplectic space over $\mathbb{F}_{2^j}$. Here, $L$ is perfect as $nf \geq 4$. We can consider an $R$-coset in $G$ which corresponds to a regular unipotent element in $L$, whose fixed point subspace in $W$ has size $2^j$. By Lemma 7.2.1, this coset contains an element $h$ with $|\mathrm{Trace}(h)|^2 = 2^j$. By hypothesis, $2^j$ is a power of $q$. The same argument applies to the case $L = {}^2B_2(2^j) < \mathrm{Sp}_4(2^j)$ of Theorem 8.3.1(v) (where $j = nf/2 > 1$), since any element of order 4 in $L$ must have one Jordan block of size 4 on $\mathbb{F}_{2^j}^4$ and hence is regular unipotent in $\mathrm{Sp}_4(2^j)$. Suppose we are in the case $L = G_2(2^j) < \mathrm{Sp}_6(2^j)$ of Theorem 8.3.1(v). Here $j \geq nf/3 > 1$, so $L$ is perfect. Also, $L > G_2(2)$ contains an element of order 8 [**CCNPW**], which must have one Jordan block of size 6 on $\mathbb{F}_{2^j}^6$ and hence is regular unipotent in $\mathrm{Sp}_6(2^j)$. So we can repeat the same argument as before to see $2^j$ is a power of $q$.

In the case of 8.3.1(iii), there is a proper divisor $j$ of $nf$ such that $2 \nmid (nf/j)$ and $L = \mathrm{SU}(W_{2j}) \cong \mathrm{SU}_{nf/j}(2^j)$, where $W_{2j}$ is $W$ viewed as an $nf/j$-dimensional vector space over $\mathbb{F}_{2^{2j}}$ endowed with a non-degenerate Hermitian form. If $j = 1$, then $nf/j \geq 4$; in general, $nf/j \geq 3$. Hence in all cases $L$ is perfect. We consider an $R$-coset in $G$ which corresponds to a regular unipotent element in $L$, whose fixed point subspace in $W$ has size $2^{2j}$. By Lemma 7.2.1, this coset contains an element $h$ with $|\mathrm{Trace}(h)| = 2^j$. By hypothesis, $2^j$ is a power of $q$.

In the case of 8.3.1(iv), there is a divisor $j$ of $nf$ such that $nf/j \geq 2$ and $L = \Omega(W_j) \cong \Omega^-_{2nf/j}(q^j)$, where $W_j$ is $W$ viewed as a $2nf/j$-dimensional vector space over $\mathbb{F}_{2^j}$ endowed with a non-degenerate quadratic form of type $-$. Here $L$ is perfect. We consider an $R$-coset in $G$ which corresponds to some element in $L$, whose fixed point subspace in $W$ has size $2^{2j}$. By Lemma 7.2.1, this coset contains an element $h$ with $|\mathrm{Trace}(h)| = 2^j$. By hypothesis, $2^j$ is a power of $q$.

In the cases (ii), (iii), (vi) of 8.3.3, we have $q^n = 2^2$, $2^5$, and $2^5$. Since $n \geq 2$, we must have $q = 2$, and so we are done. □

LEMMA 8.5.4. *Suppose $n > m_1 > \ldots > m_r \geq 0$, $n \geq 2$, and $q = 2^f$ a power of 2 are such that $q^d \geq 2^4$ and $\mathcal{G}(n, m_1, \ldots, m_r; q)$ is geometrically irreducible, with geometric monodromy group $G$.*

(a) *For any $g \in G$, $|\mathrm{Trace}(g)|$ is zero or a power of $q$.*
(b) *Suppose that $E := \mathbf{O}_2(H_1^-) \lhd G \leq H_1^-$, with $H_1^-$ defined in Theorem 8.2.1 for $2^N = q^n$. Set $q_0 := 2$, $d := 2N$, and suppose that $L := \mathbf{O}^{\ell'}(G/E)$ is perfect and satisfies one of the conclusions* (i)–(v) *of Theorem 8.3.1, or* (i)–(iii), (vi) *of Proposition 8.3.3. Then $W = E/\mathbf{Z}(E)$ carries an $\mathbb{F}_q L$-module structure.*

PROOF. (a) follows from Corollaries 8.1.2 and 8.1.5, working over finite extensions of $\mathbb{F}_{q^2}$.

(b) follows from (a) and Lemma 8.5.3; note that $W$ (viewed over $\mathbb{F}_2$) carries an $\mathbb{F}_2$-valued $L$-invariant non-degenerate quadratic form induced by the map $x \mapsto x^2$ on $E$. □

For coprime positive integers $A \neq B$, we will consider the hypergeometric sheaf

$$\mathcal{H}_{small,A,B} := \mathcal{H}yp_\psi(\mathsf{Char}(A) \smallsetminus \{\mathbb{1}\}; \mathsf{Char}(B) \smallsetminus \{\mathbb{1}\}), \tag{8.5.4.1}$$

of type $(A-1, B-1)$ and rank $\max(A,B) - 1$. It is pure of weight $A + B - 3$. For each multiplicative character $\chi$ with $\chi^A \neq \mathbb{1}$, we consider the hypergeometric sheaf

$$\mathcal{H}_{big,A,B,\chi} := \mathcal{H}yp_\psi(\mathsf{Char}(A); \mathsf{Char}(B, \overline{\chi})), \tag{8.5.4.2}$$

of rank $\max(A,B)$. These sheaves have been studied in [**KT6**, §3].

THEOREM 8.5.5. *Assume $q = 2^f$ and $n > m \geq 1$ are integers such that $N := nf \geq 4$, $2|nm$, and $\gcd(n,m) = 1$. Then the following statements hold.*

(i) *The geometric monodromy group $G = G_{\mathrm{geom}}$ of the local system $\mathcal{G}(n,m;q)$ defined in* (8.5.0.1) *is isomorphic to the subgroup $H_f^\circ \cong 2_-^{1+2N} \cdot \Omega_{2n}^-(q)$ of the group $\Gamma(2,N,-) = H_1^-$, as defined in* (8.2.2.1).
(ii) *The hypergeometric sheaf $\mathcal{H}_{small,q^n+1,q^m+1}$ defined in* (8.5.4.1) *has geometric monodromy group equal to $G \cong H_f^\circ$.*
(iii) *If $f = 1$, then over any finite extension $k$ of $\mathbb{F}_2$, for the arithmetic monodromy group $G_{\mathrm{arith},k}$ of $\mathcal{G}$ over $k$ we have $G_{\mathrm{arith},k} = G = H_1^\circ$ if $k \supseteq \mathbb{F}_4$, and $G_{\mathrm{arith},k} \cong H_1^-$ otherwise.*
(iv) *Furthermore, both $H_1^\circ$ and $H_1^-$ satisfy* (**S**+).

PROOF. (a) By [**KT6**, Corollary 3.10(i)], $\mathcal{G}(n,m;q)$ is geometrically isomorphic to the $[A]^\star$ Kummer pullback of the hypergeometric sheaf $\mathcal{H} := \mathcal{H}_{small,A,B}$ defined in (8.5.4.1) with $A := q^n + 1$ and $B := q^m + 1$. The integrality result Theorem 8.1.1 and [**KT2**, Lemma 5.1] show that both $G$ and the geometric monodromy group $H$ of $\mathcal{H}$ are finite, with $G \lhd H$ and $H/G \hookrightarrow C_A$.

The choice of $n, m$ ensures that $\gcd(A,B) = 1$, see Lemma 10.3.2, and $A \geq 17$, hence $\mathcal{H}$ satisfies (**S**+) by Corollary 10.1.9. Moreover, $\mathcal{H}$ is symplectically self-dual by [**Ka-ESDE**, 8.8.1-2], whence $H < \mathrm{Sp}_{2^N}(\mathbb{C})$. Now, a generator $g_0$ of the image of $I(0)$ in $H$ is an $\mathsf{ssp}$-element of central order $A = 2^N + 1$, since the "upstairs" characters of $\mathcal{H}$ are $\mathsf{Char}_{\mathrm{ntriv}}(A)$. Next, the wild part $\mathsf{Wild}$ of $\mathcal{H}$ has dimension $A - B = q^m(q^{n-m} - 1)$, and the "downstairs" character of $\mathcal{H}$ are $\mathsf{Char}_{\mathrm{ntriv}}(B)$. Hence, a generator $g_\infty$ of the image of $I(\infty)$ modulo the image of $P(\infty)$ in $H$ permutes transitively the $q^{n-m} - 1$ simple $P(\infty)$-summands on $\mathsf{Wild}$, and has spectrum $\mu_B \smallsetminus \{1\}$ on $\mathsf{Tame}$, see [**KRLT4**, Proposition 5.9]. In particular,

(8.5.5.1) $$|H| \text{ is divisible by } \mathrm{lcm}(q^n + 1, q^m + 1, q^{n-m} - 1).$$

Now we can apply Theorem 8.4.5(a) to $H$. In the case of 8.4.5(a)($\beta$), we have that $q_1 := 2^{N+1} + 1$ is a Fermat prime and $H = \mathrm{SL}_2(q_1)$, so $2 \nmid N = nf$ and hence $2|m$. Also, by [**KRLT4**, Proposition 5.9], when $mf \geq 4$, the image of $P(\infty)$ in $H$ has order at least

$$(q^{n-m} - 1)q^{2m} = q^{n+m} - q^{2m} \geq q^{n+m} - q^{n+m-1} \geq q^{n+m-1} \geq 2^{N+3},$$

whereas the Sylow 2-subgroups of $\mathrm{SL}_2(q_1)$ have order $2^{N+2}$, a contradiction. So $mf = 2$, $q = 2$, $m = 2$. Now $H = \mathrm{SL}_2(q_1)$ has order divisible by $q^m + 1 = 5$ by (8.5.5.1), which is impossible since $q_1 \equiv 2 (\mathrm{mod}\ 5)$. So $E := \mathbf{O}_2(H_1^-) \lhd H \leq H_1^-$. Since $H/G \hookrightarrow C_A$, we also have that

(8.5.5.2) $$E \lhd G \leq H_1^-.$$

(b) We will now identify $\bar{H} := H/E \leq \mathrm{O}(W)$, where $W = E/\mathbf{Z}(E)$, a quadratic space of type $-$ and dimension $2N$ over $\mathbb{F}_2$, with quadratic form $\mathsf{Q}(x\mathbf{Z}(E)) = x^2 \in \mathbf{Z}(E)$ (and we have identified $\mathbf{Z}(E)$ with $\mathbb{F}_2$). Clearly, (8.5.5.1) implies that $|\bar{H}|$ is still divisible by $\mathrm{lcm}(q^n + 1, q^m + 1, q^{n-m} - 1)$, and moreover

(8.5.5.3) $$\bar{H} \text{ contains an element of order } 2^N + 1.$$

By the first part of Theorem 8.3.4,

$$L := \mathbf{O}^{\ell'}(\bar{H})$$

is not cyclic (where $\ell$ is as chosen in Theorem 8.3.1 and Proposition 8.3.3). In order to be able to apply the second part of Theorem 8.3.4, we need to show that the $L$-module $W$ carries an

$\mathbb{F}_q$-structure. To show this, we will assume $q > 2$ and apply Theorem 8.3.1 and Proposition 8.3.3, with $q_0 = 2$ and thus viewing $\bar{H} \leq \mathrm{O}_{2N}(2)$. We will use the observation that if $L$ is perfect, then $G \geq [H,H]$ and (8.5.5.2) imply that $G \geq EL$. Now Lemma 8.5.4 shows that $W$ carries an $\mathbb{F}_q L$-module structure in the cases (i)–(v) of 8.3.1, and (i)–(iii), (vi) of 8.3.3.

Assume we are in the cases (vii), (viii) of 8.3.3 and $L = \mathsf{A}_l$. Then $L$ acts absolutely irreducibly on $W = \mathbb{F}_2^{2N}$, whence $\mathbf{C}_{\bar{H}}(L) \leq \mathbf{C}_{\mathrm{GL}(W)}(L) = 1$ and so $\bar{H} \hookrightarrow \mathsf{S}_l$. In particular, $\bar{H}$ cannot satisfy (8.5.5.3), a contradiction.

In the remaining cases (vi) of 8.3.1, and (iv), (v), (vii), (viii) of 8.3.3 (with $L \not\cong \mathsf{A}_l$ in the last two cases), we can check directly that $|\mathrm{Aut}(L)|$ is not divisible by $(q^m+1)(q^{n-m}-1)$. The arguments used in deducing (8.3.4.2) show that this contradicts (8.5.5.1).

(c) Now we can apply the second part of Theorem 8.3.4, viewing $L \leq \mathrm{GL}_{2n}(q)$, to arrive at one of the following two possibilities for $L$ .

(c1) $(n,m,q) = (5,2,2)$ and $L = \mathsf{A}_{11}$ or $\mathsf{A}_{12}$. In this case, the action of $L$ on $W$ is absolutely irreducible, so $\mathrm{End}_L(W) \cong \mathbb{F}_2$; in particular, $\mathbf{C}_{\mathrm{O}(W)}(L) = 1$. On the other hand, the action of $\bar{H}$ on $L$ induces a subgroup of $\mathrm{Aut}(L) = L \cdot 2$. It follows that $\mathsf{A}_{11} \leq L \leq \bar{H} \leq \mathrm{Aut}(L) \leq \mathsf{S}_{12}$; in particular, $\bar{H} = H/E$ contains no element of order 33. But this contradicts the fact that $g_0$ has order 33.

(c2) $L = \Omega(W_f) \cong \Omega_{2n}^-(q)$, where $W_f$ is $W$ viewed as a $2n$-dimensional vector space over $\mathbb{F}_q$ endowed with a non-degenerate quadratic form $\mathsf{Q}_f$ of type $-$. Moreover, there is $\alpha \in \mathbb{F}_q^\times$ such that $\mathsf{Q}(u) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\alpha \cdot \mathsf{Q}_f(u))$ for all $u \in W_f$.

Rescaling $\mathsf{Q}_f$ suitably (without any effect on $L$), we may assume that $\mathsf{Q}(u) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\mathsf{Q}_f(u))$ for all $u \in W_f$, whence $H_f^\circ \lhd H \leq H_1^-$. As $[H,H] \leq G \leq H$, we also have $H_f^\circ \lhd G \leq H_1^-$; let $a_1 := |G/H_f^\circ|$. If $a_1 = 1$, then $G = H_f^\circ$ as stated.

Assume that $a_1 > 1$. Since $\mathcal{G}(n,m;q)$ lives over $\mathbb{A}^1$, $G = \mathbf{O}^{2'}(G)$ and so $2|a_1$. Now we can apply Theorem 8.2.5(iii) to see that $G \geq H_f^-$. Hence, by Theorem 8.2.5(ii), $G$ contains an element $h \in H_f^-$ with $|\mathrm{Trace}(h)| = \sqrt{q}$, contrary to Corollary 8.1.2.

When $q = 2$ (so that $f = 1$), we also note that, since $H/G$ has odd order and $G = H_1^\circ \leq H \leq H_1^-$, we have shown that $H = H_1^\circ$. As $\mathcal{H}$ satisfies $(\mathbf{S}+)$, we conclude that both $H_1^\circ$ and $H_1^-$ satisfy $(\mathbf{S}+)$.

(d) Here we will show that $H = G$. Since $N \geq 4$, $2^{2N}-1$ has a primitive prime divisor $s$ by [**Zs**], which then divides $q^n+1$. Recall that $G/E = H_f^\circ/E = \Omega_{2n}^-(q)$ contains a cyclic torus $\langle \bar{t} \rangle$ of order $q^n+1$. An inverse image $t$ of $\bar{t}$ in $G$ has order divisible by $q^n+1$, and so for some power $g_1$ of $t$ that has order $s$, we have

$$q^n + 1 \text{ divides } |\mathbf{C}_G(g_1)|. \tag{8.5.5.4}$$

It is clear that the Sylow $s$-subgroups in $\mathrm{Sp}_{2n}(2)$ are cyclic, hence the same holds for Sylow $s$-subgroups in $H$. As a consequence, all cyclic subgroups of order $s$ in $H$ are conjugate. As mentioned above, the element $g_0$ of $H$ has order divisible by $q^n+1$, so some power $g_1'$ of it has order $s$. Conjugating $g_0$ suitably, we may assume that $\langle g_1 \rangle = \langle g_1' \rangle$. Replacing $g_1$ by an $s'$-power of it it, we may in fact assume that $g_1' = g_1$. Since $H/G \hookrightarrow C_A$, we also have

$$e := [\mathbf{C}_H(g_1) : \mathbf{C}_G(g_1)] \text{ divides } q^n + 1. \tag{8.5.5.5}$$

By the choice of $s$, the element $g_1$, which acts nontrivially on $W = \mathbb{F}_2^{2N}$, acts irreducibly on $W$. By Lemma 8.3.2(i), $\mathbb{E} := \mathbf{C}_{\mathrm{End}(W)}(g_1)$ is a finite extension of $\mathbb{F}_2$, and $W$ considered as an $\mathbb{E}\langle g_1\rangle$-module is absolutely irreducible. Any such module is of dimension 1 as $\langle g_1\rangle$ is cyclic. It follows that $1 = \dim_{\mathbb{E}} W$, i.e. $|\mathbb{E}| = |W| = 2^{2N} = q^{2n}$. In particular, $|\mathbf{C}_{\mathrm{Sp}_{2n}(2)}(g_1)|$ divides $q^{2n}-1$, and so $\mathbf{C}_H(g_1)$ has order dividing $|E|(q^{2n}-1) = 2q^{2n}(q^{2n}-1)$. Writing $|\mathbf{C}_G(g_1)| = a(q^n+1)$ for some $a \in \mathbb{Z}$ using (8.5.5.4), we then have

$$|\mathbf{C}_H(g_1)| = ae(q^n+1)$$

divides $2q^{2n}(q^{2n}-1)$; in particular $e$ divides $2q^{2n}(q^n-1)$, which is coprime to $q^n+1$. Together with (8.5.5.5), this implies that $e = 1$. Thus $\mathbf{C}_H(g_1) \leq G$. Since $g_0$ obviously centralizes $g_1' = g_1$, we have therefore shown that $g_0 \in G$. On the other hand, the wild part of $\mathcal{H}$ has dimension $q^n - q^m \geq 2$, so by [**KT5**, Theorem 4.1], $H$ is the normal closure of $\langle g_0\rangle$, and $G \lhd H$. Consequently, $H = G$.

(e) Now we determine $G_{\mathrm{arith},k}$ when $f = 1$. Over $\mathbb{F}_2$, $\mathcal{G}$ is symplectically self-dual by [**Ka-MMP**, Theorem 3.10.6], hence $G_{\mathrm{arith},\mathbb{F}_2} \leq \mathrm{Sp}_{2^N}(\mathbb{C})$. As $G_{\mathrm{arith},\mathbb{F}_2}$ normalizes $G_{\mathrm{geom}} = H_1^\circ$, it also normalizes $E := \mathbf{O}_2(H_1^\circ)$, so by Theorem 8.2.1, $G_{\mathrm{arith},\mathbb{F}_2} \leq \mathbf{N}_{\mathrm{Sp}_{2^N}(\mathbb{C})} = H_1^-$, and thus $H_1^\circ \leq G_{\mathrm{arith},\mathbb{F}_2} \leq H_1^-$. Observe that the trace of $\mathsf{Frob}_{1,\mathbb{F}_2}$ is $-\sqrt{2}$. On the other hand, $|\mathrm{Trace}(g)|$ is an integer for any $g \in H_1^\circ$ by Theorem 8.2.5(i). Hence $G_{\mathrm{arith},\mathbb{F}_2} = H_1^-$. □

COROLLARY 8.5.6. *Let $n \in \mathbb{Z}_{\geq 4}$. Then the geometric monodromy group $G_{\mathrm{geom}}$ of the local system $\mathcal{G}^\sharp(n, n-1, \ldots, 0; 2)$ defined in* (8.5.1.1) *is isomorphic to $H_1^\circ \cong 2_-^{1+2n} \cdot \Omega_{2n}^-(2)$. Furthermore, its arithmetic monodromy group $G_{\mathrm{arith},k}$ over any finite extension $k/\mathbb{F}_2$ is $H_1^- = 2_-^{1+2n} \cdot \mathrm{O}_{2n}^-(2)$ if $k \not\supseteq \mathbb{F}_4$, and $H_1^\circ = G_{\mathrm{geom}}$ if $k \supseteq \mathbb{F}_4$.*

PROOF. The integrality result Theorem 8.1.1 (applied with a change of variable $x \mapsto x/s_0$) and [**KT2**, Lemma 5.1] show that both $G_{\mathrm{geom}}$ and $G_{\mathrm{arith},k}$ are finite subgroups of $\mathrm{Sp}_{2^n}(\mathbb{C})$. Next, a pullback of $\mathcal{G}^\sharp(n, n-1, \ldots, 0; 2)$ yields the sheaf $\mathcal{G}(n, n-1; 2)$ which has geometric monodromy group $H_{\mathrm{geom}} = H_1^\circ$, and arithmetic monodromy group $H_{\mathrm{arith},k} = H_{\mathrm{geom}}$ if $k \supseteq \mathbb{F}_4$ and $H_1^-$ otherwise, according to Theorem 8.5.5. Thus $G_{\mathrm{arith},\mathbb{F}_2}$ is a finite subgroup of $\mathrm{Sp}_{2^n}(\mathbb{C})$ which contains $H_1^-$, and $H_1^-$ satisfies $(\mathbf{S}+)$. Applying Theorem 8.4.5(c), we obtain $G_{\mathrm{arith},\mathbb{F}_2} = H_1^-$. Now, $|\mathrm{Trace}(g)|$ is an integer for any $g \in G_{\mathrm{arith},\mathbb{F}_4}$ by Theorem 8.1.1, and

$$H_1^- \geq G_{\mathrm{arith},\mathbb{F}_4} \geq H_{\mathrm{arith},\mathbb{F}_4} = H_{\mathrm{geom}} = H_1^\circ.$$

As $H_1^- = H_{\mathrm{arith},\mathbb{F}_2}$ admits elements $h$ with $|\mathrm{Trace}(h)|^2 = 2$ (e.g. $\mathsf{Frob}_{1,\mathbb{F}_2}$), and has index 2 over $H_1^\circ$, we conclude that $G_{\mathrm{arith},\mathbb{F}_4} = H_1^\circ$. Finally,

$$H_1^\circ = G_{\mathrm{arith},\mathbb{F}_4} \geq G_{\mathrm{geom}} \geq H_{\mathrm{geom}} = H_1^\circ,$$

so $G_{\mathrm{geom}} = H_1^\circ$. □

THEOREM 8.5.7. *Assume $q = 2^f$, $r \geq 1$, and $n > m_1 > \ldots > m_r \geq 1$ are integers such that $nf \geq 4$, $2 \nmid nm_1 \ldots m_r$, and $\gcd(n, m_1, \ldots, m_r) = 1$. Then the local system $\mathcal{G} := \mathcal{G}(n, m_1, \ldots, m_r; q)$ over $\mathbb{A}^r/\mathbb{F}_2$, defined in* (8.5.0.1)*, has geometric monodromy group $G = G_{\mathrm{geom}} \cong \mathrm{SU}_n(q)$ acting in its total Weil representation. Over any finite extension $k$ of $\mathbb{F}_2$, for the arithmetic monodromy group $G_{\mathrm{arith},k}$ of $\mathcal{G}$ over $k$ we have $G_{\mathrm{arith},k} = G$ if $k \supseteq \mathbb{F}_{q^4}$ and $G_{\mathrm{arith},k} \cong (C_2 \times G) \cdot \mathrm{Gal}(\mathbb{F}_{q^2}/k)$ if $k \subseteq \mathbb{F}_{q^2}$. In the latter case, $\mathrm{Gal}(\mathbb{F}_{q^2}/k)$ may be identified with the subgroup $\mathrm{Gal}(\mathbb{F}_{q^2}/k)$ of outer field automorphisms in $\mathrm{Out}(G) \cong C_{\gcd(n,q+1)} \rtimes C_{2f}$, and $C_2$ is the scalar subgroup of order 2.*

PROOF. (a) Let $N := nf$, and define $m_{r+1} := 1$ if $2|f$ and $m_{r+1} := 2$ if $2 \nmid f$. Then $\mathcal{G}$ is the specialization $s_{r+1} = 0$ of the local system $\tilde{\mathcal{G}} := \mathcal{G}(nf, m_1 f, \ldots, m_r f, m_{r+1}; 2)$ on $\mathbb{A}^{r+1}/\mathbb{F}_2$. Again by Theorem 8.1.1 and [**KT2**, Lemma 5.1], $\tilde{\mathcal{G}}$ has finite geometric monodromy group $\tilde{G}$ that contains $G$. On the other hand, the specialization $s_1 = \ldots = s_r = 0$ of $\tilde{\mathcal{G}}$ is the local system $\mathcal{G}(nf, m_{r+1}; 2)$ on $\mathbb{A}^1/\mathbb{F}_2$ considered in Theorem 8.5.5. Hence $\tilde{G}$ contains the geometric monodromy group $H_1^\circ$ of the latter, which was shown to satisfy (**S**+) and contains an $\mathsf{ssp}$-element of central order $2^N + 1$. Also, $\tilde{\mathcal{G}}$ is symplectically self-dual by [**Ka-MMP**, Theorem 3.10.6], so that $\tilde{G} \leq \mathrm{Sp}_{2^N}(\mathbb{C})$. Hence we can apply Theorem 8.4.5(a) to $\tilde{G}$ and conclude (since $H_1^\circ \not\leq \mathrm{SL}_2(2^{N+1}+1)$) that $\tilde{G} \leq H_1^-$, and thus $G \leq H_1^-$.

Note that $2 \nmid nm_1 \ldots m_r$ and $\gcd(n, m_1, \ldots, m_r) = 1$ imply by Lemma 10.3.2(iii) that

$$\gcd(q^n + 1, q^{m_1} + 1, \ldots, q^{m_{r+1}} + 1) = q + 1.$$

Applying [**KT6**, Corollary 2.7], we see that $\mathcal{G}$ is geometrically isomorphic to the direct sum of $q + 1$ pairwise non-isomorphic sheaves, one $\mathcal{G}_0$ of rank $(q^n - q)/(q + 1)$ and $q$ of rank $(q^n + 1)/(q + 1)$, say $\mathcal{G}_i$ with $1 \leq i \leq q$. Now we can apply Theorem 8.4.4 to arrive at one of the following two cases.

(a1) $\mathrm{SU}_n(q) \lhd G \leq C_2 \times \mathrm{GU}_n(q)$, with $\mathrm{SU}_n(q)$ and $\mathrm{GU}_n(q)$ acting in total Weil representations. In this case, $[G, G] \cong \mathrm{SU}_n(q)$, and $G/[G, G] \hookrightarrow C_2 \times C_{q+1}$. However, $\mathcal{G}$ lives over $\mathbb{A}^r/\mathbb{F}_2$, so $G = \mathbf{O}^{2'}(G)$ by Theorem 1.3.4, and therefore $G = \mathrm{SU}_n(q)$ or $C_2 \times \mathrm{SU}_n(q)$. In the latter case, $C_2 = \mathbf{Z}(E) = \langle \boldsymbol{j} \rangle$, with $\boldsymbol{j}$ acting as the scalar $-1$ on $\mathcal{G}$. In particular, $\boldsymbol{j}$ has determinant $-1$ on each of the $q$ subsheaves $\mathcal{G}_i$ with $i > 0$, of odd rank $(q^n + 1)/(q + 1)$, and this contradicts Corollary 2.3.8(iii-bis). Hence $G = \mathrm{SU}_n(q)$, as stated.

(a2) $(n, q) = (5, 2)$ and $G \rhd L_1 \in \{\mathrm{PSL}_2(11), \mathrm{SL}_2(11)\}$; in particular, $m_1, \ldots, m_r \in \{1, 3\}$. As shown in part (c3) of the proof of Theorem 8.4.4, $G \leq (AL_1) \cdot 2$, with $|A| \leq 2$, whence the Sylow 2-subgroups of $G$ have order at most $2^5$. Now, if $m_r = 1$, then by applying Theorem 10.2.7 to the specialization $m_1 = \ldots = m_{r-1} = 0$ of $\mathcal{G}$, we see that the image of the geometric monodromy group of the specialization, which is a subgroup of $G$, on each of the three subsheaves of the specialization is (the image of) $\mathrm{SU}_5(2)$ on a Weil representation. This clearly violates the indicated upper bound on $G$. Hence we must have that $(r, m_1) = (1, 3)$. In this case, each of $\mathcal{G}_i$ has wild part of dimension 8, so by [**KRLT4**, Proposition 5.9], the Sylow 2-subgroups of $G$ have irreducible representations of degree $\geq 8$ and hence of order at least $2^7$, again a contradiction.

(b) Over $\mathbb{F}_2$, we know that $\widetilde{\mathcal{G}}$ is symplectically self-dual by [**Ka-MMP**, Theorem 3.10.6]. Next, by Theorem 8.5.5 (and its proof), over $\mathbb{F}_2$ the arithmetic monodromy group of $\mathcal{G}(nf, m_{r+1}; 2)$ is $H_1^-$ and satisfies (**S**+). Hence $H_1^-$ is a maximal finite subgroup of $\mathrm{Sp}_{2^N}(\mathbb{C})$ by Theorem 8.4.5(c). As the arithmetic monodromy group of $\widetilde{\mathcal{G}}$ over $\mathbb{F}_2$ is finite, contains that of $\mathcal{G}(nf, m_{r+1}; 2)$ (which is $H_1^-$), and is contained in $\mathrm{Sp}_{2^N}(\mathbb{C})$, the maximality of $H_1^-$ implies that it is $H_1^-$. Specializing back to $\mathcal{G}$, we see that $G_{\mathrm{arith}, \mathbb{F}_2} \leq H_1^-$.

Now, over $\mathbb{F}_{q^2}$ the system $\mathcal{G}$ is still a direct sum of $q+1$ irreducible subsheaves $\mathcal{G}_i$, see [**KT6**, Corollary 2.7]. Hence we can apply Theorem 8.4.4 to $G_{\mathrm{arith}, \mathbb{F}_{q^2}} \leq G_{\mathrm{arith}, \mathbb{F}_2} \leq H_1^-$, and using $G_{\mathrm{arith}, \mathbb{F}_{q^4}} \rhd G_{\mathrm{geom}} = \mathrm{SU}_n(q)$, we now see that $\mathrm{SU}_n(q) \lhd G_{\mathrm{arith}, \mathbb{F}_{q^4}} \leq G_{\mathrm{arith}, \mathbb{F}_{q^2}} \leq C_2 \times \mathrm{GU}_n(q)$, with both $\mathrm{SU}_n(q)$ and $\mathrm{GU}_n(q)$ acting in their total Weil representations. Furthermore, each

$\mathcal{G}_i$ has trivial arithmetic determinant by Corollary 2.3.8(iii-ter). Applying Lemma 8.4.3(iv), we conclude that $G_{\mathrm{arith},\mathbb{F}_{q^4}} = G_{\mathrm{geom}}$.

Next, over $\mathbb{F}_{q^2}$, the determinant of the subsheaves $\mathcal{G}_i$ is trivial for the unique one of even rank $(q^n - q)/(q+1)$, and $-1$ for all other $q$ of odd rank $(q^n+1)/(q+1)$ by Corollary 2.3.8(iii-ter). As $G_{\mathrm{arith},\mathbb{F}_{q^4}} = \mathrm{SU}_n(q)$ is perfect, it follows that $G_{\mathrm{arith},\mathbb{F}_{q^2}} = \langle G_{\mathrm{geom}}, h\rangle$, of index 2 over $G_{\mathrm{geom}}$. Using perfectness again, the determinant of $G_{\mathrm{geom}}$ on each $\mathcal{G}_i$ is trivial, so the determinant of $h$ on $\mathcal{G}_i$ must be $-1$ for odd-rank subsheaves, and 1 for the even-rank one. Recalling $C_2 = \mathbf{Z}(E) = \langle \boldsymbol{j}\rangle$, with the central involution $\boldsymbol{j}$ acting via $-1$, we have that $\boldsymbol{j}h$ has determinant 1 on every $\mathcal{G}_i$. By Lemma 8.4.3(iv), this implies that $\boldsymbol{j}h \in \mathrm{SU}_n(q) \leq G_{\mathrm{arith},\mathbb{F}_{q^2}}$. It follows that $\boldsymbol{j} \in G_{\mathrm{arith},\mathbb{F}_{q^2}}$, and so $G_{\mathrm{arith},\mathbb{F}_{q^2}} = C_2 \times \mathrm{SU}_n(q)$.

Let $g$ denote the image of $\mathsf{Frob}_{(1,0,\ldots,0),\mathbb{F}_2}$ in $G_{\mathrm{arith},\mathbb{F}_2}$, so that $G_{\mathrm{arith},\mathbb{F}_2} = \langle G_{\mathrm{arith},\mathbb{F}_{q^2}}, g\rangle$. We will now show that $G_{\mathrm{arith},\mathbb{F}_2}/G_{\mathrm{arith},\mathbb{F}_{q^2}} \cong C_{2f} \cong \mathrm{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_2)$, and moreover, the conjugation by $g$ induces an element of order $2f$ modulo $\mathrm{Inndiag}(G) \cong \mathrm{PGU}_n(q)$ in $\mathrm{Aut}(G)$ for $G = \mathrm{SU}_n(q)$. First, the construction of $G$ inside $H_1^-$ in Proposition 8.4.2 shows that $G \lhd D := C_2 \times \mathrm{GU}_n(q) \leq H_1^-$, whence $C \geq \mathbf{C}_D(G) = \mathbf{Z}(D) = C_2 \times \mathbf{Z}(\mathrm{GU}_n(q))$ for $C := \mathbf{C}_{H_1^-}(G)$. In fact, we have

$$C = \mathbf{C}_D(G). \tag{8.5.7.1}$$

Indeed, since the action of $G$ on $\mathcal{G}$ splits it into $q+1$ pairwise inequivalent irreducible subsheaves $\mathcal{G}_i$, $C$ preserves each of the summands $\mathcal{G}_i$. Hence, Theorem 8.4.4 applied to $CG$ shows that $CG \leq D$, and so $C \leq \mathbf{C}_D(G) = C_2 \times \mathbf{Z}(\mathrm{GU}_n(q))$.

Now let $j$ denote the order modulo $\mathrm{Inndiag}(G)$ of the automorphism of $G$ induced by the conjugation by $g$; in particular, $j|2f$ as $g^{2f} \in G_{\mathrm{arith},\mathbb{F}_{q^2}} = C_2 \times G$. By (8.5.7.1), $D$ induces the subgroup $D/C \cong \mathrm{Inndiag}(G)$ of $\mathrm{Aut}(G)$. Hence we can find $c \in \mathbf{C}_{H_1^-}(G)$ and $d \in D$ such that $g^j = cd$ and thus $g^j \in D = C_2 \times \mathrm{GU}_n(q)$. As $\mathrm{GU}_n(q)$ acts via its total Weil representation, it follows that $|\mathrm{Trace}(g^j)|^2$ is a power of $q^2 = 2^{2f}$. On the other hand, since $2 \nmid nm_1$, for any $x \in \mathbb{F}_{2^j}$ we have $x^{q^n+1} = x^{q+1} = x^{q^{m_1}+1}$, and so $\psi_{\mathbb{F}_{2^j}}(x^{q^n+1} + x^{q^{m_1}+1}) = \psi_{\mathbb{F}_{2^j}}(0) = 1$. As $g^j$ is the image of $\mathsf{Frob}_{(1,0,\ldots,0),\mathbb{F}_{2^j}}$ in $G_{\mathrm{arith},\mathbb{F}_2}$, it follows that $|\mathrm{Trace}(g^j)|^2 = |-2^{j/2}|^2 = 2^j$. Thus $2f|j$, and so $j = 2f$ as stated; in particular, $G_{\mathrm{arith},\mathbb{F}_2}/G_{\mathrm{arith},\mathbb{F}_{q^2}} \cong C_{2f}$.

Recall that $\mathrm{Out}(G) \cong C_{\gcd(n,q+1)} \rtimes C_{2f}$, with $C_{2f}$ generated by the field automorphism $\sigma : y \mapsto y^p$. As $2|q$, any involution in this group is conjugate to $\tau := \sigma^f$. But $g^f$ has order 2 in $\mathrm{Out}(G)$, so we may assume that $g^f$ induces $\tau$ modulo $\mathrm{Inn}(G)$. Clearly $g$ centralizes $g^f$, so the image of $g$ in $\mathrm{Out}(G)$ is contained in the centralizer of $\tau$. Next, $\tau$ centralizes the subgroup $C_{2f} = \langle\sigma\rangle$ of $\mathrm{Out}(L)$, but acts as inversion on the odd-order subgroup $C_{\gcd(n,q+1)} = \mathrm{Inndiag}(G)/\mathrm{Inn}(G)$. It follows that the image of $g$ in $\mathrm{Out}(G)$ belongs to this subgroup $C_{2f}$. As the order of $g$ modulo $\mathrm{Inndiag}(G)$ is $2f$, we conclude that, modulo $\mathrm{Inn}(G)$, $g$ generates the subgroup $C_{2f} = \langle\sigma\rangle$. Thus $G_{\mathrm{arith},\mathbb{F}_2} = (2 \times G) \cdot \mathrm{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_2)$, completing the proof of the theorem. □

THEOREM 8.5.8. *Assume $q = 2^f$, $r \geq 1$, and $n > m_1 > \ldots > m_r \geq 1$ are integers such that $nf \geq 4$, $2 \nmid nm_1 \ldots m_r$, and $\gcd(n, m_1, \ldots, m_r) = 1$. Then the local system $\mathcal{G} := \mathcal{G}(n, m_1, \ldots, m_r, 0; q)$ over $\mathbb{A}^{r+1}/\mathbb{F}_2$, defined in (8.5.0.1), has geometric monodromy group $G = E \rtimes \mathrm{SU}_n(q) < H_f^\circ \leq H_1^\circ$, with $E := \mathbf{O}_2(H_1^-) = 2_-^{1+2nf}$ and with $\mathrm{SU}_n(q)$ acting in its total Weil representation. Over any finite extension $k$ of $\mathbb{F}_2$, for the arithmetic monodromy group $G_{\mathrm{arith},k}$ of $\mathcal{G}$ over $k$ we have $G_{\mathrm{arith},k} = G$ if $k \supseteq \mathbb{F}_{q^2}$ and $G_{\mathrm{arith},k} \cong G \cdot \mathrm{Gal}(\mathbb{F}_{q^2}/k)$ if*

*$k \subseteq \mathbb{F}_{q^2}$. In the latter case,* $\mathrm{Gal}(\mathbb{F}_{q^2}/k)$ *may be identified with the subgroup* $\mathrm{Gal}(\mathbb{F}_{q^2}/k)$ *of outer field automorphisms of* $\mathrm{SU}_n(q)$.

PROOF. (a) As $2 \nmid n$ and $nf \geq 4$, in fact we have $nf \geq 5$. Define $m_{r+1} := 1$ if $2|f$ and $m_{r+1} := 2$ if $2 \nmid f$. Then $\mathcal{G}$ is the specialization $s_{r+1} = 0$ of the local system $\tilde{\mathcal{G}} := \mathcal{G}(nf, m_1 f, \ldots, m_r f, m_{r+1}, 0; 2)$ on $\mathbb{A}^{r+2}/\mathbb{F}_2$, which, by Theorem 7.1.2 and [**KT2**, Lemma 5.1], has finite geometric monodromy group $\tilde{G}$ that contains $G$. Next, the specialization $s_1 = \ldots = s_r = s_{r+2} = 0$ of $\tilde{\mathcal{G}}$ is the local system $\mathcal{G}(nf, m_2; 2)$ on $\mathbb{A}^1/\mathbb{F}_2$ considered in Theorem 8.5.5. Hence $\tilde{G}$ contains the geometric monodromy group $H_1^\circ$ of the latter, which is shown to satisfy (**S**+) and contains an $\mathsf{ssp}$-element of central order $2^N + 1$. As mentioned above, $\tilde{\mathcal{G}}$ is symplectically self-dual, so that $\tilde{G} \leq \mathrm{Sp}_{2^N}(\mathbb{C})$. Hence we can apply Theorem 8.4.5(a) to $\tilde{G}$ and conclude (since $H_1^\circ \not\leq \mathrm{SL}_2(2^{N+1}+1)$) that $\tilde{G} \leq H_1^\circ$, and thus $G \leq H_1^\circ$; in particular, $G$ normalizes $E := \mathbf{O}_2(H_1^-)$.

On the other hand, the specialization $s_1 = 0$ of $\mathcal{G}$ is the irreducible Pink-Sawin local system considered in Theorem 7.3.8, so $G$ is irreducible and contains $E_1 := 2_-^{1+2N}$. Yet another specialization $s_{r+1} = 0$ of $\mathcal{G}$ (which is also the specialization $s_{r+1} = s_{r+2} = 0$ of $\tilde{\mathcal{G}}$) is the sheaf $\mathcal{G}(n, m_1, \ldots, m_r; q)$ over $\mathbb{A}^r/\mathbb{F}_2$ considered in Theorem 8.5.7. This shows that $G$ contains $S := \mathrm{SU}_n(q)$ acting in its total Weil representation. The rest of the proof is to show that $G = E \rtimes S$.

(b) We aim to show that $G \rhd E$ and to determine

$$\bar{G} := EG/G \leq H_1^\circ/E = \Omega_{2N}^-(2),$$

a subgroup of $\Omega(W)$ that preserves the natural quadratic form $\mathsf{Q}(x\mathbf{Z}(E)) = x^2$ on $W := E/\mathbf{Z}(E)$. As $G \geq S$ and $E \cap S \leq \mathbf{O}_2(S) = 1$, $S \hookrightarrow \bar{G}$; in particular, $|\bar{G}|$ is divisible by a primitive prime divisor $\ell$ of $q^{2n} - 1 = 2^{2N} - 1$, as chosen in 8.3.1 and 8.3.3. We can now apply Theorem 8.3.1 and Proposition 8.3.3 (with $q_0 = 2$ and thus viewing $\bar{G} \leq \mathrm{GL}_{2N}(2)$) to determine $L := \mathbf{O}^{\ell'}(\bar{G})$. Note that $\mathbf{O}^{\ell'}(S) = S$, so $S \hookrightarrow L$; in particular, $L$ is not cyclic.

In the case of 8.3.1(vi), $q^n = 2^{10}$, so $(n,q) = (5,4)$, but then $S = \mathrm{SU}_5(4)$ cannot embed in $L = \mathrm{PSL}_2(41)$.

Case 8.3.3(ii) cannot occur, since $q^n = 2^{nf} \geq 2^4$.

In the cases (iii) and (vi) of 8.3.3, $q^n = 2^5$, so $(n,q) = (5,2)$, but then $S = \mathrm{SU}_5(2)$ cannot embed in any $L \in \{\mathrm{PSL}_2(11), M_{11}, M_{12}, M_{22}, \mathsf{A}_{11}, \mathsf{A}_{12}\}$ (since the smallest index of proper subgroups of $S$ is 165, see [**CCNPW**]).

In the cases (iv) and (vii) of 8.3.3, $q^n = 2^6$, so $(n,q) = (3,4)$, but then $S = \mathrm{SU}_3(4)$ cannot embed in any $L \in \{\mathrm{PSL}_2(13), \mathrm{PSL}_2(25), \mathrm{SL}_3(3), \mathsf{A}_{13}, \mathsf{A}_{14}\}$ (since the smallest index of proper subgroups of $S$ is 65, see [**CCNPW**]).

In the cases (v) and (viii) of 8.3.3, $q^n = 2^9$, so $(n,q) = (3,8)$ or $(9,2)$, but then $S \geq \mathrm{SU}_3(8)$ cannot embed in any $L \in \{3 \cdot \mathsf{J}_3, \mathrm{PSL}_2(19), \mathsf{A}_{19}, \mathsf{A}_{20}\}$ (since $7||S|$ and the smallest index of proper subgroups of $S$ is $\geq 513$, see [**CCNPW**]).

We have therefore shown that either (iii) or (iv) of Theorem 8.3.1 occurs; in particular, $L = \mathrm{SU}_c(2^d)$ with $c \geq 3$ and $cd = N$, or $\Omega_{2c}^-(2^d)$ with $c \geq 2$ and $cd = N$; in both cases $c$ divides $nf \geq 5$. As $L$ acts irreducibly on $W$, we note that $\mathbf{C}_{\bar{G}}(L)$ embeds in the finite field $\mathrm{End}_L(W)$ and so is cyclic; on the other hand $L$ is quasisimple. Hence $\bar{G}/L\mathbf{C}_{\bar{G}}(L)$ is solvable, and so $\bar{G}^{(\infty)} = L$.

Note that $G \geq \mathbf{Z}(E_1) = \mathbf{Z}(E)$. Next, any element of order $\ell$ of $\mathrm{O}(W)$ acts irreducibly on $W$. The same is true for $G$, so either $G \cap E = \mathbf{Z}(E)$, or $G \geq E$. Suppose we are in the former case. Then $\bar{G} = EG/E \cong G/(G \cap E) = G/\mathbf{Z}(E)$. Hence $G^{(\infty)}$ has order either $|L| = |\bar{G}^{(\infty)}|$ or $2|L|$, and $G^{(\infty)}$ is a cover of $\mathrm{PSU}_c(2^d)$ or $\Omega^-_{2c}(2^d)$, which contains the perfect subgroup $S$ as $S \hookrightarrow G$. As mentioned above, $G$ acts irreducibly on $\mathcal{G}$ of dimension $2^N$. It follows that every irreducible $G^{(\infty)}$-summand on $\mathcal{G}$ has dimension dividing $2^{cd}$. Applying [**TZ1**, Theorem 1.1], we see that this is possible only when $c = 2$ and $G^{(\infty)} = \Omega^-_4(2^d) \cong \mathrm{SL}_2(2^N)$. However in this case the $G^{(\infty)}$-module $\mathcal{G}$ is irreducible and orthogonally self-dual, a contradiction.

Therefore we are in the latter case: $G \geq E$, and so $G \rhd E$.

(c) Now we can apply Lemma 8.5.4 to see that $W$ carries an $\mathbb{F}_q L$-module structure. As $|L|$ is still divisible by $\ell$, we can again apply Theorem 8.3.1 and Proposition 8.3.3, now with $q_0 = q$ and thus viewing $L \leq \mathrm{GL}_{2n}(q)$, to determine $L = \mathbf{O}^{\ell'}(L)$. The arguments in (b) show that, in fact, we have one of the cases (iii) and (iv) of Theorem 8.3.1.

In the case of 8.3.1(iv), there is a divisor $j$ of $n$ such that $n/j \geq 2$ and $L = \Omega(W_{fj}) \cong \Omega^-_{2n/j}(q^j)$, where $W_{fj}$ is $W$ viewed as a $2n/j$-dimensional vector space over $\mathbb{F}_{q^j}$ endowed with a non-degenerate quadratic form of type $-$. In fact, since $2 \nmid n$, we have that $2 \nmid j \leq n/3$; also $nf \geq 5$. In particular, $(2n-2j)f \geq 4nf/3 > 6$. Hence by [**Zs**] we can find a primitive prime divisor $\ell_1$ of $2^{2(n-j)f} - 1$, which then divides both $(q^j)^{n/j-1} + 1$ and $|L|$.

Certainly, $L$ contains an element of order $\ell_1$, which lifts to an element $g \in G$ of (odd) order $\ell_1$. Now, $a := \mathrm{Trace}(g)$ is an integer, so $\mathrm{Trace}(g^i) = a$ for $1 \leq i \leq \ell_1 - 1$ (by Galois action). On the other hand, $\mathrm{Trace}(\mathrm{Id}) = q^n$. Computing the multiplicity of the trivial character in the character of $\langle g \rangle$ acting on $\mathcal{G}$, we get $\mathbb{Z} \ni (q^n + a(\ell_1 - 1))/\ell_1$, i.e.

$$a \equiv q^n (\mathrm{mod}\ \ell_1); \tag{8.5.8.1}$$

in particular, $a \neq 0$. By Theorem 7.1.2(d), $a = \pm q^k < q^n$ for some $0 \leq k \leq n$. Suppose $a = q^k$, so that $0 \leq k < n$. Then (8.5.8.1) implies that $\ell_1 | (q^{n-k} - 1)$, so by primitivity of $\ell_1$ we have $(2n-2j)|(n-k)$, a contradiction since $2n-2j \geq 4n/3 > n-k > 0$. Hence $a = -q^k$, in which case (8.5.8.1) implies that $\ell_1 | (q^{n-k}+1)$. By primitivity of $\ell_1$ we have $(n-j)|(n-k)$. Note that $k \neq n$ as $g$ has order $\ell_1 > 2$, so $0 < n-k < 4n/3 \leq 2(n-j)$. It follows that $n-k = n-j$, i.e. $a = -q^j$. As $2 \nmid j$, we now have that $\mathrm{Trace}(g) = -q^j \equiv 1 (\mathrm{mod}\ (q+1))$. But this contradicts Corollary 7.1.5, according to which $\mathrm{Trace}(g) \equiv -1 (\mathrm{mod}\ (q+1))$.

(d) We have shown that $L$ satisfies 8.3.1(iii), i.e. there is a proper divisor $j$ of $n$ such that $2 \nmid (n/j)$ and $L = \mathrm{SU}(W_{2fj}) \cong \mathrm{SU}_{n/j}(q^j)$, where $W_{2fj}$ is $W$ viewed as an $n/j$-dimensional vector space over $\mathbb{F}_{q^{2j}}$ endowed with a non-degenerate Hermitian form. Since $\mathrm{SU}_n(q) \hookrightarrow L$, we have $j = 1$ (by order consideration). Thus $L = \mathrm{SU}_n(q)$. By Proposition 8.4.1(b2), we now have that

$$L \lhd \bar{G} = G/E \leq \mathrm{GU}_n(q) \rtimes C_{2f}.$$

Suppose that $\bar{G}/L$ has *even* order. As $L \cong \mathrm{SU}_n(q)$, we may assume that $G$ contains an element $h$, whose image in $\bar{G}$ is $t\sigma$, where $t := \mathrm{diag}(1, \ldots, 1, \lambda)$ in some orthonormal basis $(e_1, \ldots, e_n)$ of the Hermitian $\mathbb{F}_{q^2}$-space $W_{2f} = \mathbb{F}^n_{q^2}$, $\lambda^{q+1} = 1$, and $\sigma$ acts via $\sum_i x_i e_i \mapsto x_i^q e_i$. Since the equation $x^{q-1} = \lambda$ has $q-1$ roots in $\mathbb{F}_{q^2}$ for any such $\lambda$, we see that $|\mathbf{C}_{W_f}(t\sigma)| = q^n$. It follows from Lemma 7.2.1 that the coset $hE$ in $G$ contains some element $h_1$ with $|\mathrm{Trace}(h_1)|^2 = q^n$. On the other hand, working over extensions of $\mathbb{F}_{q^2}$, we have $|\mathrm{Trace}(h_1)|^2 = 0$ or an even power of $q$ by Corollary 8.1.5, and this is a contradiction since $2 \nmid n$.

We have shown that $\bar{G}/L$ has odd order. Since $\mathcal{G}$ lives over $\mathbb{A}^{r+1}$, $G = \mathbf{O}^{2'}(G)$ by Theorem 1.3.4. It follows that $\bar{G} = L$, $G = E \cdot L$, and so $G = E \rtimes S$. We also note that $G < H_f^\circ$, since $L < \Omega_{2n}^-(q)$ by Proposition 8.4.1(b2).

(e) To determine $G_{\mathrm{arith},k}$, let $H = H_{\mathrm{geom}} = \mathrm{SU}_n(q)$ and $H_{\mathrm{arith},k}$ denote the geometric monodromy group and the arithmetic monodromy group over $k$ of the specialization $s_{r+1} = 0$ of $\mathcal{G}$, which is the sheaf $\mathcal{G}(n, m_1, \ldots, m_r; q)$ over $\mathbb{A}^r/\mathbb{F}_2$ considered in Theorem 8.5.7. By [**KRLT4**, Lemma 4.1], $G_{\mathrm{arith},\mathbb{F}_2} = \langle G_{\mathrm{geom}}, g\rangle$ for the image $g$ of any element $\mathsf{Frob}_{(s_1,s_2,\ldots,s_{r+1}),\mathbb{F}_2}$ in $G_{\mathrm{arith},\mathbb{F}_2}$ with $s_i \in \mathbb{F}_2$. Choosing $s_{r+1} = 0$, we can identify $g := \mathsf{Frob}_{(s_1,s_2,\ldots,s_{s_r},0),\mathbb{F}_2}$, which tautologically lies in the subgroup $H_{\mathrm{arith},\mathbb{F}_2}$ of $G_{\mathrm{arith},\mathbb{F}_2}$, with the element $\mathsf{Frob}_{(s_1,s_2,\ldots,s_r),\mathbb{F}_2}$ in $H_{\mathrm{arith},\mathbb{F}_2}$. In particular, by Theorem 8.5.7, $g^{2f} \in H_{\mathrm{arith},\mathbb{F}_{q^2}} = C_2 \times H$, with $C_2$ acting as the scalar subgroup of order 2 and thus $C_2 = \mathbf{Z}(E)$. As $G = E \rtimes H$, we conclude that $g^{2f} \in G$ and thus $G_{\mathrm{arith},\mathbb{F}_2}/G \hookrightarrow C_{2f}$. It follows that the order $j$ of $g$ modulo $G$ divides $2f$, and $G_{\mathrm{arith},\mathbb{F}_{q^2}} = G$.

We next observe that

$$\mathbf{N}_G(H) = \mathbf{Z}(E) \times H. \tag{8.5.8.2}$$

Indeed, $\mathbf{N}_G(H)$ certainly contains $\mathbf{Z}(E)H$. If $\mathbf{N}_G(H) > \mathbf{Z}(E)H$, then $\mathbf{N}_G(H) \cap E > \mathbf{Z}(E)$ as $G = EH$. It follows that $1 \neq (\mathbf{N}_G(H) \cap E)/\mathbf{Z}(E)$ is normalized by $\mathbf{N}_G(H) > H$. As $H$ acts irreducibly on $E/\mathbf{Z}(E)$, we must have that $\mathbf{N}_G(H) \geq E$ and thus $\mathbf{N}_G(H) = G$, i.e. $H \lhd G$. As $G = EH$, $E \lhd G$, and $E \cap H = 1$, we then have that $G = E \times H$, a contradiction.

Now, $g \in H_{\mathrm{arith},\mathbb{F}_2}$ normalizes $H$, so $g^j \in \mathbf{N}_G(H)$. Hence (8.5.8.2) implies that $g^j \in H_{\mathrm{arith},\mathbb{F}_{q^2}}$, and so $2f|j$ since $H_{\mathrm{arith},\mathbb{F}_2} = \langle H, g\rangle$ has quotient $C_{2f}$ over $H_{\mathrm{arith},\mathbb{F}_{q^2}}$. Thus $j = 2f$ and $G_{\mathrm{arith},\mathbb{F}_2}/G \cong C_{2f}$. By Theorem 8.5.7, $g$ induces the subgroup $C_{2f}$ of outer field automorphisms of $H$, and so we are done. □

THEOREM 8.5.9. *Assume $q = 2^f$, $r \geq 1$, and $n > m_1 > \ldots > m_r \geq 0$ are integers with $nf \geq 4$. If $m_r \geq 1$, we assume that $2|nm_1 \ldots m_r$ and* $\gcd(n, m_1, \ldots, m_r) = 1$. *If $m_r = 0$, we assume $r \geq 2$, $2|nm_1 \ldots m_{r-1}$ and* $\gcd(n, m_1, \ldots, m_{r-1}) = 1$. *Then the geometric monodromy group $G$ of the local system $\mathcal{G} := \mathcal{G}(n, m_1, \ldots, m_r; q)$, defined in* (8.5.0.1), *is isomorphic to the subgroup $H_f^\circ \cong 2_-^{1+2nf} \cdot \Omega_{2n}^-(q)$ of the group $\Gamma(2, nf, -) = H_1^-$, as defined in* (8.2.2.1). *Over any finite extension $k$ of $\mathbb{F}_2$, for the arithmetic monodromy group $G_{\mathrm{arith},k}$ of $\mathcal{G}$ over $k$ we have $G_{\mathrm{arith},k} = G$ if $k \supseteq \mathbb{F}_{q^2}$ and $G_{\mathrm{arith},k} \cong G \cdot \mathrm{Gal}(\mathbb{F}_{q^2}/k)$ if $k \subseteq \mathbb{F}_{q^2}$. In the latter case,* $\mathrm{Gal}(\mathbb{F}_{q^2}/k)$ *may be identified with the subgroup* $\mathrm{Gal}(\mathbb{F}_{q^2}/k)$ *of outer automorphisms of* $\Omega_{2n}^-(q)$.

PROOF. (a) Define $m_{r+1} := 1$ if $2|N := nf$ and $m_{r+1} := 2$ if $2 \nmid N$. Then $\mathcal{G}$ is the specialization $s_{r+1} = 0$ of the local system $\tilde{\mathcal{G}} := \mathcal{G}(nf, m_1 f, \ldots, m_r f, m_{r+1}; 2)$ on $\mathbb{A}^{r+1}/\mathbb{F}_2$. Again by Theorem 8.1.1 and [**KT2**, Lemma 5.1], $\tilde{\mathcal{G}}$ has finite geometric monodromy group $\tilde{G}$ that contains $G$. On the other hand, the specialization $s_1 = \ldots = s_r = 0$ of $\tilde{\mathcal{G}}$ is the local system $\mathcal{G}(nf, m_{r+1}; 2)$ on $\mathbb{A}^1/\mathbb{F}_2$ considered in Theorem 8.5.5. Hence $\tilde{G}$ contains the geometric monodromy group $H_1^\circ$ of the latter, which was shown to satisfy (**S**+) and contains an $\mathsf{ssp}$-element of central order $2^N + 1$. Also, $\tilde{\mathcal{G}}$ is symplectically self-dual by [**Ka-MMP**, Theorem 3.10.6], so that $\tilde{G} \leq \mathrm{Sp}_{2^N}(\mathbb{C})$. Hence we can apply Theorem 8.4.5(a) to $\tilde{G}$ and conclude (since $H_1^\circ \not\leq \mathrm{SL}_2(2^{N+1} + 1)$) that $\tilde{G} \leq H_1^-$, and thus $G \leq H_1^\circ$; in particular, $G$ normalizes $E := \mathbf{O}_2(H_1^-)$.

Write

$$e_i := \gcd(n, m_i), \; n_i := n/e_i, \text{ and } k_i := m_i/e_i$$

for all $i$ such that $m_i > 0$. Suppose that $n_i k_i = nm_i/e_i^2$ is odd for all such $i$. Now if $n$ is odd, then $e_i|n$ is odd, whence $2 \nmid m_i$ for all such $i$, and thus $n\prod_{i:m_i>0} m_i$ is odd, a contradiction. Hence $n$ is even, forcing $2|e_i$, whence $2|m_i$ for all such $i$, and thus $\gcd(n, m_i \mid m_i > 0)$ is even, a contradiction. Therefore, we can find $i_0 \geq 1$ such that

$$2 \nmid n_{i_0}k_{i_0}, \; \gcd(n_{i_0}, k_{i_0}) = 1.$$

Now the specialization $s_i = 0$ for all $i \neq i_0$ of $\mathcal{G}$ is the sheaf $\mathcal{G}(n_{i_0}, k_{i_0}; q^{e_{i_0}})$ over $\mathbb{A}^1/\mathbb{F}_2$ considered in Theorem 8.5.5, hence $G$ is irreducible and contains

$$H_0 := H^\circ_{fe_{i_0}} = E_0 \cdot S_0, \text{ where } E_0 \cong E \text{ and } S_0 := \Omega^-_{2n_{i_0}}(q^{e_{i_0}}).$$

Note that both $\mathbf{Z}(E_0)$ and $\mathbf{Z}(E)$ is generated by the central involution $\boldsymbol{j}$ (acting as the scalar $-1$ on $\mathcal{G}$), so $G \geq \mathbf{Z}(E_0) = \mathbf{Z}(E)$.

(b) We aim to show that $E = E_0$, so that $G \rhd E$, and to determine

$$\bar{G} := EG/G \leq H^\circ_1/E = \Omega^-_{2N}(2),$$

a subgroup of $\Omega(W)$ that preserves the natural quadratic form $\mathsf{Q}(x\mathbf{Z}(E)) = x^2$ on $W := E/\mathbf{Z}(E)$. As $|G|$ is divisible by the order of the simple group $S_0$; $|\bar{G}|$ is divisible by a primitive prime divisor $\ell$ of $q^{2n} - 1 = 2^{2N} - 1$, as chosen in 8.3.1 and 8.3.3. Note that any element of order $\ell$ of $\mathrm{O}(W)$ acts irreducibly on $W$. The same is true for $H_0 \geq \mathbf{Z}(E_0) = \mathbf{Z}(E)$. This irreducible action shows that $\mathbf{O}_2(H_0)$ must act trivially on $W$. On the other hand, $H_0 \leq H^-_1$ and $H^-_1/E = \mathrm{O}(W)$ acts faithfully on $W$. Hence $E_0 = \mathbf{O}_2(H_0) \leq E$, and so $E_0 = E$ by order comparison, and $G \rhd E$.

Now we apply Theorem 8.3.1 and Proposition 8.3.3 (with $q_0 = 2$ and thus viewing $\bar{G} \leq \mathrm{GL}_{2N}(2)$) to determine $L := \mathbf{O}^{\ell'}(\bar{G})$. Note that $\mathbf{O}^{\ell'}(S_0) = S_0$, so $S_0 = H_0/E \hookrightarrow L$; in particular, $L$ is not cyclic. To rule out various cases, we note that $S_0$ contains an element of order $(q^{e_{i_0}})^{n_{i_0}} + 1 = q^n + 1$.

Case 8.3.1(vi) is ruled out since $\mathrm{PSL}_2(41)$ does not contain an element of order $q^n + 1 = 1025$.

Case 8.3.3(ii) cannot occur, since $q^n = 2^{nf} \geq 2^4$.

Cases (iii) and (vi) of 8.3.3 are ruled out since none of the groups $\mathrm{PSL}_2(11)$, $M_{11}$, $M_{12}$, $M_{22}$, $\mathsf{A}_{11}$, $\mathsf{A}_{12}$ can contain elements of order $q^n + 1 = 33$, see [**CCNPW**]).

Cases (iv) and (vii) of 8.3.3 cannot occur since none of the groups $\mathrm{PSL}_2(13)$, $\mathrm{PSL}_2(25)$, $\mathrm{SL}_3(3)$, $\mathsf{A}_{13}$, $\mathsf{A}_{14}$ can contain elements of order $q^n + 1 = 65$, see [**CCNPW**]).

Cases (v) and (viii) of 8.3.3 are also ruled out since none of the groups $3 \cdot \mathsf{J}_3$, $\mathrm{PSL}_2(19)$, $\mathsf{A}_{19}$, $\mathsf{A}_{20}$ can contain elements of order $q^n + 1 = 513$, see [**CCNPW**]).

We have therefore shown that either (iii) or (iv) of Theorem 8.3.1 occurs; in particular, $L = \mathrm{SU}_c(2^d)$ with $2 \nmid c \geq 3$ and $cd = N$, or $\Omega^-_{2c}(2^d)$ with $c \geq 2$ and $cd = N$. As $L$ acts irreducibly on $W$, we note that $\mathbf{C}_{\bar{G}}(L)$ embeds in the finite field $\mathrm{End}_L(W)$ and so is cyclic; on the other hand $L$ is quasisimple. Hence $\bar{G}/L\mathbf{C}_{\bar{G}}(L)$ is solvable, and so $\bar{G}^{(\infty)} = L$.

(c) Now we can apply Lemma 8.5.4 to see that $W$ carries an $\mathbb{F}_qL$-module structure. As $|L|$ is still divisible by $\ell$, we can again apply Theorem 8.3.1 and Proposition 8.3.3, now with

$(q_0, d) = (q, 2n)$ and thus viewing $L \leq \mathrm{GL}_{2n}(q)$, to determine $L = \mathbf{O}^{\ell'}(L)$. The arguments in (b) show that, in fact, we have one of the cases (iii) and (iv) of Theorem 8.3.1.

In the case of 8.3.1(iii), there is a proper divisor $j$ of $n$ such that $2 \nmid (n/j)$ and $L = \mathrm{SU}(W_{2fj}) \cong \mathrm{SU}_{n/j}(q^j)$, where $W_{2fj}$ is $W$ viewed as an $n/j$-dimensional vector space over $\mathbb{F}_{q^{2j}}$ endowed with a non-degenerate Hermitian form. Let $d(X)$ denote the smallest degree of nontrivial complex representations of the quasisimple group $S_0$. Then, according to [**TZ1**, Theorem 1.1], $d(S_0) = q^n - 1$ when $n_{i_0} = 2$ (and so $S_0 = \Omega_4^-(q^{n/2}) \cong \mathrm{SL}_2(q^n)$), $d(S_0) = (q^{4n/3} - 1)/(q^{n/3} + 1) > q^n/2$ when $n_{i_0} = 3$ (and so $S_0 = \Omega_6^-(q^{n/3}) \cong \mathrm{SU}_4(q^{n/3})$), and $d(S_0) > q^{e_{i_0}(2n_{i_0}-3)} > q^n$ when $n_{i_0} \geq 4$. On the other hand, $d(L) = (q^n - q^j)/(q^j + 1) < q^n/2$, and this contradicts the embedding $S_0 \hookrightarrow L$.

(d) Hence we must be in the case of 8.3.1(iv), i.e. there is a divisor $j$ of $n$ such that $n/j \geq 2$ and $L = \Omega(W_{fj}) \cong \Omega^-_{2n/j}(q^j)$, where $W_{fj}$ is $W$ viewed as a $2n/j$-dimensional vector space over $\mathbb{F}_{q^j}$ endowed with a non-degenerate quadratic form $\mathsf{Q}_{fj}$ of type $-$.

We will show that $j = 1$. Since

$$\gcd(e_i \mid m_i > 0) \text{ divides } \gcd(n, m_i \mid m_i > 0) = 1,$$

it suffices to show that

$$j|e_i \text{ for all } i \text{ with } m_i > 0. \tag{8.5.9.1}$$

Consider any such $i$. Then the specialization $s_{i'} = 0$ for all $i' \neq i$ of $\mathcal{G}$ is the sheaf $\mathcal{G}(n_i, k_i; q^{e_i})$ over $\mathbb{A}^1/\mathbb{F}_2$ considered in Theorem 8.5.5 when $2|n_ik_i$ and in Theorem 8.5.7 when $2 \nmid n_ik_i$.

(d1) When $2|n_ik_i$, Theorem 8.5.5 shows that $G$ contains

$$H_i := E_i \cdot S_i, \text{ where } E_i \cong E \text{ and } S_i := \Omega^-_{2n_i}(q^{e_i}).$$

The arguments in (b) show that $E_i = E$ and thus $S_i \hookrightarrow L$ as $S_i$ is simple. First suppose that $n_i \geq 3$, so that $(n_i - 1)e_i > n_ie_i/2 = n/2$. Now, if $((n_i - 1)e_i, q) \neq (3, 2)$, then $(q^{e_i})^{2(n_i-1)} - 1$ has a primitive prime divisor $\ell_i$ [**Zs**], which then divides both $|S_i|$ and $|L|$. It follows that there is some $1 \leq t \leq n/j$ such that $\ell_i$ divides $q^{2tj} - 1$. Note that $tj \leq n < 2e_i(n_i - 1)$, so by primitivity of $\ell_i$ we have $tj = e_i(n_i - 1) = n - e_i$. Since $j|n$, (8.5.9.1) follows. In the case $((n_i - 1)e_i, q) = (3, 2)$, as $n_i \geq 3$ we have $e_i = 1$, $n_i = 4$, $n = 4$, and $S_i = \Omega_8^-(2) \hookrightarrow \Omega^-_{8/j}(2^j)$, implying $j = 1$.

Next suppose that $n_i = 2$, i.e. $S_i = \Omega_4^-(q^{n/2}) \cong \mathrm{SL}_2(q^n)$. Now, if $(n, q) \neq (6, 2)$, then, as $n \geq 2$ and $2|q$, $q^n - 1$ has a primitive prime divisor $\ell_i$ [**Zs**], which then divides both $|S_i|$ and $|L|$. Since $\ell_i \nmid (q^n + 1)$, it follows that there is some $1 \leq t < n/j$ such that $\ell_i$ divides $q^{2tj} - 1$. Note that $2tj < 2n$, so by primitivity of $\ell_i$ we have $2tj = n$, i.e $j|(n/2) = e_i$, and (8.5.9.1) follows. In the case $(n, q) = (6, 2)$, as $j|n$ and $j \leq n/2$ we have $j \in \{1, 2, 3\}$. If $j \neq 2$, then $j|(n/2) = 3$ and (8.5.9.1) follows. If $j = 2$, then $\mathrm{SL}_2(q^6) = S_i \hookrightarrow L = \Omega_6^-(q^2) = \mathrm{SU}_4(q^2)$, which is a contradiction since $d(L) = (q^8 - 1)/(q^2 + 1) < q^6 - 1 = d(S_i)$ in such a case, see [**TZ1**, Theorem 1.1].

(d2) When $2 \nmid n_ik_i$, Theorem 8.5.7 shows that $G$ contains $S_i := \mathrm{SU}_{n_i}(q^{e_i})$. Since $\mathbf{O}_2(S_i) = 1$, $S_i \hookrightarrow L$. In the case $((n_i - 1)e_i, q) = (6, 2)$, as $2 \nmid n_i \geq 3$ we have $(e_i, n_i, n) = (3, 3, 9)$ or $(1, 7, 7)$. As $j|n$ and $j < n$, $j|e_i$ and (8.5.9.1) follows in both cases.

So we may assume that $((n_i - 1)e_i, q) \neq (6, 2)$. Then $(q^{e_i})^{n_i-1} - 1$ has a primitive prime divisor $\ell_i$ [**Zs**], which then divides both $|S_i|$ and $|L|$. Now suppose that there is some $1 \leq t < n/j$ such that $\ell_i$ divides $q^{2tj} - 1$. Since $n_i \geq 3$, $2tj < 2n < 3e_i(n_i - 1)$. So by primitivity of $\ell_i$ we either have $tj = e_i(n_i - 1) = n - e_i$ or $2tj = e_i(n_i - 1) = n - e_i$. Since $j|n$, (8.5.9.1) follows in both cases. In the remaining case, $\ell_i$ is coprime to $\prod_{t'=1}^{n/j-1}(q^{2t'j} - 1)$. Hence the divisor $\ell_i$ of $|L|$ must divide $(q^j)^{n/j} + 1 = (q^{e_i})^{n_i} + 1$. By the choice of $\ell_i$, it follows that $\ell_i|(q^{e_i} + 1)$ and so $(n_i, e_i) = (3, n/3)$. In particular, the Sylow $\ell_i$-subgroups of $S_i = \mathrm{SU}_3(q^{n/3})$ are *not cyclic*, whereas the Sylow $\ell_i$-subgroups of $L$ are contained in maximal tori of order $q^n + 1$ and are cyclic. This again contradicts the embedding $S_i \hookrightarrow L$.

(e) We have shown that $L = \Omega(W_f) \cong \Omega^-_{2n}(q)$, where $W_f$ is $W$ viewed as a $2n$-dimensional vector space of $\mathbb{F}_q$ with quadratic form $\mathsf{Q}_f$. Now, the arguments in part (iii) of the proof of Theorem 8.3.4 show that there is $\alpha \in \mathbb{F}_q^\times$ such that $\mathsf{Q}(u) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\alpha \cdot \mathsf{Q}_f(u))$ for all $u \in W_f$. Rescaling $\mathsf{Q}_f$ suitably (without any effect on $L$), we may assume that $\mathsf{Q}(u) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\mathsf{Q}_f(u))$ for all $u \in W_f$, whence $H^\circ_f \lhd G \leq H^-_1$. Suppose that $a_1 := |G/H^\circ_f| > 1$. By Theorem 1.3.4, $G = \mathbf{O}^{2'}(G)$, and so $2|a_1$. Now we can apply Theorem 8.2.5(iii) to see that $G \geq H^-_f$. Hence, by Theorem 8.2.5(ii), $G$ contains an element $h \in H^-_f$ with $|\mathrm{Trace}(h)| = \sqrt{q}$, contrary to Corollary 8.1.2 when $m_r > 0$ and Corollary 8.1.5 when $m_r = 0$. Hence $a_1 = 1$, i.e. $G = H^\circ_f$ as stated.

(f) Now we determine $G_{\mathrm{arith},k}$. Over $\mathbb{F}_2$, we know that $\mathcal{G}$ is symplectically self-dual by [**Ka-MMP**, Theorem 8.10.6]. Also, $G_{\mathrm{arith},\mathbb{F}_2} \rhd G = H^\circ_f$. Hence, by Theorem 8.2.5(iii),

$$G \lhd G_{\mathrm{arith},\mathbb{F}_2} \leq \mathbf{N}_{\mathrm{Sp}_{2N}(\mathbb{C})}(G) = G \cdot C_{2f};$$

in particular, $G_{\mathrm{arith},\mathbb{F}_2}/G \hookrightarrow C_{2f}$ and $G_{\mathrm{arith},\mathbb{F}_{q^2}} = G$.

Let $g$ denote the image of $\mathsf{Frob}_{(1,0,\dots,0),\mathbb{F}_2}$ in $G_{\mathrm{arith},\mathbb{F}_2}$, so that $G_{\mathrm{arith},\mathbb{F}_2} = \langle G, g\rangle$. Then $b_1 := |G_{\mathrm{arith},\mathbb{F}_2}/G|$ is the order of $g$ modulo $G$, and $b_1|2f$. For any $x \in \mathbb{F}_2$ we have $x^{q^n+1} = x^2 = x^{q^{m_1}+1}$, and so $\psi_{\mathbb{F}_2}(x^{q^n+1} + x^{q^{m_1}+1}) = \psi_{\mathbb{F}_2}(0) = 1$. It follows that $|\mathrm{Trace}(g)|^2 = 2$. Now, if $2 \nmid b_1$, then $b_1|f$, and statements (iii)(b) and (i) of Theorem 8.2.5 imply that $|\mathrm{Trace}(g)|^2$ is either 0 or a power of $2^{2f/b_1}$, which is a power of 4, a contradiction. Hence $2|b_1$, and $b_1 = 2b$ with $b|f$. In the notation of Proposition 8.2.3(iii) and Theorem 8.2.5(iii), $G_{\mathrm{arith},\mathbb{F}_2} = \langle H^\circ_f, s^{f/b}\rangle \leq H^-_{f/b}$. It follows from Theorem 8.2.5(ii) that $2 = |\mathrm{Trace}(g)|^2$ is either 0 or a power of $2^{f/b}$, whence $b = f$.

We have shown that $G_{\mathrm{arith},\mathbb{F}_2}/G \cong C_{2f} \cong \mathrm{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_2)$, and

$$G_{\mathrm{arith},\mathbb{F}_2} = \mathbf{N}_{\mathrm{Sp}_{2N}(\mathbb{C})}(H^\circ_f). \tag{8.5.9.2}$$

In particular, $G_{\mathrm{arith},\mathbb{F}_2}$ contains the element $s$ constructed in Theorem 8.2.5(iii) which corresponds to the automorphism $\sigma$ of $S := \Omega^-_{2n}(q)$, constructed in Proposition 8.2.5 so that $\mathrm{Aut}(S) = \langle S, \sigma\rangle \cong S \rtimes C_{2f}$. The proof is now completed, since for any subfield $k \subseteq \mathbb{F}_{q^2}$, $[G_{\mathrm{arith},k} : G_{\mathrm{arith},\mathbb{F}_{q^2}}]$ divides $[\mathbb{F}_{q^2} : k]$ and $[G_{\mathrm{arith},\mathbb{F}_2} : G_{\mathrm{arith},k}]$ divides $[k : \mathbb{F}_2]$. □

REMARK 8.5.10. It is shown in [**KT8**, Theorem 4.4(i), (ii)] that the assumption $nf \geq 4$ in both Theorems 8.5.5 and 8.5.9 can be removed. Similarly, in the excluded case $(n, f) = (3, 1)$ of Theorem 8.5.8, it is shown in [**KT8**, Theorem 4.4(iii)] that, over any extensions $k$ of $\mathbb{F}_4$, $\mathcal{G} = \mathcal{G}(3, 1, 0; 2)$ has $G_{\mathrm{arith},k} = G_{\mathrm{geom}} = 2^{1+6}_{-} \cdot \mathrm{SU}_3(2)$, whereas over $\mathbb{F}_2$ it has $G_{\mathrm{arith},\mathbb{F}_2} = G_{\mathrm{geom}} \cdot 2$.

CHAPTER 9

# Two further kinds of local systems in characteristic 2

## 9.1. Another kind of hypergeometric sheaf in characteristic 2

In the paper [**KRLT3**, §4], we considered the following situation, in arbitrary characteristic $p > 0$. We were given two integers $A, B$, each $\geq 3$ and prime to $p$, with $\gcd(A, B) = 1$. We formed the hypergeometric sheaf

$$\mathcal{H}yp_\psi(A \times B; \mathbb{1}),$$

whose "upstairs" characters are the $(A-1)(B-1)$ characters of the form $\chi\rho$ with $\chi \neq \mathbb{1}, \chi^A = \mathbb{1}$ and $\rho \neq \mathbb{1}, \rho^B = \mathbb{1}$, and whose "downstairs" character is the single character $\mathbb{1}$. It is defined on $\mathbb{G}_m/\mathbb{F}_q$ for any finite extension of $\mathbb{F}_p$ containing the $AB^{\text{th}}$ roots of unity. One knows [**Ka-ESDE**, 8.4.2(4)] that $\mathcal{H}yp_\psi(A \times B; \mathbb{1})$ is pure of weight $(A-1)(B-1)$, and geometrically irreducible. We showed [**KRLT3**, 4.1, 4.2] that $\mathcal{H}yp_\psi(A \times B; \mathbb{1})$ has geometrically trivial determinant, and that in chararcteristic $p = 2$, it is orthogonally self-dual. We also gave the criterion for the Tate twist

$$\mathcal{H}yp_\psi(A \times B; \mathbb{1})((A-1)(B-1)/2),$$

to have finite arithmetic and geometric monodromy in terms of Kubert's $V$-function. The criterion is that for all $x \in (\mathbb{Q}/\mathbb{Z})_{\text{prime to } p}$, we have

$$V(ABx) + V(x) + V(-x) \geq V(Ax) + V(Bx).$$

Equivalently, since this trivially holds for $x = 0$, the criterion is that for all nonzero $x \in (\mathbb{Q}/\mathbb{Z})_{\text{prime to } p}$, we have

$$V(ABx) + 1 \geq V(Ax) + V(Bx).$$

Theorem 9.1.1. *Let $a, b$ be positive integers such that $\gcd(2^a + 1, 2^b + 1) = 1$. Then in characteristic $p = 2$, with*

$$A := 2^a + 1, \quad B := 2^b + 1,$$

*the sheaf*

$$\mathcal{H}_0 := \mathcal{H}yp_\psi(A \times B; \mathbb{1})((A-1)(B-1)/2)$$

*has finite arithmetic and geometric monodromy.*

Proof. The criterion in terms of Kubert's $V$-function is that for all nonzero $x \in (\mathbb{Q}/\mathbb{Z})_{\text{prime to } 2}$, we have

$$V((2^a + 1)(2^b + 1)x) + 1 \geq V((2^a + 1)x) + V((2^b + 1)x).$$

In fact, this inequality is the $p = 2$ case of the following Theorem 9.1.2. [But notice that Theorem 9.1.2 can only be relevant to a $\mathcal{H}yp(A \times B, \mathbb{1})$ situation when $p = 2$.] □

Theorem 9.1.2. *Let $p$ be a prime, $a, b$ positive integers. Then for all nonzero $x \in (\mathbb{Q}/\mathbb{Z})_{\text{prime to } p}$, we have*

$$V((p^a+1)(p^b+1)x) + 1 \geq V((p^a+1)x) + V((p^b+1)x).$$

To give the proof, we need the following lemma.

Lemma 9.1.3. *Let $p$ be a prime and $c$ a non-negative integer. Then for all $x \in (\mathbb{Q}/\mathbb{Z})_{\text{prime to } p}$, we have the inequality*

$$1 + V(x + p^c x) \geq 2V(x).$$

Proof. If $x = 0$, this trivially holds. Because $V(p^c x) = V(x)$, we may rewrite this as

$$1 + V(x + p^c x) \geq V(x) + V(p^c x).$$

If $x$ is nonzero, then this is a special case of the assertion that for $x, y$ both nonzero in $(\mathbb{Q}/\mathbb{Z})_{\text{prime to } p}$, we have

$$1 + V(x + y) \geq V(x) + V(y).$$

To see this, use again the relation $V(z) = 1 - V(-z)$ for nonzero $z$, and rewrite this as

$$1 + 1 - V(-x-y) \geq 1 - V(-x) + 1 - V(-y),$$

i.e.,

$$V(-x) + V(-y) \geq V(-x-y).$$

That this last inequality holds, in fact for all $x, y$, is one of the fundamental inequalities of Kubert's $V$-function. It trivially holds if any of $x, y$ or $x + y$ vanishes. If they are all nonzero, it reflects the fact that a Jacobi sum is an algebraic integer, so has nonnegative $p$-adic order. □

Equipped with this Lemma 9.1.3, we now give the proof of Theorem 9.1.2.

Proof. We must show that

$$1 + V((p^a+1)(p^b+1)x) \geq V((p^a+1)x) + V((p^b+1)x).$$

We expand the first argument to get

$$1 + V((p^a+1)(p^b+1)x) = 1 + V(p^a(p^b+1)x + (p^b+1)x),$$

which by Lemma 9.1.3, applied with $c = a$, and $x$ there taken to be $(p^b+1)x$, is at least $2V((p^b+1)x)$. Interchanging the two factors $p^a+1$ and $p^b+1$, we get the inequality

$$1 + V((p^a+1)(p^b+1)x) \geq 2V((p^a+1)x).$$

Adding these two inequalities, we get

$$2\big(1 + V((p^a+1)(p^b+1)x)\big) \geq 2\big(V((p^a+1)x) + V((p^b+1)x)\big),$$

which is two times the asserted inequality. □

Proposition 9.1.4. *Let $a, b$ be positive integers such that* $\gcd(2^a+1, 2^b+1) = 1$ *and* $a + b \geq 3$. *Then in characteristic $p = 2$, with $A := 2^a+1$, $B := 2^b+1$, the sheaf $\mathcal{H}(a,b) := \mathcal{H}yp_\psi(A \times B; \mathbb{1})$ is primitive and tensor indecomposable. If $a+b \geq 4$, then $\mathcal{H}$ satisfies* $(\mathbf{S}+)$. *If $a+b = 3$, then $\mathcal{H}$ is either in the almost quasisimple case* (i)(b) *or the extraspecial normalizer case* (i)(c) *of* [**KT5**, Lemma 1.1].

PROOF. First we show that $\mathcal{H}$ is primitive. As $\mathcal{H}$ has only one character downstairs, it is visibly not Kummer induced. Suppose that it is Belyi induced and apply [**KRLT3**, Proposition 1.2]. Again because the tame part $\mathsf{Tame}$ of $\mathcal{H}$ has dimension 1, $\mathcal{H}$ can only be in case (ii)(a) of [**KRLT3**, Proposition 1.2], that is, there are positive odd integers $C, D$ and a multiplicative characters $\Lambda$ such that $C + D = 2^{a+b}$ and the "upstairs" characters of $\mathcal{H}$ are all of the $C^{\rm th}$ roots of $\Lambda$ and all of the $D^{\rm th}$ roots of $\sigma := \Lambda^{-1}$. Now, the given set of "upstairs" characters in $\mathcal{H}$ is stable under complex conjugation, so $C = D$ and thus $C = 2^{a+b-1}$ is even, a contradiction.

Note that $\mathcal{H}$ has finite monodromy by Theorem 9.1.1. Now, if $a + b \geq 4$, then $\mathcal{H}$ has rank $2^{a+b} \geq 16$, and so $\mathcal{H}$ satisfies (**S**+) by Theorem 5.2.9. Consider the case $a + b = 3$. By [**KT5**, Proposition 4.10], the image $J$ of $I(\infty)$ in the geometric monodromy group $G$ of $\mathcal{H}$ acts irreducibly on $\mathsf{Wild}$ of dimension 7. Applying Theorem 1.3.1, we see that $\mathcal{H}$ is tensor indecomposable. Recall by Theorem 9.1.1 that $G$ is finite; in particular, 7 divides $|J|$ and $|G|$. Assume $\mathcal{H}$ is not in the case (b) or (c) of [**KT5**, Lemma 1.1(i)(c)]. By Lemma 1.1.7 (and its proof), $E(G) = L_1 * L_2 * L_3$ is a central product of 3 copies $L_1 \cong \ldots \cong L_n$ of a finite quasisimple group, which are transitively permuted by $G$, and $E(G)$ is irreducible on $\mathcal{H}$ (and in fact $\mathcal{H}$ is 3-tensor induced). By Schur's lemma, $\mathbf{C}_G(E(G)) \leq \mathbf{Z}(G)$, and $\mathbf{Z}(G) \leq C_2$ since $\mathcal{H}$ is self-dual. It follows that 7 divides $|E(G)|$ and $|L_1|$. On the other hand, the only quasisimple group that can have a nontrivial 2-dimensional representation over $\mathbb{C}$ is $\mathrm{SL}_2(5)$ (see e.g. [**HM**]), a contradiction. □

The next key observation is that the sheaf $\mathcal{H}(af, bf) = \mathcal{H}yp_\psi(A \times B; \mathbb{1})$, with $q := 2^f$, $A := q^a + 1$, $B := q^b + 1$, and $\gcd(A, B) = 1$, is the same as the sheaf $\mathrm{Total}(1, A, B)$ considered in [**KT7**, §6], with $M = 1$; it is geometrically isomorphic to the local system whose trace function is given in [**KT7**, Theorem 6.1]: for any finite extension $E$ of $\mathbb{F}_2$, the trace at $t \in E^\times$ is given (recalling that both $A, B$ are odd) by

$$t \mapsto \varphi_E(t) := \frac{1}{\#E} \sum_{x,w \in E} \psi_E\big(xw - t^{-\alpha}x^{q^b+1} - t^\beta w^{q^a+1}\big), \tag{9.1.4.1}$$

for some fixed $\alpha, \beta \in \mathbb{Z}$ such that $\alpha A - \beta B = 1$. (Recall that $\psi$ is the non-principal character of $(\mathbb{F}_2, +)$, and $\psi_E(x) = \psi(\mathrm{Tr}_{E/\mathbb{F}_2}(x))$. By [**KT7**, Theorem 12.1] (and its proof), the $[AB]^\star$ pullback of $\mathrm{Total}(1, A, B)$ admits the trace function

$$t \mapsto \varphi_E^\star(t) := \frac{1}{\#E} \sum_{x,w \in E} \psi_E\big(txw - x^{q^b+1} - w^{q^a+1}\big), \tag{9.1.4.2}$$

Now we describe some integrality properties of the trace function $\varphi_E$, which holds even without the assumption $\gcd(A, B) = 1$. For any finite extension $E$ of $\mathbb{F}_2$, and any $s, t \in E^\times$, we denote by $\varphi_E(s, t)$ the function

$$(s, t) \mapsto \varphi_E(s, t) := \frac{1}{\#E} \sum_{x,w \in E} \psi_E\big(xw - sx^{q^b+1} - tw^{q^a+1}\big). \tag{9.1.4.3}$$

THEOREM 9.1.5. *For any $a, b, f \in \mathbb{Z}_{\geq 1}$, the following statement holds for the function $\varphi_E$ in* (9.1.4.3)*. Let $K$ be a subfield of $\mathbb{F}_q$. If $E \supseteq K$ and $s, t \in E^\times$, then $\varphi_E(s, t)$ is either* 0*, or* $\pm$ *a power of $\#K$.*

Proof. Set

$$F_K(v) := F_K(x,w) := \mathrm{Tr}_{E/K}\big(xw - sx^{q^b+1} - tw^{q^a+1}\big),\ \langle u,v\rangle_K := F_K(u+v) - F_K(u) - F_K(v),$$

$$F(v) := F(x,w) := \mathrm{Tr}_{K/\mathbb{F}_2}\big(F_K(x,w)\big),\ \langle u,v\rangle = \mathrm{Tr}_{K/\mathbb{F}_2}\big(\langle u,v\rangle_K\big),$$

for any $u \in E \times E$ and $v = (x,w) \in E \times E$. As shown in 11.8.2 of the proof of [**KT7**, Theorem 11.8], $|\varphi_E(s,t)|^2$ is either 0, or $\#\mathrm{Null}(E)$, where

$$\mathrm{Null}(E) := \{v \in E \times E \mid \langle u,v\rangle = 0,\ \forall u \in E \times E\};$$

furthermore, $\mathrm{Null}(E)$ is a $K$ vector space, via $\lambda \cdot (x,w) = (\lambda x, \lambda w)$.

Note that $\langle u,v\rangle_K$ is a $K$-bilinear form on $E \times E$; moreover, it is alternating as the characteristic is 2. Set

$$\mathrm{Null}_K(E) := \{v \in E \times E \mid \langle u,v\rangle_K = 0,\ \forall u \in E \times E\}.$$

Clearly, if $v \in \mathrm{Null}_K(E)$ then $v \in \mathrm{Null}(E)$. Conversely, assume that $v \in \mathrm{Null}(E)$. Then for any $\lambda \in K$, $\lambda v \in \mathrm{Null}(E)$. Also, $F_K(\lambda u) = \lambda^2 \cdot F_K(u)$. Hence, for any $u \in E \times E$ we have

$$0 = \langle \lambda u, \lambda v\rangle = \mathrm{Tr}_{K/\mathbb{F}_2}\big(F_K(\lambda(u+v)) - F_K(\lambda u) - F_K(\lambda v)\big) = \mathrm{Tr}_{K/\mathbb{F}_2}\big(\lambda^2 \cdot \langle u,v\rangle_K\big).$$

Since this is true for all $\lambda \in K$, we must have that $\langle u,v\rangle_K = 0$, i.e. $v \in \mathrm{Null}_K(E)$.

We have shown that $\mathrm{Null}(E) = \mathrm{Null}_K(E)$. If $d := [E : K]$, then $\dim_K(E \times E) = 2d$. On the other hand, $\langle u,v\rangle_K$ is a non-degenerate alternating $K$-bilinear form on $(E \times E)/\mathrm{Null}(E)$, so the latter quotient has even dimension $2e$ over $K$, for some $e \in \mathbb{Z}$. Thus $\#\mathrm{Null}(E) = (\#K)^{2(d-e)}$, and so either $\varphi_E(t) = 0$, or $|\varphi_E(t)|^2 = (\#K)^{2(d-e)}$. Since we also know that $\varphi_E(t) \in \mathbb{Z}$, in the latter case we have $\varphi_E(t) = \pm(\#K)^{d-e}$, and the statement follows. □

Before treating the "generic" case $(a+b)f \geq 4$, we analyze the special case $a+b=3$, $q=p=2$. First we recall the following theorem, which is proven but not stated(!) in [**KRLT4**, Theorem 6.5].

Theorem 9.1.6. *Let $\mathcal{F}$ be a lisse $\overline{\mathbb{Q}_\ell}$-sheaf on $\mathbb{G}_m/k$, $k$ a finite field of characteristic $p \neq \ell$, which is pure of weight zero and tame at* 0. *Denote*

$$h^2_c := \dim(H^2_c(\mathbb{G}_m/\overline{k}, \mathcal{F})).$$

*Define the constants*

$$C := \text{dimension of the space of } I(0)\text{-invariants in } \mathcal{F}.$$

$$B := \mathsf{Swan}_\infty(\mathcal{F}) + h^2_c.$$

$$A := B - C.$$

*Then we have the following estimate, for $\mathbb{F}_q/k$ a finite extension.*

$$\left|\frac{1}{q-1}\sum_{u \in \mathbb{F}_q^\times} \mathrm{Trace}(\mathsf{Frob}_{\mathbb{F}_q,u}|\mathcal{F})\right| \leq \frac{q}{q-1}h^2_c + \frac{A\sqrt{q}}{q-1} + \frac{B}{q-1}.$$

Consider the hypergeometric sheaf

$$\mathcal{H} := \mathcal{H}yp(\mathsf{Char}^\times(15), \mathbb{1}) = \mathcal{H}yp_\psi(A \times B; \mathbb{1}), \tag{9.1.6.1}$$

with $A = 2+1$, $B = 2^2+1$.

THEOREM 9.1.7. *The $M_{2,2}$ moment of the sheaf $\mathcal{H}$ defined in* (9.1.6.1) *satisfies* $M_{2,2}(\mathcal{H}) \geq 4$.

PROOF. The hypergeometric sheaf $\mathcal{H}$ is of type $(8,1)$. By [**Ka-ESDE**, 8.8.1-2], $\mathcal{H}$ is (geometrically) orthogonally self-dual. Therefore $M_{2,2}(\mathcal{H}) \geq 3$, with equality if and only if in the natural decomposition

$$\mathcal{H} \otimes \mathcal{H} = (\mathsf{S}^2(\mathcal{H})/\mathbb{1}) \quad \oplus \mathbb{1} \ \oplus \ \wedge^2(\mathcal{H})$$

each of these constituents, of ranks $35, 1, 28$ respectively, is geometrically irreducible.

To show that $M_{2,2}(\mathcal{H}) \geq 4$, we will show that the rank 7 Kloosterman sheaf

$$\mathcal{K}l := \mathcal{K}l_\psi(\mathsf{Char}^\times(3) \cup \mathsf{Char}(5))$$

is a constituent of $\mathcal{H} \otimes \mathcal{H}$. By [**Ka-ESDE**, 8.8.1-2], $\mathcal{K}l$ is (geometrically) orthogonally self-dual. Because both $\mathcal{K}l$ and $\mathcal{H}$ are pure, each is geometrically semisimple, cf. [**De2**, 3.4.1(iii)]. Thus it is equivalent to show that

$$\mathrm{Hom}_{\pi_1^{\mathrm{geom}}}(\mathcal{K}l, \mathcal{H} \otimes \mathcal{H}) = H^2_c(\mathbb{G}_m/\overline{\mathbb{F}_2}, \mathcal{H} \otimes \mathcal{H} \otimes \mathcal{K}l)$$

is nonzero.

The question is geometric, so we may replace $\mathcal{H}$ by the lisse sheaf $\mathcal{H}_0$ on $\mathbb{G}_m/\mathbb{F}_2$ which is pure of weight zero and whose trace function is given at points $t \in E^\times$ for $E/\mathbb{F}_2$ a finite extension by (9.1.4.1) in the special case $q = 2, a = 1, b = 2, A = 3, B = 5, (\alpha, \beta) = (2, 1)$. Thus the trace function of $\mathcal{H}_0$ is

$$t \mapsto \varphi_E(t) := \frac{1}{\#E} \sum_{x,w \in E} \psi_E\big(xw - t^{-2}x^5 - tw^3\big), \tag{9.1.7.1}$$

Similarly, we may replace $\mathcal{K}l$ by the pure of weight zero Pink-Sawin sheaf $\mathcal{K}l_0$ on $\mathbb{G}_m/\mathbb{F}_2$, cf. [**KRLT3**, 1.2] which is

$$\mathcal{K}l_0 := f_\star(\overline{\mathbb{Q}_\ell})/\overline{\mathbb{Q}_\ell} \ \text{ for } f : x \mapsto x^3(x-1)^5.$$

Its trace function is given, at points $t \in E^\times$ for $E/\mathbb{F}_2$ a finite extension by

$$t \mapsto -1 + \#\{x \in E | x^3(x-1)^5 = t\}.$$

With these explicit formulas for the trace functions of $\mathcal{H}_0$ and for $\mathcal{K}l_0$, we thus have explicit formulas for the trace function of the sheaf

$$\mathcal{F} := \mathcal{H}_0 \otimes \mathcal{H}_0 \otimes \mathcal{K}l_0,$$

which is lisse of rank $8^2 7 = 448$ and pure of weight zero on $\mathbb{G}_m/\mathbb{F}_2$. A calculation in Magma gives

$$\sum_{t \in \mathbb{F}^\times_{2^{12}}} \mathrm{Trace}(\mathsf{Frob}_{\mathbb{F}_{2^{12}},t} | \mathcal{F}) = 4286. \tag{9.1.7.2}$$

We now apply Theorem 9.1.6 to $\mathcal{F}$, with $q = 2^{12}$. The sheaf $\mathcal{H}$ is of type $(8,1)$, so its nonzero $\infty$-slopes are all $1/7$. The sheaf $\mathcal{K}l$ is Kloosterman of rank 7, so all of its $\infty$-slopes are $1/7$. Therefore $\mathcal{F}$ has all its $\infty$-slopes $\leq 1/7$, and hence

$$\mathsf{Swan}_\infty(\mathcal{F}) \leq 64.$$

In terms of a character $\chi$ ot $I(0)$ of order 15, the character of the $I(0)$-representation of $\mathcal{H}$ is

$$\chi + \chi^2 + \chi^4 + \chi^7 + \chi^8 + \chi^{11} + \chi^{13} + \chi^{14},$$

and the character of the $I(0)$-representation of $\mathcal{K}l$ is

$$\chi^5 + \chi^{10} + \chi^3 + \chi^6 + \chi^9 + \chi^{12} + \chi^0.$$

Each of these $I(0)$-representations is semisimple, because each is the sum of pairwise distinct linear characters. Checking in Mathematica, by the command,

$\texttt{PolynomialMod}([x+x^2+x^4+x^7+x^8+x^{11}+x^{13}+x^{14})^2*(x^5+x^{10}+x^3+x^6+x^9+x^{12}+1), x^{15}-1]$,

one finds that

$$40 = \text{dimension of the space of } I(0)\text{-invariants in } \mathcal{F}.$$

We now argue by contradiction. Suppose that $h_c^2 = 0$, i.e., that $\mathcal{K}l$ is not a constituent of $\mathcal{H} \otimes \mathcal{H}$. Then in Theorem 9.1.6, we have $C = 40$, $B \leq 64$, $A \leq 24$, and hence, over the field $\mathbb{F}_{2^{12}}$, we have the estimate

$$\Big|\frac{1}{4095} \sum_{t \in \mathbb{F}_{2^{12}}^\times} \mathrm{Trace}(\mathsf{Frob}_{\mathbb{F}_{2^{12}},t}|\mathcal{F})\Big| \leq \frac{24 \cdot 64}{4095} + \frac{64}{4095} = 0.39072 < 1.$$

But this sum of traces is 4286 by (9.1.7.2), and $4286/4095 > 1$, the desired contradiction.

In fact, a faster calculation in Magma over the field of $2^{10}$ elements shows that

$$\sum_{t \in \mathbb{F}_{2^{10}}^\times} \mathrm{Trace}(\mathsf{Frob}_{\mathbb{F}_{2^{10}},t}|\mathcal{F}) = 1099.$$

By Theorem 9.1.6 if $h_c^2$ were zero, we would have the estimate

$$\Big|\frac{1}{1023} \sum_{t \in \mathbb{F}_{2^{10}}^\times} \mathrm{Trace}(\mathsf{Frob}_{\mathbb{F}_{2^{10}},t}|\mathcal{F})\Big| \leq \frac{24 \cdot 32}{1023} + \frac{64}{1023} = 0.813294 < 1.$$

But $1099/1023 > 1$, again giving the desired contradiction. □

THEOREM 9.1.8. *Over any finite extension $k/\mathbb{F}_2$, the local system $\mathcal{H}_0$ defined in* (9.1.7.1) *has*

$$G_{\mathrm{geom}} = G_{\mathrm{arith},k} = 2\mathsf{A}_8.$$

PROOF. As mentioned in the proof of Theorem 9.1.7, $\mathcal{H}_0$ is orthogonally self-dual; furthermore, the character $\varphi$ of the corresponding representation of $H := G_{\mathrm{arith},\mathbb{F}_2}$ takes integer values by (9.1.4.1), in particular,

$$\mathbf{Z}(G) \leq \mathbf{Z}(H) \leq C_2$$

for $G := G_{\mathrm{geom}}$. Since $\mathcal{H}$ is of type $(8,1)$ in characteristic 2, the wild part has dimension 7, and so $G$ contains elements $g_\infty$ of order 7, as well as $g_0$ of order 15 (because of the "upstairs" characters). Now we can apply Proposition 9.1.4 to $G$ and $H$.

First we consider the extraspecial normalizer case: $G = EX$, with $E = 2_+^{1+6}$ and $X \leq \mathrm{O}_6^+(2) \cong \mathsf{S}_8$. In fact $X \leq \mathsf{A}_8$ as $G = \mathbf{O}^{2'}(G)$ by [**KT5**, Theorem 4.1]. The existence of $g_\infty$ and $g_0$ implies (using [**CCNPW**]) that $X = \mathsf{A}_8$. But in this case it is easy to check (see also [**GT2**, Theorem 1.5]) that $M_{2,2} = 3$, contradicting Theorem 9.1.7.

Hence we are in the almost quasisimple case: $S \lhd G/\mathbf{Z}(G) \leq H/\mathbf{Z}(H) \leq \mathrm{Aut}(H)$, with $E(G) = E(H)$ acting irreducibly on $\mathcal{H}$. Again using the aforementioned information on $\varphi$, $\mathbf{Z}(H)$, and $g_0$, $g_\infty$, and inspecting the list of linear groups in dimension 8 [**HM**], we see that

$$E(G) \in \{2\mathsf{A}_8, \mathsf{A}_9, 2\mathsf{A}_9, 2\Omega_8^+(2)\}.$$

The last two cases $E(G) = 2\mathsf{A}_9$ and $2\Omega_8^+(2)$ are ruled out by Theorem 9.1.7. In the case $E(G) = \mathsf{A}_9$, $\varphi|_{E(G)}$ would be the character of the deleted permutation module and hence take value 5 on a 3-cycle, which violates Theorem 9.1.5.

This leaves only the possibility $E(G) = 2\mathsf{A}_8$, and hence $2\mathsf{A}_8 \leq G \leq H \leq 2\mathsf{S}_8$. Since $G = \mathbf{O}^{2'}(G)$, we must have that $G = 2\mathsf{A}_8$. Now, if $H \neq G$, then $H = 2\mathsf{S}_8$ (the one in which 2-cycles lift to elements of order 4), and $\mathsf{Frob}_{\mathbb{F}_2,1}$ must be in $H \smallsetminus G$. However, direct calculation of the traces on $\mathcal{H}_0$ of the first eight powers of $\mathsf{Frob}_{\mathbb{F}_2,1}$, i.e. the traces of $\mathsf{Frob}_{\mathbb{F}_{2^n},1}$ for $n \leq 8$, shows that its eigenvalues are the primitive 30th roots of unity, Hence $\mathsf{Frob}_{\mathbb{F}_2,1}$ has order 30, and any such element in $2\mathsf{S}_8$ lies in $2\mathsf{A}_8$. Therefore $H = 2\mathsf{A}_8$, as stated. □

PROPOSITION 9.1.9. *Let $a, b$ be positive integers such that* $\gcd(2^a+1, 2^b+1) = 1$ *and* $a+b \geq 4$. *Then in characteristic $p = 2$, with $A := 2^a+1$, $B := 2^b+1$, the sheaf $\mathcal{H}(a,b) := \mathcal{H}yp_\psi(A \times B; \mathbb{1})$ is in the extraspecial normalizer case* (i)(c) *of* [**KT5**, Lemma 1.1]. *In fact, $G \rhd E$ with $E \cong 2_+^{1+2(a+b)}$ acting irreducibly.*

PROOF. By Proposition 9.1.4, the (finite) geometric monodromy group $G$ of $\mathcal{H}(a,b)$ satisfies (**S**+) and is either in case (i)(b) or case (i)(c) of [**KT5**, Lemma 1.1]. Suppose we are in the former case: $G$ is almost quasisimple with $S$ the unique non-abelian composition factor. Let $g_0$ be a generator of the image of $I(0)$ in $G$. By Proposition 2.4.3(i), $g_0$ has simple spectrum on the underlying representation $V$ of $G$, and thus $G$ satisfies the hypothesis $(\star)$ of [**KT5**, §6]. Hence we can apply the classification results of [**KT5**, §6] to determine $S$ and $E(G)$, which is also irreducible on $V$ by [**KT5**, Lemma 1.4].

Note that

$$\dim(V) = 2^{a+b} \geq 16 \tag{9.1.9.1}$$

and

$$\bar{\mathsf{o}}(g_0) = (2^a+1)(2^b+1). \tag{9.1.9.2}$$

Hence $S$ is not a sporadic group or $\mathsf{A}_7$ by [**KT5**, Theorem 6.4]. Suppose $S = \mathsf{A}_n$ with $n \neq 7$. Using [**GAP**] we can check that in fact $n \geq 8$. Hence [**KT5**, Theorem 6.2] applies and implies from (9.1.9.1) that $n = 2^{a+b}+1$, and $\bar{\mathsf{o}}(g_0) = n$ or $k(n-k)$ with $1 \leq k \leq n-1$, whence $\bar{\mathsf{o}}g_0 \leq n$ or $\bar{\mathsf{o}}(g_0) \geq 2(n-2)$. On the other hand, $a+b \geq 4$ implies that $(2^a-1)(2^b-1) \geq 7$, and so $n < \bar{\mathsf{o}}(g_0) < 2(n-2)$ by (9.1.9.2), a contradiction.

We conclude that $S$ is a finite simple group of Lie type in characteristic $r$. Applying Theorem 3.1.10, we get $r = 2$. Next we can apply Theorem 3.1.5 to deduce from (9.1.9.1) that $S = \mathrm{SL}_2(q)$ with $q = 2^{a+b}$ and $\bar{\mathsf{o}}(g_0) \leq q+1$. The latter however contradicts (9.1.9.2).

Hence we are in the extraspecial normalizer case. Since the sheaf is orthogonally self-dual of rank $2^{a+b}$, we are done by [**KT5**, Theorem 9.19]. □

LEMMA 9.1.10. *Let $r \in \{3,5,7,11,13\}$ and suppose that $r \nmid abf$. If $r \neq 5$, then the trace function $\varphi^\star_E$ in* (9.1.4.2) *attains the value* 2 *or* $-2$ *for $E = \mathbb{F}_{2^r}$. If $r = 5$ and $E = \mathbb{F}_2^5$, then $\varphi^\star_E$*

*attains the value* $2$ *or* $-2$ *when* $abf^2 \equiv \pm 1 (\mathrm{mod}\ 5)$*, and it attains the value* $4$ *or* $-4$ *when* $abf^2 \equiv \pm 2 (\mathrm{mod}\ 5)$*.*

Proof. Note that when $x \in E$ and $af \equiv e(\bmod\ r)$ we have $x^{1+2^{af}} = x^{1+2^e}$; furthermore,

$$\psi_E\big(x^{1+2^{af}}\big) = \psi_E\big(x^{1+2^e}\big) = \psi_E\big((x^{1+2^e})^{2^{r-e}}\big) = \psi_E\big(x^{1+2^{r-e}}\big).$$

Hence, when we compute $\varphi_E^\star$ we can replace $af$ by $e'$ with $1 \leq e' \leq (r-1)/2$ and $af \equiv \pm e' (\mathrm{mod}\ r)$, and similarly for $b$. The computation is then done using Magma. □

Theorem 9.1.11. *Let* $a, b, f$ *be positive integers such that* $\gcd(a,b) = 1$*,* $2|ab$*, and* $(a+b)f \geq 4$*. Then in characteristic* $p = 2$*, with* $A := 2^{af}+1$*,* $B := 2^{bf}+1$*, the following statements hold for the sheaf* $\mathcal{H} := \mathcal{H}yp_\psi(A \times B; \mathbb{1})$*.*

(i) $\mathcal{H}$ *has geometric monodromy group* $G \cong 2^{1+2nf}_+ \cdot \Omega^+_{2n}(q)$*, with* $n := a+b$ *and* $q := 2^f$*.*
(ii) *The arithmetic monodromy group* $G_{\mathrm{arith},k}$ *of the sheaf* $\mathcal{H}_0 := \mathcal{H}((A-1)(B-1)/2)$ *over any finite extension* $k \supseteq \mathbb{F}_q$ *is equal to* $G$*.*
(iii) *Suppose that some Frobenius has trace* $\pm 2$*, or that* $2 \nmid f$ *and some Frobenius has trace* $\pm 4$ *on* $\mathcal{H}_0$*. Then for any subfield* $k \subseteq \mathbb{F}_q$ *we have* $G_{\mathrm{arith},k} \cong G \cdot \mathrm{Gal}(\mathbb{F}_q/k)$*.*
(iv) *Suppose that* $f = 1$*, or that* $abf$ *is coprime to some* $r \in \{3, 7, 11, 13\}$*, or that* $2 \nmid f$ *and* $abf$ *is coprime to* $5$*. Then for any subfield* $k \subseteq \mathbb{F}_q$ *we have* $G_{\mathrm{arith},k} \cong G \cdot \mathrm{Gal}(\mathbb{F}_q/k)$*.*

Proof. (a) By Proposition 9.1.9, $G$ is finite and in fact in the extraspecial normalizer case: $G \rhd E$ with $E = 2^{1+2nf}_+$ that acts irreducibly on the underlying representation $V$. It follows that

$$E \lhd G \leq \mathbf{N}_{\mathrm{O}(V)}(E) \cong E \cdot \mathrm{O}(\mathsf{Q}) \cong E \cdot \mathrm{O}^+_{2nf}(2),$$

see [**NRS**, §2], where $\mathsf{Q}(x\mathbf{Z}(E)) = x^2$ is the quadratic form on $W := E/\mathbf{Z}(E) \cong \mathbb{F}_2^{2nf}$. Thus $G/E \hookrightarrow \mathrm{O}(W)$. The definition of $\mathcal{H}$ tells us that a generator $g_0$ of the image of $I(0)$ in $G$ has simple spectrum

$$\{\alpha\beta \mid 1 \neq \alpha \in \mu_A,\ 1 \neq \beta \in \mu_B\}$$

on $V$. As shown in [**KT5**, Theorem 8.5] (whose proof uses Theorem 8.2.1 and Lemma 8.2.2), the coset $g_0E$ can be identified with a generator $\bar{g}_0$ of a maximal torus $C_{2^{af}+1} \times C_{2^{bf}+1}$ of $\Omega(W)$.

Next, some power $g'$ of a generator $g_\infty$ of the image of $I(\infty)$ modulo the image of $P(\infty)$ in $G$ has spectrum $\mu_{2^{(a+b)f}-1}$ on the wild part Wild and eigenvalue 1 on the tame part Tame. Hence, $\mathsf{o}(g') = 2^{nf}-1$ and $\varphi(g') = 1$, if $\varphi$ denotes the character of $G$ on $V$. It follows from Lemma 7.2.1 that $\mathbf{C}_W(\bar{g}') = 0$, if $\bar{g}'$ denotes the coset $g'E$. Now we can apply Theorem 8.3.6 to $\bar{G} := G/E$ to see that $L := \bar{G}^{(\infty)}$ is $\Omega(W_j) \cong \Omega^+_{2nf/j}(2^j)$ for some

$$j|nf, \text{ and } j \leq nf/2. \tag{9.1.11.1}$$

(b) We will now show that $j = f$ and $\bar{G} = \Omega(W_f)$, so that $G = 2^{1+2nf}_+ \cdot \Omega^+_{2n}(q)$.

First, $\Omega(W_j) = \Omega^+_{2nf/j}(2^j)$ contains an element $\bar{h}$ with a 2-dimensional fixed point subspace on $W_j$, and hence $|\mathbf{C}_W(\bar{h})| = 2^{2j}$. By Lemma 7.2.1, the coset $\bar{h}$ in $G/E$ contains an element $h$ with $|\varphi(h)| = 2^j$. Applying Theorem 9.1.5, we see that $2^j$ is a power of $q = 2^f$, and thus

$$f|j. \tag{9.1.11.2}$$

Recall that $a > b \geq 1$. Consider the case $af = 3$. Then $(a, b, f) = (3, 2, 1)$ and $n = 5$, in which case (9.1.11.1) implies that $j = 1 = f$. It follows that $\Omega^+_{10}(2) \lhd \bar{G} \leq \mathrm{O}(W) = \mathrm{O}^+_{10}(2)$. Since $[\mathrm{O}(W) : \Omega(W)] = 2$ and $G = \mathbf{O}^2(G)$ by [**KT5**, Theorem 4.1], we have $G = E \cdot \Omega(W)$ as stated.

Assume now that $af \neq 3$, in which case one can find a primitive prime divisor $\ell_1 = \mathrm{ppd}(2, 2af)$, which divides $\bar{\mathsf{o}}(g_0)$. Then $\ell_1 > 2af \geq 4$ and $2af > nf$, so $\ell_1 \nmid (2^j - 1)$. As $L$ acts absolutely irreducibly on $W_j$, $|\mathrm{End}_L(W)| = 2^j$ by Lemma 8.3.2(ii), and so $\mathbf{C}_{\bar{G}}(L) \hookrightarrow C_{2^j-1}$. It follows that $\ell_1$ divides $|\bar{G}/\mathbf{C}_{\bar{G}}(L)|$ and $|\mathrm{Aut}(L)| = |\mathrm{Aut}(\Omega^+_{2nf/j}(2^j))|$, which in turn implies the existence of some $1 \leq i \leq nf/j$ such that $\ell_1 | (2^{2ij} - 1)$. The primitivity of $\ell_1$ now shows that $af | ij$. Since $ij \leq nf < 2af$, we must have that $af = ij$, and $bf = (a+b)f - af = nf - ij$. Since $j | nf$ by (9.1.11.1) and $\gcd(a, b) = 1$, it follows that $j$ divides $\gcd(af, bf) = f$. Using (9.1.11.2), we can now deduce that $j = f$ and thus $L = \Omega^+_{2n}(q)$.

As $n = a + b \geq 3$ is odd, $\mathrm{Aut}(L) = \mathrm{O}^+_{2n}(q) \cdot C_f$ (see [**KlL**, Table 5.1.A]), and this group certainly embeds in $\mathrm{O}(W)$. We claim that

$$\mathbf{C}_{\mathrm{O}(W)}(L) = 1.$$

Indeed, Lemma 8.3.2 shows that $\mathrm{End}_L(W)$ consists of the scalar maps on $W_f$. On the other hand, the form $\mathsf{Q}_f$ on $W_f$ links to the form $\mathsf{Q}$ on $W$ via $\mathsf{Q}(v) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\alpha \cdot \mathsf{Q}_f(v))$ for some $\alpha \in \mathbb{F}_q^\times$. Suppose that the map $v \mapsto \lambda v$ belongs to $\mathbf{C}_{\mathrm{O}(W)}(L)$ for some $\lambda \in \mathbb{F}_q^\times$. Then for all $v \in W_f$ we have

$$\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\alpha \cdot \mathsf{Q}_f(v)) = \mathsf{Q}(v) = \mathsf{Q}(\lambda v) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\alpha \cdot \mathsf{Q}_f(\lambda v)) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\alpha\lambda^2 \cdot \mathsf{Q}_f(v)).$$

Since $n \geq 3$, $\mathsf{Q}_f$ takes all values in $\mathbb{F}_q$. Hence the previous equality implies that $\lambda = 1$, and the claim follows. We have therefore shown that

$$\Omega^+_{2n}(q) = L \lhd \bar{G} \leq \mathrm{O}^+_{2n}(q) \cdot C_f. \tag{9.1.11.3}$$

As mentioned above, $\bar{g}_0 = \mathrm{diag}(\bar{g}_1, \bar{g}_2)$ is a generator of a cyclic torus $C_{q^a+1} \times C_{q^b+1} < \Omega(W)$. We may assume that $\bar{g}_1$ generates the $C_{q^a+1}$ factor of a maximal torus $T \cong C_{q^a+1} \times C_{q^b+1} < L$. Now $\bar{g}_0$ belongs to

$$\mathbf{C}_{\mathrm{O}^+_{2n}(q) \cdot C_f}(C_{q^a+1}) = C_{q^a+1} \times \mathrm{O}^-_{2b}(q) < \mathrm{O}^+_{2n}(q)$$

(since $C_f$ acts on $C_{q^a+1}$ via field automorphisms), whence $\bar{g}_0 \in \mathrm{O}^+_{2n}(q)$. In fact, as $\mathsf{o}(g_0)$ is odd, $\bar{g}_0 \in L$. Again using $G = \mathbf{O}^2(G)$, we conclude that $G = E \cdot \Omega(W_f)$.

(e) The rest of the proof is to deal with the arithmetic monodromy group $H := G_{\mathrm{arith}, \mathbb{F}_2}$ of $\mathcal{H}_0$. Clearly, $H$ normalizes $G = E \cdot L$ and $E = \mathbf{O}_2(G)$. Since the underlying representation $V$ is orthogonal, we now have

$$E \lhd H \leq \mathbf{N}_{\mathrm{O}(V)}(E) \cong E \cdot \mathrm{O}(\mathsf{Q}) \cong E \cdot \mathrm{O}^+_{2nf}(2).$$

The proof of (9.1.11.3), together with Proposition 8.2.4, then shows that

$$\Omega^+_{2n}(q) = L \lhd H/E \leq A \cong \mathrm{O}^+_{2n}(q) \cdot C_f. \tag{9.1.11.4}$$

Here, $A/L \cong C_{2f}$ if $2 \nmid f$ and $A/L \cong C_2 \times C_f$ if $2 | f$.

Suppose $2|f$. Then $\exp(A/L) = f$, so $h^f \in G$ for any $h \in H$. As $H = \langle G, \mathsf{Frob}_{\mathbb{F}_2,1} \rangle$, it follows that $\mathsf{Frob}_{\mathbb{F}_{2^f},1} = \mathsf{Frob}^f_{\mathbb{F}_2,1} \in G$. Since $G_{\mathrm{arith}, \mathbb{F}_q} = \langle G, \mathsf{Frob}_{\mathbb{F}_{2^f},1} \rangle$, we conclude that $G_{\mathrm{arith}, \mathbb{F}_q} = G$. We have also shown that $|H/G|$ divides $f$.

(f) Here we consider the case $f$ is odd.

Suppose $H/G$ has even order. As $A \cong C_{2f}$, it follows from (9.1.11.4) that $H/G \cong (H/E)/L$ contains the central involution of $A/L$, and hence $H \geq E \cdot \mathrm{O}^+_{2n}(q)$. Thus $H/E$ contains a reflection $\boldsymbol{\rho}$ of $\mathrm{O}(W_f)$, which has a fixed point subspace of size $q = 2^f$ on $W$. Lemma 7.2.1 applied to $\boldsymbol{\rho}$ then yields an element $\boldsymbol{\rho}_1 \in H$ with $|\varphi(\boldsymbol{\rho}_1)| = 2^{f/2}$, where $\varphi$ is the character of $V$. But this means $\varphi(\boldsymbol{\rho}_1) \notin \mathbb{Z}$, contrary to Theorem 9.1.5.

We have shown that $H/G$ has odd order, and hence $H/G \hookrightarrow C_f$. So we again have $h^f \in G$ for all $h \in G$. The final argument in (e) can be repeated to show that $G_{\mathrm{arith},\mathbb{F}_q} = G$. In particular, we are done if $f = 1$.

By Lemma 9.1.10, we may now assume that $|\varphi(h_0)| \in \{2, 4\}$ for some $h_0 \in H$, and need to show that $e := |H/G|$ equals to $f$. Part (b) of the proof of Proposition 8.2.4 shows that $H/G = \langle \sigma^{f/e} \rangle$, with $\sigma$ defined in (8.2.4.2). The fixed point subspace of $\sigma^{f/e}$ acting on $W$ has size $2^{2nf/e}$, of even dimension over $\mathbb{F}_{2^{f/e}}$. It follows that $H/E = \langle L, \sigma^{f/e} \rangle \leq \Omega^+_{2ne}(2^{f/e})$. In particular, the fixed point subspace of any element $h \in H$ while acting on $W$ has even dimension over $\mathbb{F}_{2^{f/e}}$. This implies by Lemma 7.2.1 that $|\varphi(h)|$ is a power of $2^{f/e}$. Applying this to $h_0$, we see that $e = f$, as desired.

(g) Finally we complete the case $2|f$. By Lemma 9.1.10, we may assume that

$$|\varphi(h_0)| = 2 \tag{9.1.11.5}$$

for some $h_0 \in H$, and need to show that $e := |H/G|$ equals to $f$. As shown in (e), $e|f$. Assume the contrary that $e < f$; in particular $e \leq f/2$.

Recall from the proof of Proposition 8.2.4 that $H/G \leq A/L = \langle \boldsymbol{j}, \sigma \rangle \cong C_2 \times C_f$, with $\sigma$ defined in (8.2.4.2) and $\boldsymbol{j}$ defined in (8.2.4.2). Now if $H/G \leq \langle \sigma \rangle$, then $H/G = \langle \sigma^{f/e} \rangle$, and the last paragraph of (f) shows that $|\varphi(h)|$ is a power of $2^{f/e}$ for any $h \in H$. But this contradicts (9.1.11.5).

Hence $H/G = \langle \boldsymbol{j}\sigma^k \rangle$ for some $k \in \mathbb{Z}$. As $\boldsymbol{j}\sigma^k$ has order $e$, we must have that $2|e$ and $f|(ke)$, i.e.

$$2|e,\ e|f,\ e \leq \frac{f}{2},\ \frac{f}{e} \text{ divides } k. \tag{9.1.11.6}$$

Note that

$$\boldsymbol{j} \in \mathrm{O}^+_{2n}(q) = \mathrm{O}^+_{2n}(2^f) < \Omega^+_{4n}(2^{f/2}) \leq \Omega^+_{2ne}(2^{f/e}).$$

Furthermore, $\sigma^{f/e}$ is $\mathbb{F}_{2^{f/e}}$-linear, and $|\mathbf{C}_W(\sigma^{f/e})| = 2^{2f/e}$, so $\sigma^{f/e} \in \Omega^+_{2ne}(2^{f/e})$. Using (9.1.11.6) we then have that $\sigma^k \in \Omega^+_{2ne}(2^{f/e})$, and so

$$\boldsymbol{j}\sigma^k \in \Omega^+_{2ne}(2^{f/e}) \geq \Omega^+_{2n}(q).$$

It follows that the fixed point subspace of any element $h \in H$ while acting on $W$ has even dimension over $\mathbb{F}_{2^{f/e}}$. Again, this implies by Lemma 7.2.1 that $|\varphi(h)|$ is a power of $2^{f/e}$ for any $h \in H$. But this contradicts (9.1.11.5) since $e \leq f/2$. □

The Pink–Sawin sheaf $\mathcal{K}l(\mathsf{Char}_{\mathrm{ntriv}}(p^n + 1))$, and the local systems in Theorem 8.5.5 and Theorem 9.1.11 are hypergeometric sheaves in characteristic $p$ with finite monodromy groups which are extraspecial $p$-normalizers. The converse of this statement is settled in [**Y**].

## 9.2. Local systems in characteristic 2 with Witt vectors: The $\mathbb{F}_2$ story

Fix a primitive 4th root of unity $i \in \mathbb{C}$. Given an integer $n \geq 2$ and a list of odd integers

$$A_1 > A_2 > \ldots > A_n \geq 1,$$

we consider the local system

$$\mathcal{G}^\sharp(A_1, \ldots, A_n) \tag{9.2.0.1}$$

on $\mathbb{G}_m \times \mathbb{A}^{n-1}/\mathbb{F}_2$ of rank $A_1 - 1$ whose trace function is given as follows: for $k/\mathbb{F}_2$ a finite extension, and $(t_1, \ldots, t_n) \in k^\times \times k^{n-1}$,

$$\mathrm{Trace}\big(\mathsf{Frob}_{(t_1,\ldots,t_n),k}|\mathcal{G}^\sharp(A_1, \ldots, A_n)\big) = \frac{-1}{(1+i)^{\deg(k/\mathbb{F}_2)}} \sum_{x \in k} \psi_k(t_1^{A_1}x^{A_1} + \sum_{j=2}^{n} t_j x^{A_j}).$$

[Up to the half Tate twist, this is the trace function of $R^1 f_! \mathcal{L}_{\psi(t_1^{A_1}x^{A_1} + \sum_{j=2}^n t_j x^{A_j})}$ for $f$ the projection $(x, t_1, \ldots, t_n) \mapsto (t_1, \ldots, t_n)$.] We also consider the local system

$$\mathcal{G}(A_1, \ldots, A_n) \tag{9.2.0.2}$$

on $\mathbb{A}^{n-1}/\mathbb{F}_2$ of rank $A_1 - 1$ whose trace function is given as follows: for $k/\mathbb{F}_2$ a finite extension, and $(t_2, \ldots, t_n) \in k^{n-1}$,

$$\mathrm{Trace}\big(\mathsf{Frob}_{(t_2,\ldots,t_n),k}|\mathcal{G}(A_1, \ldots, A_n)\big) = \frac{-1}{(1+i)^{\deg(k/\mathbb{F}_2)}} \sum_{x \in k} \psi_k(x^{A_1} + \sum_{j=2}^{n} t_j x^{A_j}). \tag{9.2.0.3}$$

By means of the change of variables $(x, t_1, \ldots, t_n) \mapsto (x/t_1, 1, t_2/t_1^{A_2}, \ldots, t_n/t_1^{A_n})$, we see that the local system $\mathcal{G}^\sharp(A_1, \ldots, A_n)$ on $\mathbb{G}_m \times \mathbb{A}^{n-1}/\mathbb{F}_2$ is isomorphic to the pullback, by

$$\mathrm{pr}_2 : \mathbb{G}_m \times \mathbb{A}^{n-1} \to \mathbb{A}^{n-1}, \quad (t_1, \ldots, t_n) \mapsto (t_2, \ldots, t_n),$$

of the local system $\mathcal{G}(A_1, \ldots, A_n)$ on $\mathbb{A}^{n-1}/\mathbb{F}_2$. In other words, $\mathcal{G}^\sharp(A_1, \ldots, A_n)$ on $\mathbb{G}_m \times \mathbb{A}^{n-1}/\mathbb{F}_2$ is the external tensor product of the constant sheaf $\overline{\mathbb{Q}_\ell}$ on $\mathbb{G}_m/\mathbb{F}_2$ with the local system $\mathcal{G}(A_1, \ldots, A_n)$ on $\mathbb{A}^{n-1}/\mathbb{F}_2$. In particular, the two local systems

$$\mathcal{G}^\sharp(A_1, \ldots, A_n) \text{ and } \mathcal{G}(A_1, \ldots, A_n)$$

have the same $G_{\mathrm{arith}}$ as each other, and the same $G_{\mathrm{geom}}$ as each other.

We next consider some local systems built out of *Witt vectors* of length 2 in characteristic 2 and the aforementioned local systems $\mathcal{G}(A_1, \ldots, A_n)$ and $\mathcal{G}^\sharp(A_1, \ldots, A_n)$.

We fix the isomorphism $W_2(\mathbb{F}_2) \cong \mathbb{Z}/4\mathbb{Z}$ given by the map

$$[a, b] \mapsto a^2 + 2b \pmod 4,$$

and denote by $\psi_2$ the additive character of $W_2(\mathbb{F}_2)$ given by $n \mapsto i^n$. For $k/\mathbb{F}_2$ a finite extension, we denote by $\psi_{2,k}$ the additive character of $W_2(k)$ given by composition with

$$\mathrm{Trace}_{k/\mathbb{F}_2} : W_2(k) \to W_2(\mathbb{F}_2).$$

The first is the local system

$$\mathcal{W}(A_1, \ldots, A_n) \tag{9.2.0.4}$$

of rank $A_1 - 1$ on $\mathbb{A}^n/\mathbb{F}_2$, with coordinates $(s, t_2, \ldots, t_n)$, whose trace function is given as follows. For $k/\mathbb{F}_2$ a finite extension, and $(s, t_2, \ldots, t_n) \in k^n$,

$$\mathrm{Trace}\big(\mathsf{Frob}_{(s,t_2,\ldots,t_n),k}|\mathcal{W}(A_1,\ldots,A_n)\big) = \frac{-1}{(1+i)^{\deg(k/\mathbb{F}_2)}} \sum_{x\in k} \psi_{2,k}([sx, x^{A_1} + \sum_{j=2}^{n} t_j x^{A_j}]).$$

The second is the local system

$$(9.2.0.5) \qquad \mathcal{W}^\sharp(A_1,\ldots,A_n)$$

of rank $A_1 - 1$ on $\mathbb{G}_m \times \mathbb{A}^{n-1}/\mathbb{F}_2$ whose trace function is given as follows: for $k/\mathbb{F}_2$ a finite extension, and $(t_1, \ldots, t_n) \in k^\times \times k^{n-1}$,

$$\mathrm{Trace}\big(\mathsf{Frob}_{(t_1,\ldots,t_n),k}|\mathcal{W}^\sharp(A_1,\ldots,A_n)\big) = \frac{-1}{(1+i)^{\deg(k/\mathbb{F}_2)}} \sum_{x\in k} \psi_{2,k}([x, t_1^{A_1} x^{A_1} + \sum_{j=2}^{n} t_j x^{A_j}]).$$

The third is the local system

$$(9.2.0.6) \qquad \mathcal{W}_0^\sharp(A_1,\ldots,A_n)$$

of rank $A_1 - 1$ on $\mathbb{A}^{n-1}/\mathbb{F}_2$ whose trace function is given as follows: for $k/\mathbb{F}_2$ a finite extension, and $(t_2, \ldots, t_n) \in k^{n-1}$,

$$\mathrm{Trace}\big(\mathsf{Frob}_{(t_2,\ldots,t_n),k}|\mathcal{W}_0^\sharp(A_1,\ldots,A_n)\big) = \frac{-1}{(1+i)^{\deg(k/\mathbb{F}_2)}} \sum_{x\in k} \psi_{2,k}([x, x^{A_1} + \sum_{j=2}^{n} t_j x^{A_j}]).$$

Thus $\mathcal{W}_0^\sharp$ is lisse on $\mathbb{A}^{n-1}$, obtained from $\mathcal{W}$ by pullback to $s = 1$, or obtained from $\mathcal{W}^\sharp$ by pullback to $t_1 = 1$.

LEMMA 9.2.1. *Let $k/\mathbb{F}_2$ be a finite extension, $f(x) \in k[x]$ a polynomial of odd degree $A \geq 3$, $B$ an odd integer with $1 \leq B < A$. Consider the local system $\mathcal{T}(f, B)$ of rank $A - 1$ on $\mathbb{A}^1/k$ whose trace function is given as follows: for $L/k$ a finite extension, and $t \in L$,*

$$\mathrm{Trace}\big(\mathsf{Frob}_{t,L}|\mathcal{T}(f,B)\big) = \frac{-1}{(1+i)^{\deg(L/\mathbb{F}_2)}} \sum_{x\in L} \psi_{2,L}([x, f(x) + tx^B]).$$

*Then $\mathcal{T}(f, B)$ is pure of weight zero and is geometrically irreducible.*

PROOF. The purity goes back to Weil and is immediate from the fact that, for each $t$,

$$\mathcal{L}_{\psi_{2,L}([x, f(x)+tx^B])}$$

is pure of weight zero and lisse of rank one on the affine $x$-line, and is (totally) wildly ramified at $\infty$ (indeed with $\mathrm{Swan}_\infty = A_1$). To see the geometric irreducibility, we compute the second absolute moment $M_{1,1}$, cf. [**KT6**, Prop. 2.1]. Over a fixed finite extension $L/k$, the empirical

$M_{1,1}$ is the sum

$$\begin{aligned}&\frac{1}{(\#L)^2}\sum_{x,y,t\in L}\psi_{2,L}([x,f(x)+tx^B])\psi_{2,L}(-[y,f(y)+ty^B])\\ =&\frac{1}{(\#L)^2}\sum_{x,y,t\in L}\psi_{2,L}([x,f(x)+tx^B]-[y,f(y)+ty^B])\\ =&\frac{1}{(\#L)^2}\sum_{x,y,t\in L}\psi_{2,L}([x,f(x)+tx^B]+[y,y^2+f(y)+ty^B])\\ =&\frac{1}{\#L}\sum_{x,y\in L}\psi_{2,L}([x+y,xy+y^2+f(x)+f(y)])\big(\frac{1}{\#L}\sum_{t\in L}\psi_L(t(x^B+y^B))\big).\end{aligned}$$

The second factor is 1 if $x^B = y^B$ and 0 otherwise. Thus over a field $L$ which contains the $B^{\text{th}}$ roots of unity, the empirical $M_{1,1}$ is

$$\frac{1}{\#L}\big(-(B-1)+\sum_{\zeta\in\mu_B}\sum_{x,y=\zeta x\in L}\psi_{2,L}([x+y,xy+y^2+f(x)+f(y)])\big),$$

the initial $-(B-1)$ to compensate for overcounting the $B$ pairs $(x,y)=(0,0)$. The summand for $\zeta=1$, i.e. $x=y$, is identically $\#L$. Each of the other summands is

$$\sum_{x\in L}\psi_{2,L}([(1+\zeta)x,\zeta x^2+\zeta^2x^2+f(x)+f(\zeta x)]).$$

The key point is that, when $1+\zeta\neq 0$, this last sum has absolute value $\leq (A-1)\sqrt{\#L}$. To see this, note that any lisse sheaf $\mathcal{L}_{\psi_{2,L}([(1+\zeta)x,\text{ any polynomial}])}$ is lisse of rank one, pure of weight zero. So it suffices to note that it is geometrically nonconstant, because its tensor square is

$$\mathcal{L}_{\psi((\zeta+1)^2x^2)}\cong\mathcal{L}_{\psi((\zeta+1)x)},$$

which is geometrically non-constant, having $\mathrm{Swan}_\infty=1$. □

Corollary 9.2.2. *Each of the local systems*

$$\mathcal{W}(A_1,\ldots,A_n),\ \mathcal{W}^\sharp(A_1,\ldots,A_n),\ \textit{and}\ \mathcal{W}_0^\sharp(A_1,\ldots,A_n),$$

*see* (9.2.0.4), (9.2.0.5), (9.2.0.6), *is geometrically irreducible.*

Proof. Indeed, each has a geometrically irreducible pullback. □

Lemma 9.2.3. *None of the local systems $\mathcal{T}(f,B)$ of Lemma 9.2.1 is geometrically self-dual.*

Proof. The claim here is that $\mathrm{Hom}_{\pi_1^{\mathrm{geom}}}(\mathcal{T}(f,B)^\vee,\mathcal{T}(f,B))=0$. This in turn amounts to the statement that the literal second moment $M_{2,0}=0$, i.e. that as $L/\mathbb{F}_{16}$ grows, the empirical $M_{2,0}$, which is the sum

$$\begin{aligned}&\frac{1}{(\#L)^2}\sum_{x,y,t\in L}\psi_{2,L}([x,f(x)+tx^B])\psi_{2,L}([y,f(y)+ty^B])\\ =&\frac{1}{(\#L)^2}\sum_{x,y,t\in L}\psi_{2,L}([x,f(x)+tx^B]+[y,f(y)+ty^B])\\ =&\frac{1}{\#L}\sum_{x,y\in L}\psi_{2,L}([x+y,xy+f(x)+f(y)])\big(\frac{1}{\#L}\sum_{t\in L}\psi_L(t(x^B+y^B))\big).\end{aligned}$$

Exactly as in the proof of Lemma 9.2.1, over a field $L/\mathbb{F}_{16}$ which contains the $B^{\text{th}}$ roots of unity, the empirical $M_{2,0}$ is

$$\frac{1}{\#L}\big(-(B-1)+\sum_{\zeta\in\mu_B}\sum_{x,y=\zeta x\in L}\psi_{2,L}([x+y,xy+f(x)+f(y)])\big).$$

The summand for $\zeta=1$ is

$$\sum_{x\in L}\psi_{2,L}([0,x^2])=\sum_{x\in L}\psi_L(x^2)=\sum_{x\in L}\psi_L(x)=0.$$

For each $\zeta$ with $\zeta+1\neq 0$, the summand for $\zeta$ has absolute value $\leq (A-1)\sqrt{\#L}$, just as in the proof of Lemma 9.2.1. □

Corollary 9.2.4. *None of the local systems* $\mathcal{W}(A_1,\ldots,A_n)$*,* $\mathcal{W}^\sharp(A_1,\ldots,A_n)$*, or* $\mathcal{W}_0^\sharp(A_1,\ldots,A_n)$ *is geometrically self-dual.*

Proof. Indeed, each has a pullback which is not geometrically self-dual. □

When we restrict $\mathcal{W}(A_1,\ldots,A_n)$ to the open set where $s$ is invertible, which changes neither its $G_{\text{arith}}$ nor its $G_{\text{geom}}$, the change of variable $x\mapsto x/s$ gives an equality of trace functions

$$\text{Trace}\big(\mathsf{Frob}_{(s,t_2,\ldots,t_n),k}|\mathcal{W}(A_1,\ldots,A_n)\big)=\text{Trace}\big(\mathsf{Frob}_{(1/s,t_2/s^{A_2},\ldots,t_n/s^{A_n}),k}|\mathcal{W}^\sharp(A_1,\ldots,A_n)\big).$$

Thus the automorphism $\Phi:(s,t_2,\ldots,t_n)\mapsto(1/s,t_2/s^{A_2},\ldots,t_n/s^{A_n})$ of $\mathbb{G}_m\times\mathbb{A}^{n-1}/\mathbb{F}_2$, gives an isomorphism of local systems

$$\mathcal{W}(A_1,\ldots,A_n)|_{\mathbb{G}_m\times\mathbb{A}^{n-1}}\cong\Phi^\star\mathcal{W}^\sharp(A_1,\ldots,A_n).$$

On the other hand, we recover $\mathcal{G}(A_1,\ldots,A_n)$ on $\mathbb{A}^{n-1}/\mathbb{F}_2$ as the pullback of $\mathcal{W}(A_1,\ldots,A_n)$ to the hyperplane $s=0$. Thus we have equalities and inclusions of monodromy groups as follows:

$$\text{(9.2.4.1)}\quad \begin{aligned}G_{\text{arith},\mathcal{W}^\sharp(A_1,\ldots,A_n)}=G_{\text{arith},\mathcal{W}(A_1,\ldots,A_n)}\geq G_{\text{arith},\mathcal{G}(A_1,\ldots,A_n)}=G_{\text{arith},\mathcal{G}^\sharp(A_1,\ldots,A_n)},\\ G_{\text{geom},\mathcal{W}^\sharp(A_1,\ldots,A_n)}=G_{\text{geom},\mathcal{W}(A_1,\ldots,A_n)}\geq G_{\text{geom},\mathcal{G}(A_1,\ldots,A_n)}=G_{\text{geom},\mathcal{G}^\sharp(A_1,\ldots,A_n)}.\end{aligned}$$

Now, for any odd integers

$$A_1>A_2>\ldots A_m\geq 1,$$

we consider one more local system $\mathcal{W}^*(A_1,\dots,A_m)$ on $\mathbb{A}^1 \times \mathbb{G}_m \times (\mathbb{A}^1)^{m-1}$, whose trace formula is given by

$$(9.2.4.2) \qquad (s,t_1,\dots,t_m) \mapsto \frac{-1}{(1+i)^{\deg(k/\mathbb{F}_2)}} \sum_{x\in k} \psi_{2,k}([sx, \sum_{j=1}^{m} t_j x^{A_j}]).$$

Proposition 9.2.5. *For any $n, m \in \mathbb{Z}_{\geq 2}$ and any $q = 2^f$, let*

$$A_1 = q^n + 1,\ A_2 = q^{n_2} + 1, \dots, A_{m-1} = q^{n_{m-1}} + 1,$$

*and either $A_m = q^{n_m} + 1$ with $n > n_2 > \ldots > n_m \geq 1$, or $n > n_2 > \ldots > n_{m-1} \geq 1$ and $A_m = 1$. Then each of the local systems $\mathcal{W}^*(A_1,\dots,A_m)$, $\mathcal{W}(A_1,\dots,A_m)$, $\mathcal{W}^\sharp(A_1,\dots,A_m)$, and $\mathcal{W}_0^\sharp(A_1,\dots,A_m)$ is geometrically irreducible of rank $2^n$, has finite arithmetic monodromy groups, and is geometrically non-self-dual. Furthermore, all the arithmetic traces are Gaussian integers. Moreover, over any finite extension $k \supseteq \mathbb{F}_2$, the square absolute values of arithmetic traces are either $0$ or a $2$-power; and in fact they are either $0$ or a power of $q$ if $k \supseteq \mathbb{F}_q$.*

Proof. The geometric irreducibility and geometric non-self-duality are special cases of Corollaries 9.2.2 and 9.2.4. It is visible from the formula for Frobenius traces that these traces all lie in $\mathbb{Q}(i)$. The van der Geer–van der Vlugt argument, cf. [**vdG-vdV**, §5] and the proof of [**AKNOT**, Proposition 9.9] then shows that these traces lie in $\mathbb{Z}[i]$.

To prove the last statement for any of the listed local systems, it suffices to work with the more general trace formula (9.2.4.2) for $\mathcal{W} := \mathcal{W}^*(A_1,\dots,A_m)$. If $A_m = q^{n_m} + 1$ with $n_m \geq 1$, then we rewrite the input Witt vector at $(s,t_1,\dots,t_m)$ as

$$(9.2.5.1) \qquad V(x) := [sx, xR(x)] \ \text{ with } R(x) := \sum_{i=1}^{m} t_i x^{q^{n_i}}.$$

When $A_m = 1$, then we define $n_m = 0$ and note that the term $t_m x$ is Artin-Schreier equivalent to $t_m^2 x_m^2 = t_m^2 x_m^{q^{n_m}+1}$, and can use the same formula (9.2.5.1) with $t_m$ suitable adjusted. With this rewriting, we apply the idea of van der Geer-van der Vlugt, cf. [**vdG-vdV**, §5], as follows. In Witt vector addition in $\mathbb{F}_2$-algebras, using the fact that $R(x)$ is an additive polynomial, we get

$$\begin{aligned} V(x+y) - V(x) - V(y) &= [s(x+y), (x+y)(R(x)+R(y))] + [sx, xR(x) + s^2x^2] + [sy, yR(y) + s^2y^2] \\ &= [sy, s^2(x+y)x + (x+y)(R(x)+R(y)) + xR(x) + s^2x^2] + [sy, yR(y) + s^2y^2] \\ &= [0, s^2y^2 + s^2(x+y)x + (x+y)(R(x)+R(y)) + xR(x) + s^2x^2 + yR(y) + s^2y^2] \\ &= [0, s^2xy + xR(y) + yR(x)] \\ &= [0, \langle x,y\rangle] \end{aligned}$$

for

$$\langle x,y\rangle := s^2xy + xR(y) + yR(x).$$

The key point is that $\langle x,y\rangle$ on $k\times k$ is a symmetric $\mathbb{F}_2$-bilinear map to $k$, and $\mathrm{Trace}_{k/\mathbb{F}_2}(\langle x,y\rangle)$ is a symmetric $\mathbb{F}_2$-bilinear form on $k\times k$ as $\mathbb{F}_2$ vector space. Then

$$|\mathrm{Trace}(\mathsf{Frob}_{(s,t_1,\dots,t_m),k}|\mathcal{W})|^2 = (1/\#k) \sum_{x,y\in k} \psi_2\big(\mathrm{Trace}_{k/\mathbb{F}_2}(V(x) - V(y))\big)$$

(by the shearing transformation $(x, y) \mapsto (x + y, y)$)

$$= (1/\#k) \sum_{x,y \in k} \psi_2\big(\mathrm{Trace}_{k/\mathbb{F}_2}(V(x+y) - V(y))\big)$$

$$= (1/\#k) \sum_{x,y \in k} \psi_2\big(\mathrm{Trace}_{k/\mathbb{F}_2}(V(x) + [0, \langle x, y\rangle])\big)$$

$$= \sum_{x \in k} \psi_2\big(\mathrm{Trace}_{k/\mathbb{F}_2}(V(x))\big)\bigg((1/\#k)\sum_{y \in k} \psi\big(\mathrm{Trace}_{k/\mathbb{F}_2}(\langle x, y\rangle)\big)\bigg).$$

The second summand vanishes unless the given $x \in k$ has $\mathrm{Trace}_{k/\mathbb{F}_2}(\langle x, y\rangle) = 0$ for all $y \in k$, in which case it is 1.

Note that for $x, y \in k$,

$$\langle x, y\rangle = s^2xy + xR(y) + yR(x) = s^2xy + \sum_{i=1}^{m} t_i x y^{q^{n_i}} + \sum_{i=1}^{m} y t_i x^{q^{n_i}}$$

has the same $\mathrm{Trace}_{k/\mathbb{F}_2}$ as $\big(s^2x + \sum_{i=1}^m (t_i x)^{1/q^{n_i}} + \sum_{i=1}^m t_i x^{q^{n_i}}\big)y$. So by nondegeneracy of the trace, $x \in k$ has $\mathrm{Trace}_{k/\mathbb{F}_2}(\langle x, y\rangle) = 0$ for all $y \in k$ if and only if

(9.2.5.2)

$$s^2x + \sum_{i=1}^{m}(t_i x)^{1/q^{n_i}} + \sum_{i=1}^{m} t_i x^{q^{n_i}} = 0, \text{ equivalently, } s^{2q^n}x^{q^n} + \sum_{i=1}^{m} t_i^{q^{n-n_i}} x^{q^{n-n_i}} + \sum_{i=1}^{m} t_i^{q^n} x^{q^{n+n_i}} = 0.$$

Note that the set $\mathrm{Ker}_{s,t_1,\ldots,t_m}(k)$ of all $x \in k$ satisfying (9.2.5.2) is a vector space over $\mathbb{F}_2$, and we have

$$\big|\mathrm{Trace}(\mathsf{Frob}_{(s,t_1,\ldots,t_m),k}|\mathcal{W})\big|^2 = \sum_{x \in \mathrm{Ker}_{s,t_1,\ldots,t_m}(k)} \psi_2\big(\mathrm{Trace}_{k/\mathbb{F}_2}(V(x))\big).$$

Now, on $\mathrm{Ker}_{s,t_1,\ldots,t_m}(k)$, the map $x \mapsto \mathrm{Trace}_{k/\mathbb{F}_2}(V(x))$ is additive, i.e. a linear form. If it is nontrivial, the sum giving $|\mathrm{Trace}(\mathsf{Frob}_{(s,t_1,\ldots,t_m),k}|\mathcal{W})|^2$ vanishes. If it is trivial, this sum is $\#\mathrm{Ker}_{s,t_1,\ldots,t_m}(k)$, and hence a 2-power. If in addition $k \supseteq \mathbb{F}_q$, then $\mathrm{Ker}_{s,t_1,\ldots,t_m}(k)$ is a vector space over $\mathbb{F}_q$, and hence $|\mathrm{Trace}(\mathsf{Frob}_{(s,t_1,\ldots,t_m),k}|\mathcal{W})|^2$ is either 0 or a power of $q$. □

THEOREM 9.2.6. *Let $k/\mathbb{F}_2$ be a finite extension and $f(x) \in k[x]$ a polynomial of odd degree $A \geq 5$. Consider the local system $\mathcal{T}(f, 3, 1)$ on $\mathbb{A}^2/k$ whose trace function is given as follows. For $L/k$ a finite extension, and $(s, t) \in L^2$,*

$$\mathrm{Trace}\big(\mathsf{Frob}_{(s,t),L}|\mathcal{T}(f,3,1)\big) = \frac{-1}{(1+i)^{\deg(L/\mathbb{F}_2)}} \sum_{x \in L} \psi_{2,L}([x, f(x) + sx^3 + tx]).$$

*Then $\mathcal{T}(f, 3, 1)$ is pure of weight zero and has $M_{2,2} = 2$.*

PROOF. The purity goes back to Weil. For $L/k$ a finite extension, the empirical $M_{2,2}(L)$ is the sum

$$\frac{1}{(\#L)^2}\sum_{s,t \in L} |\mathrm{Trace}(\mathsf{Frob}_{(s,t),L}|\mathcal{T}(f,3,1))|^4 = \frac{1}{(\#L)^4}\sum_{s,t \in L}\sum_{x,y,z,w \in L}$$

$$\psi_{2,L}([x, f(x) + sx^3 + tx] + [y, f(y) + sy^3 + ty] - [z, f(z) + sz^3 + tz] - [w, f(w) + sw^3 + tw]).$$

The argument of $\psi_{2,L}$ is thus the Witt vector sum

$$\begin{aligned} &[x, f(x) + sx^3 + tx] + [y, f(y) + sy^3 + ty] \\ &+ [z, z^2 + f(z) + sz^3 + tz] + [w, w^2 + f(w) + sw^3 + tw] \\ &= [x + y, xy + f(x) + f(y) + s(x^3 + y^3) + t(x + y)] \\ &+ [z + w, zw + z^2 + w^2 + f(z) + f(w) + s(z^3 + w^3) + t(z + w)] \\ &= \begin{matrix} [x + y + z + w, (x + y)(z + w) + xy + zw + z^2 + w^2 + \\ f(x) + f(y) + f(z) + f(w) + s(x^3 + y^3 + z^3 + w^3) + t(x + y + z + w)], \end{matrix} \end{aligned}$$

which we write as the sum of the two Witt vectors

$$[x + y + z + w, (x + y)(z + w) + xy + zw + z^2 + w^2 + f(x) + f(y) + f(z) + f(w)]+$$
$$+[0, s(x^3 + y^3 + z^3 + w^3) + t(x + y + z + w)].$$

Denoting $\tilde{f}(x, y, z, w) := (x + y)(z + w) + xy + zw + z^2 + w^2 + f(x) + f(y) + f(z) + f(w)$, the empirical $M_{2,2}(L)$ is the sum

$$\frac{1}{(\#L)^2}\sum_{x,y,z,w\in L}\psi_{2,L}([x{+}y{+}z{+}w, \tilde{f}(x, y, z, w)])\cdot\frac{1}{(\#L)^2}\sum_{s,t\in L}\psi_L\big(s(x^3{+}y^3{+}z^3{+}w^3){+}t(x{+}y{+}z{+}w)\big).$$

This last sum over $s, t$ vanishes unless both $x^3 + y^3 + z^3 + w^3 = 0$ and $x + y + z + w = 0$.

One knows, cf. [**Ka-MMP**, Sublemma 3.11.4] that in $L$ the only simultaneous solutions of the two equations $x^3 + y^3 + z^3 + w^3 = x + y + z + w = 0$ are given by the three planes

$$P_1 : x = y, z = w, \quad P_2 : x = z, y = w, \quad \text{and } P_3 : x = w, y = z.$$

Let us recall the argument. Substituting for $w$ as $x + y + z$, we get the single equation

$$x^3 + y^3 + z^3 + (x + y + z)^3 = 0.$$

Over $\mathbb{F}_2$, this cubic form factors as $(x{+}y)(x{+}z)(y{+}z)$, and we are done. The intersection of any two of these planes is the line $D : x = y = z = w$. On any of these planes, the quantities $x, y, z, w$ agree in pairs, so whatever the polynomial $f$, we have $f(x){+}f(y){+}f(z){+}f(w) = 0$, and also $x + y + z + w = 0$. So our empirical $M_{2,2}(L)$ is the sum

$$\sum_{i=1,2,3}\frac{1}{(\#L)^2}\sum_{(x,y,z,w)\in P_i(L)}\psi_L((x + y)(z + w) + xy + zw + z^2 + w^2)$$

minus twice the sum over $D$, namely

$$\frac{1}{(\#L)^2}\sum_{x=y=z=w\in L}\psi_L((x + y)(z + w) + xy + zw + z^2 + w^2) = \frac{1}{(\#L)^2}\sum_{x=y=z=w\in L}\psi_L(0) = \frac{1}{\#L}.$$

The sum over $P_1$ vanishes, because it is

$$\frac{1}{(\#L)^2}\sum_{x,z\in L}\psi_L((x{+}x)(z{+}z){+}x^2{+}z^2{+}z^2{+}z^2) = \frac{1}{(\#L)^2}\sum_{x,z\in L}\psi_L(x^2{+}z^2) = \frac{1}{(\#L)^2}\sum_{x,z\in L}\psi_L(x{+}z) = 0.$$

The sum over each of $P_2$, $P_3$ is identically 1, because the argument $(x{+}y)(z{+}w){+}xy{+}zw{+}z^2{+}w^2$ vanishes: when, for example, $x = w$ and $y = w$, the argument is $(x{+}y)^2{+}xy{+}xy{+}x^2{+}y^2$. Thus the empirical $M_{2,2}(L)$ is $2 - 2/\#L$. Its "large $L$ limit" is thus 2. □

Fix any $n \in \mathbb{Z}_{\geq 2}$. As shown in [**Gri**, Theorem 5(b)], there is a 2-group $\tilde{E}$ of order $2^{2n+2}$, which is a central product $E * \langle \boldsymbol{z} \rangle$ of the extraspecial 2-group $E = 2_-^{1+2n}$ with the cyclic group $\langle \boldsymbol{z} \rangle$ of order 4, so that $\mathbf{Z}(E) = \langle \boldsymbol{z}^2 \rangle$ and

$$\mathrm{Aut}^+(\tilde{E}) = \tilde{E}/\mathbf{Z}(\tilde{E}) \cdot \mathrm{Sp}_{2n}(2),$$

where $\mathrm{Aut}^+(\tilde{E}) = \{\sigma \in \mathrm{Aut}(\tilde{E}) \mid \sigma(\boldsymbol{z}) = \boldsymbol{z}\}$ has index 2 in $\mathrm{Aut}(\tilde{E})$. Note that, up to equivalence, $\tilde{E}$ has two (dual to each other) faithful irreducible complex representations of degree $2^n$, which restrict to the unique irreducible representation of degree $2^n$ of $E$. Each of them is invariant under $\mathrm{Aut}^+(E)$ and extends to yield a finite irreducible subgroup

$$\tilde{\Gamma}(2, n) \cong \tilde{E} \cdot \mathrm{Sp}_{2n}(2) < \mathrm{GL}_{2^n}(\mathbb{C}) \tag{9.2.6.1}$$

(that induces $\mathrm{Aut}^+(\tilde{E})$ while acting via conjugation on $\tilde{E}$); moreover,

$$\mathbf{N}_{\mathrm{GL}_{2^n}(\mathbb{C})}(\tilde{E}) = \mathbf{Z}(\mathrm{GL}_{2^n}(\mathbb{C}))\tilde{\Gamma}(2, n). \tag{9.2.6.2}$$

Suppose now $n = bs \geq 3$ with $b, s \in \mathbb{Z}_{\geq 1}$. By a *standard subgroup* $\mathrm{Sp}_{2b}(2^s)$ of $\mathrm{Sp}_{2n}(2)$ we mean a subgroup $\mathrm{Sp}(U_s)$ with $U_s = \mathbb{F}_{2^s}^{2b}$ equipped with a non-degenerate $\mathbb{F}_{2^s}$-valued alternating form $(\cdot, \cdot)_s$, and then embedded in $\mathrm{Sp}(U_1) \cong \mathrm{Sp}_{2n}(2)$ with $U_1 = \mathbb{F}_2^{2n}$ equipped with the non-degenerate $\mathbb{F}_2$-valued alternating form $\mathrm{Tr}_{\mathbb{F}_{2^s}/\mathbb{F}_2}\big((\cdot, \cdot)_s\big)$. Note that the normalizer of such subgroup in $\mathrm{Sp}(U_1)$ is the semidirect product $\mathrm{Sp}(U_s) \rtimes C_s$ of $\mathrm{Sp}(U_s)$ by a cyclic group of order $s$ induced by the absolute Frobenius $x \mapsto x^2$. Let $\tilde{\Gamma}^\circ(2^s, b) = \tilde{E} \cdot \mathrm{Sp}_{2b}(2^s)$ denote the full inverse of such a standard subgroup $\mathrm{Sp}_{2b}(2^s)$ in $\tilde{\Gamma}(2, n)$, and let $\tilde{\Gamma}(2^s, b) = \tilde{E} \cdot (\mathrm{Sp}_{2b}(2^s) \rtimes C_s)$ denote the full inverse of $\mathrm{Sp}_{2b}(2^s) \rtimes C_s$ in $\tilde{\Gamma}(2, n)$.

Lemma 9.2.7. (i) *If $n \geq 3$ then $\tilde{\Gamma}(2, n) = \tilde{E} \cdot \mathrm{Sp}_{2n}(2)$ is perfect.*

(ii) *Suppose $n = bs \geq 3$ with $b, s \in \mathbb{Z}_{\geq 1}$. Then $\tilde{\Gamma}^\circ(2^s, b) = \tilde{E} \cdot \mathrm{Sp}_{2b}(2^s)$ is perfect.*

(iii) *Suppose $n = 3s$ with $s \in \mathbb{Z}_{\geq 2}$. Then the full inverse image $\tilde{E} \cdot G_2(2^s)$ of $G_2(2^s)$ in the subgroup $\tilde{\Gamma}^\circ(2^s, 3) = \tilde{E} \cdot \mathrm{Sp}_6(2^s)$ is perfect.*

Proof. (i) Since $\Gamma := \tilde{\Gamma}(2, n)$ contains $H_1^\circ = 2_-^{1+2n} \cdot \Omega_{2n}^-(2)$ which is perfect (as mentioned after (8.2.2.1)), we see that $Z[\Gamma, \Gamma] \geq \tilde{E}$ and $Z \cap [\Gamma, \Gamma] \geq \langle \boldsymbol{z}^2 \rangle$ for $Z := \mathbf{Z}(\tilde{E}) = \langle \boldsymbol{z} \rangle$. But $\mathrm{Sp}_{2n}(2)$ is simple when $n \geq 3$, so $Z[\Gamma, \Gamma] = \Gamma$.

If $[\Gamma, \Gamma] \geq Z$, then $[\Gamma, \Gamma] = \Gamma$ as stated. Otherwise for $F := [\Gamma, \Gamma] \cap \tilde{E} \lhd \Gamma$ we have $FZ = \tilde{E}$, $Z \cap F = \langle \boldsymbol{z}^2 \rangle =: Z_1$, and $|F| = 2^{2n+1}$. In this case, $Z_1 = [\tilde{E}, \tilde{E}] = [FZ, FZ] = [F, F]$. Next, $F/Z_1 = F/(F \cap Z) \cong FZ/Z = \tilde{E}/Z$ is elementary abelian, so $\Phi(F) = Z_1$. Since $FZ = \tilde{E}$ is centralized by $\mathbf{Z}(F)$, we also have $\mathbf{Z}(F) = \mathbf{Z}(\tilde{E}) \cap F = Z \cap F = Z_1$. Thus $F$ is an extraspecial 2-group of type $\epsilon = \pm$: $F \cong 2_\epsilon^{1+2n}$. Since $F$ acts faithfully on $\mathbb{C}^{2^n}$, this action is irreducible, and $F \lhd \Gamma$ now implies that $\Gamma$ embeds in $\mathbf{N}_{\mathrm{GL}_{2^n}(\mathbb{C})}(F) = \mathbf{Z}(\mathrm{GL}_{2^n}(\mathbb{C}))F \cdot \mathrm{O}_{2n}^\epsilon(2)$, which is impossible.

(ii) Denote $X := \tilde{\Gamma}^\circ(2^s, b)$ and $Y := X^{(\infty)}$. Since the simple group $\mathrm{Sp}_{2b}(2^s)$ acts faithfully and irreducibly on $\tilde{E}/\mathbf{Z}(\tilde{E})$, we have that $\mathbf{Z}(\tilde{E})Y = X$ and so $[X : Y]$ divides 4. If $[X : Y] = 4$, then $X = \mathbf{Z}(\tilde{E}) \times Y$ and so $\tilde{E} = \mathbf{Z}(\tilde{E}) \times (\tilde{E} \cap Y)$ splits over $\mathbf{Z}(E)$, a contradiction. It remains to consider the case $[X : Y] = 2$, whence $\boldsymbol{z}^2 \in Y$ and $Y \cap \mathbf{Z}(\tilde{E}) = \langle \boldsymbol{z}^2 \rangle$. In this case, the arguments in (i) again show that $F := Y \cap \tilde{E}$ is extraspecial of order $2^{1+2n}$, and $X$ embeds in $\mathbf{N}_{\mathrm{GL}_{2^n}(\mathbb{C})}(F) = \mathbf{Z}(\mathrm{GL}_{2^n}(\mathbb{C}))F \cdot \mathrm{O}_{2n}^\epsilon(2)$. This gives rise to an embedding $\mathrm{Sp}_{2b}(2^s) \hookrightarrow \mathrm{O}_{2n}^\epsilon(2)$

and so $\mathrm{Sp}_{2b}(2^s)$ supports a non-degenerate $\mathbb{F}_2$-valued quadratic form on $U_s = \mathbb{F}_{2^s}^{2b}$, which is impossible, see Theorem 8.3.1 and its proof.

(iii) Argue as in (ii), using the fact that $G_2(2^s)$ cannot support a non-degenerate $\mathbb{F}_2$-valued quadratic form on $U_s = \mathbb{F}_{2^s}^6$ when $s \geq 2$. □

The main result of this section is the following theorem, which, for the first time, produces explicit local systems with geometric monodromy groups of shape $(4 * 2_{\pm}^{1+2n}) \cdot \mathrm{Sp}_{2n}(2)$:

THEOREM 9.2.8. *Let $n \in \mathbb{Z}_{\geq 4}$ and $A_1 = 2^n + 1$. If $2|n$, let $r = 3$, $A_2 = 3$, $A_3 = 1$. If $2 \nmid n$, let $r = 4$, $A_2 = 5$, $A_3 = 3$, $A_4 = 1$. Then each of the local systems $\mathcal{W}(A_1, \ldots, A_r)$ and $\mathcal{W}^\sharp(A_1, \ldots, A_r)$, introduced in* (9.2.0.4), (9.2.0.5), *has both arithmetic and geometric monodromy groups equal to the group $\tilde{\Gamma}(2, n)$ defined in* (9.2.6.1).

PROOF. (a) By (9.2.4.1), it suffices to prove the statement for $\mathcal{W} := \mathcal{W}(A_1, \ldots, A_r)$. Let $G = G_{\mathrm{geom}}$, respectively $\tilde{G} = G_{\mathrm{arith},\mathbb{F}_2}$, denote the geometric, respectively arithmetic, monodromy group of $\mathcal{W}$. Let $V = \mathbb{C}^{2^n}$ denote the underlying representation for $\tilde{G}$ and $G$. By (9.2.4.1), we have

$$G \geq G_{\mathrm{geom},\mathcal{G}(A_1,\ldots,A_r)}, \ \tilde{G} \geq G_{\mathrm{arith},\mathcal{G}(A_1,\ldots,A_r),\mathbb{F}_2}.$$

Let us also set $m_1 := 1$ if $2|n$, and $(m_1, m_2) := (2, 1)$ if $2 \nmid n$. The trace formula (9.2.0.3) shows that $\mathcal{G}(A_1, \ldots, A_m)$ is the same as the local system $\mathcal{G}(n, m_1, \ldots, m_{r-2}, 0; 2)$ considered in §8.5, but with a different clearing factor. Note that a change of clearing factor does not affect the geometric monodromy group, and also preserves the image of the arithmetic monodromy group in $\mathrm{PGL}(V)$. It then follows from Theorem 8.5.9 (and its proof) that

$$\mathscr{Z}G \geq H_1^\circ = E \cdot \Omega_{2n}^-(2), \ \mathscr{Z}\tilde{G} \geq H_1^- = \Gamma(2, n, -) = E \cdot \mathrm{O}_{2n}^-(2) \tag{9.2.8.1}$$

where $\mathscr{Z} := \mathbf{Z}(\mathrm{GL}(V))$, and $H_1^\circ$ satisfies $(\mathbf{S}+)$; in particular, both $G$ and $\tilde{G}$ satisfy $(\mathbf{S}+)$. Moreover, Lemma 8.2.2 shows that a cyclic torus $C_{2^n+1}$ in $\Omega_{2n}^-(2)$ gives rise to an $\mathsf{ssp}$-element of order $2^n + 1$ in $G$. As $\tilde{G}$ is finite by Proposition 9.2.5, we can apply Theorem 8.4.5(a) to $G$ and $\tilde{G}$. Taking derived subgroups in (9.2.8.1) we obtain

$$[\tilde{G}, \tilde{G}] \geq [G, G] \geq [H_1^\circ, H_1^\circ] = H_1^\circ = E \cdot \Omega_{2n}^-(2). \tag{9.2.8.2}$$

It follows that

$$|G/\mathbf{Z}(G)| \geq 2^{2n}|\Omega_{2n}^-(2)| > 2^{n(2n+1)-2} > (2^{n+1} + 1)^4,$$

so the case $\mathrm{PSL}_2(q) \leq G/\mathbf{Z}(G) \leq \mathrm{Aut}(\mathrm{PSL}_2(q))$ with $q \leq 2^{n+1} + 1$ is impossible. Hence $G$ and $\tilde{G}$ must be in the extraspecial normalizer case of [**KT5**, Lemma 1.1], i.e.

$$R \lhd G \lhd \tilde{G},$$

where $R = \mathbf{Z}(R)E_1$ with $E_1 = 2_\epsilon^{1+2n}$ and $\mathbf{Z}(R) \hookrightarrow C_4$.

(b) Consider the case $R = E_1$. Then $\tilde{G} \leq \mathbf{N}_{\mathrm{GL}(V)}(E_1) = \mathscr{Z}E_1 \cdot \mathrm{O}_{2n}^\epsilon(2) = \mathscr{Z}H_1^-$. Together with (9.2.8.1), this implies that $\epsilon = -$. The key observation now is that, in this situation, $\tilde{G}$ and $G$ have

$$M_{2,2}(V) = 3. \tag{9.2.8.3}$$

(Indeed, $\tilde{G}$ and $H_1^-$ have the same image in $\mathrm{PGL}(V)$, so they share the same decomposition of $V \otimes V^*$ into simple submodules. By [**GT2**, Theorem 1.5], $H_1^-$ and $H_1^\circ$ have $M_{2,2}(V) = 3$, so the

$H_1^-$-module $V \otimes V^*$ is the sum of three simple submodules. This implies $M_{2,2}(\tilde{G}, V) \geq 3$. On the other hand, $M_{2,2}(\tilde{G}, V) \leq M_{2,2}(G, V) \leq M_{2,2}(H_1^\circ, V) = 3$. It follows that $M_{2,2}(\tilde{G}, V) = M_{2,2}(G, V) = 3$.) But (9.2.8.3) contradicts Theorem 9.2.6.

(c) We have shown that $\mathbf{Z}(R) = C_4$, and hence $\mathcal{Z} \cap \tilde{G} = \mathbf{Z}(\tilde{G}) = \mathbf{Z}(G) = \mathbf{Z}(R)$. In this case we can identify $R$ with $\tilde{E}$, and obtain $\tilde{G}/\tilde{E} \cong \mathcal{Z}\tilde{G}/\mathcal{Z}\tilde{E} \hookrightarrow \mathrm{Sp}_{2n}(2)$ from (9.2.6.2). Now the subgroup $H_1^\circ = E \cdot \Omega_{2n}^-(2)$ acts on $\tilde{E}$ via conjugation, see (9.2.8.2), and this action induces a subgroup $\bar{H}$ of $\mathrm{Sp}(W) \cong \mathrm{Sp}_{2n}(2)$ where $W := \tilde{E}/\mathbf{Z}(\tilde{E}) \cong \mathbb{F}_2^{2n}$. Suppose that the image $\bar{E}$ of $E$ in $\bar{H}$ is nontrivial. Then $\mathbf{O}_2(\bar{H}) \neq 1$ and hence it has a nonzero proper fixed point subspace $W_1$ on $W$. In this case, $\Omega_{2n}^-(2)$ also acts on $W_1$, and as $1 \leq \dim_{\mathbb{F}_2} W_1 < 2n$, this action is trivial, and thus $\bar{H}$ acts trivially on $W_1$. We can apply the same argument to the action of $\bar{H}$ on the fixed point subspace of $\bar{E}$ on $W/W_1$. Repeating this process, we see that $\bar{H}$ is a unitriangular subgroup of $\mathrm{Sp}(W)$ and hence it is solvable. But $H_1^\circ$ is perfect, so $H_1^\circ$ acts trivially on $W$. By (9.2.6.1) and (9.2.6.2), this means that $H_1^\circ$ induces only inner automorphisms of $\tilde{E}$, and hence injects into a solvable subgroup of $\mathbf{N}_{\mathrm{GL}(V)}(\tilde{E})$, a contradiction.

We have shown that $E$ has trivial image in $\bar{H}$, which means $E$ only induces inner automorphisms of $\tilde{E}$, i.e. $E \leq \mathcal{Z}\tilde{E}$. In particular, $\mathcal{Z}\tilde{E} \cap H_1^- \geq E$, and $[E, \mathcal{Z}\tilde{E}] \leq [\mathcal{Z}\tilde{E}, \mathcal{Z}\tilde{E}] = C_2 = \mathbf{Z}(E)$, whence

$$E \lhd \mathcal{Z}\tilde{E}. \tag{9.2.8.4}$$

Since $\mathcal{Z}\tilde{E}$ is nilpotent and $\Omega_{2n}^-(2)$ is simple, $\mathcal{Z}\tilde{E} \cap H_1^\circ = E$. Now, if $\mathcal{Z}\tilde{E} \cap H_1^- > E$, then, since $\mathcal{Z}\tilde{E} \cap H_1^- \lhd H_1^-$, we must have $\mathrm{O}_{2n}^-(2) = H_1^-/E \cong \Omega_{2n}^- \times C_2$, a contradiction.

Thus $\mathcal{Z}\tilde{E} \cap H_1^- = E$. Now we observe from(9.2.8.1) that $\mathcal{Z}\tilde{G}$ contains the subgroup $X := \mathcal{Z}\tilde{E}H_1^-$, with $X/\mathcal{Z}\tilde{E} \cong H_1^-/(\mathcal{Z}\tilde{E} \cap H_1^-) = H_1^-/E \cong \mathrm{O}_{2n}^-(2)$. It follows that $\mathrm{O}_{2n}^-(2)$ is a subgroup of $\mathcal{Z}\tilde{G}/\mathcal{Z}\tilde{E} \cong \mathrm{Sp}_{2n}(2)$, of index $2^{n-1}(2^n - 1)$, which is the smallest index of proper subgroups in $\mathrm{Sp}_{2n}(2)$, see [**KlL**, Table 5.3.A]. Hence either $\mathcal{Z}\tilde{G} = X$, or $\mathcal{Z}\tilde{G}/\mathcal{Z}\tilde{E} \cong \mathrm{Sp}_{2n}(2)$. In the former case, by (9.2.8.2) and (9.2.8.4) we have $E \lhd \tilde{G}$, but this contradicts the result of (b).

We have shown that $\mathcal{Z}\tilde{G}/\mathcal{Z}\tilde{E} \cong \mathrm{Sp}_{2n}(2)$; in particular, $\mathcal{Z}\tilde{G} = \mathcal{Z}\tilde{\Gamma}(2, n)$ by (9.2.6.1). Taking the derived subgroups, we see by Lemma 9.2.7(i) that $[\tilde{G}, \tilde{G}] \geq \tilde{\Gamma}(2, n)$. On the other hand, $\mathbf{C}_{\tilde{G}}(\tilde{E}) = \mathbf{Z}(\tilde{G}) = \mathbf{Z}(\tilde{E}) \cong C_4$ and $|\tilde{G}/\mathbf{C}_{\tilde{G}}(\tilde{E})| \leq |\mathrm{Aut}^+(\tilde{E})| = |\tilde{\Gamma}(2, n)/\mathbf{Z}(\tilde{E})|$. Hence $\tilde{G} = \tilde{\Gamma}(2, n)$. As $G \lhd \tilde{G}$ and $\tilde{G}/G$ is cyclic, we conclude from Lemma 9.2.7 that $G = \tilde{G}$. □

As a consequence of Theorem 9.2.8, we deduce the following result about a certain omnibus sheaf:

THEOREM 9.2.9. *For any $n \geq 4$, consider the local system*

$$\hat{\mathcal{W}} := \hat{\mathcal{W}}(2^n + 1, 2^{n-1} + 1, \dots, 2^2 + 1, 3, 1)$$

*on $(\mathbb{A}^1 \times \mathbb{G}_m \times \mathbb{A}^n)/\mathbb{F}_2$ whose trace function for any $(s, t_1, \dots, t_{n+1}) \in k \times k^\times \times k^n$ is given by*

$$\mathrm{Trace}\big(\mathsf{Frob}_{(s,t_1,\dots,t_{n+1}),k} | \hat{\mathcal{W}}\big) = \frac{-1}{(1+i)^{\deg(k/\mathbb{F}_2)}} \sum_{x \in k} \psi_{2,k}([sx, \sum_{j=1}^{n} t_j x^{2^{n-j+1}+1} + t_{n+1}x]).$$

*Then $\hat{\mathcal{W}}$ has its geometric and arithmetic monodromy group equal to $\tilde{\Gamma}(2, n)$.*

PROOF. Suitable specializations of $\hat{\mathcal{W}}$ yield the sheaf $\mathcal{W}(2^n+1,3,1)$ when $2|n$, and the sheaf $\mathcal{W}(2^n+1,5,3,1)$ when $2 \nmid N$, both considered in Theorem 9.2.8. Hence it follows from Theorem 9.2.8 that the arithmetic (over $\mathbb{F}_2$) and geometric monodromy groups of $\hat{\mathcal{W}}$ satisfy

$$(9.2.9.1) \qquad G_{\mathrm{arith},\hat{\mathcal{W}},\mathbb{F}_2} \rhd G_{\mathrm{geom},\hat{\mathcal{W}}} \geq \tilde{\Gamma}(2,n) = R \cdot \mathrm{Sp}_{2n}(2),$$

where $R = C_4 * E$ with $E = 2^{1+2n}_{-}$. These containments show that $G_{\mathrm{arith},\hat{\mathcal{W}},\mathbb{F}_2}$ and $G_{\mathrm{geom},\hat{\mathcal{W}}}$ both satisfy (**S**+) and contain an $\mathsf{ssp}$-element of order $2^n+1$; on the other hand, both of them are finite and have center of order dividing 4 by Proposition 9.2.5. Arguing as in part (a) of the proof of Theorem 9.2.8, we see that either one of these groups, call it $G$, must be in the extraspecial normalizer case of [**KT5**, Lemma 1.1]. Letting $V$ be the underlying representation, we then have

$$R_2 \lhd G \leq \mathbf{N}_{\mathrm{GL}(V)}(R_2) \leq \mathscr{Z}R_2 \cdot \mathrm{Sp}_{2n}(2) \leq \tilde{\Gamma}(2,n)\mathscr{Z},$$

where $R_2 = \mathbf{Z}(R_2)E_2$, $\mathscr{Z} := \mathbf{Z}(\mathrm{GL}(V))$, and $E_2 = 2^{1+2n}_{\pm}$. Taking the derived subgroup, we get $[G,G] \hookrightarrow \tilde{\Gamma}(2,n)$; note that $\tilde{\Gamma}(2,n)$ is perfect by Lemma 9.2.7. Together with (9.2.9.1), this shows that $[G,G] = \tilde{\Gamma}(2,n)$ and hence $G$ contains $R = \mathbf{O}_2([R,R])$ as a normal subgroup. In turn, this implies that $G \leq \mathbf{N}_{\mathrm{GL}(V)}(R) = \mathscr{Z}\tilde{\Gamma}(2,n)$, and so

$$G = (\mathscr{Z} \cap G)\tilde{\Gamma}(2,n) = \mathbf{Z}(G)\tilde{\Gamma}(2,n) = \tilde{\Gamma}(2,n)$$

(since $\mathbf{Z}(G) \leq C_4 = \mathbf{Z}(R)$). We have therefore shown that $G_{\mathrm{arith},\hat{\mathcal{W}},\mathbb{F}_2} = G_{\mathrm{geom},\hat{\mathcal{W}}} = \tilde{\Gamma}(2,n)$. □

## 9.3. Local systems with Witt vectors: The $\mathbb{F}_q$ story

Local systems in characteristic 2 with Witt vectors: The $\mathbb{F}_q$ story

We now turn to the "$q$ situation". We will need an elementary case of Lang–Weil estimates:

LEMMA 9.3.1. *Let $n > m \geq 1$ be odd integers. Then the number $N$ of $\mathbb{F}_q$-points in the intersection of the Fermat hypersurfaces $H_m$ and $H_n$, where*

$$H_n := \{(x,y,z,t) \in \mathbb{A}^4 \mid x^n+y^n+z^n+w^n = 0\},\ H_m := \{x,y,z,t) \in \mathbb{A}^4 \mid x^m+y^m+z^m+w^m = 0\},$$

*is at most $m^2nq^2$.*

PROOF. In $\mathbb{A}^4/\overline{\mathbb{F}_2}$, $H_m$ is irreducible, and lisse outside the origin, of degree $m$. Now, the hypersurfaces $H_m$ and $H_n$ intersect properly, with every irreducible component of $H_m \cap H_n$ of dimension $\leq 2$. By [**LW**, Lemma 1], we have an estimate $N \leq O(1)((\#L)^2)$ for some constant $O(1)$ depending only on $m$ and $n$.

Alternatively, we give an elementary proof giving the explicit upper bound $m^2nq^2$. First we fix $a, b \in \mathbb{F}_q$ and bound the number $N(a,b)$ of common solutions to $x^n+y^n = a$, $x^m+y^m = b$. Then

$$(b-x^m)^n = y^{mn} = (a-x^n)^m,$$

and so $f_{a,b}(x) = 0$ for $f_{a,b}(t) := (b-x^m)^n - (a-x^n)^m \in \mathbb{F}_q[t]$. Note that $f$ has degree $m(n-1)$ if $b \neq 0$, $n(m-1) < m(n-1)$ if $b = 0$ but $a \neq 0$, and identically 0 if $a = b = 0$. So unless $a = b = 0$, the number of roots $x \in \mathbb{F}_q$ of $f_{a,b}$ is at most $m(n-1)$, and for each $x$

there are at most $m$ possibilities for $y$ such that $x^m + y^m = b$. Thus unless $a = b = 0$, we have $N(a, b) \leq m^2(n-1)$. On the other hand, $N(0, 0) \leq mq$, since $y^m = -x^m$ in this case.

Now for any $(z, w) \in \mathbb{F}_q^2$, take $a = -z^n - w^n$ and $b = -y^m - z^m$. Then the number of $(x, y) \in \mathbb{F}_q^2$ such that $(x, y, z, w) \in H_m \cap H_n$ is $N(a, b)$, and $N(a, b) \leq m^2(n-1)$ as shown above if $(a, b) \neq (0, 0)$. On the other hand, the number of $(z, w) \in \mathbb{F}_q^2$ such that $a = b = 0$ is at most $mq$, and then the number of corresponding points $(x, y, z, w) \in H_m \cap H_n$ is at most $mq$, as shown above. Hence $N \leq q^2m^2(n-1) + m^2q^2 = m^2nq^2$. □

Now we can prove a full generalization of Theorem 9.2.6:

Theorem 9.3.2. *Let $q = 2^e$ and let $k/\mathbb{F}_q$ be a finite extension. Let $f(x) \in k[x]$ be an odd polynomial (in the sense that it only has terms of odd degree) of degree $N$. Let $a > b \geq 1$ be odd integers, and suppose that $N > a$. Consider the local system $\mathcal{T} = \mathcal{T}(f, a, b)$ on $\mathbb{A}^2/k$ of rank $N - 1$, whose trace function is given as follows: for $L/k$ a finite extension, and $(s, t) \in L^2$, given by*

$$\mathrm{Trace}(\mathsf{Frob}_{(s,t),L}|\mathcal{T}(f, a, b)) := \frac{-1}{(1+i)^{\deg(L/\mathbb{F}_2)}} \sum_{x \in L} \psi_{2,L}([x, f(x) + sx^a + tx^b]).$$

*Then $\mathcal{T}$ is pure of weight zero and has $M_{2,2} = 2$.*

Proof. The purity goes back to Weil. Let us denote by $\mathrm{Trace}(s, t, L)$ this trace. Then the empirical $M_{2,2}(L)$ is given by

$$\frac{1}{(\#L)^2} \sum_{s,t \in L} |\mathrm{Trace}(s, t, L)|^4.$$

Expanding this out, we get that $M_{2,2}(L)$ is

$$\frac{1}{(\#L)^4} \sum_{s,t \in L} \sum_{x,y,z,w \in L} \psi_{2,L}([x, f(x) + sx^a + tx^b] + [y, f(y) + sy^a + ty^b]$$
$$-[z, f(z) + sz^a + tz^b] - [w, f(w) + sw^a + tw^b]).$$

The argument of $\psi_{2,L}$ is thus the Witt vector sum

$$\begin{aligned}
&[x, f(x) + sx^a + tx^b] + [y, f(y) + sy^a + ty^b] \\
&+ [z, z^2 + f(z) + sz^a + tz^b] + [w, w^2 + f(w) + sw^a + tw^b] \\
&= [x + y, xy + f(x) + f(y) + s(x^a + y^a) + t(x^b + y^b)] \\
&+ [z + w, zw + z^2 + w^2 + f(z) + f(w) + s(z^a + w^a) + t(z^b + w^b)] \\
&= [x + y + z + w, ((x + y)(z + w) + xy + zw + z^2 + w^2) + s(x^a + y^a + z^a + w^a) \\
&+ t(x^b + y^b + z^b + w^b) + f(x) + f(y) + f(z) + f(w)],
\end{aligned}$$

which we write as the sum of the two Witt vectors

$$[x + y + z + w, ((x + y)(z + w) + xy + zw + z^2 + w^2) + f(x) + f(y) + f(z) + f(w)]+$$
$$+[0, s(x^a + y^a + z^a + w^a) + t(x^b + y^b + z^b + w^b)].$$

Denoting

$$\tilde{f}(x, y, z, w) := ((x + y)(z + w) + xy + zw + z^2 + w^2) + f(x) + f(y) + f(z) + f(w),$$

and by

$$\Sigma_a := x^a + y^a + z^a + w^a,\ \Sigma_b := x^b + y^b + z^b + w^b,$$

the empirical $M_{2,2}(L)$ is thus

$$\frac{1}{(\#L)^4}\sum_{x,y,z,w\in L}\psi_{2,L}([x+y+z+w,\tilde{f}(x,y,z,w)])\sum_{s,t\in L}\psi_L\big(s\Sigma_a+t\Sigma_b\big).$$

The sum over $s,t$ vanishes unless $\Sigma_a=\Sigma_b=0$, i.e., unless $(x,y,z,w)$ lies in the intersection

$$H := H_a \cap H_b$$

of Fermat hypersurfaces $H_a$ and $H_b$ (as defined in Lemma 9.3.1), in which case it is $(\#L)^2$. So the empirical $M_{2,2}(L)$ is

$$\frac{1}{(\#L)^2}\sum_{(x,y,z,w)\in H(L)}\psi_{2,L}([x+y+z+w,\tilde{f}(x,y,z,w)]). \tag{9.3.2.1}$$

The idea now is to compute, for any given $A\in L$ and any given polynomial $h(x)\in L[x]$, the sum

$$\sum_{r\in L}\psi_{2,L}([rA,h(r)]).$$

Suppose first that $A\neq 0$. Then $\mathcal{L}_{\psi_2([rA,h(r)])}$ is lisse on $\mathbb{A}^1$ of rank one, with $\mathsf{Swan}_\infty \le \max(2,\deg(h))$ (with equality if $h(x)$ has odd degree). By Weil, this exponential sum is pure of weight one and of rank $\mathsf{Swan}_\infty - 1 \le \max(1,\deg(h)-1) \le 1+\deg(h)$. Hence we have

$$\big|\sum_{r\in L}\psi_{2,L}([rA,h(r)])\big| \le (1+\deg(h))\sqrt{\#L} \text{ if } A\neq 0. \tag{9.3.2.2}$$

Suppose now that $A=0$ and that $h(x)$ is not Artin-Schreier trivial (i.e., not of the form $g(x)^2-g(x)$ for any $g(x)\in\overline{k}[x]$), then by Weil

$$\big|\sum_{r\in L}\psi_{2,L}([rA,h(r)])\big| = \big|\sum_{r\in L}\psi_L(h(r))\big| \le (\deg(h)-1))\sqrt{\#L}. \tag{9.3.2.3}$$

The next key observation is that $H(L)$ is homogeneous, and $H(L)$ is a union of one-dimensional vector spaces over $L$, the sets of whose nonzero points are disjoint. Consider any such line $\Omega(v)$, generated by $v:=(x_0,y_0,z_0,w_0)$, and parametrize the points in $\Omega(v)$ as $rv$ with $r\in L$. Then set

$$A := x_0+y_0+z_0+w_0,\ h(r) := \tilde{f}(rx_0,ry_0,rz_0,rw_0).$$

(so that $A$ and $h$ depend on $v$). By Lemma 9.3.1, $H(L)$ is the union of $O(\#L)$ such lines $\Omega(v)$. According to (9.3.2.2) and (9.3.2.3),

$$\big|\sum_{(0,0,0,0)\neq(x,y,z,w)\in\Omega(v)}\psi_{2,L}([x+y+z+w,\tilde{f}(x,y,z,w)])\big| = \big|\sum_{r\in L}\psi_{2,L}([rA,h(r)])-1\big|$$

is $O((\#L)^{1/2})$, unless $A=0$ and $h(x)$ is Artin-Schreier trivial. Thus the total contribution to (9.3.2.1) of the nonzero points of the lines $\Omega(v)\subset H(L)$, for which either $A\neq 0$ or $h(x)$ is not Artin-Schreier trivial, is at most $O((\#L)^{3/2})/(\#L)^2 = O(1/\sqrt{\#L})$, which dies in the large $L$ limit.

Now we consider the lines $\Omega(v)$ for which $A = 0$ and $h(x)$ is Artin-Schreier trivial. Since $f$ is 0 or odd, the coefficient $c_2$ of $x^2$ in $h(x)$ is $Q(v) = (x_0+y_0)(z_0+w_0)+x_0y_0+z_0w_0+z_0^2+w_0^2$, and the linear and constant terms of $h(x)$ vanish. And all terms, if any, of degree $\geq 3$ in $h(x)$ have odd degree (because $f$ has only terms of odd degree). Thus if $h(x)$ is Artin-Schreier trivial, then in fact $h(x) = 0$. [Indeed, suppose

$$\sum_{i=0}^{N} c_i x^i = h(r) = g(x)^2 - g(x)$$

for some $g(x) = \sum_{i=0}^{M} a_i x^i \in \overline{k}[x]$. Then $c_i = a_i$ if $2 \nmid i$ and $c_i = a_i - a_{i/2}^2$ if $2|i > 0$. As $c_1 = 0$, we have $a_1 = 0$, and $c_2 = a_2$. As $c_{2^j} = 0$ for $j \geq 3$, we have $a_{2^j} = a_{2^{j-1}}^2$, which shows $a_{2^j} = a_2^{2^{j-1}}$. Taking $j$ so that $2^j > M$, we get $a_{2^j} = 0$, and hence $a_2 = 0$ and $c_2 = 0$ as stated.]

Considering the quadric

$$Q := \{(x,y,z,w) \mid (x+y)(z+w)+xy+zw+z^2+w^2 = 0\},$$

and recalling that $A = 0$ is the equation of $H_1$, and $Q(v)$ is the coefficient for $r^2$ in $h(r)$, we see that $v$ belongs to $H_1 \cap Q$. Now note that if $(x,y,z,w) \in H_1 \cap Q$, then $w = x+y+z$ and $0 = z^2+xz+yz+xy = (x+z)(y+z)$. Hence $H(L) \cap H_1(L) \cap Q(L)$ is just the union of the two planes

$$P_0 : x = z, y = w, \text{ and } P_\infty : x = w, y = z$$

in $L^4$. Thus the large $L$ limit of the sum in (9.3.2.1) becomes

$$\sum_{\alpha=0,\infty} \frac{1}{(\#L)^2} \sum_{(x,y,z,w)\in P_\alpha} \psi_L(\tilde{f}(x,y,z,w)).$$

The intersection $P_0 \cap P_\infty$ is the locus $x = y = z = w$, so the sum over this intersection is trivially bounded by

$$\frac{(\text{number of summands} = (\#L))}{(\#L)^2} = \frac{1}{\#L},$$

and hence this intersection does not contribute to the large $L$ limit. On the other hand,

$$\tilde{f}(x,y,z,w) = ((x+y)(z+w)+xy+zw+z^2+w^2) + f(x)+f(y)+f(z)+f(w)$$

is identically zero on $P_0$ and on $P_\infty$, since $f$ is an odd polynomial. Thus each of the sums over $P_0$ and $P_\infty$ equals 1. Consequently, the large $L$ limit of $M_{2,2}$ is indeed 2. □

Next we give a degenerate variant of Theorem 9.3.2:

THEOREM 9.3.3. *Let $q = 2^e$ and let $k/\mathbb{F}_q$ be a finite extension. Let $f(x) \in k[x]$ be an odd polynomial (in the sense that is either 0 or only has terms of odd degree) of degree $N$. Let $a > b \geq 1$ be odd integers, and suppose that $N < a$. Consider the local system $\mathcal{T} = \mathcal{T}(f,a,b)$ on $(\mathbb{G}_m \times \mathbb{A}^1)/k$ of rank $a-1$, whose trace function is given as follows: for $L/k$ a finite extension, and $s \in L^\times, t \in L$,*

$$\mathrm{Trace}(\mathsf{Frob}_{(s,t),L}|\mathcal{T}(f,a,b)) := \frac{-1}{(1+i)^{\deg(L/\mathbb{F}_2)}} \sum_{x\in L} \psi_{2,L}([x, f(x)+sx^a+tx^b]).$$

*Then $\mathcal{T}$ is pure of weight zero and has $M_{2,2} = 2$.*

Proof. For every $(s,t) \in L^2$, let us define Trace$(s,t,L)$ by the formula

$$\mathrm{Trace}(s,t,L) := \frac{-1}{(1+i)^{\deg(L/\mathbb{F}_2)}} \sum_{x \in L} \psi_{2,L}([x, f(x) + sx^a + tx^b]).$$

The proof of Theorem 9.3.2, which makes no explicit reference to the degree of $f$, shows that as $L$ runs over extensions of $\mathbb{F}_q$, the large $L$ limit of

$$\frac{1}{(\#L)^2} \sum_{s,t \in L} |\mathrm{Trace}(s,t,L)|^4$$

is 2. Now $M_{2,2}$ for our $\mathcal{W}$ is the large $L$ limit of

$$\frac{1}{(\#L)(\#L-1)} \sum_{t \in L, s \in L^\times} |\mathrm{Trace}(s,t,L)|^4.$$

But the ratio $\frac{(\#L)(\#L-1)}{(\#L)}$ tends to 1 as $L$ grows, so it suffices to show that the large $L$ limit of

$$\frac{1}{(\#L)^2} \sum_{r,t \in L, s \in L^\times} |\mathrm{Trace}(s,t,L)|^4$$

is 2. Thus we must show that the large $L$ limit of

$$\frac{1}{(\#L)^2} \sum_{r,t \in L} |\mathrm{Trace}(0,t,L)|^4$$

vanishes. In fact, we will show that it is $O(1/\#L)$, i.e., that

$$\sum_{t \in L} |\mathrm{Trace}(0,t,L)|^4 = O(\#L).$$

Each individual sum

$$\mathrm{Trace}(0,t,L) := \frac{-1}{(1+i)^{\deg(L/\mathbb{F}_2)}} \sum_{x \in L} \psi_L(f(x) + tx^b])$$

is bounded in absolute value by $(\max(\deg(f), b) - 1)$, with the possible exception of a single $t_0$ for which $f(x) + t_0 x^b = 0$, in which the sum is trivially bounded by $\sqrt{\#L}$. Thus

$$\sum_{t \in L} |\mathrm{Trace}(0,t,L)|^4 \le (\#L)(\max(\deg(f), b) - 1) + \sqrt{\#L}.$$

□

Remark 9.3.4. In Theorem 9.3.3, the case when $f$ has degree equal to $a$ can also be included, just do an additive translation of the parameter $s$ to first replace $f$ by $f-$ its leading term to reduce to the situation of the theorem.

We now turn to discussion of the local system $\mathcal{R}_q$ on $(\mathbb{A}^1 \times \mathbb{G}_m \times \mathbb{A}^1)/\mathbb{F}_2$ whose trace function is given as follows: for $L/\mathbb{F}_2$ a finite extension, and $(r,s,t) \in L^3, s \neq 0$,

$$\mathrm{Trace}(\mathsf{Frob}_{(r,s,t),L}|\mathcal{R}_q) := \frac{-1}{(1+i)^{\deg(L/\mathbb{F}_2)}} \sum_{x \in L} \psi_{2,L}([rx, sx^{q+1} + tx]), \tag{9.3.4.1}$$

and its Kummer pullback $\mathcal{R}_q^\circ$ by $[s \mapsto s^{q+1}]$, whose trace function is given as follows: for $L/\mathbb{F}_2$ a finite extension, and $(r,s,t) \in L^3, s \neq 0$,

$$\text{(9.3.4.2)} \qquad \mathrm{Trace}(\mathsf{Frob}_{(r,s,t),L}|\mathcal{R}_q^\circ) := \frac{-1}{(1+i)^{\deg(L/\mathbb{F}_2)}} \sum_{x\in L} \psi_{2,L}([rx, s^{q+1}x^{q+1}+tx]).$$

We next relate $\mathcal{R}_q^\circ$ to the sheaf $\mathcal{W}(q+1,1)$ of (9.2.0.4).

LEMMA 9.3.5. (i) *The sheaf* $\mathcal{R}_q$ *as defined in* (9.3.4.1) *is lisse of rank* $q$*, pure of weight zero, geometrically irreducible, and all its Frobenius traces lie in* $\mathbb{Z}[i]$*. Moreover, it has* $M_{2,2}=2$*.*

(ii) *The sheaves* $\mathcal{W}(q+1,1)$ *of* (9.2.0.4) *and* $\mathcal{R}_q^\circ$ *as defined in* (9.3.4.2) *have the same geometric, respectively arithmetic, monodromy groups.*

PROOF. (i) For $L/\mathbb{F}_2$ a finite extension, and $(r,s,t)\in L\times L^\times \times L$, the rank one lisse sheaf $\mathcal{L}_{\psi_2([rx,sx^{1+q}+tx])}$ on the $x$ line has $\mathsf{Swan}_\infty = q+1$ (because $s\neq 0$) and is pure of weight zero. That $\mathcal{R}_q$ is lisse on $(\mathbb{A}^1\times\mathbb{G}_m\times\mathbb{A}^1)/\mathbb{F}_2$ of rank $q$ then results from Deligne's semicontinuity theorem cf. [**Lau**] or [**Ka-Scont**, Proposition 11]. That it is pure of weight zero goes back to Weil. It is geometrically irreducible because it has a geometrically irreducible pullback, e.g. take $r=0, s=1$ and we obtain the Fourier transform of $\mathcal{L}_{\psi([x^{1+q}])}$ on the $t$-line. Finally the traces lie in $\mathbb{Z}[i]$ by the van der Geer–van der Vlugt argument as in the proof of Proposition 9.2.5. That $M_{2,2}=2$ for $\mathcal{R}_q$ results from the fact that already its pullback to $(\mathbb{G}_m\times\mathbb{A}^1)/\mathbb{F}_2$ obtained by fixing $r=1$ has $M_{2,2}=2$ by Theorem 9.3.3. But $M_{2,2}$ can only increase under pullback, and is always $\geq 2$ in any rank $\geq 2$.

(ii) The change of variable $x\mapsto x/s$ shows that $\mathcal{R}_q^\circ$ on $(\mathbb{A}^1\times\mathbb{G}_m\times\mathbb{A}^1)/\mathbb{F}_2$ has the same trace function as the pullback of $\mathcal{W}$ on $(\mathbb{A}^1\times\mathbb{A}^1)/\mathbb{F}_2$ by the map

$$\Phi : \mathbb{A}^1\times\mathbb{G}_m\times\mathbb{A}^1 \to \mathbb{A}^1\times\mathbb{A}^1 : \quad (r,s,t)\mapsto (r/s, t/s).$$

Notice that $\mathcal{R}_q^\circ$ is geometrically irreducible, because already its pullback to the locus $r=0, s=1$ is geometrically irreducible, being the Fourier transform $\mathrm{FT}_\psi(\mathcal{L}_{\psi(x^{q+1})})$. In particular, $\mathcal{R}_q^\circ$ is arithmetically irreducible. By Chebotarev, it follows that we have an arithmetic isomorphism

$$\mathcal{R}_q^\circ \cong \Phi^\star\mathcal{W},$$

as their arithmetic semisimplifications are isomorphic, and the source is arithmetically irreducible. Thus we have isomorphisms

$$G_{\mathrm{arith},\mathcal{R}_q^\circ}\cong G_{\mathrm{arith},\Phi^\star\mathcal{W}}, \quad G_{\mathrm{geom},\mathcal{R}_q^\circ}\cong G_{\mathrm{geom},\Phi^\star\mathcal{W}}.$$

The map $\Phi$ has a retraction

$$\Psi : \mathbb{A}^1\times\mathbb{A}^1 \to \mathbb{A}^1\times\mathbb{G}_m\times\mathbb{A}^1 : \quad (r,t)\mapsto (r,1,t).$$

Thus $\Psi^\star(\Phi^\star\mathcal{W}) = \mathcal{W}$, and hence $\mathcal{W}$ and $\Phi^\star\mathcal{W}$ have the same $G_{\mathrm{arith}}$ as each other and the same $G_{\mathrm{geom}}$ as each other, because each of these two local systems is the pullback of the other. Thus we have

$$G_{\mathrm{arith},\mathcal{R}_q^\circ}\cong G_{\mathrm{arith},\mathcal{W}}, \quad G_{\mathrm{geom},\mathcal{R}_q^\circ}\cong G_{\mathrm{geom},\mathcal{W}}.$$

□

LEMMA 9.3.6. *Write $q = 2^f$. The geometric monodromy group $G_{\mathrm{geom},\mathcal{R}_q}$ of $\mathcal{R}_q$ contains as a subgroup the group $E \rtimes C_{q+1}$ with $E = 2_-^{1+2f}$, and $C_{q+1}$ acting on $\mathcal{R}_q$ via the sum of its nontrivial irreducible representations.*

PROOF. This results from the fact that the pullback of $\mathcal{R}_q$ to the one-parameter system $\mathcal{K}_q$ on $\mathbb{G}_m/\mathbb{F}_2$ obtained by fixing $r = 0, t = 1$ has $E \rtimes C_{q+1}$ as its $G_{\mathrm{geom}}$. This pullback $\mathcal{K}_q$ has trace function given as follows. For $L/\mathbb{F}_2$ a finite extension, and $s \in L^\times$,

$$\mathrm{Trace}(\mathsf{Frob}_{s,L}|\mathcal{K}_q) = \frac{-1}{(1+i)^{\deg(L/\mathbb{F}_2)}} \sum_{x \in L} \psi_L(sx^{q+1} + x).$$

As explained in [**KRLT2**, Lemma 1.2], we have a geometric isomorphism

$$[\mathsf{inv}]^\star \mathcal{K}_q \cong \mathcal{K}l_\psi(\mathsf{Char}_{\mathrm{nontriv}}(q+1)).$$

We also have (by $x \mapsto xs$) a geometric isomorphism

$$[q+1]^\star [\mathsf{inv}]^\star \mathcal{K}_q \cong \mathrm{FT}_\psi(\mathcal{L}_{\psi(x^{q+1})}).$$

The local system $\mathcal{F}_q := \mathrm{FT}_\psi(\mathcal{L}_{\psi(x^{1+q})})$ is geometrically irreducible, and its $G_{\mathrm{geom},\mathcal{F}_q}$ is $E = 2_-^{1+2f}$, see Theorem 7.3.8. Thus

$$E = G_{\mathrm{geom},\mathcal{F}_q} \lhd G_{\mathrm{geom},[\mathsf{inv}]^\star \mathcal{K}_q}$$

is a normal 2-subgroup of index dividing $q + 1$.

In the terminology of [**Ka-LGE**, 1.5], $[\mathsf{inv}]^\star \mathcal{K}_q \cong \mathcal{K}l_\psi(\mathsf{Char}_{\mathrm{nontriv}}(q+1))$ is a canonical extension. Note that the local monodromy at 0 of $\mathcal{K}l_\psi(\mathsf{Char}_{\mathrm{nontriv}}(q+1))$ is cyclic of order $q+1$ and acts on $\mathcal{K}_q$ via the sum of its nontrivial irreducible representations. It results from [**Ka-LGE**, 1.4.12] that we have

$$G_{\mathrm{geom},[\mathsf{inv}]^\star \mathcal{K}_q} = G_{\mathrm{geom},\mathcal{K}l_\psi(\mathsf{Char}_{\mathrm{nontriv}}(q+1))} \cong G_{\mathrm{geom},\mathcal{F}_q} \rtimes C_{q+1}.$$

□

Our next result is concerned with the Pink-Sawin-Witt local systems:

THEOREM 9.3.7. *Let $q = 2^n \geq 16$. The following statements hold for the geometric monodromy group $G$ and the arithmetic monodromy group $G_{\mathrm{arith},k}$ of each of the local systems $\mathcal{W}(q+1, 1)$ of (9.2.0.4), $\mathcal{W}^\sharp(q+1, 1)$ of (9.2.0.5), and $\mathcal{R}_q$ of (9.3.4.1).*

(i) $G = \tilde{\Gamma}^\circ(q, 1) \cong (4 * 2_-^{1+2n}) \cdot \mathrm{Sp}_2(q)$.

(ii) *Over any finite extension $k$ of $\mathbb{F}_2$, for the arithmetic monodromy group $G_{\mathrm{arith},k}$ of either system over $k$ we have $G_{\mathrm{arith},k} = G$ if $k \supseteq \mathbb{F}_q$ and $G_{\mathrm{arith},k} \cong G \cdot \mathrm{Gal}(\mathbb{F}_q/k)$ if $k \subseteq \mathbb{F}_q$.*

PROOF. (a) By (9.2.4.1), it suffices to prove the statement for $\mathcal{W} := \mathcal{W}(q+1, 1)$ and $\mathcal{R}_q$. Let $G = G_{\mathrm{geom}}$, respectively $\tilde{G} = G_{\mathrm{arith},\mathbb{F}_2}$, denote the geometric, respectively arithmetic, monodromy group of $\mathcal{W}$. Let $H = G_{\mathrm{geom},\mathcal{R}_q}$, respectively $\tilde{H} = G_{\mathrm{arith},\mathcal{R}_q,\mathbb{F}_2}$, denote the geometric, respectively arithmetic, monodromy group of $\mathcal{R}_q$. The specialization $s = 1$ of $\mathcal{R}_q$ yields $\mathcal{W}$, showing $G \leq H$ and $\tilde{G} \leq \tilde{H}$. Let $V = \mathbb{C}^{2^{nf}}$ denote the underlying representation for $\tilde{H}$, with character say $\varphi$. By (9.2.4.1), we now have

$$H \geq G \geq G_{\mathrm{geom},\mathcal{G}(q+1,1)}, \ \tilde{H} \geq \tilde{G} \geq G_{\mathrm{arith},\mathcal{G}(q+1,1),\mathbb{F}_2}. \tag{9.3.7.1}$$

It then follows from Lemma 9.3.6 that

$$H \geq K := E \rtimes \langle g^* \rangle \tag{9.3.7.2}$$

where $E = 2^{1+2n}_{-}$ and $\langle g^* \rangle \cong C_{q+1}$. Note that $\tilde{H}$ is finite and $|\mathbf{Z}(\tilde{H})|$ divides 4 by Proposition 9.2.5. By assumption $n \geq 4$, hence $2^{2n} - 1$ admits a primitive prime divisor $\ell = \mathrm{ppd}(2, 2n)$ which divides $q + 1$.

Another consequence of the containments (9.3.7.1) is that we get an element $g \in \tilde{G}$ with

$$|\mathrm{Trace}(g^j)|^2 = 2^j, \text{ for any } j|f, \tag{9.3.7.3}$$

namely the element of $G_{\mathrm{arith}, \mathcal{G}(2^n+1,1), \mathbb{F}_2}$ given by the action of of $\mathsf{Frob}_{1,\mathbb{F}_2}$ on the sheaf $\mathcal{G}(n, 0; 2)$, cf. Lemma 8.5.2.

Now consider the local system

$$\hat{\mathcal{W}} := \hat{\mathcal{W}}(2^n + 1, 2^{n-1} + 1, \ldots, 2^2 + 1, 3, 1)$$

of Theorem 9.2.9. A suitable specialization of $\hat{\mathcal{W}}$ yields $\mathcal{R}$. This shows that

$$H \lhd \tilde{H} \leq \tilde{\Gamma}(2, n) = R \cdot \mathrm{Sp}_{2n}(2) \tag{9.3.7.4}$$

with $R = 4 * 2^{1+2n}_{\pm}$.

(b) Here we show that $\mathcal{Z}R = \mathcal{Z}E$ with $E = 2^{1+2n}_{-}$ from (9.3.7.2) and $\mathcal{Z} = \mathbf{Z}(\mathrm{GL}(V))$. To this end, we use (9.3.7.4) and the resulting action of $G$ via conjugation on $R$ which gives rise to the inclusion $\mathbf{Z}(R)G/R \hookrightarrow \mathrm{Out}^+(R) \cong \mathrm{Sp}(W) \cong \mathrm{Sp}_{2n}(2)$, where $W := R/\mathbf{Z}(R) \cong \mathbb{F}_2^{2n}$. Now the action of the subgroup $K = E \rtimes \langle g^* \rangle$ induces a subgroup $\bar{K}$ of $\mathrm{Sp}(W)$. Suppose that the image $\bar{E}$ of $E$ in $\bar{K}$ is nontrivial. Then $\mathbf{O}_2(\bar{K}) \neq 1$ and hence it has a nonzero proper fixed point subspace $W_1$ on $W$. In this case, the cyclic subgroup $\langle g^* \rangle$ of $K$ also acts on $W_1$, and as $\ell = \mathrm{ppd}(2, 2n)$, this action is trivial. By Lemma 7.2.1 applied to $R \lhd \tilde{\Gamma}(2, n)$, $|\varphi(g^*)|^2$ is either 0 or at least $|W_1| \geq 2$. On the other hand, $|\varphi(g^*)| = 1$ by Lemma 9.3.6, a contradiction.

We have shown that $E$ has trivial image in $\bar{K}$, which means $E$ only induces inner automorphisms of $R$, i.e. $E \leq \mathcal{Z}R$. Now, $\mathcal{Z} \cap E = \mathbf{Z}(E)$, so

$$\mathcal{Z}E/\mathcal{Z} \cong E/\mathbf{Z}(E) \cong W \cong R/\mathbf{Z}(R) \cong \mathcal{Z}R/\mathcal{Z},$$

whence $\mathcal{Z}E = \mathcal{Z}R$.

(c) With the result of (b) and using (9.3.7.2) and (9.3.7.4), we see that $\mathcal{Z}H \geq \mathcal{Z}R$ and $\bar{H} := \mathcal{Z}H/\mathcal{Z}R$ injects as a subgroup of $\mathrm{Out}^+(R) \cong \mathrm{Sp}_{2n}(2)$. At this point, we invoke Lemma 9.3.5 to conclude that $M_{2,2}(H) = M_{2,2}(\mathcal{Z}H) = 2$. As explained in [**GT2**, Lemma 5.1], the latter equality implies that the induced action of $\bar{H}$ on the nonzero vectors of $W = \mathcal{Z}R/\mathcal{Z}$ is transitive. Since $n \geq 4$, applying [**BNRT**, Theorem 5] we arrive at one of the following two possibilities:

($\alpha$) $n = bs$ for some integers $b, s \geq 1$, and $\mathrm{Sp}_{2b}(2^s) \lhd \bar{H} \leq \mathrm{Sp}_{2b}(2^s) \rtimes C_s$.

($\beta$) $n = 3s$ for some integer $s \geq 2$; and $G_2(2^s) \lhd \bar{H} \leq G_2(2^s) \rtimes C_s$.

In either case, as explained in the proof of Lemma 8.5.3, $\bar{G}$ contains a regular unipotent element $\bar{h}$ of $\mathrm{Sp}_{2b}(2^s)$ while acting on $W$ considered as $\mathbb{F}_{2^s}^{2b}$, i.e. $\bar{h}$ has $2^s$ fixed points on $W$. Applying Lemma 7.2.1, we see that the coset $\bar{h}$ in $\bar{H} = \mathcal{Z}H/\mathcal{Z}R$ contains an element $h \in H$ with $|\mathrm{Trace}(h)|^2 = 2^s$. On the other hand, as $h \in H = G_{\mathrm{arith}, \mathcal{R}_q, k}$ for some large enough extension $k \supseteq \mathbb{F}_q$, Proposition 9.2.5 applied to $k \supseteq \mathbb{F}_q$ ensures that $|\mathrm{Trace}(h)|^2$ is either 0 or a power of $q$. We have therefore shown that $2^s$ is a power of $q = 2^n$. Since $s|n$, we must have that $s = n$, and we are in $(\alpha)$ with $\mathrm{Sp}_2(q) \lhd \bar{H} \leq \mathrm{Sp}_2(q) \rtimes C_n$.

Taking the derived subgroup and using Lemma 9.2.7(ii), we see that $H \geq [\mathcal{Z}H, \mathcal{Z}H]$ contains the perfect subgroup $\tilde{\Gamma}^\circ(q,1) = \tilde{E} \cdot \mathrm{Sp}_2(q)$, and $\tilde{E} = R = \mathbf{Z}(R)E$.

The same arguments apply to $\tilde{H}$ since $M_{2,2}(\tilde{H}) = 2$. Recall that $H \lhd \tilde{H}$ and $\tilde{\Gamma}(2,n) = \tilde{E} \cdot \mathrm{Sp}_{2n}(2)$. Together with preceding results and (9.3.7.4), we have shown that

$$\tilde{\Gamma}^\circ(q,1) = \tilde{E} \cdot \mathrm{Sp}_2(q) \lhd H \lhd \tilde{H} \leq \tilde{E} \cdot (\mathrm{Sp}_2(q) \rtimes \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_2)).$$

In particular, $\tilde{H}/H \hookrightarrow C_n$, which implies that $G_{\mathrm{arith}, \mathcal{R}_q, k} = H$ whenever $k \supseteq \mathbb{F}_q$. Next we make use of the element $g$ in (9.3.7.3). We note that $\tilde{H} = \langle H, g \rangle$, simply because $g \in G_{\mathrm{arith}, \mathcal{R}_q, \mathbb{F}_2}$ is an $\mathbb{F}_2$-Frobenius. Denoting $d := |\tilde{H}/H|$, we then have $d|n$ and $g^d \in H = G_{\mathrm{arith}, \mathcal{R}_q, \mathbb{F}_q}$. By Proposition 9.2.5 applied to $k = \mathbb{F}_q$, $|\mathrm{Trace}(g^d)|^2$ is 0 or a power of $q$. But $|\mathrm{Trace}(g^d)|^2 = 2^d$, hence $2^d$ is a power of $q = 2^n$, hence $n|d$, and thus $d = n$. We have shown that $\tilde{H}/H \cong C_n$, and hence $H = \tilde{\Gamma}^\circ(q,1)$ and $\tilde{H} = \tilde{E} \cdot (\mathrm{Sp}_2(q) \rtimes C_n)$.

(d) As $\mathcal{R}_q^\circ$ is the Kummer pullback of $\mathcal{R}_q$ by $[s \mapsto s^{q+1}]$, the geometric monodromy group $H^\circ$ of $\mathcal{R}_q^\circ$ is a normal subgroup of $H$, with $H/H^\circ$ being cyclic. But $H = R \cdot \mathrm{Sp}_2(q)$ is perfect, so $H^\circ = H$. Applying Lemma 9.3.5, we then get $G = H$. On the other hand, $G \lhd \tilde{G} \leq \tilde{H} = H \cdot C_n$, so $|\tilde{G}/G|$ divides $n$ and $G = G_{\mathrm{arith}, \mathcal{W}, \mathbb{F}_q}$. Again using the element $g$ of (9.3.7.3) and arguing as above, we conclude $|\tilde{G}/G| = n$ and thus $\tilde{G} = \tilde{H}$. $\square$

For later use, we need to consider some analogues of $\mathcal{R}_q$ and $\mathcal{R}_q^\circ$. Fix $q = 2^f$ and odd integers $n > m \geq 1$. Consider the local system $\mathcal{R}(n,m;q)$ on $(\mathbb{A}^1 \times \mathbb{G}_m \times \mathbb{A}^1)/\mathbb{F}_2$ whose trace function is given as follows: for $L/\mathbb{F}_2$ a finite extension, and $(r,s,t) \in L^3, s \neq 0$,

$$\text{(9.3.7.5)} \qquad \mathrm{Trace}(\mathsf{Frob}_{(r,s,t),L} | \mathcal{R}(n,m;q)) := \frac{-1}{(1+i)^{\deg(L/\mathbb{F}_2)}} \sum_{x \in L} \psi_{2,L}([rx, sx^{q^n+1} + tx^{q^m+1}]),$$

and its Kummer pullback $\mathcal{R}^\circ(n,m;q)$ by $[s \mapsto s^{q^n+1}]$, whose trace function is given as follows: for $L/\mathbb{F}_2$ a finite extension, and $(r,s,t) \in L^3, s \neq 0$,
(9.3.7.6)

$$\mathrm{Trace}(\mathsf{Frob}_{(r,s,t),L} | \mathcal{R}^\circ(n,m;q)) := \frac{-1}{(1+i)^{\deg(L/\mathbb{F}_2)}} \sum_{x \in L} \psi_{2,L}([rx, s^{q^n+1}x^{q^n+1} + tx^{q^m+1}]).$$

Under the additional proviso that $\gcd(m, q+1) = 1$ (e.g. $m = 1$), we will also consider the pullback $\mathcal{G}(n,m;q)_{bis}$ of of $\mathcal{R}(n,m;q)$ by $r = 0$, $t = 1$, which is a local system on $\mathbb{G}_m$ whose trace function is given as follows: for $L/\mathbb{F}_2$ a finite extension, and $s \in L^\times$,

$$\text{(9.3.7.7)} \qquad \mathrm{Trace}(\mathsf{Frob}_{(s,L)} | \mathcal{G}(n,m;q)_{bis}) := \frac{-1}{\sqrt{\#L}} \sum_{x \in L} \psi_L(sx^{q^n+1} + x^{q^m+1}).$$

Note that this is the $p = 2$ analogue of the sheaves $\mathcal{W}_{bis}^{n,m}$ considered in [**KT6**, Theorem 10.6] for odd characteristics.

LEMMA 9.3.8. *Suppose the sheaf $\mathcal{R}^\circ(n,m;q)$ of* (9.3.7.6) *is geometrically irreducible. Then the sheaves $\mathcal{W}(q^n+1, q^m+1)$ as defined in* (9.2.0.4) *and $\mathcal{R}^\circ(n,m;q)$ have the same geometric, respectively arithmetic, monodromy groups.*

Proof. The change of variable $x \mapsto x/s$ shows that $\mathcal{R}^\circ(n,m;q)$ on $(\mathbb{A}^1 \times \mathbb{G}_m \times \mathbb{A}^1)/\mathbb{F}_2$ has the same trace function as the pullback of $\mathcal{W} := \mathcal{W}(q^n+1, q^m+1)$ on $(\mathbb{A}^1 \times \mathbb{A}^1)/\mathbb{F}_2$ by the map

$$\Phi : \mathbb{A}^1 \times \mathbb{G}_m \times \mathbb{A}^1 \to \mathbb{A}^1 \times \mathbb{A}^1 : \quad (r,s,t) \mapsto (r/s, t/s).$$

By hypothesis, $\mathcal{R}^\circ(n,m;q)$ is geometrically irreducible, and so arithmetically irreducible. By Chebotarev, it follows that we have an arithmetic isomorphism

$$\mathcal{R}^\circ(n,m;q) \cong \Phi^\star \mathcal{W},$$

as their arithmetic semisimplifications are isomorphic, and the source is arithmetically irreducible. Thus we have isomorphisms

$$G_{\mathrm{arith},\mathcal{R}^\circ(n,m;q)} \cong G_{\mathrm{arith},\Phi^\star\mathcal{W}}, \quad G_{\mathrm{geom},\mathcal{R}^\circ(n,m;q)} \cong G_{\mathrm{geom},\Phi^\star\mathcal{W}}.$$

The map $\Phi$ has a retraction

$$\Psi : \mathbb{A}^1 \times \mathbb{A}^1 \to \mathbb{A}^1 \times \mathbb{G}_m \times \mathbb{A}^1 : \quad (r,t) \mapsto (r,1,t).$$

Thus $\Psi^\star(\Phi^\star\mathcal{W}) = \mathcal{W}$, and hence $\mathcal{W}$ and $\Phi^\star\mathcal{W}$ have the same $G_{\mathrm{arith}}$ as each other and the same $G_{\mathrm{geom}}$ as each other, because each of these two local systems is the pullback of the other. Thus we have

$$G_{\mathrm{arith},\mathcal{R}^\circ(n,m;q)} \cong G_{\mathrm{arith},\mathcal{W}}, \quad G_{\mathrm{geom},\mathcal{R}^\circ(n,m;q)} \cong G_{\mathrm{geom},\mathcal{W}}.$$

□

Now we can prove the main result of this section, which, again for the first time, produces explicit local systems with geometric monodromy groups of shape $(4 * 2_-^{1+2nf}) \cdot \mathrm{Sp}_{2n}(2^f)$.

Theorem 9.3.9. *Assume $q = 2^f$, $r \geq 1$, and $n > m_1 > \ldots > m_r \geq 0$ are integers with $nf \geq 4$. Set*

$$A_0 := q^n + 1, \ \ \textit{and } A_i := q^{m_i} + 1 \textit{ for } 1 \leq i \leq r-1.$$

*If $m_r \geq 1$, we assume* $\gcd(n, m_1, \ldots, m_r) = 1$ *and set $A_r := q^{m_r} + 1$. If $m_r = 0$, we assume that $r \geq 2$ and* $\gcd(n, m_1, \ldots, m_{r-1}) = 1$, *and set $A_r := 1$. Then the following statements hold for the geometric monodromy group $G_{\mathrm{geom}}$ and the arithmetic monodromy group $G_{\mathrm{arith},k}$ of each of the local systems $\mathcal{W}(A_0, A_1, \ldots, A_r)$, $\mathcal{W}^\sharp(A_0, A_1, \ldots, A_r)$, and $\mathcal{W}^*(A_0, A_1, \ldots, A_r)$, introduced in* (9.2.0.4), (9.2.0.5), *and* (9.2.4.2).

(i) $G_{\mathrm{geom}} = \tilde{\Gamma}^\circ(q,n) \cong (4 * 2_-^{1+2nf}) \cdot \mathrm{Sp}_{2n}(q)$, *with the possible exception of the case $n = 3$, $f > 1$, $r = 1$, $m_1 = 1$, where we might instead have $G_{\mathrm{geom}} = (4 * 2_-^{1+6f}) \cdot G_2(q)$.* [This possible exception will be ruled out in Theorem 9.3.10.]

(ii) *Over any finite extension $k$ of $\mathbb{F}_2$, for the arithmetic monodromy group $G_{\mathrm{arith},k}$ of either system over $k$ we have $G_{\mathrm{arith},k} = G_{\mathrm{geom}}$ if $k \supseteq \mathbb{F}_q$ and $G_{\mathrm{arith},k} \cong G_{\mathrm{geom}} \cdot \mathrm{Gal}(\mathbb{F}_q/k)$ if $k \subseteq \mathbb{F}_q$.*

Proof. (a) By (9.2.4.1), it suffices to prove the statement for

$$\mathcal{W} := \mathcal{W}(A_0, A_1, \ldots, A_r) \text{ or } \mathcal{W}^*(A_0, A_1, \ldots, A_r).$$

If $r > 1$, let $G = G_{\mathrm{geom}}$, respectively $\tilde{G} = G_{\mathrm{arith},\mathbb{F}_2}$, denote the geometric, respectively arithmetic, monodromy group of $\mathcal{W}$ (the latter over $\mathbb{F}_2$).

In the case $r = 1$ (and so $m_1 \geq 1$), we also need to consider the sheaf $\mathcal{R} := \mathcal{R}(n, m_1; q)$ on $(\mathbb{A}^1 \times \mathbb{G}_m \times \mathbb{A}^1)/\mathbb{F}_2$ and its Kummer pullback $\mathcal{R}^\circ := \mathcal{R}^\circ(n, m_1; q)$ by $[s \mapsto s^{q^n+1}]$. Let

$G = G_{\mathrm{geom},\mathcal{R}}$, respectively $\tilde{G} = G_{\mathrm{arith},\mathcal{R},\mathbb{F}_2}$, denote the geometric, respectively arithmetic, monodromy group of $\mathcal{R}$.

Let $V = \mathbb{C}^{2^{nf}}$ denote the underlying representation for $\tilde{G}$ and $G$. A key observation for $G$ is that

$$M_{2,2}(G,V) = 2. \tag{9.3.9.1}$$

Indeed, if $r \geq 2$, this is a consequence of Theorems 9.3.2 applied to the pullback $s = 1$ of the sheaf $\mathcal{W}(A_0, \ldots, A_r)$. If $r = 1$, this is a consequence of Theorem 9.3.3 applied to (a pullback of) $\mathcal{R}$.

(b) By (9.2.4.1), we have

$$G \geq G_{\mathrm{geom},\mathcal{G}(A_0,A_1,\ldots,A_r)}, \ \tilde{G} \geq G_{\mathrm{arith},\mathcal{G}(A_0,A_1,\ldots,A_r),\mathbb{F}_2}. \tag{9.3.9.2}$$

The trace formula (9.2.0.3) shows that the local system $\mathcal{G}(A_0, A_1, \ldots, A_r)$ is the same as the local system $\mathcal{G}(n, m_1, \ldots, m_r; q)$ considered in §8.5, but with a different clearing factor (though one of the same absolute value). Note that a change of clearing factor does not affect the geometric monodromy group, nor does it affect the square absolute values of traces, and it preserves the image of the arithmetic monodromy group in $\mathrm{PGL}(V)$.

Note that $\tilde{G}$ is finite and $|\mathbf{Z}(\tilde{G})|$ divides 4 by Proposition 9.2.5. Assume for the moment that $2|nm_1 \ldots m_r$. It then follows from Theorems 8.5.8 and 8.5.9 that

$$\mathscr{Z}G \geq H^\circ := E \cdot S; \tag{9.3.9.3}$$

where $\mathscr{Z} := \mathbf{Z}(\mathrm{GL}(V))$, $E = 2^{1+2nf}_{-}$, and furthermore,

$$S := \Omega^-_{2n}(q)$$

if $m_r \geq 1$, or if $m_r = 0$ and $2|nm_1 \ldots m_{r-1}$, and

$$S := \mathrm{SU}_n(q)$$

if $m_r = 0$ and $2 \nmid nm_1 \ldots m_{r-1}$. By assumption $nf \geq 4$, hence $2^{2nf} - 1$ admits a primitive prime divisor $\ell = \mathrm{ppd}(2, 2nf)$. Now observe that $S$ contains a cyclic subgroup, of order $q^n + 1$ in the case $S = \Omega^-_{2n}(q)$, and of order $(q^n + 1)/(q + 1)$ in the case $S = \mathrm{SU}_n(q)$, which gives rise to a cyclic subgroup $\langle g^* \rangle$ of the same order in $H$; note that $\ell$ divides $\bar{\mathsf{o}}(g^*)$.

We now show that (9.3.9.3) (and hence the existence of the element $g^*$) also holds in the case $2 \nmid nm_1 \ldots m_r$ with

$$S \cong \mathrm{SU}_n(q)$$

and with $E \in \{E_1, 4 * E_1\}$ where $E_1 = 2^{1+2nf}_{\pm}$. Indeed, applying Theorem 8.5.7 to the pullback $r = 0$, we see that $\mathscr{Z}G$ contains a subgroup $S \cong \mathrm{SU}_n(q)$ acting in its total Weil representation. Since $G$ is irreducible, it follows from Theorem 8.4.5(b) that $G$ satisfies $(\mathbf{S}+)$ on $V$. Now, (9.3.9.1) allows us to apply [**GT2**, Theorem 1.5], see also [**BNRT**, Theorem 3], to $G$. However, since $\dim V = q^n$, the almost quasisimple case cannot occur. (Indeed, in such a case, either $\dim V = (2^a - (-1)^a)/3$ for some $a \geq \mathbb{Z}_{\geq 1}$ which is absurd, or $16 \leq 2^{nf} = \dim V = (3^a \pm 1)/2$ for some $a \in \mathbb{Z}_{\geq 4}$. If $2^{nf} = (3^a + 1)/2$, then $a$ is odd, in which case $2^{nf}$ has an odd divisor $(3^a + 1)/4 > 1$, a contradiction. Hence $2^{nf} = (3^a - 1)/2$ and $2|a$. If $4|a$, then $(3^a - 1)/2$ is divisible by 5, a contradiction. If $a \equiv 2 \pmod 4$, then $2^{nf}$ has an odd divisor $(3^{a/2} - 1)/2$, again a contradiction.) Hence the extraspecial case must occur, and therefore $G$ admits a normal subgroup $E$ with $E = E_1$ or $E = 4 * E_1$, where $E_1 = 2^{1+2nf}_{\pm}$. To complete the proof, we observe that $E \cap S = 1$. For, $E \cap S \leq \mathbf{O}_2(S)$ and so $E \cap S \leq \mathbf{Z}(S)$. But any nontrivial element$z$ of $\mathbf{Z}(S)$ has $|\mathrm{Trace}(z)| = 1$, whereas $|\mathrm{Trace}(y)| = 0$ or $q^n$ for any $y \in E$. Thus $G \geq E \rtimes S$.

(c) Another consequence of the containments (9.3.9.2) is that we get an element $g \in \tilde{G}$ with

$$|\mathrm{Trace}(g^j)|^2 = 2^j, \text{ for any } j|f, \tag{9.3.9.4}$$

namely the element of $G_{\mathrm{arith},\mathcal{G}(A_0,A_1,\dots,A_r),\mathbb{F}_2}$ given by the action of of $\mathsf{Frob}_{(0,0,\dots,1),\mathbb{F}_2}$ on the sheaf $\mathcal{G}(n, m_1, \dots, m_r; q)$, cf. Lemma 8.5.2.

Set $N := nf$, and consider the local system

$$\hat{\mathcal{W}} := \mathcal{W}(2^N + 1, 2^{N-1} + 1, \dots, 2^2 + 1, 3, 1).$$

A suitable specialization of $\hat{\mathcal{W}}$ yields $\mathcal{W}$, respectively $\mathcal{S}$, and so, by Theorem 9.2.9, this shows that

$$G \lhd \tilde{G} \leq \tilde{\Gamma}(2, N) = R \cdot \mathrm{Sp}_{2N}(2) \tag{9.3.9.5}$$

with $R = 4 * 2^{1+2N}_{\pm}$.

(d) Here we show that $\mathcal{Z}R \cap \mathcal{Z}H^\circ = \mathcal{Z}R = \mathcal{Z}E$ with $E = \mathbf{O}_2(H^\circ)$ from (9.3.9.3). To this end, we use (9.3.9.5) and the resulting action of $G$ via conjugation on $R$ which gives rise to the inclusion $\mathbf{Z}(R)G/R \hookrightarrow \mathrm{Out}^+(R) \cong \mathrm{Sp}(W) \cong \mathrm{Sp}_{2N}(2)$, where $W := R/\mathbf{Z}(R) \cong \mathbb{F}_2^{2N}$. Now the action of the subgroup $H^\circ = E \cdot S$ induces a subgroup $\bar{H}$ of $\mathrm{Sp}(W)$. Suppose that the image $\bar{E}$ of $E$ in $\bar{H}$ is nontrivial. Then $\mathbf{O}_2(\bar{H}) \neq 1$ and hence it has a nonzero proper fixed point subspace $W_1$ on $W$. In this case, the cyclic subgroup $\langle g^* \rangle$ from (b) also acts on $W_1$, and as $\ell = \mathrm{ppd}(2, 2N)$, this action is trivial. But $S$ is the normal closure of $\langle g^* \rangle$ in it, so $S$ acts trivially on $W_1$, and thus $\bar{H}$ acts trivially on $W_1$. We can apply the same argument to the action of $\bar{H}$ on the fixed point subspace of $\bar{E}$ on $W/W_1$. Repeating this process, we see that $\bar{H}$ is a unitriangular subgroup of $\mathrm{Sp}(W)$ and hence it is solvable. In particular, the perfect group $(H^\circ)^{(\infty)}$, which has $S/\mathbf{Z}(S)$ as its composition factor, acts trivially on $W$. By (9.2.6.1) and (9.2.6.2), this means that $(H^\circ)^{(\infty)}$ induces only inner automorphisms of $R$, and hence injects into a solvable subgroup of $\mathbf{N}_{\mathrm{GL}(V)}(R)$, a contradiction.

We have shown that $E$ has trivial image in $\bar{H}$, which means $E$ induces only inner automorphisms of $R$, i.e. $E \leq \mathcal{Z}R$. Now, $\mathcal{Z} \cap E = \mathbf{Z}(E)$, so

$$\mathcal{Z}E/\mathcal{Z} \cong E/\mathbf{Z}(E) \cong W \cong R/\mathbf{Z}(R) \cong \mathcal{Z}R/\mathcal{Z},$$

whence $\mathcal{Z}E = \mathcal{Z}R$. Since $S$ is quasisimple and $\mathcal{Z}R$ is solvable, we now have $\mathcal{Z}H^\circ \cap \mathcal{Z}R = \mathcal{Z}R$, as stated.

(e) With the result of (d) and using (9.3.9.3), we see that $\bar{G} := \mathcal{Z}G/\mathcal{Z}R$ injects as a subgroup of $\mathrm{Out}^+(R) \cong \mathrm{Sp}_{2N}(2)$ that contains $S$. At this point, we again use (9.3.9.1) which says that $M_{2,2}(G, V) = M_{2,2}(\mathcal{Z}G, V) = 2$. As explained in [**GT2**, Lemma 5.1], the latter equality implies that the induced action of $\bar{G}$ on the nonzero vectors of $W$ is transitive. Since $N = nf \geq 4$, applying [**BNRT**, Theorem 5] we arrive at one of the following two possibilities:

($\alpha$) $N = bs$ for some integers $b, s \geq 1$, and $\mathrm{Sp}_{2b}(2^s) \lhd \bar{G} \leq \mathrm{Sp}_{2b}(2^s) \rtimes C_s$.

($\beta$) $N = 3s$ for some integer $s \geq 2$; and $G_2(2^s) \lhd \bar{G} \leq G_2(2^s) \rtimes C_s$; set $b := 3$ in this case.

In either case, as explained in the proof of Lemma 8.5.3, $\bar{G}$ contains a regular unipotent element $\bar{h}$ of $\mathrm{Sp}_{2b}(2^s)$ while acting on $W$ considered as $\mathbb{F}_{2^s}^{2b}$, i.e. $\bar{h}$ has $2^s$ fixed points on $W$. Applying Lemma 7.2.1, we see that the coset $\bar{h}$ in $\bar{G} = \mathcal{Z}G/\mathcal{Z}R$ contains an element $h \in G$ with $|\mathrm{Trace}(h)|^2 = 2^s$. On the other hand, as $h \in G = G_{\mathrm{arith},k}$ for some large enough extension $k \supseteq \mathbb{F}_q$, Proposition 9.2.5 (and its proof) applied to $k \supseteq \mathbb{F}_q$ ensures that $|\mathrm{Trace}(h)|^2$ is either 0 or a power of $q$. We have therefore shown that $2^s$ is a power of $q$, i.e. $s = tf$ for some $t \in \mathbb{Z}_{\geq 1}$, $2^s = q^t$, and $2 \leq n = bt$.

Recalling $S \hookrightarrow \bar{G}$, we see that the quasisimple group $\mathrm{SU}_{bt}(q)$ embeds in $\mathrm{Sp}_{2b}(q^t)$ in $(\alpha)$, and in $G_2(q^t)$ in $(\beta)$. Comparing order, in the case of $(\alpha)$ we have

$$q^{b^2t^2-2} < |\mathrm{SU}_{bt}(q)| \leq |\mathrm{Sp}_{2b}(q^t)| < q^{2b^2t+bt},$$

whence $b^2t^2 \leq 2b^2t + bt + 1$, showing that $t \leq 2$ or $(b,t) = (1,3)$. However, when $(b,t) = (1,3)$ the Sylow 2-subgroups of $\mathrm{Sp}_{2b}(q^t) = \mathrm{Sp}_2(q^3)$ are abelian, so $\mathrm{SU}_{bt}(q) = \mathrm{SU}_3(q)$ cannot embed in $\mathrm{Sp}_{2b}(q^t)$. Consider the case $t = 2$. Then $n = bt$ is even, hence in fact $S = \Omega^-_{4b}(q)$ embeds in $\mathrm{Sp}_{2b}(q^2)$, and this is impossible by order comparison, unless $(b,n) = (1,2)$ in which case we have $S = [\bar{G}, \bar{G}]$. In such a case, $\mathcal{Z}H^\circ = \mathcal{Z}[G,G]$, whence

$$H^\circ = [\mathcal{Z}H^\circ, \mathcal{Z}H^\circ] = [[G,G],[G,G]] \lhd G.$$

But then, since $H^\circ$ is symplectically self-dual on $V$, $G$ fixes the 1-dimensional fixed point subspace of $H^\circ$ on $\wedge^2(V)$, and this contradicts $M_{2,2}(G) = 2$. Thus $t = 1$ in this case. Taking the derived subgroup and using Lemma 9.2.7(ii), we see that $G \geq [\mathcal{Z}G, \mathcal{Z}G]$ contains the perfect subgroup $\tilde{\Gamma}^\circ(q,n) = \tilde{E} \cdot \mathrm{Sp}_{2n}(q)$, and $\tilde{E} = R = \mathbf{Z}(R)E$.

In the case of $(\beta)$ we have

$$q^{9t^2-2} < |\mathrm{SU}_{3t}(q)| \leq |G_2(q)| < q^{14t},$$

whence $9t^2 \leq 14t + 1$, and so again $t = 1$, and $n = 3$. Since $\Omega^-_6(q)$ cannot embed in $G_2(q)$, in this case we must have that $2 \nmid nm_1 \ldots m_r$, i.e. $r = m_1 = 1$. Taking the derived subgroup and using Lemma 9.2.7(iii), we again see that $G \geq [\mathcal{Z}G, \mathcal{Z}G]$ contains the perfect $\tilde{E} \cdot G_2(q)$, and $\tilde{E} = R = \mathbf{Z}(R)E$; and in fact $G^{(\infty)} = \tilde{E} \cdot G_2(q)$. Assume in addition that $r \geq 2$. Then we observe that a pullback of $\mathcal{W}$ yields $\mathcal{W}(q^3+1, 1)$, which has (perfect by Lemma 9.2.7(ii)) geometric monodromy group $(4 * 2^{1+6f}_-) \cdot \mathrm{Sp}_2(q^3)$ by Theorem 9.3.7. It follows that an extension of $\mathrm{Sp}_2(q^3)$ by a 2-group embeds in $G_2(q)$. In particular, $G_2(q)$ contains a cyclic subgroup $C_{q^3+1}$, which is impossible (indeed, the largest order of semisimple elements in $G_2(q)$ is $q^2+q+1$). We have therefore ruled out $(\beta)$ unless $n = 3$ and $r = m_1 = 1$.

(f) Assume now that $(n, r, m_1) \neq (3,1,1)$. The arguments in (e) also apply to $\tilde{G}$, since we also have $M_{2,2}(\tilde{G}, V) = 2$. Recall that $G \lhd \tilde{G}$ and $\tilde{\Gamma}(2,N) = \tilde{E} \cdot \mathrm{Sp}_{2N}(2)$. Together with the results of (e) and (9.3.9.5), we have shown that

$$\tilde{\Gamma}^\circ(q,n) = \tilde{E} \cdot \mathrm{Sp}_{2n}(q) \lhd G \lhd \tilde{G} \leq \tilde{E} \cdot (\mathrm{Sp}_{2n}(q) \rtimes C_f).$$

In particular, $\tilde{G}/G \hookrightarrow C_f$, which implies that $G_{\mathrm{arith},k} = G$ whenever $k \supseteq \mathbb{F}_q$.

Next we make use of the element $g$ in (9.3.9.4). We note that $\tilde{G} = \langle G, g \rangle$, simply because $g \in G_{\mathrm{arith},\mathcal{W},\mathbb{F}_2}$ is an $\mathbb{F}_2$-Frobenius. Denoting $d := |\tilde{G}/G|$, we then have $d|f$ and $g^d \in G = G_{\mathrm{arith},\mathbb{F}_q}$. By Proposition 9.2.5 applied to $k = \mathbb{F}_q$, $|\mathrm{Trace}(g^d)|^2$ is 0 or a power of $q$. But $|\mathrm{Trace}(g^d)|^2 = 2^d$, hence $2^d$ is a power of $q = 2^f$, hence $f|d$, and thus $d = f$. We have shown that $\tilde{G}/G \cong C_f$, and hence $G = \tilde{\Gamma}^\circ(q,n)$, $\tilde{G} = \tilde{E} \cdot (\mathrm{Sp}_{2n}(q) \rtimes C_f)$. In particular, we are done if $r > 1$.

It remains to consider the case $r = 1$, still with $m_1 > 1$. As $\mathcal{R}^\circ$ is the Kummer pullback of $\mathcal{R}$ by $[s \mapsto s^{q^n+1}]$, the geometric monodromy group $G_{\mathrm{geom},\mathcal{R}^\circ}$ of $\mathcal{R}^\circ$ is a normal subgroup of $G$, with $G/G_{\mathrm{geom},\mathcal{R}^\circ}$ being cyclic. But $G = \tilde{\Gamma}^\circ(q,n)$ is perfect, so $G_{\mathrm{geom},\mathcal{R}^\circ} = G$; in particular, $\mathcal{R}^\circ$ is geometrically irreducible. Applying Lemma 9.3.8, we then get $G_{\mathrm{geom},\mathcal{W}} = G_{\mathrm{geom},\mathcal{R}^\circ} = G$. Now,

$$G = G_{\mathrm{geom},\mathcal{W}} \lhd G_{\mathrm{arith},\mathcal{W},\mathbb{F}_2} \leq \tilde{G} = G \cdot C_f,$$

so $|G_{\mathrm{arith},\mathcal{W},\mathbb{F}_2}/G_{\mathrm{geom},\mathcal{W}}|$ divides $f$ and $G_{\mathrm{geom},\mathcal{W}} = G_{\mathrm{arith},\mathcal{W},\mathbb{F}_q}$. Again using the element $g$ of (9.3.9.4) and arguing as above, we conclude $|G_{\mathrm{arith},\mathcal{W},\mathbb{F}_2}/G_{\mathrm{geom},\mathcal{W}}| = f$ and thus $G_{\mathrm{arith},\mathcal{W},\mathbb{F}_2} = \tilde{G}$.

In the case of $(\beta)$, which can possibly occur only when $(n,r,m_1) = (3,1,1)$, the same arguments using (9.3.9.4) as above first show that $G = \tilde{E} \cdot G_2(q)$ and $\tilde{G} = \tilde{E} \cdot (G_2(q) \rtimes C_f)$, and then that $G_{\mathrm{geom},\mathcal{W}} = G$ and $G_{\mathrm{arith},\mathcal{W},\mathbb{F}_2} = \tilde{G}$. □

As promised, we will now rule out the possible exception listed in Theorem 9.3.9(ii).

THEOREM 9.3.10. *Let $q = 2^f$ and let $n > m \geq 1$ be odd integers such that* $\gcd(n,m) = 1$ *and $(n,q) \neq (3,2)$.*

(i) *Suppose* $\gcd(m, q+1) = 1$. *Then the local system $\mathcal{G}(n,m;q)_{bis}$ of* (9.3.7.7) *has geometric monodromy group isomorphic to* $\mathrm{GU}_n(q)$, *acting via its total Weil representation with character $\tilde{\zeta}_n$ defined in* (8.4.0.1).

(ii) *Each of the local systems $\mathcal{R}(n,m;q)$ of* (9.3.7.5), *$\mathcal{R}^\circ(n,m;q)$ of* (9.3.7.6), *$\mathcal{W}(q^n+1, q^m+1)$ as defined in* (9.2.0.4), *and $\mathcal{W}^\sharp(q^n+1, q^m+1)$ as defined in* (9.2.0.5), *have geometric monodromy group $\tilde{\Gamma}^\circ(q,n) = (4 * 2_-^{1+2nf}) \cdot \mathrm{Sp}_{2n}(q)$.*

PROOF. (i) Let $V$ denote the underlying representation. Note that the Kummer pullback $\mathcal{K} = [q^m+1]^\star\mathcal{G}(n,m;q)$ of $\mathcal{G} := \mathcal{G}(n,m;q)$ has trace function at $s \in k^\times$

$$s \mapsto \frac{-1}{\sqrt{\#k}} \sum_{x \in L} \psi_k\bigl(x^{q^n+1} + (sx)^{q^m+1}\bigr) = \frac{-1}{\sqrt{\#k}} \sum_{x \in k} \psi_k\bigl((s^{-1}x)^{q^n+1} + x^{q^m+1}\bigr)$$

on $\mathbb{G}_m/k$. We will consider only extensions $k$ of $\mathbb{F}_{2^8}$, and so the clearing factors $-1/\sqrt{\#k}$ and $-1/(1+i)^{\deg(k/\mathbb{F}_2)}$ are the same. Then the pullback $\mathcal{K}'$ by $[s \mapsto s^{-1}]$ of the Kummer pullback $[q^n+1]^\star\mathcal{G}(n,m;q)_{bis}$ of $\mathcal{G}(n,m;q)_{bis}$ has trace function at $u \in L^\times$

$$s \mapsto \frac{-1}{\sqrt{\#k}} \sum_{x \in k} \psi_k\bigl((s^{-1}x)^{q^n+1} + x^{q^m+1}\bigr).$$

Thus $\mathcal{K}'$ and $\mathcal{K}$ have equal trace functions. So their geometric monodromy groups are the same $K_{\mathrm{geom}} = K'_{\mathrm{geom}}$ by Theorem 1.3.3.

The aforementioned pullback relationships imply that $K_{\mathrm{geom}}$ is a normal subgroup of $G_{\mathrm{geom},\mathcal{G}}$ with cyclic quotient of order dividing $q^m+1$. By Theorem 8.5.7, $G_{\mathrm{geom},\mathcal{G}} \cong \mathrm{SU}_n(q)$, acting on $V$ by its total Weil representation. Therefore, $K'_{\mathrm{geom}} = K_{\mathrm{geom}} \cong \mathrm{SU}_n(q)$. On the other hand, $K := K'_{\mathrm{geom}}$ is a normal subgroup of

$$L := G_{\mathrm{geom},\mathcal{G}(n,m;q)_{bis}}$$

with cyclic quotient of order dividing $q^n+1$, so we also have

$$K := [L,L] \cong \mathrm{SU}_n(q) \text{ and } |L/K| \text{ divides } q^n+1; \tag{9.3.10.1}$$

with $K$ acting on $V$ via its total Weil representation.

Our next observation is that $\mathcal{G}(n,m;q)_{bis}$ is also a pullback of the system

$$\hat{\mathcal{G}} := \mathcal{G}^\sharp(nf, nf-1, \ldots, 0; 2)$$

of Corollary 8.5.6, whence

$$L \leq G_{\mathrm{geom},\hat{\mathcal{G}}} = H_1^\circ = 2_-^{1+2nf} \cdot \Omega^-_{2nf}(2) < \mathrm{GL}(V). \tag{9.3.10.2}$$

Now we define

$$A = (q^n+1)/(q+1),\ B = (q^m+1)/(q+1),$$

which are coprime integers since $n, m$ are coprime odd integers, and make use of the additional condition that $\gcd(m, q+1) = 1$. In this case, as explained in [**KT6**, Remark 5.12], $\mathcal{G}(n,m;q)_{bis}$ is the pullback by $[s \mapsto s^{-1}]$ of the $[B]^\star$ Kummer pullback of the sheaf $\mathcal{H}^{n,m}_{bis}$, which itself is the direct sum of $q+1$ hypergeometric sheaves, 1 of rank $(q^n-q)/(q+1)$ and $q$ of rank $(q^n+1)/(q+1)$ each, see [**KT6**, (5.12.1)]. Again, clearing factors do not matter, since we work with geometric monodromy groups. A fortiori, this implies that $L$ acts on $V$ with $q+1$ summands, one of dimension $(q^n-q)/(q+1)$ and $q$ of dimension $(q^n+1)/(q+1)$ each. On the other hand, as stated in (9.3.10.1), the subgroup $K$ of $L$ acts on $V$ via its total Weil representation, whose irreducible summands have exactly these $q+1$ dimensions. Applying Theorem 8.4.4, we obtain that

$$L \leq C_2 \times M \text{ for some subgroup } M \cong \mathrm{GU}_n(q) \text{ of } \mathrm{GL}(V),$$

and furthermore $M$ acts on $V$ via its total Weil representation with character $\tilde{\zeta}_n$ defined in (8.4.0.1). In particular, $\mathrm{SU}_n(q) \cong K = [L,L] \leq [M,M] \cong \mathrm{SU}_n(q)$. It follows that $K = [M,M]$, and now we see that $L/K \leq C_2 \times M/K$ with $M/K \cong C_{q+1}$. On the other hand, $|L/K|$ is odd by (9.3.10.1), so $L/K \leq M/K$. We have shown that

$$\mathrm{SU}_n(q) \cong K \leq L \leq M \cong \mathrm{GU}_n(q). \tag{9.3.10.3}$$

Now, if $R$ denotes the geometric monodromy group of $\mathcal{H}^{n,m}_{bis}$, then

$$L \lhd R, \text{ with } R/L \cong C_e \text{ for some } e \text{ dividing } B = (q^m+1)/(q+1). \tag{9.3.10.4}$$

In particular, we again have $[R,R] = [L,L] = K$.

By our choice, $A - B \geq 2$, and moreover $B$ is coprime to $q+1$ as $\gcd(m, q+1) = 1$. Hence, if we choose $\chi$ to be a multiplicative character of $k \supseteq \mathbb{F}_{q^2}$ of order $q+1$, then $\chi^B \neq \mathbb{1}$. For such $\chi$, the summand $\mathcal{H}^\sharp_{big,A,\chi,B}$ of $\mathcal{H}^{n,m}_{bis}$, cf. [**KT6**, (5.12.1)], has geometric determinant $\mathcal{L}_\chi$ by [**KT6**, Lemma 3.2]. It follows that the action of $R$ on this summand has determinant of order $q+1$, and hence

$$q+1 \text{ divides } |R/K|.$$

Together with (9.3.10.4) and $\gcd(B, q+1) = 1$, this implies that $|L/K|$ is divisible by $q+1$. Using (9.3.10.3), we can now conclude that $L = M \cong \mathrm{GU}_n(q)$.

(ii) For $n > 3$, the statement has already been proved in Theorem 9.3.9. So, using Theorem 9.3.9 we may assume that $n = 3$ (so that $m = 1$) and that $\mathcal{R} := \mathcal{R}(n,m;q)$ has geometric monodromy group $G_{\mathrm{geom},\mathcal{R}} = (4 * 2_-^{1+6f}) \cdot G_2(q)$. Note that the pullback $r = 0,\ t = 1$

of $\mathcal{R}$ is precisely $\mathcal{G}(3,1;q)_{bis}$, which has geometric monodromy group $\mathrm{GU}_3(q)$ by the result of (i). It follows that $\mathrm{GU}_3(q)$ embeds in $G_2(q)$; in particular, $G_2(q)$ contains a cyclic subgroup of order $q^3+1$, which is impossible. □

Our second main result in this section shows that the Witt local systems in Theorems 9.3.7 and 9.3.9 are the only ones among $\mathcal{W}(A_0,\ldots,A_r)$ and $\mathcal{W}^\sharp(A_0,\ldots,A_r)$ that have finite monodromy.

THEOREM 9.3.11. *Let $r \geq 1$ and let $A_0 > A_1 > \ldots > A_r \geq 1$ be odd integers with $A_0 \geq 7$. Suppose that at least one (equivalently both) of the local systems $\mathcal{W}(A_0,A_1,\ldots,A_r)$ and $\mathcal{W}^\sharp(A_0,A_1,\ldots,A_r)$ in characteristic* 2*, as defined in* (9.2.0.4), (9.2.0.5)*, has finite geometric monodromy group. Then $\mathcal{W}(A_0,\ldots,A_r)$ and $\mathcal{W}^\sharp(A_0,\ldots,A_r)$ are as described in Theorems 9.3.7 and 9.3.9. More precisely, there exist integers $q=2^f$ and $n > m_1 > \ldots > m_r \geq 0$ such that*

$$A_0 = q^n+1,\ A_1 = q^{m_1}+1,\ldots,\ A_{r-1} = q^{m_{r-1}}+1,$$

*and either*

(i) *$m_r \geq 1$, $A_r = q^{m_r}+1$, and* $\gcd(n,m_1,\ldots,m_r)=1$*, or*
(ii) *$r \geq 2$, $m_r = 0$, $A_r = 1$, and* $\gcd(n,m_1,\ldots,m_{r-1})=1$*, or*
(iii) *$r=1$, $m_1=0$, and $A_1=1$.*

PROOF. (a) According to (9.2.4.1), both $\mathcal{W} := \mathcal{W}(A_0,\ldots,A_r)$ and $\mathcal{W}^\sharp := \mathcal{W}^\sharp(A_0,\ldots,A_r)$ have the same geometric monodromy group $G$, which is finite by hypothesis, and contains the geometric monodromy group $H$ of $\mathcal{G}(A_0,\ldots,A_r)$; in particular, $H$ is also finite. Let $V=\mathbb{C}^{A_0-1}$ denote the underlying representation.

First suppose that $r \geq 2$. Then by Theorem 9.3.2 the pullback $s=1,\ t_3=t_4=\ldots=t_r=0$ of $\mathcal{W}$ has $M_{2,2}=2$. It follows that

$$M_{2,2}(G,V)=2. \tag{9.3.11.1}$$

Suppose now that $r=1$. Then note that $\mathcal{W}^\sharp$ is the $[A_0]$ Kummer pullback of the local system $\mathcal{T}(0,A_0,A_1)$, which has $M_{2,2}=2$ by Theorem 9.3.3. Letting $\tilde{G}$ denote the geometric monodromy group of $\mathcal{T}(0,A_0,A_1)$, we then have

$$M_{2,2}(\tilde{G},V)=2,\ G \lhd \tilde{G},\ \tilde{G}/G \text{ is cyclic of order dividing } A_0. \tag{9.3.11.2}$$

Since we deal with geometric monodromy groups, we have that

$$\mathbb{Q}(\varphi) \subseteq \mathbb{Q}(i) \tag{9.3.11.3}$$

for the character $\varphi$ of $G$ acting on $V$. Note that $\tilde{G}^{(\infty)} = G^{(\infty)} \leq G$ in the case $r=1$, so (9.3.11.3) also applies to $\mathbb{Q}(\varphi|_{\tilde{G}^{(\infty)}})$. Now we will use (9.3.11.1), respectively (9.3.11.2), to apply [**GT2**, Theorem 1.5] and [**BNRT**, Theorem 3], to $G$, respectively to $\tilde{G}$, and arrive at one of the following three cases, for $L := G^{(\infty)}$. Recall that $\mathcal{W}$ has rank $D=A_0-1$, which is even.

(a1) *The Lie-type case.* Here, $L$ is quasisimple, and $L$ is a central quotient of $\mathrm{Sp}_{2n}(3)$ or $\mathrm{SU}_n(2)$, acting on a Weil representation of dimension $D=(3^n\pm1)/2$ or $D=(2^n-(-1)^n)/3$. In either case, $\mathbb{Q}(\varphi|_L)=\mathbb{Q}(\zeta_3)$, contradicting (9.3.11.3) (also, $D$ is odd in the latter case as well).

(a2) *The extraspecial case.* Here, $D = 2^N$, and $R \lhd G < \mathbf{N}_{\mathrm{GL}(V)}(R)$ for some $R = \mathbf{Z}(R)E$ and $E = 2_{\pm}^{1+2N}$ acting irreducibly on $V$.

(a3) *The sporadic case.* Here $L$ is a cover of some sporadic simple group that acts irreducibly on $V$. Using (9.3.11.3), among all the possibilities listed in [**BNRT**, Table I], we can rule out all but two possibilities

$$(L, D) = (2\mathsf{Ru}, 28),\ ({}^2B_2(8), 14). \tag{9.3.11.4}$$

(b) Now we will make use of the finiteness of $H$. Over extensions of $\mathbb{F}_{2^8}$, $\mathcal{G}(A_0, \ldots, A_r)$ has the same trace function as the local system $\mathcal{F}(A_0, \ldots, A_r, \mathbb{1})$ of Theorem 11.2.4. We can therefore apply Theorem 11.2.4 to the local system $\mathcal{F}(A_0, \ldots, A_r, \mathbb{1})$ in characteristic 2, and arrive at one of the following possibilities.

(b1) We are in case (ii) of Theorem 11.2.3. This means that we are also in (a2), and arrive at one of the conclusions (i)–(iii).

(b2) We are in case (iv) of Theorem 11.2.3. Then $(L, D) = (2G_2(4), 12)$. But this does not fit in either (a2) or (a3).

(b3) We are in case (iv) of Theorem 11.2.3 or case (iii) of Theorem 11.2.4. Here, there is some $q = 2^f$, so that $d \mid (q + 1)$ for $d := \gcd(A_0, A_1, \ldots, A_r)$, $A_0 = d(q^n + 1)/(q + 1)$, $A_i = d(q^{m_i} + 1)/(q + 1)$, $1 \le i \le r$, where $n > m_1 > \ldots > m_r \ge 1$ are odd integers with $\gcd(n, m_1, \ldots, m_r) = 1$. Moreover, $H$ is the image of $\mathrm{SU}_n(q)$ in a sub-representation of degree $D = A_0 - 1$ of the total Weil representation.

Assume in addition that we are in the case of (a3), so that (9.3.11.4) holds. Now we have that $(q^n + 1)/(q + 1)$ divides $D + 1$ and $D + 1$ divides $q^n + 1$ for $D = 14$ or 28. As $n \ge 3$, the first condition first implies that $(q, n) = (4, 3)$ or $(2, 5)$ or $(2, 3)$, none of which fits with the second condition.

It remains to consider the case of (a2), so that $D = 2^N$. Again we have that $(q^n+1)/(q+1)$ divides $D + 1 = 2^N + 1$ and $2^N + 1$ divides $q^n + 1$; furthermore, $D = A_0 - 1 \ge 6$ implies that $N \ge 3$. If $N = 3$, then since $2 \nmid n \ge 3$, we have $q = 2$, $n = 3$, $d = 3$, and so we arrive at (i). We may now assume that $N \ge 4$, and so $2^{2N} - 1$ admits a primitive prime divisor $\ell_1 = \mathrm{ppd}(2, 2N)$ by [**Zs**], which then divides $2^N + 1$. Hence $\ell_1$ divides $q^n + 1 = 2^{nf} + 1$, which implies that $2N|2nf$ and that $N|nf$; in particular, $nf \ge 4$. This in turn implies that $q^{2n} - 1$ admits a primitive prime divisor $\ell_2 = \mathrm{ppd}(2, 2nf)$ by [**Zs**], which then divides $(q^n+1)/(q+1)$. Hence $\ell_2$ divides $2^N + 1$, which implies that $2nf|2N$ and that $nf|N$. It follows that $N = nf$, and $d(q^n + 1)/(q + 1) = A_0 = 2^N + 1 = q^n + 1$, whence $d = q + 1$, and we again arrive at (i). $\square$

CHAPTER 10

# One-parameter families of exponential sums

## 10.1. Generalities

In this section and the next two sections, we fix a nontrivial additive character $\psi$ of $\mathbb{F}_p$, a pair of integers $A > B > 0$ with $p \nmid AB, \gcd(A,B) = 1$. We consider the local systems

$$\mathcal{F}(A,B) = \mathcal{F}_\psi(A,B,\mathbb{1}) = \mathcal{F}(A,B,\mathbb{1})$$

and

$$\mathcal{F}_\psi(A,B,\chi) = \mathcal{F}(A,B,\chi)$$

introduced in Definition 7.3.1. These local systems are closely related to hypergeometric sheaves, cf. [**KT6**, 3.10]. Recall that $\mathsf{Char}(A)$ is the set of all characters of order dividing $A$, $\mathsf{Char}_{\rm ntriv}(A) = \mathsf{Char}(A) \smallsetminus \{\mathbb{1}\}$, and $\mathsf{Char}(A,\chi)$ is the set of characters $\rho$ with $\rho^a = \chi$. We defined

$$\mathcal{H}_{small,A,B} := \mathcal{H}yp\big(\mathsf{Char}_{\rm ntriv}(A), \mathsf{Char}_{\rm ntriv}(B)\big), \quad \mathcal{H}_{big,A,B,\chi} := \mathcal{H}yp\big(\mathsf{Char}(A); \mathsf{Char}(B,\overline{\chi})\big),$$

(see also (8.5.4.1), (8.5.4.2)). Recall the following result.

THEOREM 10.1.1. ([**KT6**, 3.10]) *We have geometric isomorphisms*

$$[A]^\star\mathcal{H}_{small,A,B} \cong [t \mapsto -At/B]^\star\mathcal{F}(\psi_{-B},A,B)$$

*and, for $\chi^A \neq \mathbb{1}$,*

$$[A]^\star\mathcal{H}_{big,A,B,\chi} \cong [t \mapsto -At/B]^\star\mathcal{F}(\psi_{-B},A,B,\chi^A).$$

THEOREM 10.1.2. *Suppose the local system $\mathcal{F}(A,B,\chi)$ on $\mathbb{A}^1/\mathbb{F}_{q^2}$ has finite geometric monodromy group $G_{\rm geom}$. Then the"half Tate twist"*

$$\mathcal{G}(A,B,\chi) := \mathcal{F}(A,B,\chi)(1/2) := \mathcal{F}(A,B,\chi) \otimes \big(q^{-\deg/\mathbb{F}_{q^2}}\big)$$

*has finite arithmetic monodromy group $G_{\rm arith}$.*

PROOF. The statement is invariant under finite extension of scalars, so we may work over an extension $E$ of $\mathbb{F}_{q^2}$ over which the hypergeometric sheaves of Theorem 10.1.1 are defined. One then checks that the constant field twists which (implicitly) occur in its proof are $\pm 1$ times powers of $\sqrt{\#E}$. This fact results from the Hasse-Davenport identity via [**Ka-GKM**, 5.6.2]. See [**KT3**, 7.1,7.2, 8.1, 8.2] and [**KRLT2**, 1.1,1.2] for complete details. Once we have this, the theorem then follows from [**KT7**, Corollary 14.15], applied to the hypergeometric sheaves of Theorem 10.1.1. □

LEMMA 10.1.3. *Suppose $\mathcal{F}(A,B,\theta)$ is Lie irreducible and Lie self-dual. Then $\mathcal{F}(A,B,\theta)$ is self-dual.*

PROOF. In view of Theorem 10.1.1, this results from Corollary 2.4.8, applied to either $\mathcal{H}_{small,A,B}$ or to $\mathcal{H}_{big,A,B,\chi}$. □

Lemma 10.1.4. *Suppose $A - B \geq 2$ and $\mathcal{F}(A, B, \theta)$ has $G^{\circ}_{\mathrm{geom}} = \mathrm{SL}_D$ (for $D :=$ the rank of $\mathcal{F}(A, B, \theta)$). Then $\mathcal{F}(A, B, \theta)$ has $G_{\mathrm{geom}} = \mathrm{SL}_D$.*

Proof. In view of Theorem 10.1.1, this results from Corollary 2.4.10, applied to either $\mathcal{H}_{small,A,B}$ or to $\mathcal{H}_{big,A,B,\chi}$. □

Theorem 10.1.5. *Suppose $A - B = 1$ and $\mathcal{F}(A, B, \theta)$ has infinite $G_{\mathrm{geom}}$. Then $G^{\circ}_{\mathrm{geom}} = \mathrm{SL}_D$ (for $D :=$ the rank of $\mathcal{F}(A, B, \theta)$), and $\mathcal{F}(A, B, \theta)$ has $G_{\mathrm{geom}} = \{\gamma \in \mathrm{GL}_D | \det(\gamma)^p = 1\}$.*

Proof. In view of Theorem 10.1.1, this results from Theorem 4.1.1, which asserts that $G^{\circ}_{\mathrm{geom}} = \mathrm{SL}_D$, together with Remark 2.4.11, applied to either $\mathcal{H}_{small,A,B}$ or to $\mathcal{H}_{big,A,B,\chi}$. □

Theorem 10.1.6. *Let $A > B > 0$ with $\gcd(A, B) = 1$ and $p \nmid AB$, and $\theta$ a (possibly trivial) multiplicative character. Then we have the following results about the possible self-duality of $\mathcal{F}(A, B, \theta)$.*

(i) *If $AB$ is even, then $\mathcal{F}(A, B, \theta)$ is not geometrically self-dual.*
(ii) *If $AB$ is odd and $\theta$ has order $> 2$, then $\mathcal{F}(A, B, \theta)$ is not geometrically self-dual.*
(iii) *If $AB$ is odd, then $\mathcal{F}(A, B, \mathbb{1})$ is geometrically self-dual, and the self-duality is symplectic.*
(iv) *If $AB$ is odd and $p \neq 2$, then $\mathcal{F}(A, B, \chi_2)$ is geometrically self-dual, and the self-duality is orthogonal.*

Proof. We first note that statements (iii) and (iv) hold because when $AB$ is odd, $\mathcal{H}_{small,A,B}$ and $\mathcal{H}_{big,A,B,\chi_2}$ are themselves self-dual of the asserted type, as results from [**Ka-ESDE**, Theorems 8.8.1 and 8.8.2].

We now turn to proving (i) and (ii). In general, for a lisse, geometrically irreducible $\mathcal{F}$ on $\mathbb{A}^1/\mathbb{F}_q$ which is pure of weight one, $\mathcal{F}$ is self-dual if and only if the cohomology group $H^2_c(\mathbb{A}^1/\overline{\mathbb{F}_p}, \mathcal{F} \otimes \mathcal{F})$ is nonzero (in which case it is automatically of dimension one). This cohomology group is pure of weight 4, whereas $H^1_c(\mathbb{A}^1/\overline{\mathbb{F}_p}, \mathcal{F} \otimes \mathcal{F})$ is mixed of weight $\leq 3$. So we use the Lefschetz trace formula to compute the dimension of the $H^2_c$ as the limsup over growing finite extensions $k/\mathbb{F}_{q_0}$ (for any choice of $q_0$ such that $\theta$ began life over $\mathbb{F}_{q_0}$ and which contains the $B^{\mathrm{th}}$ roots of $\pm 1$) of the quantity

$$(1/\#k)^2 \sum_{t \in k} (-\sum_{x \in k} \psi_k(x^A + tx^B)\theta_k(x))^2 =$$

$$= (1/\#k)^2 \sum_{t \in k} \sum_{x,y \in k} \psi_k(x^A + y^A + t(x^B + y^B))\theta_k(xy) =$$

$$(1/\#k) \sum_{x,y \in k \text{ with } x^B + y^B = 0} \psi_k(x^A + y^A)\theta_k(xy).$$

Suppose first that $B$ is odd. Then the sum is over $(x, y)$ with $y^B = (-x)^B$, so with the exception of the single point $(0, 0)$, we have $y = -\zeta x$ for $\zeta \in \mu_B(\overline{\mathbb{F}_p})$. So up to an error of at most $(B + 1)/\#k$, our sum is

$$(1/\#k) \sum_{\zeta \in \mu_B} \sum_{x \in k} \psi_k(x^A + (-\zeta x)^A)\theta_k(-\zeta x^2).$$

If $A$ is even, then $p \neq 2$, and $x^A + (-\zeta x)^A = (1+\zeta^A)x^A$. Here $\zeta^A$ is a root of unity of odd order (a divisor of $B$), so is not $= 1$. Hence each $\zeta$ summand is of the form

$$\theta_k(-\zeta)\sum_x \psi_k((\text{nonzero coeff.})x^A)\theta_k^2(x),$$

which by Weil is bounded in absolute value by $A\sqrt{\#k}$. So the limsup vanishes.

Still with $B$ odd, suppose also that $A$ is odd, but that $\theta^2 \neq \mathbb{1}$. Then in the calculation of the last paragraph, the coefficient $1+(-\zeta)^A = 1-\zeta^A$ will vanish precisely for $\zeta = 1$ (because $\gcd(A,B) = 1$). Thus each of the $B-1$ terms with $\zeta \neq 1$ is bounded in absolute value by $A\sqrt{\#k}$, and the term with $\zeta = 1$ is

$$\theta_k(-\zeta)\sum_x \theta_k^2(x) = 0,$$

and again the limsup vanishes.

Finally we must treat the case when $B$ is even and $A$ is odd. Here we first choose $\gamma$ with $\gamma^B = -1$. Then $x^B + y^B = 0$ leads to $y = \zeta\gamma x$, with $\zeta \in \mu_B$. Here each coefficient $1+\zeta^A\gamma^A$ of $x^A$ inside the $\psi$ is nonzero; indeed, if $\zeta^A\gamma^A = -1$, then taking $B^{\text{th}}$ powers gives $\zeta^{AB}\gamma^{AB} = (\gamma^B)^A = (-1)^A = -1$, whereas $(-1)^B = 1$. So each individual summand is again bounded in absolute value by $A\sqrt{\#k}$, and so the limsup vanishes. □

We now analyze the primitivity of the systems $\mathcal{F}(A,1,\chi)$. We do more than primitivity, but not for $\mathcal{F}$, rather for $\mathcal{H}$. Strictly speaking, in Lemmas 10.1.7 and 10.1.8 we do not address the question of $(\mathbf{S}+)$ for the geometric monodromy group $G$ of $\mathcal{F}(A,B,\chi)$, but only for the geometric monodromy group $H$ of the hypergeometric sheaf of which it is a Kummer pullback. It is true that this is all that is needed in the proofs later, where we work with the group $H$ and never require that $G$ has $(\mathbf{S}+)$; in the subsequent cases, it follows from our determination of $G$ that $G$ indeed satisfies $(\mathbf{S}+)$. Nonetheless, it seems like a natural question to study $(\mathbf{S}+)$ for $G$ directly.

Lemma 10.1.7. (i) *Suppose $A \geq 2$ and $p \nmid A$. Then any geometrically irreducible hypergeometric sheaf $\mathcal{H}$ of type $(A,1)$, in particular any $\mathcal{H}_{big,A,1,\chi}$ with $\chi \neq \mathbb{1}$, satisfies* $(\mathbf{S}+)$.

(ii) *Suppose $A \geq 3$, $p \nmid A$. Then the local system $\mathcal{H}_{small,A,1}$ satisfies* $(\mathbf{S}+)$ *except possibly when $(A,p) = (9,2)$, $(5,2)$, $(5,3)$, in which cases it is primitive and has finite monodromy. If $A = 5$ and $p \geq 7$, it has $G_{\text{geom}} = \mathrm{Sp}_4$.*

Proof. (i) It is obvious that such an $\mathcal{H}$ cannot be Kummer induced. If it were Belyi induced, then $A$ would be a power of $p$, as one sees from checking the cases in [**KRLT3**, Proposition 1.2]. Thus $\mathcal{H}$ is primitive. Then by Theorem 5.2.9, $\mathcal{H}$ has $(\mathbf{S}+)$ if $A$ is none of $4, 8, 9$. Now apply [**KT5**, Theorem 1.9]. The cases $A = 4, 8$ have $(\mathbf{S}+)$ because $p \neq 2$ when $A = 4, 8$, and the case $A = 9$ has $(\mathbf{S}+)$ because $p \neq 3$ when $A = 9$.

(ii) It is visible that $\mathcal{K} = \mathcal{H}_{small,A,1}$ is not Kummer induced, and no Kloosterman sheaf is Belyi induced. Hence $\mathcal{K}$ is primitive of rank $A-1$. Now apply Theorem 1.2.1, which omits the case $(A,p) = (9,2)$ and the case $A = 5$. In the $(9,2)$ case, $A = q+1$ for $q = 2^3$, which is a Pink–Sawin case [**KT1**, 20.3]. Suppose now $A = 5$. For $p = 2$, we have a Pink–Sawin case, and for $p = 3$ we have an $A = (q+1)/2$ case, finite by the van der Geer–van der Vlugt argument. It remains to show that for $p \geq 7$, we have $G_{\mathrm{geom}} = \mathrm{Sp}_4$ (which automatically has $(\mathbf{S}+)$).

For this, we argue as follows. $\mathcal{K} = \mathcal{H}_{small,A,1}$ is symplectic by [**Ka-ESDE**, 8.8.1-2]. So it suffices to show that its Kummer pullback $[5]^{\star}\mathcal{H}_{small,A,1} = \mathcal{F}(A,1,\mathbb{1})$ has $G_{\mathrm{geom}} = \mathrm{Sp}_4$. $\mathcal{F}(A,1,\mathbb{1})$ is lisse on $\mathbb{A}^1$ of rank 4. So $\mathcal{F}(5,1,\mathbb{1})$ is primitive, because in characteristic $p \geq 5$, the affine line has no nontrivial finite étale coverings of degree dividing 4. By [**Ka-MG**, Prop.1], either $\mathcal{F}(5,1,\mathbb{1})$ is Lie-irreducible, or it is a tensor product $\mathcal{A} \otimes \mathcal{B}$ of local systems on $\mathbb{A}^1$ with $\mathcal{A}$ Lie-irreducible and $\mathcal{B}$ irreducible with finite monodromy group $\Gamma$. We cannot have $\mathcal{B}$ of rank 4, because $\mathcal{F}$ has geometrically trivial determinant, which would force $\mathcal{A}$ to be of finite order. If $\mathcal{B}$ has rank 2, then its Sylow $p$-subgroups are normal and abelian by Feit-Thompson. Then the quotient $\Gamma/\Gamma_{p-\mathrm{Sylow}}$ is a prime to $p$ quotient of $\pi_1(\mathbb{A}^1)$, so trivial. Thus $\Gamma$ is an abelian $p$-group, again impossible since it has a 2-dimensional irreducible representation. Thus $\mathcal{F}(5,1,\mathbb{1})$ is Lie-irreducible. So its $G_{\mathrm{geom}}$ is a subgroup of $\mathrm{Sp}_4$ whose identity component is irreducible. The only possibilities for $G^{\circ}_{\mathrm{geom}}$ are either $\mathrm{Sp}_4$ itself or the image of $\mathrm{SL}(V) \cong \mathrm{SL}_2$ on $\mathrm{Sym}^3(V)$. The second case is ruled out by Theorem 6.1.5. Therefore $\mathcal{F}(5,1,\mathbb{1})$ has $G_{\mathrm{geom}} = \mathrm{Sp}_4$ in characteristic $p \geq 7$ and hence also $(\mathbf{S}+)$. □

The following lemma is the $(A,B)$ counterpart of Lemma 10.1.7.

LEMMA 10.1.8. *Let $A > B \geq 2$, $\gcd(A,B) = 1$, and $p \nmid AB$. Then we have the following results.*

(i) *$\mathcal{H}_{small,A,B}$ is primitive.*
(ii) *For all tame $\chi$ with $\chi^A \neq \mathbb{1}$, $\mathcal{H}_{big,A,B,\chi}$ is primitive.*

PROOF. (a) We first show that neither $\mathcal{H}_{small,A,B}$ nor $\mathcal{H}_{big,A,B,\chi}$ is Kummer induced. In the case of $\mathcal{H}_{big,A,B,\chi}$ this is obvious, because it has type $(A,B)$ with $\gcd(A,B) = 1$. If $\mathcal{H}_{small,A,B}$ were Kummer induced, necessarily by $[d]_{\star}$ for some $d > 1$ a prime to $p$ divisor of $\gcd(A-1,B-1)$, then the "upstairs" characters would be stable by multiplication by a character $\rho_d$ of order $d$. Thus if $\sigma$ is an "upstairs" character, so also is $\rho_d\sigma$, and thus $\rho_d$ is a ratio of two "upstairs" characters. But any ratio of two "upstairs" characters has order dividing $A$, hence $d|A$. But $\mathcal{H}_{small,A,B}$ has type $(A-1,B-1)$, so $\rho_d$ has order dividing $A-1$. Hence $\rho_d$ has order dividing $\gcd(A,A-1) = 1$.

(b) We now must show that neither $\mathcal{H}_{small,A,B}$ nor $\mathcal{H}_{big,A,B,\chi}$ is Belyi induced. We argue by contradiction. From [**KRLT3**, Proposition 1.2], we see that if Belyi induced, it is $f_{\star}(\mathcal{L}_{\sigma}(x) \otimes \mathcal{L}_{\rho}(1-x))$ for $f$ either $x^a(1-x)^b$ or $1/x^a(1-x)^b$, some tame characters $\sigma, \rho$, with the following extra information. Of the three quantities $a, b, a+b$, precisely one of them is divisible by $p$. If $p|(a+b)$, then we use $f = x^a(1-x)^b$, otherwise we use $f = 1/x^a(1-x)^b$. We may assume $d := \gcd(a,b) = 1$, otherwise $f = g^d$ with $p \nmid d$, hence $f_{\star} = [d]_{\star}f_{\star}$, and we would be Kummer induced by $[d]_{\star}$.

We must consider four cases: whether or not $p|(a+b)$, and whether $\mathcal{H}_{small,A,B}$ or $\mathcal{H}_{big,A,B,\chi}$.

(b1) If $p|(a+b)$, say $a+b = p^n c$ with $p \nmid c$ and $n \geq 1$, then the upstairs characters are the $a^{\mathrm{th}}$ roots of $\sigma$ together with the $b^{\mathrm{th}}$ roots of $\rho$. The downstairs characters are all the $c^{\mathrm{th}}$ roots of $(\sigma\rho)^{1/p^n}$. If this is $\mathcal{H}_{big,A,B,\chi}$, then $c = B$ and $a+b = A$. But then $A = p^n B$, contradicting the fact that $p \nmid A$.

If this is $\mathcal{H}_{small,A,B}$, then we look at ratios of pairs of distinct upstairs characters. If $a > 1$, these ratios include all characters of order dividing $a$, but all such ratios have order dividing

$A$, hence $a|A$ if $a>1$. It is trivially true that $a|A$ if $a=1$. Thus in all cases $a|A$. Similarly, $b|A$. Because $\gcd(a,b)=1$, we have $ab|A$, say $A=Mab$ for some integer $M\geq 1$. But for $\mathcal{H}_{small,A,B}$, we have $a+b=A-1$. Thus we have

$$Mab=a+b+1,\quad \gcd(a,b)=1,$$

which we rewrite as

$$(M+1)ab=(a+1)(b+1).$$

Since $a$ divides $(M+1)ab$, it divides $(a+1)(b+1)$. But $\gcd(a,a+1)=1$, so $a|(b+1)$. Similarly $b|(a+1)$. Thus $a\leq b+1$ and $b\leq a+1$, hence $a\leq b+1\leq a+2$, i.e.

$$a-1\leq b\leq a+1.$$

Thus $b$ is one of $a-1,a,a+1$.

If $b=a$, then $b=a=1$, because $\gcd(a,b)=1$.

If $b=a-1$, then $Ma(a-1)=1+a+a-1=2a$, hence $M(a-1)=2$. So either $M=2,a=2$ and $b=1$ or $M=1,a=3$ and $b=2$.

If $b=a+1$, then $Ma(a+1)=1+a+a+1=2(a+1)$, hence $Ma=2$. So either $M=2,a=1$ and $b=2$ or $M=1,a=2$ and $b=3$.

Thus the cases we must rule out are $(a,b)=(1,1),(2,1),(3,2),(1,2),(2,3)$.

When $(a,b)=(1,1)$ and $p|(a+b)$ then $p=2$, our $\mathcal{H}_{small,A,B}$ has type $(2,1)$, so it is $\mathcal{H}_{small,3,2}$, but this is not allowed in characteristic 2 as $p|B$ here. When $(a,b)$ is $(1,2)$ or $(2,1)$, then $p=3$, our $\mathcal{H}_{small,A,B}$ has type $(3,1)$, so it is $\mathcal{H}_{small,4,2}$. Here the upstairs characters are $\chi_4,\chi_4\chi_2,\chi_2$, and they are (up to interchanging $a,b$) the character $\sigma$ together with both square roots $\alpha,\beta$ of $\rho$. The character $\rho$, being $\alpha^2$, has order 1 or 2. It cannot be trivial, otherwise $\mathbb{1}$ is among its square roots. Therefore $\rho=\chi_2$, whose square roots are the characters of order 4. Then $\sigma$ must be $\chi_2$. But then $\sigma\rho=\mathbb{1}$, and so the downstairs character is $\mathbb{1}$. But the downstairs character of $\mathcal{H}_{small,4,2}$ is $\chi_2$, not $\mathbb{1}$. Finally, if $(a,b)$ is $(2,3)$ or $(3,2)$, then $p=5$, the upstairs characters are the square roots of $\sigma$ together with the cube roots of $\rho$. But these characters are also the nontrivial characters of order dividing 6, namely $\chi_2,\chi_3,\chi_3^2,\chi_3\chi_2,\chi_3^2\chi_2$. Then $\rho$, whose cube roots have order dividing 6, has order dividing 2. It cannot be trivial, otherwise $\mathbb{1}$ is among its cube roots. Therefore $\rho=\chi_2$, whose cube roots are $\chi_2,,\chi_3\chi_2,\chi_3^2\chi_2$. Then the square roots of $\sigma$ are the two characters of order 3. But this is nonsense, as their ratio is not $\chi_2$. This completes the proof in the case $p|(a+b)$.

(b2) If $p\nmid(a+b)$, then either $p|a$ or $p|b$. Interchanging $0,1$ by $x\mapsto 1-x$, we may assume $p|a$, say $a=p^nc$ with $p\nmid c$ and $n\geq 1$. The upstairs characters are the $(a+b)^{\text{th}}$ roots of $\sigma\rho$. The downstairs characters are the $c^{\text{th}}$ roots of $\sigma^{1/p^n}$ together with the $b^{\text{th}}$ roots of $\rho$. Ratios of pairs of distinct upstairs characters give all nontrivial characters of order dividing $(a+b)$. But the upstairs characters of either $\mathcal{H}_{small,A,B}$ or $\mathcal{H}_{big,A,B,\chi}$ are all of order dividing $A$, hence $(a+b)|A$. In the case of $\mathcal{H}_{small,A,B}$, we have $a+b=A-1$, so that $(A-1)|A$, nonsense because $A\geq 3$.

We now treat the case of $\mathcal{H}_{big,A,B,\chi}$. By the same "ratios of pairs of distinct characters", applied to the downstairs characters, we see that $c|B$ and $b|B$. As $\gcd(a,b)=1$, we have $\gcd(c,b)=1$, and hence $bc|B$. Thus $B=Mbc$ for some integer $M\geq 1$. But $B=b+c$, thus

$$Mbc=b+c,\quad \gcd(b,c)=1.$$

Because $b$ divides $Mbc$, we get $b|c$. Similarly, we get $c|b$. Thus $b = c$ and $B = 2b$. This forces $p \neq 2$. But $A = a + b = p^n c + b = (p^n + 1)b = (\frac{p^n+1}{2})B$. Thus $B|A$, and $B \geq 2$, and so the condition $\gcd(A, B) = 1$ is violated. □

Corollary 10.1.9. *Let $A > B \geq 2$, $\gcd(A, B) = 1$, and $p \nmid AB$. Then we have the following results.*

(i) *If $A \neq 5, 9, 10$, then $\mathcal{H}_{small,A,B}$ satisfies* $(\mathbf{S}+)$.

(ii) *If $A \neq 4, 8, 9$, then for all tame $\chi$ with $\chi^A \neq \mathbb{1}$, $\mathcal{H}_{big,A,B,\chi}$ satisfies* $(\mathbf{S}+)$.

(iii) *For each of $(A, B) = (5, 2), (9, 2), (9, 4), (10, 3)$, in any characteristic $p \nmid AB$, $\mathcal{H}_{small,A,B}$ satisfies* $(\mathbf{S}+)$.

(iv) *For each of $(A, B) = (8, 3), (9, 2)$ in any characteristic $p \nmid AB$ and for any $\chi \neq \mathbb{1}$, $\mathcal{H}_{big,A,B,\chi}$ satisfies* $(\mathbf{S}+)$.

Proof. For (i) and (ii), primitivity is given by Lemma 10.1.8. Then apply Theorem 5.2.9. For (iii) and (iv), apply [**KT5**, Theorem 1.11]. □

Recall that an element $\gamma$ of a finite subgroup $G$ of $\mathrm{GL}_n(\mathbb{C})$, $n \geq 2$, is called *quadratic* if it has precisely two distinct eigenvalues. If the eigenvalue 1 occurs in $\gamma$, the codimension of the 1-eigenspace is called the *drop* of $\gamma$. [Thus a quadratic element of drop 1 is a complex reflection (:= a pseudoreflection of nontrivial determinant).

Recall also the following well-known theorem.

Theorem 10.1.10. *Suppose $G < \mathrm{GL}_n(\mathbb{C})$, $n \geq 2$, is a finite primitive subgroup. Let $\gamma \in G$ be a quadratic element of drop $r \geq 1$ and order $d$. Then $d \leq 5$, and we have the following results.*

(i) *If $d = 4$ or $d = 5$, then $n = 2r$.*

(ii) *If $d = 3$, then $n \leq 4r$.*

Proof. The non-existence when $d \geq 6$ is Blichfeldt [**Bl**, Thm. 8]. The case $d = 5$ is due to Zalesski [**Za1**, 11.2], cf. [**Ka-TLFM**, AZ.1]. The cases $d = 4, 3$ are due to Wales [**Wa**, Thm.1, Thm. 2 and Remark after Thm. 2]. □

Theorem 10.1.11. *Suppose $A - B \geq 2$, $p \nmid AB$, $\gcd(A, B) = 1$, and $\chi$ is a tame character with $\chi^A \neq \mathbb{1}$. Then we have the following results about the group $G_{\mathrm{geom}}$ for $\mathcal{H}_{big,A,B,\overline{\chi}}$.*

(i) *Suppose $p \nmid w := A - B$. If $\chi^A \neq \chi_2^B$, then $G_{\mathrm{geom}}$ contains a scalar multiple of a quadratic element $\gamma$ of drop $B$ with eigenvalues $1, \chi^A\chi_2^B$. The order of this quadratic element is the order of the nontrivial character $\chi^A\chi_2^B$.*

(ii) *Suppose $p \mid w := A - B$. Write $w = w_0 q$ with $q = p^e, e \geq 1$ and $p \nmid w_0$. If $\chi^{A(q+1)} \neq \mathbb{1}$, then $G_{\mathrm{geom}}$ contains a scalar multiple of a quadratic element $\gamma$ of drop $B$ with eigenvalues $1, \chi^{A(q+1)}$. The order of this element is the order of the nontrivial character $\chi^{A(q+1)}$.*

Proof. Denote by $\mathsf{Wild}$ the wild part of the $I(\infty)$-representation. The $I(\infty)$-representation is thus

$$\oplus_{\rho \in \mathsf{Char}(B,\chi)} \mathcal{L}_\rho \oplus \mathsf{Wild}.$$

We also note that

$$\det(\oplus_{\rho \in \mathsf{Char}(B,\chi)} \mathcal{L}_\rho) = \chi\chi_2^{B-1}.$$

(i) Consider first the case when $p \nmid w$. We know [**Ka-GKM**, 1.14 (2)] that $\mathsf{Wild}$ is the Kummer direct image $[w]_\star L$ for some rank one $L$ of rank one and Swan conductor one. Such an $L$ of the form $\mathcal{L}_\sigma \otimes \mathcal{L}_{\psi_1}$ for some multiplicative character $\sigma$ and some nontrivial additive character $\psi_1$. Geometrically, $\sigma$ is a $w^{\text{th}}$ power, say $\sigma = \sigma_1^w$. Then

$$[w]_\star L = [w]_\star([w]^\star(\mathcal{L}_{\sigma_1}) \otimes \mathcal{L}_{\psi_1}) = \mathcal{L}_{\sigma_1} \otimes [w]_\star \mathcal{L}_{\psi_1}.$$

Thus

$$\det(\mathsf{Wild}) = \det([w]_\star L) = \sigma_1^w \det([w]_\star \mathcal{L}_{\psi_1}).$$

On the other hand, we have [**Ka-GKM**, 5.6.2] the global geometric isomorphism

$$[w]_\star \mathcal{L}_{\psi_1}) \cong \mathcal{K}l_{\psi_2}(\text{ all characters of order dividing } w),$$

for $\psi_2(x) := \psi_1(x/w)$. Because $w \geq 2$, this Kloosterman sheaf has geometric determinant the product of all its "upstairs" characters, namely the characters of order dividing $w$, whose product is $(\chi_2)^{w-1}$. Thus

$$\det(\mathsf{Wild}) = \sigma_1^w(\chi_2)^{w-1}.$$

The determinant of the $I(\infty)$-representation of $\mathcal{H}_{big,A,B,\overline{\chi}}$ is then $\chi\chi_2^{B-1}\det(\mathsf{Wild})\chi\chi_2^{B-1}\sigma_1^w(\chi_2)^{w-1}$. Again because $w \geq 2$, this determinant is the product of the "upstairs" characters of $\mathcal{H}_{big,A,B,\chi}$, which is $(\chi_2)^{A-1}$. Thus

$$\chi\chi_2^{B-1}\sigma_1^w(\chi_2)^{w-1} = (\chi_2)^{A-1},$$

i.e.,

$$\chi\sigma_1^w = \chi_2.$$

Now consider the Kummer pullback $[w]^\star$ of the $I(\infty)$-representation. It is the direct sum

$$\oplus_{\rho \in \mathsf{Char}(B,\chi)} \mathcal{L}_{\rho^w} \bigoplus (\sigma_1^w \otimes [w]^\star[w]_\star \mathcal{L}_{\psi_1}).$$

But we have $[w]^\star[w]_\star \mathcal{L}_{\psi_1} = \oplus_{\zeta \in \mu_w} \mathcal{L}_{\psi_1(\zeta x)}$. Thus this Kummer pullback is

$$\oplus_{\rho \in \mathsf{Char}(B,\chi)} \mathcal{L}_{\rho^w} \bigoplus (\oplus_{\zeta \in \mu_w} \mathcal{L}_{\sigma_1^w} \otimes \mathcal{L}_{\psi_1(\zeta x)}).$$

Now evaluate this on an element $\gamma$ of $I(\infty)$ of profinite order prime to $p$ which maps onto a generator of $I(\infty)/P(\infty)$. Because $\gamma$ has order prime to $p$, each of the characters $\mathcal{L}_{\psi_1(\zeta x)}$ takes the value 1 at $\gamma$, so its eigenvalues are

$$(\{\rho^w : \rho^B = \chi\}, \sigma_1^w \text{ repeated } w \text{ times}).$$

Then $\gamma^B$ has eigenvalues

$$(\chi^w \text{ repeated } B \text{ times}, \sigma_1^{wB} \text{ repeated } w \text{ times}).$$

Now use the determinant equation above, namely $\chi\sigma_1^w = \chi_2$, to get $\sigma_1^{wB} = \chi_2^B/\chi^B$. Thus the image of $\gamma$ in $G_{\text{geom}}$ has eigenvalues

$$(\chi^w \text{ repeated } B \text{ times}, \chi_2^B/\chi^B \text{ repeated } w \text{ times}).$$

Notice that $\chi^{w+B} = \chi^A$. If $\chi^A \neq \chi_2^B$, then this element is the $\chi_2^B/\chi^B$ multiple of the quadratic element

$$(\chi^A\chi_2^B \text{ repeated } B \text{ times}, \mathbb{1} \text{ repeated } w \text{ times}).$$

Because $\chi^A$ is neither $\mathbb{1}$ nor $\chi_2^B$, this is indeed a quadratic element of drop $B$. Its order is the order of the character $\chi^A\chi_2^B$.

(ii) We now turn to the case when $p|w$. Because $w = w_0 q$, we know [**Ka-GKM**, 1.14 (2)] that $\mathsf{Wild}$ is $[w_0]_\star W_q$ for some $q$-dimensional irreducible $I(\infty)$-representation with all slopes $1/q$. According to [**Ka-ESDE**, 8.6.3], the isomorphism class of such a $W_q$ is determined up to translation by its determinant.

To exploit these facts, we introduce a particular $\mathbb{W}_q$, which will play the role that $\mathcal{L}_\psi$ played in the case when $w$ was prime to $p$. Namely, we define

$$\mathbb{W}_q := \text{ the } I(\infty)\text{-representation of } \mathcal{K}l_\psi(\mathsf{Char}(q+1) \smallsetminus \{\chi_2\}).$$

This Kloosterman sheaf has geometrically trivial determinant, so in particular $\det(\mathbb{W}_q) = \mathbb{1}$. So "our" $W_q$ is, up to a multiplicative translation, of the form $\mathcal{L}_\rho \otimes \mathbb{W}_q$ for some multiplicative character $\rho$, since as $\rho$ varies we attain all possible determinants. We may further choose a $\rho_1$ with $\rho_1^{w_0} = \rho$. Then

$$[w_0]_\star W_q = [w_0]_\star([w_0]^\star \mathcal{L}_{\rho_1} \otimes \mathbb{W}_q) = \mathcal{L}_{\rho_1} \otimes [w_0]_\star(\mathbb{W}_q).$$

At this point, we need to compute the determinant of $[w_0]_\star(\mathbb{W}_q)$, which is the $I(\infty)$-representation of

$$[w_0]_\star \mathcal{K}l_\psi(\mathsf{Char}(q+1) \smallsetminus \{\chi_2\}) \cong \mathcal{K}l_{\psi_1}(\mathsf{Char}((w_0(q+1)) \smallsetminus \mathsf{Char}(w_0, \chi_2)),$$

whose geometric determinant is thus $\chi_2/(\chi_2\chi_2^{w_0-1}) = \chi_2^{w_0-1}$. Thus $\det([w_0]_\star(\mathbb{W}_q)) = \chi_2^{w_0-1}$, and hence $\det(\mathsf{Wild}) = \rho_1^w \chi_2^{w_0-1}$. Thus the determinant of the $I(\infty)$-representation of our $\mathcal{H}$ is $\chi\chi_2^{B-1}\rho_1^w\chi_2^{w_0-1}$. But the global determinant of $\mathcal{H}$ is $\chi_2^{A-1}$, so we have $\chi\chi_2^{B-1}\rho_1^w\chi_2^{w_0-1} = \chi_2^{A-1}$. Thus we have

$$\rho_1^w = \chi_2^{w+1-w_0}/\chi. \tag{10.1.11.1}$$

Now consider the $[w_0]$ Kummer pullback of the $I(\infty)$-representation of $\mathcal{H}$. It is

$$\oplus_{\sigma \in \mathsf{Char}(B,\chi)} \mathcal{L}_{\sigma^{w_0}} \bigoplus (\oplus_{\zeta \in \mu_{w_0}} \mathcal{L}_{\rho_1^{w_0} \otimes \mathbb{W}_q(\zeta x)}).$$

Now consider its further $[q+1]$ Kummer pullback. It is

$$\oplus_{\sigma \in \mathsf{Char}(B,\chi)} \mathcal{L}_{\sigma^{w_0(q+1)}} \bigoplus (\oplus_{\zeta \in \mu_{w_0}} \mathcal{L}_{\rho_1^{w_0(q+1)} \otimes [q+1]^\star \mathbb{W}_q(\zeta x)}).$$

The key point here is that $[q+1]^\star \mathbb{W}_q$ is the $I(\infty)$-representation of

$$[q+1]^\star \mathcal{K}l_\psi(\mathsf{Char}(q+1) \smallsetminus \{\chi_2\}) \cong FT_\psi \mathcal{L}_{\psi(x^{q+1})},$$

thanks to [**Ka-ESDE**, 9.2.3]. By a result of Pink [**KT1**, 20.3], one knows that $G_{\text{geom}}$ for $FT_\psi \mathcal{L}_{\psi(x^{q+1})}$ is a finite $p$-group (and by Sawin [**KT1**, 21.1] it is a known Heisenberg group, at least for $p$ odd). Thus this further $[q+1]$ Kummer pullback is

$$\oplus_{\sigma \in \mathsf{Char}(B,\chi)} \mathcal{L}_{\sigma^{w_0(q+1)}} \bigoplus (\oplus_{\zeta \in \mu_{w_0}} \rho_1^{w_0(q+1)} \otimes (\text{dim} = w, \text{image of } I(\infty) = \text{finite } p\text{-group})).$$

Now choose an element $\gamma \in I(\infty)$ which maps onto a generator of $I(\infty)/P(\infty)$ and which has profinite order prime to $p$. Such an element must map to the identity in any finite $p$-group. Thus the image of such a $\gamma$ has eigenvalues

$$(\{\sigma^{w_0(q+1)} : \sigma^B = \chi\}, \rho_1^{w_0(q+1)} \text{ repeated } w \text{ times}).$$

The $(qB)^{\text{th}}$ power of $\gamma$ then has eigenvalues

$$(\{\sigma^{w(q+1)B} : \sigma^B = \chi\}, \rho_1^{w(q+1)B} \text{ repeated } w \text{ times}),$$

i.e.,

$$(\chi^{w(q+1)} \text{ repeated } B \text{ times}, \rho_1^{w(q+1)B} \text{ repeated } w \text{ times}).$$

By (10.1.11.1), $\rho_1^{w(q+1)B} = 1/\chi^{(q+1)B}$. Thus the image of the $(qB)^{\text{th}}$ power of $\gamma$ is $1/\chi^{(q+1)B}$ times the element with eigenvalues

$$(\chi^{A(q+1)} \text{ repeated } B \text{ times}, \mathbb{1} \text{ repeated } w \text{ times}),$$

which is the asserted complex reflection when $\chi^{A(q+1)}$ is nontrivial. □

Specializing $B = 1$ in Theorem 10.1.11 and recalling that a quadratic element of drop 1 is a complex reflection, we obtain:

THEOREM 10.1.12. *Suppose $A \geq 3$, $p \nmid A$, and $\chi$ is a tame character with $\chi^A \neq \mathbb{1}$. Then we have the following results about the group $G_{\text{geom}}$ for $\mathcal{H}_{big,A,1,\overline{\chi}}$.*

(i) *Suppose $p \nmid w := A - 1$. If $\chi^A \neq \chi_2$, then $G_{\text{geom}}$ contains a scalar multiple of a complex reflection $\gamma$ of determinant $\chi^A\chi_2$. Moreover, the complex reflection $\gamma$ has order 3 if $\mathsf{o}(\chi^A) = 6$, 4 if $\mathsf{o}(\chi^A) = 4$, and otherwise $\gamma$ has order $\geq 5$. In particular, $\mathsf{o}(\gamma) \geq 4$ if $\chi^{6A} \neq \mathbb{1}$.*

(ii) *Suppose $p \mid w := A - 1$. Write $w = w_0 q$ with $q = p^e, e \geq 1$ and $p \nmid w_0$. If $\chi^{A(q+1)} \neq \mathbb{1}$, then $G_{\text{geom}}$ contains a scalar multiple of a complex reflection $\gamma$ of determinant $\chi^{A(q+1)}$. In particular, if $\chi^{2A(q+1)} \neq \mathbb{1}$ then $\mathsf{o}(\gamma) > 2$, and if $\chi^{6A(q+1)} \neq \mathbb{1}$ then $\mathsf{o}(\gamma) \geq 4$.*

Next we give an analogue of Theorem 10.1.12 for $A = 2$.

LEMMA 10.1.13. *Suppose $A = 2$, $p > 2$, and $\chi$ is a tame character with $\chi^2 \neq \mathbb{1}$ and $\chi^2 \neq \chi_2$. Then the group $G_{\text{geom}}$ for $\mathcal{H}_{big,A,1,\overline{\chi}}$ contains a scalar multiple of a complex reflection of determinant $\chi^2\chi_2$.*

PROOF. The key point here is that we have a geometric isomorphism $\det(\mathcal{H}_{big,2,1,\overline{\chi}}) = \mathcal{L}_\psi \otimes \mathcal{L}_{\chi_2}$, a special case of [**Ka-ESDE**, 8.8.12 (2)] in which the $\Lambda$ there is $\chi_2$. The $I(\infty)$-representation is thus

$$\mathcal{L}_\chi \oplus (\mathcal{L}_\psi \otimes \mathcal{L}_{\overline{\chi}\chi_2}).$$

Now choose an element $\gamma \in I(\infty)$ of pro-order prime to $p$ which generates the tame quotient $I(\infty)/P(\infty)$. Its eigenvalues are $\chi(\gamma)$ and $\overline{\chi}(\gamma)\chi_2(\gamma)$, so it is a scalar multiple, by $\overline{\chi}(\gamma)\chi_2(\gamma)$, of the complex reflection with determinant $(\chi^2\chi_2)(\gamma)$. □

THEOREM 10.1.14. *Suppose $A \geq 3$, $A - B \geq 2$, $\gcd(A, B) = 1$, and $p \nmid AB$. Suppose that $\mathcal{F}(A, B, \theta)$ has finite $G_{\text{geom}}$. Then we have the following results.*

(i) *Suppose $p \nmid w := A - B$. Then $\theta\chi_2^B$ has order $\leq 3$. In particular, if $B$ is even then $\theta$ has order $\leq 3$, while if $B$ is odd then $\theta$ has order $\leq 6$.*

(ii) *Suppose $p | w := A - B$. Write $w = w_0 p^e$ with $e \geq 1$ and $p \nmid w_0$. Then $\theta^{p^e+1}$ has order $\leq 3$. In particular, $\theta$ has order $\leq 3(p^e + 1)$.*

(iii) *If in addition both $B = 1$ and $A > 4$, then $\theta\chi_2$, respectively $\theta^{p^e+1}$, has order $\leq 2$.*

PROOF. If $\theta = \mathbb{1}$, we are saying nothing. If $\theta$ is nontrivial, pick a character $\rho$ with $\rho^A = \overline{\theta}$. In view of Theorem 10.1.1, $\mathcal{H}_{big,A,B,\rho}$ has finite $G_{\text{geom}}$, which by Lemma 10.1.7 and 10.1.8 is a finite primitive subgroup of $\mathrm{GL}_n(\mathbb{C})$. If $\theta\chi_2$, respectively $\theta^{p^e+1}$ has order $\geq 4$, then by Theorem 10.1.11 this group contains a quadratic element of drop $B$ and order $\geq 4$. By Theorem 10.1.10, this impossible if the order is $\geq 6$, while if the order is 4 or 5, then $A = 2B$, contradicting $\gcd(A, B) = 1$. For assertion (iii), one knows [**Mit**, Theorem 1] that a finite primitive group in $> 4$ variables contains no complex reflection of order $> 2$. □

We will also need the following extension of Proposition 2.4.3:

LEMMA 10.1.15. *Let $A > B \geq 1$ be coprime integers, and let $p \nmid AB$. Consider the local system $\mathcal{H} = \mathcal{H}_{small,A,B}$ or $\mathcal{H}_{big,A,B,\chi}$ in characteristic $p$, with geometric monodromy group $G$ and wild part of dimension $w = A - B$, and let $g_\infty$ be a $p'$-element that generates the image $J$ of $I(\infty)$ in $G$ modulo the image $Q$ of $P(\infty)$. Then $g_\infty$ is an* m2sp*-element of finite order acting on the underlying representation $V = V_{\mathcal{H}}$. Moreover, the following statements hold.*

- (i) *Suppose $p \nmid w$. Then $\bar{\mathsf{o}}(g_\infty)$ is divisible by $w$; in fact it is divisible by $(A - B)B$ unless possibly when $B = 2$ and $\mathcal{H} = \mathcal{H}_{small,A,2}$. In all cases, the total multiplicity of repeated eigenvalues of $g_\infty$ on $V$ is at most 2, i.e. $g_\infty$ is an* asp*-element.*
- (ii) *Suppose $w = w_0 p^e$ with $e \geq 1$. Then $\bar{\mathsf{o}}(g_\infty)$ is divisible by $C := w_0(p^e + 1)$; in fact it is divisible by $\mathrm{lcm}(B, C)$ unless possibly when $B = 2$ and $\mathcal{H} = \mathcal{H}_{small,A,2}$. In all cases, the total multiplicity of repeated eigenvalues of $g_\infty$ on $V$ is at most $2d$, where $d := \gcd(B, C) = \gcd(B, p^e + 1)$, and the ratio between any two repeated eigenvalues is a $d^{\mathrm{th}}$ root of unity.*

PROOF. Applying Proposition 2.4.3 to $G$, we obtain that $g_\infty$ is m2sp on $V$, and it is ssp on Wild and on Tame. Excluding the case $\mathcal{H} = \mathcal{H}_{small,A,2}$, we have that the spectrum of $g_\infty$ on Tame contains two eigenvalues who ratio is $\zeta_B$ if $B \geq 2$, whence the central order of $g_\infty$ on Tame is always divisible by $B$, which implies the statements about $\bar{\mathsf{o}}(g_\infty)$.

Assume that $\alpha$ is a repeated eigenvalue on $V$ for $g_\infty$. Since $g_\infty$ is ssp on both Wild and Tame, it must be the case that $\alpha$ has multiplicity 1 on Wild and multiplicity 1 on Tame, and so its total multiplicity is 2. Now assume that $\alpha' \neq \alpha$ is another repeated eigenvalue for $g_\infty$ on $V$. Then $\alpha$ and $\alpha'$ are distinct eigenvalues for $g_\infty$ on Wild and on Tame; in particular, $1 \neq \alpha'/\alpha$ is a $B^{\mathrm{th}}$ root of unity, and this shows $\mathcal{H} \neq \mathcal{H}_{small,A,2}$. If $p \nmid w$, then by [**KRLT4**, Proposition 4.8], $\alpha'/\alpha$ is a $w^{\mathrm{th}}$ root of unity, whence $\alpha = \alpha'$ since $\gcd(w, B) = \gcd(A, B) = 1$, a contradiction. Suppose now that $p | w = w_0 p^e$. By [**KRLT4**, Proposition 4.9], $\alpha'/\alpha$ is a $C^{\mathrm{th}}$ root of unity, whence it is a $d^{\mathrm{th}}$ root of unity. Thus there exist at most $d$ possibilities for repeated eigenvalues of $g_\infty$, and each has multiplicity 2. Also note that $\gcd(w_0, B)$ divides $\gcd(w, B) = \gcd(A - B, B) = 1$, so $d = \gcd(B, p^e + 1)$. □

We give the following lemma for later use:

LEMMA 10.1.16. *Suppose $W$ is a totally wild $I(\infty)$-representation of odd dimension $D$, with all slopes $1/D$. If $p$ is odd, then $W|_{P(\infty)}$ is not self-dual as $P(\infty)$-representation.*

PROOF. Suppose first that $D = p^a$ for some $a \geq 0$. Then $W$ is $P(\infty)$-irreducible by [**Ka-GKM**, 1.14(2)]. If $W$ and its $I(\infty)$-dual $W^\vee$ are $P(\infty)$-isomorphic, then we have an $I(\infty)$-isomorphism $W^\vee \cong W \otimes \chi$ for some character $\chi$ of $I(\infty)/P(\infty)$ (simply because $P(\infty) \lhd I(\infty)$). Because $p$ is odd, there exists a character $\rho$ of $I(\infty)/P(\infty)$ with $\rho^2 = \chi$. But then $W \otimes \rho$ is $I(\infty)$-self-dual, which for $p$ odd is impossible by [**Ka-ESDE**, 8.8.3] because its rank $p^a$ is odd.

Suppose now that $D = n_0 p^a$ with $a \geq 0$ and $p \nmid n_0$. Then as $I(\infty)$-representation, $W$ is the Kummer direct image $[n_0]_\star V$ for some $V$ an $I(\infty)$ of rank $p^a$ with all slopes $1/p^a$. Then the Kummer pullback $[n_0]^\star W$ is the direct sum

$$[n_0]^\star W \cong \bigoplus_{\zeta \in \mu_{n_0}(\overline{\mathbb{F}_p})} \mathrm{Mult.Transl}_\zeta(V).$$

The Kummer pullback does not change the $P(\infty)$-representation, hence

$$W_{P(\infty)} \cong \bigoplus_{\zeta \in \mu_{n_0}(\overline{\mathbb{F}_p})} \mathrm{Mult.Transl}_\zeta(V_{P(\infty)}).$$

By [**Ka-GKM**, 1.14(4)], these $n_0$ multiplicative translates are pairwise nonisomorphic as irreducible $P(\infty)$-representations. By the argument above, none of these multiplicative translates is $P(\infty)$-self-dual. So if $W$ is to be $P(\infty)$-self-dual, these $n_0$ multiplicative translates must fall into pairs of $P(\infty)$-duals. But this is impossible, as $n_0$ is odd. □

Lemma 10.1.17. *Let $X/\mathbb{F}_q$ be smooth and geometrically connected, $\ell \neq p$, and $\mathcal{F}$ a lisse $\overline{\mathbb{Q}_\ell}$-adic sheaf on $X$ which is pure of weight zero. Suppose $G_{\mathrm{arith}}$ is finite. Suppose there exists a point $x_0 \in X(\mathbb{F}_q)$ such that* $\mathrm{Trace}(\mathsf{Frob}_{x_0,\mathbb{F}_q}|\mathcal{F}) = \mathrm{rank}(\mathcal{F})$. *Then $G_{\mathrm{geom}} = G_{\mathrm{arith}}$.*

Proof. Indeed the quotient $G_{\mathrm{arith}}/G_{\mathrm{geom}}$ is a quotient of $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$, so generated by the image in $G_{\mathrm{arith}}/G_{\mathrm{geom}}$ of any $\mathsf{Frob}_{x,\mathbb{F}_q}$ for any $x \in X(\mathbb{F}_q)$. The image of $\mathsf{Frob}_{x_0,\mathbb{F}_q}$ in $G_{\mathrm{arith}}$ is the identity element $\mathrm{id}_{G_{\mathrm{arith}}}$ of $G_{\mathrm{arith}}$, simply because in a finite group $G < \mathrm{GL}_{\mathrm{rank}(\mathcal{F})}(\mathbb{C})$, only the identity has trace equal to the dimension. But $\mathrm{id}_{G_{\mathrm{arith}}}$ lies in $G_{\mathrm{geom}}$. □

We now given a "rationality" result for multiplicative characters. Recall that a nonzero one-variable polynomial $f(x)$ over an $\mathbb{F}_p$-algebra is said to be *Artin-Schreier reduced* if it has no constant term, and if any monomial appearing with a nonzero coefficient has degree prime to $p$. Given a nonzero Artin-Schreier reduced polynomial $f(x)$, we denote by

$$\mathrm{gcd}_{\mathrm{deg}}(f)$$

the greatest common divisor of the degrees of the monomials appearing in $f$.

Theorem 10.1.18. *Let $\mathbb{F}_q/\mathbb{F}_{p^2}$ be a finite extension, $f(x) \in \mathbb{F}_q[x]$ a nonzero Artin-Schreier reduced polynomial. Let $B \geq 1$ be an integer with $p \nmid B$ and $B < \deg(f)$. Suppose $\mathbb{F}_q^\times$ contains $\mu_B(\overline{\mathbb{F}_q})$, i.e. that $q \equiv 1 (\mathrm{mod}\ B)$. Suppose that*

$$\gcd(B, \mathrm{gcd}_{\mathrm{deg}}(f)) = 1.$$

*Let $\theta$ be a nontrivial multiplicative character of $\mathbb{F}_q^\times$. Consider the lisse sheaf $\mathcal{G}(f, B, \theta)$ on $\mathbb{A}^1/\mathbb{F}_q$ whose trace function is given as follows: for $k/\mathbb{F}_q$ a finite extension,*

$$t \in \mathbb{A}^1(k) = k \mapsto \frac{-1}{\sqrt{\#k}} \sum_{x \in k^\times} \psi_k(f(x) + tx^B)\theta_k(x).$$

*Then we have the following results.*

(i) *$\mathcal{G}(f, B, \theta)$ is geometrically irreducible, and pure of weight zero.*

(ii) *Suppose $\rho$ is a nontrivial multiplicative character of $\mathbb{F}_q^\times$. If $\rho \neq \theta$, then $\mathcal{G}(f, B, \theta)$ and $\mathcal{G}(f, B, \rho)$ are not geometrically isomorphic.*

(iii) *Suppose $\mathcal{G}(f, B, \theta)$ has finite $G_{\text{arith}}$. Let $K/\mathbb{Q}(\zeta_p)$ be a finite extension such that the field of traces of $G_{\text{geom}}$ lies in $K$. Then $\theta$ takes values in $K$.*

Proof. The first assertion is proven in [**KT6**, Proposition 2.6]. The second assertion implies the third. Indeed, If $\theta$ does not have values in $K$, then $K(\theta)$ is a nontrivial galois extension of $K$. If we apply a nontrivial element $\sigma \in \text{Gal}(K(\theta)/K)$ to the trace function of $\mathcal{G}(f, B, \theta)$, we get the trace function of $\mathcal{G}(f, B, \theta^\sigma)$. Therefore $\mathcal{G}(f, B, \theta^\sigma)$ also has finite $G_{\text{arith}}$ (by the integrality of its traces), and hence has finite $G_{\text{geom}}$. Because $G_{\text{arith}}$ is finite, the element $\mathsf{Frob}_{0,\mathbb{F}_q}$ has finite order. So replacing $\mathbb{F}_q$ by a finite extension $k$, e.g. by $\mathbb{F}_{q^n}$ for $n$ the order of $\mathsf{Frob}_{0,\mathbb{F}_q}$, we may assume that $\mathsf{Frob}_{0,k}|\mathcal{G}(f, B, \theta)$ is the identity, or equivalently that $\text{Trace}(\mathsf{Frob}_{0,k}|\mathcal{G}(f, B, \theta)) = \deg(f)$. Because the integer $\deg(f)$ is fixed by $\sigma$, we get $\text{Trace}(\mathsf{Frob}_{0,k}|\mathcal{G}(f, B, \theta^\sigma)) = \deg(f)$, i.e. that $\mathsf{Frob}_{0,k}|\mathcal{F}(f, B, \theta^\sigma)$ is the identity. It then follows by Lemma 10.1.17 that for both $\mathcal{G}(f, B, \theta))$ and $\mathcal{G}(f, B, \theta^\sigma)$, when pulled back to $\mathbb{A}^1/k$, each has $G_{\text{geom}} = G_{\text{arith}}$. Therefore for $\mathcal{G}(f, B, \theta)$, the trace field of its $G_{\text{arith}}$ lies in $K$. But $\sigma$ fixes $K$, therefore $\mathcal{G}(f, B, \theta^\sigma)$ has the same Frobenius traces over extensions of $k$ as $\mathcal{G}(f, B, \theta)$. By Chebotarev, $\mathcal{G}(f, B, \theta)$ and $\mathcal{G}(f, B, \theta^\sigma)$ are arithmetically isomorphic (both being geomerically, and hence arithmetically, irreducible). Therefore $\mathcal{G}(f, B, \theta)$ and $\mathcal{G}(f, B, \theta^\sigma)$ are geometrically isomorphic. By assertion (ii), this implies that $\theta = \theta^\sigma$. Thus $\theta$ is fixed by $\text{Gal}(K(\theta)/K)$, hence has values in $K$.

It remains to prove (ii). We argue by contradiction. If $\rho \neq \theta$ but $\mathcal{G}(f, B, \theta)$ and $\mathcal{G}(f, B, \rho)$ are geometrically isomorphic, then the cohomology group

$$H^2_c(\mathbb{A}^1/\overline{\mathbb{F}_q}, \mathcal{G}(f, B, \theta) \otimes \mathcal{G}(f, B, \rho)^\vee)$$

has dimension one, and is pure of weight two. On the other hand, the $H^1_c$ is mixed of weight $\leq 1$, so by the Lefschetz trace formula we would recover 1 as lim sup over larger and larger extensions $k/\mathbb{F}_q$ of

$$\begin{aligned}
&\frac{1}{\#k}\sum_{t\in k} \text{Trace}(\mathsf{Frob}_{t,k}|\mathcal{G}(f, B, \theta))\text{Trace}(\mathsf{Frob}_{t,k}|\mathcal{G}(f, B, \rho)^\vee) \\
&= \big(\frac{1}{\#k}\big)^2 \sum_{t\in k}\sum_{x,y\in k^\times} \psi_k(f(x) - f(y) + t(x^B - y^B))\theta(x)\overline{\rho}(y) \\
&= \frac{1}{\#k}\sum_{x,y\in k^\times, x^B = y^B} \psi_k(f(x) - f(y))\theta(x)\overline{\rho}(y) \\
&= \frac{1}{\#k}\sum_{\zeta\in\mu_B}\sum_{x\in k^\times} \psi_k(f(x) - f(\zeta x))\theta(x)\overline{\rho}(\zeta x).
\end{aligned}$$

The hypothesis that $\gcd(B, \gcd_{\deg}(f)) = 1$ means precisely that for $\zeta \in \mu_B$ and $\zeta \neq 1$, $f(x) - f(\zeta x)$ is a nonzero Artin-Schreier reduced polynomial. The sum

$$\sum_{x\in k^\times} \psi_k(f(x) - f(\zeta x))\theta(x)\overline{\rho}(\zeta x)$$

is then of absolute value $\leq \deg(f)\sqrt{\#k}$ by Weil, so it contributes 0 to the lim sup. For $\zeta = 1$, the sum is

$$\sum_{x\in k^\times} \psi_k(f(x) - f(x))\theta(x)\overline{\rho}(\zeta x) = \sum_{x\in k^\times} \theta(x)\overline{\rho}(\zeta x) = 0,$$

the last equality because $\theta\overline{\rho}$ is nontrivial. Thus the lim sup is 0, not 1, a contradiction. $\square$

## 10.2. The $(A, 1)$-case

In this section, we completely determine the geometric monodromy groups of the local systems $\mathcal{F}(A, 1, \chi)$. We begin with a group-theoretic observation.

LEMMA 10.2.1. *Let $p$ be a prime, $m \in \mathbb{Z}_{\geq 1}$, and let $G \leq \mathrm{GL}_m(p)$. Suppose $\ell$ is a primitive prime divisor of $p^m - 1$, cf.* [**Zs**]. *If a $p$-subgroup $R$ of $G$ is normalized by an element $g \in G$ of order $\ell$, then $R = 1$.*

PROOF. By the choice of $\ell$, $g$ acts irreducibly on the natural module $V = \mathbb{F}_p^m$. Since $g$ fixes the (nonzero) fixed point subspace $U$ of $R$ on $V$, it follows that $R = V$, and so $R = 1$. $\square$

LEMMA 10.2.2. *Let $2 \nmid N \geq 3$, and let $G_{\mathrm{geom}}$ be the geometric monodromy group of the Kloosterman sheaf $\mathcal{K} := \mathcal{K}l(\mathsf{Char}_{\mathrm{ntriv}}(N))$ in characteristic $p = 2$. If $G_{\mathrm{geom}}$ is infinite, then $G_{\mathrm{geom}} = \mathrm{Sp}_{N-1}$. Similarly, if $G_{\mathrm{geom}}$ denotes the geometric monodromy group of $\mathcal{F}(57, B, \mathbb{1})$ in characteristic $p = 2$, for any odd $1 \leq B \leq 55$, then $G_{\mathrm{geom}}^\circ \not\cong E_7$.*

PROOF. By Lemma 10.1.7, $\mathcal{K}$ satisfies (**S**+). Its $G_{\mathrm{geom}}$ is infinite, so it is Lie irreducible, and symplectic by [**Ka-ESDE**, 8.8.1–2] (in fact, it is symplectic for any odd $N \geq 3$ in any characteristic $p \nmid N$). Its Kummer pullback $[N]^\star\mathcal{K}l(\mathsf{Char}_{\mathrm{ntriv}}(N))$ is the Fourier transform $FT(\mathcal{L}_{\psi(x^N)})$, which is an Airy sheaf in the terminology of [**Such**]. So the result is a special case of [**Such**, Proposition 11.7], unless $N = 57$ and $G_{\mathrm{geom}}^\circ = E_7$. In this case, $g_0$ has spectrum $\mu_{57} \smallsetminus \{1\}$, so $g_0^{19}$ has order 3 and spectrum $\big(1^{[18]}, \zeta_3^{[19]}, \overline{\zeta}_3^{[19]}\big)$, which is impossible by [**CG**, Proposition 4.1]. The same argument applies to $\mathcal{F}(57, B, \mathbb{1})$. $\square$

LEMMA 10.2.3. *Let $\mathcal{F} = \mathcal{F}(A, B, \theta)$ in characteristic $p \nmid AB$ with $A > B \geq 1$ coprime, of dimension $D$ and with $G = G_{\mathrm{geom}}$. Then none of the following cases can occur.*

(a) *$(p, D) = (2, 6)$, and $G^\circ$ acts on $\mathcal{H}$ as $\mathrm{SL}_3 = \mathrm{SL}(V)$ acts on $\mathrm{Sym}^2(V)$ or $\mathrm{Sym}^2(V^*)$.*
(b) *$D = 8$ and $G^\circ = \mathrm{Spin}_7$ acts on $\mathcal{H}$ as on its spin module.*
(c) *$D = 8$, and $G^\circ$ acts on $\mathcal{H}$ as $\mathrm{SL}_3 = \mathrm{SL}(V)$ acts on the adjoint module.*
(d) *$D = 4, 5$ and $G^\circ$ is $\mathrm{SL}_2$ or $\mathrm{PSL}_2$.*

PROOF. In each case, we argue by contradiction.

Suppose we are in case (a). Since $p = 2 \nmid AB$, we have $A = 7$, $\theta = \mathbb{1}$. In this case, $\mathcal{F}$ is symplectic by Theorem 10.1.6(iii), hence it is symplectic over $G^\circ$, whereas it is not self-dual over $\mathrm{SL}_3$.

Suppose we are in case (b). Note that the spin module is orthogonal over $\mathrm{Spin}_7$, cf. [**Bour**, Table 1, p. 213]. Hence $\mathcal{F}$ is orthogonally self-dual by Lemma 10.1.3. By Theorem 10.1.6, the latter implies that $2 \nmid AB$, whence $A = 9$, $\theta = \mathbb{1}$, but in this case $\mathcal{F}$ would be symplectically self-dual, a contradiction.

Suppose we are in case (c). Note that the adjoint module of $\mathrm{SL}_3$ is orthogonal over $\mathrm{SL}_3$, so $\mathcal{F}$ is orthogonally self-dual by Lemma 10.1.3. By Theorem 10.1.6, the latter implies that $2 \nmid AB$, whence $A = 9$, $\theta = \mathbb{1}$, but in this case $\mathcal{F}$ would be symplectically self-dual, a contradiction.

In case (d), the $\mathrm{SL}_2$-module is self-dual, of orthogonal type if $D = 5$ and of symplectic type if $D = 4$. By Lemma 10.1.3, $\mathcal{F}$ is self-dual, of the same type, so $2 \nmid AB$ by Theorem 10.1.6; in particular, $A - 5$. Now, if $D = 4$, then the symplectic type tells us that $\theta = \mathbb{1}$; also, $p = 3$ and $m = 2$ by Theorem 6.1.5, but then $p|B = 3$, a contradiction. If $D = 5$, then the orthogonal type tells us that $p > 2$, and this is impossible by Theorem 6.1.5. □

THEOREM 10.2.4. *Let $p$ be a prime and let $A \in \mathbb{Z}_{\geq 3}$ be coprime to $p$. Consider the local system $\mathcal{F}(A, 1, \theta)$ in characteristic $p$, of rank $D = A - 1$ if $\theta = \mathbb{1}$ and $D = A$ otherwise, with geometric monodromy group $G_{\mathrm{geom}}$. Assume in addition that $D \geq 3$ and $G_{\mathrm{geom}}$ is infinite. Then we have the following results.*

(i) *If $A$ is even, then for every $\theta$, $\mathcal{F}(A, 1, \theta)$ has $G_{\mathrm{geom}} = \mathrm{SL}_D$.*
(ii) *If $A$ is odd and $\theta \neq \mathbb{1}, \chi_2$, then $G_{\mathrm{geom}} = \mathrm{SL}_D$.*
(iii) *If $A$ is odd and $\theta = \mathbb{1}$, then $G_{\mathrm{geom}} = \mathrm{Sp}_D$.*
(iv) *If $A$ is odd, $A \neq 7$, $p \neq 2$, and $\theta = \chi_2$, then $G_{\mathrm{geom}} = \mathrm{SO}_D$.*
(v) *If $A = 7$, $p \neq 2$, and $\theta = \chi_2$, then $G_{\mathrm{geom}} = G_2$.*

PROOF. (A) We first show that $\mathcal{G} := G^{\circ}_{\mathrm{geom}}$ must be either $G_2$ in rank 7 or one of the classical groups $\mathrm{SL}_D$ with $D \geq 2$, $\mathrm{SO}_D$ with $D \geq 3, D \neq 4$, or $\mathrm{Sp}_D$ with $2|D$. [Sometimes $\mathrm{SL}_2$ will occur naturally as itself, other times as $\mathrm{Sp}_2$. And the image of $\mathrm{SL}_2 = \mathrm{SL}(V)$ in $\mathrm{Sym}^2(V)$ will occur as $\mathrm{SO}_3$.]

Consider $\mathcal{H} = \mathcal{H}_{small,A,1}$ if $\theta = \mathbb{1}$ and consider $\mathcal{H} = \mathcal{H}_{big,A,1,\beta}$ with $\beta^A = \theta$ if $\theta \neq \mathbb{1}$. Let $H$ denote the geometric monodromy group of $\mathcal{H}$. By Theorem 10.1.1, $G := G_{\mathrm{geom}}$ is finite if and only if $H$ is finite; indeed, $G$ has index dividing $A$ in $H$. Furthermore, since $D \geq 2$, either $H$ is known to be finite (the cases $(A = 9, \theta = \mathbb{1}, p = 2)$ and $(A = 5, p = 2, 3)$) or $H$ satisfies $(\mathbf{S}+)$ by Lemma 10.1.7, and so we can apply Lemmas 1.1.3 and 1.1.6 to $H$. By Proposition 2.4.3(i), a generator $g_0$ of the image of $I(0)$ is an $\mathsf{ssp}$-element on the underlying representation $V$ of $\mathcal{H}$; more precisely, its spectrum is $\mu_A \smallsetminus \{1\}$ if $\theta = \mathbb{1}$ and $\mu_A$ otherwise, and so $\bar{\mathsf{o}}(g_0) = A$.

(b) Since $G$ is infinite, $G^{\circ} = H^{\circ}$ is a simple algebraic group by Lemma 1.1.3. Hence we can apply Theorem 3.3.4 and arrive at one of the following possibilities.

(b1) $H^{\circ}$ is a classical group $\mathrm{SL}_D$, $\mathrm{Sp}_D$, or $\mathrm{SO}_D$, or $D = 7$ and $H^{\circ} = G_2$.

(b2) One of (a)–(d) listed in Lemma 10.2.3, and so they are all ruled out.

(b3) $p = 2$, $H^{\circ} = \mathrm{HSpin}_N$ with $N \in \{10, 12, 16\}$ and $D = 2^{N/2-1}$. As $p \nmid A$, in this case we must have $A = q + 1$, leading to finite $G_{\mathrm{geom}}$ by Pink–Sawin, a contradiction.

(b4) $k = 2, 3$, $H^{\circ}$ is the image of $\mathrm{SL}_6 = \mathrm{SL}(V)$ in the representation $\wedge^k(V)$, and $2 \leq p \leq k$. If $k = 2$, then $p = 2$ rules out $A = 16$, and the case $A = 15$ is impossible by Lemma 6.1.18. If $(k, p) = (3, 2)$, then $p = 2$ rules out $A = 20$, and the case $A = 21$ is impossible by Lemma 10.2.2. If $(k, p) = (3, 3)$, then $p = 3$ rules out $A = 21$, and the case $A = 20$ is impossible by Lemma 6.1.17.

(b5) $p = 2, 3$ and $(H^\circ, D) = (E_6, 27)$ or $(E_7, 56)$. Here, $m = 0$ by Theorems 6.2.12 and 6.2.13. Moreover, if $D = 27$, then $p = 3$, $A = 28$, again leading to the Pink–Sawin sheaf with finite monodromy, cf. Theorem 10.2.7(iv). If $D = 56$, then $A = 57$, so $p = 2$, and this case is ruled out by Lemma 10.2.2. [Note that it will be shown in Theorem 10.2.7(ii) that in fact $\mathcal{F}(57, 1, \mathbb{1})$ has $G_{\rm geom} = {\rm PSU}_3(8)$.]

(B) We have shown that $\mathcal{G}$ is either $G_2$ in rank 7 or one of the classical groups in its standard (or dual of standard) representation. Because $A \geq 3$, in all cases we have wild part $w = A - 1 \geq 2$ for both $\mathcal{H} := \mathcal{H}_{small,A,1}$ if $\theta = \mathbb{1}$ and for $\mathcal{H} := \mathcal{H} = \mathcal{H}_{big,A,1,\beta}$ with $\beta^A \neq \mathbb{1}$. We first compute the groups $G_{\rm geom}$ for these $\mathcal{H}$. We will use the fact that if $\mathcal{H}$ is Lie self-dual, meaning that its $G^\circ_{\rm geom}$ is SO or Sp, then for some tame character $\chi$, $\mathcal{L}_\chi \otimes \mathcal{H}$ will be self-dual.

Consider first the case of $\mathcal{H} = \mathcal{H}_{small,A,1}$ with $A$ odd. This $\mathcal{H}$ is itself symplectic, so by the paucity of choice it has $G_{\rm geom} = {\rm Sp}_{A-1}$. Similarly, if $A$ is odd and $p$ is odd, then $\mathcal{H} := \mathcal{H}_{big,A,1,\chi_2}$ is orthogonally self-dual and has geometrically trivial determinant, so by the paucity of choice it has $G_{\rm geom} = {\rm SO}_A$ except possibly if $A = 7$. In this $A = 7$ case, it results from [**Ka-G2**, 3.1 and 6.1] that when $G_{\rm geom}$ is infinite (as it in fact is for $p > 3$), it is $G_2$.

Now consider that case of $\mathcal{H} := \mathcal{H}_{big,A,1,\chi}$ when $A$ is odd and $\chi^A \neq \mathbb{1}$, $\chi^2 \neq \mathbb{1}$. If it were Lie self-dual, then some $\mathcal{L}_\rho \otimes \mathcal{H}$ would be self-dual. Its upstairs characters would be $\rho\mathsf{Char}(A)$, which would need to be stable by complex conjugation. The set $\mathsf{Char}(A)$ is stable, so we would have $\overline{\rho}\mathsf{Char}(A) = \rho\mathsf{Char}(A)$, so $\rho^2\mathsf{Char}(A) = \mathsf{Char}(A)$, so $\rho^2 \in \mathsf{Char}(A)$. Because $A$ is odd, either $\rho \in \mathsf{Char}(A)$, or, if $p$ is odd, $\rho \in \chi_2\mathsf{Char}(A)$. In the first case, at the expense of multiplying $\chi$ by a character of order dividing $A$, we arrive at a self-dual $\mathcal{H} := \mathcal{H}_{big,A,1,\chi}$ still with $\chi^A \neq \mathbb{1}$, $\chi^2 \neq \mathbb{1}$. In the second case, we have $\mathcal{L}_{\chi_2}$ times such an $\mathcal{H} := \mathcal{H}_{big,A,1,\chi}$ being self-dual, and hence with $\mathcal{H} := \mathcal{H}_{big,A,1,\chi}$ itself being self-dual. But this self-duality forces the downstairs character $\chi$ to be fixed by complex conjugation, which it is not. Thus if $A$ is odd but $\chi^2 \neq \mathbb{1}$, we are not Lie self-dual. By the paucity of choice, we have $G^\circ_{\rm geom} = {\rm SL}_A$. As $\det(\mathcal{H})$ is geometrically trivial, we have $G_{\rm geom} = {\rm SL}_A$.

Next consider the case of $\mathcal{H} = \mathcal{H}_{small,A,1}$ with $A$ even. Then $p$ must be odd, and any $\mathcal{L}_\chi \otimes \mathcal{H}$ is still a Kloosterman sheaf of odd rank $A - 1$, so cannot be self-dual, cf. [**Ka-ESDE**, 8.8.1]. Thus here we have $G^\circ_{\rm geom} = {\rm SL}_{A-1}$. Here $\det(\mathcal{H}) = \mathcal{L}_{\chi_2}$, so $H = \{\gamma \in {\rm GL}_{A-1} | \det(\gamma) = \pm 1\}$.

Finally consider the case of $\mathcal{H} := \mathcal{H}_{big,A,1,\chi}$ with $A$ even. Here we must have $p$ odd. Any $\mathcal{L}_\chi \otimes \mathcal{H}$ still have wild part of odd dimension $A - 1$, so cannot be self-dual. Just as in the preceding case, we have $H = \{\gamma \in {\rm GL}_A | \det(\gamma) = \pm 1\}$.

When we form the $[A]^\star$ pullbacks, we get the asserted values of $G_{\rm geom}$ for the $\mathcal{F}(A, 1, \chi)$ (remembering that when $A$ is even, this pullback kills the $\mathcal{L}_{\chi_2}$ determinant). □

REMARK 10.2.5. In Theorem 10.2.4 above, we omitted the case $D = 2$. For $\mathcal{H} := \mathcal{H}_{small,3,1}$, $\mathcal{H}$ is symplectic, so when its $G_{\rm geom}$ is infinite, it must be ${\rm Sp}_2 = {\rm SL}_2$, and so $\mathcal{F}(3, 1, \mathbb{1})$ will have the same $G_{\rm geom} = {\rm Sp}_2$ when infinite. By Theorem 2.4.4, $G_{\rm geom}$ will be infinite for $p > 2w + 1 = 5$. For $p = 5$ and for $p = 2$, $G_{\rm geom}$ is finite: for $p = 5$ it is a case of $A = (q + 1)/2$, and for $p = 2$ it is Pink-Sawin. For $\mathcal{H} := \mathcal{H}_{big,2,1,\theta}$, we have $p$ odd, and its determinant is $\mathcal{L}_\psi \otimes \mathcal{L}_{\chi_2}$, so when its $G_{\rm geom}$ is infinite, it must be $\{\gamma \in {\rm GL}_2 | \det(\gamma)^{2p} = 1\}$. Thus $\mathcal{F}(2, 1, \theta)$ will have $G_{\rm geom} = \{\gamma \in {\rm GL}_2 | \det(\gamma)^p = 1\}$. Again by Theorem 2.4.4, $G_{\rm geom}$ for $\mathcal{F}(2, 1, \chi)$ will be infinite for $p > 5$. In fact for $p = 3$, $G_{\rm geom}$ is finite precisely when $\chi = \chi_2$, and for $p = 5$ $G_{\rm geom}$ is infinite for all nontrivial $\chi$. This "in fact" statement is an instance of the computer calculation used for low $D$ in Theorem 10.2.6 below.

Now we can prove the main result of the section, which determines which $\mathcal{F}(A,1,\chi)$ have finite monodromy.

THEOREM 10.2.6. *Let $p$ be a prime and let $A \in \mathbb{Z}_{\geq 2}$ be coprime to $p$. Consider the local system $\mathcal{F}(A,1,\chi)$ in characteristic $p$, of rank $D = A-1$ if $\chi = \mathbb{1}$ and $D = A$ otherwise, with geometric monodromy group $G = G_{\mathrm{geom}}$. Assume in addition that $D \geq 2$. Then $G$ is finite if and only if one of the following condition holds.*

(i) *$p > 2$, $A = (q+1)/2$ for some power $q = p^f$, and $\chi = \mathbb{1}$ or $\chi = \chi_2$.*
(ii) *$p$ arbitrary, $q = p^f$, $A = (q^n+1)/(q+1)$ for some odd integer $n \geq 3$, and $\chi^{q+1} = \mathbb{1}$.*
(iii) *$p > 2$, $A = 2q-1$ for some power $q = p^f$, and $\chi = \chi_2$.*
(iv) *$q = p^f$, $A = q+1$, and $\chi = \mathbb{1}$.*
(v) *$p = 3$, $A = 23$, and $\chi = \chi_2$.*
(vi) *$p = 5$, $A = 7$, and $\chi = \mathbb{1}$.*

PROOF. (a) The fact that $\mathcal{F} := \mathcal{F}(A,1,\chi)$ has finite monodromy in the cases (i)–(vi) is known. In cases (i) and (ii), finiteness results from the van der Geer-van der Vlugt argument, cf [**KT1**, Theorems 4.2 and 4.3]. For case (iii), cf. [**GKT**, Theorem 3.1]. Case (iv) is the Pink–Sawin case, cf. [**KT1**, 4.1 and 20.3]. Case (v) is $\mathsf{Co}_3$, cf. [**KRLT1**, Theorem 4.2], and case (vi) is $2.\mathrm{J}_2$, cf. [**KRL**, Theorem 3.4].

We will keep the same notations $H$, $\mathcal{H}$, $g_0$ and the opening arguments in part (a) of the proof of Theorem 10.2.4. From now on we assume that $G$ is finite. Leaving aside the cases of $\mathcal{F}(9,1,\mathbb{1})$ and $\mathcal{F}(5,1,\mathbb{1})$ with $p=2$ included in (iv), and $\mathcal{F}(5,1,\mathbb{1})$ with $p=3$ included in (i), we may assume by Lemma 10.1.7 that $\mathcal{H}$ is (**S**+). Since $G$ is finite, $H$ is finite, and we can apply Lemma 1.1.3 to $H$.

(b) Note that for $A \geq 3$, the dimension of the wild part of $\mathcal{H}$ is $w = A-1 \geq 2$; let $q_0$ denote the $p$-part of $w$. By Mitchell's theorem [**Mit**], for $D > 4$, no finite primitive subgroup of $\mathrm{GL}_D$ contains a complex reflection of order $\geq 3$, and for $D = 3,4$, no finite primitive subgroup of $\mathrm{GL}_D$ contains a complex reflection of order $\geq 4$. Combining this with Theorem 2.4.4 and Theorem 10.1.12, we see that $\mathcal{F}(A,1,\chi)$ with nontrivial $\chi$ can have finite monodromy in given characteristic $p$ only for $p \leq 2A-1$ and for an explicit finite list of possible $\chi$ for each pair $(p, A=D)$, namely $\chi^{2(q_0+1)} = \mathbb{1}$ if $D > 4$ and $\chi^{6(q_0+1)} = \mathbb{1}$ if $D = 3,4$. And for $\mathcal{F}(A,1,\mathbb{1})$ of rank $D = A-1$, we must check each of these, again for $p \leq 2A-1$.

In the case $A = 2$, no finite primitive subgroup of $\mathrm{GL}_A$ contains a complex reflection of order $\geq 6$. (Indeed, any such group satisfies (**S**+) by Lemma 1.1.2, and so is either almost quasisimple, or an extraspecial normalizer by Lemma 1.1.3. In dimension $A = 2$ and up to extension by a group of scalars, any group of the first kind is $\mathrm{SL}_2(5)$, and any (primitive) group of the second kind is either $2\mathsf{A}_4 \cong \mathrm{SL}_2(3)$ or isoclinic to $2\mathsf{S}_4 \cong \mathrm{GL}_2(3)$, see e.g. Lemma 1.1 and Theorem 1.2 of [**DZ**]. For these groups, the statement can be checked using [**GAP**].) By Theorem 2.4.4, $G_{\mathrm{geom}}$ must be infinite for $p \geq 7$. As $p$ is odd for $\mathcal{H}_{big,2,1,\overline{\rho}}$, we need only check finiteness in characteristics $p = 3,5$. By Lemma 10.1.13, $G_{\mathrm{geom}}$ contains a scalar multiple of a complex reflection of determinant $\rho^2\chi_2$ if $\rho^2 \neq \chi_2$, hence $\rho^2\chi_2$ must have order $\leq 5$ if $G_{\mathrm{geom}}$ is possibly finite. Thus $\chi = \rho^2$ must have order $\leq 10$, so the only cases we need examine for finiteness are $\mathcal{F}(2,1,\chi)$ with $\chi$ of order $\leq 10$ in characteristics $p = 3,5$.

A computer check of the $V$-criterion for finiteness run on Mathematica shows that for $2 \leq D \leq 28$, one of (i)–(vi) holds whenever the monodromy is finite. [More precisely, the

$V$-test fails except in these cases, and as noted above we know that these cases indeed have finite monodromy.] Hence, from here on we may assume that $D \geq 29$.

First consider the case $H$ is an extraspecial normalizer in characteristic $r$; in particular, $D = q$ is a power of $r$. Since $D \geq 11$, we have $p = r$ by [**KT5**, Theorem 9.19]. This rules out the cases $\chi \neq \mathbb{1}$, as otherwise we would have $p|D = A$. Hence $\chi = \mathbb{1}$, $A = D + 1 = q + 1$, and we arrive at the Pink–Sawin case (iv).

We may henceforth assume that $H$ is almost quasisimple; let $S$ denote the non-abelian composition factor of $H$, and recall that $g_0$ is $\mathsf{ssp}$ on $V$ and that (3.1.0.1) holds. Then $L := H^{(\infty)}$ is a quasisimple cover of $S$ and acts irreducibly on $V$ by Lemma 1.1.6.

By Theorem 3.1.3, the assumption $D \geq 29$ rules out the case $S$ is a sporadic simple group. We will now analyze the remaining possibilities for $S$. Note that, in the case $S$ is of Lie type, since $D \geq 15$, by Theorem 3.1.10 we have that the defining characteristic of $S$ is $p$, and will apply Theorem 3.1.5 to $H$. Let $Q$ denote the image of $P(\infty)$ in $H$, and let $g_\infty$ be a $p'$-element that generates the image of $I(\infty)$ modulo $Q$, cf. Proposition 2.4.3(ii).

(c) Here we consider the case $S = \mathrm{PSL}_2(q)$, with $q = p^f$, and $13 \leq D \leq q+1$. Then $q \geq 13$, and so $L$ is a quotient of $\mathrm{SL}_2(q)$. As $L$ is irreducible on $V$, we see that $D = q$, $q \pm 1$, or $p > 2$ and $D = (q \pm 1)/2$.

Suppose $D = (q-1)/2$. If $\chi \neq \mathbb{1}$, then $\bar{\mathsf{o}}(g_0) = A = (q-1)/2$, and this case is impossible by [**KT5**, Theorem 9.11]. If $\chi = \mathbb{1}$, then $A = (q+1)/2$, leading to (i).

Suppose $D = (q+1)/2$. If $\chi \neq \mathbb{1}$, then $A = (q+1)/2$, $w = (q-1)/2$, and $q_0 = 1$. Now, the case $\chi = \chi_2$ is included in (i), whereas $\chi^2 \neq \mathbb{1}$ is impossible since it would yield a scalar multiple of a complex reflection in $H$ by Theorem 10.1.12. Assume now that $\chi = \mathbb{1}$, so that $w = (q+1)/2$. As $p \nmid D$, $p \nmid |\mathbf{Z}(H)|$ by [**KT5**, Proposition 4.8(iv)], whence $Q$ embeds in the subgroup $\mathrm{PSL}_2(q) \rtimes C_f$ of $\mathrm{Aut}(S)$. Since $q = p^f \geq 27$, by [**Zs**] we can find a primitive prime divisor $\ell$ of $p^{2f} - 1$, so that $\ell|(q+1)$ and $\ell \geq 2f + 1$. By [**KRLT4**, Proposition 4.8], some power $h$ of $g_\infty$ has central order $\ell$, hence $h \in \mathbf{Z}(H)L$. Now, $h$ normalizes $Q_1 := Q \cap \mathbf{Z}(H)L$, which can be viewed as a $p$-subgroup of $\mathrm{SL}_2(q)$. By Lemma 10.2.1, $Q_1 = 1$. This in turn imply that $Q \hookrightarrow H/\mathbf{Z}(H)L$, and so $|Q| \leq f < (q+1)/2$. This is impossible, since $Q$ has $(q+1)/2$ distinct linear characters on $\mathsf{Wild}$ by [**KRLT4**, Proposition 4.8].

Suppose $D = q$. As $p \nmid A$, we have $A = D + 1$ and $\chi = \mathbb{1}$, leading to (iv).

Suppose $D = q+1$. If $\chi = \mathbb{1}$, then $w = q+1$, and we can repeat the above arguments of $(D, \chi) = ((q+1)/2, \mathbb{1})$ verbatim to rule it out. So $\chi \neq \mathbb{1}$, $w = q$, and $|Q| \geq q^2$ by [**KRLT4**, Proposition 4.9]. On the other hand, as $p \nmid \mathbf{Z}(H)$ by [**KT5**, Proposition 4.8(iv)], $Q \hookrightarrow \mathrm{PSL}_2(q) \rtimes C_f$ and so $|Q| \leq qf < q^2$, a contradiction.

Finally, assume that $D = q - 1 \geq 29$. As $p \nmid A$, we have $A = D$, and so $\chi \neq \mathbb{1}$ and $w = q - 2$. Suppose $p > 2$. Then, by Proposition 2.4.3(ii), $q - 2$ divides $\bar{\mathsf{o}}(g_\infty)$, hence also $|\mathrm{Aut}(S)| = 2fq(q^2-1)$. It follows that $p^f - 2 \leq 3f$, which is impossible. Suppose $p = 2$. Then, by Proposition 2.4.3(ii), $q/2 - 1$ divides $\bar{\mathsf{o}}(g_\infty)$, hence also $|\mathrm{Aut}(S)| = fq(q^2-1)$. It follows that $2^{f-1} - 1 \leq 3f$, which is impossible unless $q = 2^5$. In the latter case, $p \nmid D$, so $p \nmid |\mathbf{Z}(H)|$ by [**KT5**, Proposition 4.8(iv)], and so $Q$ embeds in $\mathrm{SL}_2(q) \rtimes C_5$. In particular, $Q$ is abelian, which is impossible by [**KRLT4**, Proposition 4.9] since $2|w$.

(d) Here we consider the case $S = \mathrm{PSL}_n(q)$ with $q = p^f$ and $n \geq 3$. As $D \geq 29$, by Theorem 3.1.5 we have that $L$ is a quotient of $\mathrm{SL}_n(q)$ and $D = (q^n - q)/(q-1)$ or $(q^n - 1)/(q-1)$.

Suppose $D = (q^n - q)/(q-1)$. As $p \nmid A$, we must have that $A = D+1$, whence $\chi = \mathbb{1}$ and $w = D$. In this case, Proposition 2.4.3 shows that $\bar{\mathsf{o}}(g_\infty)$ is divisible by $(q+1)(q^{n-1} - 1)/(q-1) > (q^n - 1)/(q-1)$, contradicting the equality

$$\text{(10.2.6.1)} \qquad \mathrm{meo}(\mathrm{Aut}(S)) = (q^n - 1)/(q-1)$$

of [**GMPS**, Theorem 2.16].

Suppose $D = (q^n - 1)/(q-1)$; in particular $q > 2$. If $\chi \neq \mathbb{1}$, then $w = D - 1 = (q^n - q)/(q-1)$. In this case, Proposition 2.4.3 shows that $\bar{\mathsf{o}}(g_\infty)$ is divisible by $(q+1)(q^{n-1} - 1)/(q-1) > (q^n - 1)/(q-1)$, contradicting (10.2.6.1). Hence $\chi = \mathbb{1}$, and $w = D$. By Theorem 3.1.8, $H/\mathbf{Z}(H) \cong \mathrm{PGL}_n(q)$. As $p \nmid D$, $p \nmid |\mathbf{Z}(H)|$ by [**KT5**, Proposition 4.8(iv)], whence $Q$ embeds in $\mathrm{PSL}_n(q)$. Since $D \geq 29$ and $q > 2$, by [**Zs**] we can find a primitive prime divisor $\ell$ of $p^{nf} - 1$, so that $\ell | w$ and $\ell$ is coprime to $q - 1$ and $|H/\mathbf{Z}(H)L|$. By [**KRLT4**, Proposition 4.8], some power $h$ of $g_\infty$ has central order $\ell$, hence $h \in \mathbf{Z}(H)L$. Now, $h$ normalizes $Q$, which can be viewed as an elementary abelian of $\mathrm{SL}_n(q)$. By Lemma 10.2.1, $Q = 1$, a contradiction.

(e) Next assume that $S = \mathrm{PSp}_{2n}(q)$ with $q = p^f$, $p > 2$, and $n \geq 2$. As $D \geq 29$, by Theorem 3.1.5 we have that $L$ is a quotient of $\mathrm{Sp}_{2n}(q)$ and $D = (q^n \pm 1)/2$.

Suppose $D = (q^n - 1)/2$. If $\chi \neq \mathbb{1}$, then $\bar{\mathsf{o}}(g_0) = A = (q^n - 1)/2$, and this case is impossible by [**KT5**, Theorem 9.11]. If $\chi = \mathbb{1}$, then $A = (q^n + 1)/2$, leading to (i).

Suppose $D = (q^n + 1)/2$. If $\chi \neq \mathbb{1}$, then $A = D$, $w = (q^n - 1)/2$, and $q_0 = 1$. Now, the case $\chi = \chi_2$ is included in (i), whereas $\chi^2 \neq \mathbb{1}$ is impossible since it would yield a scalar multiple of a complex reflection in $H$ by Theorem 10.1.12. Assume now that $\chi = \mathbb{1}$, so that $w = (q^n + 1)/2$. By Theorem 3.1.8, $H/\mathbf{Z}(H) \cong S$, so $H = \mathbf{Z}(H)L$. As $p \nmid D$, $p \nmid |\mathbf{Z}(H)|$ by [**KT5**, Proposition 4.8(iv)], whence $Q$ embeds in $S$. Since $n \geq 2$, by [**Zs**] we can find a primitive prime divisor $\ell$ of $p^{2nf} - 1$, so that $\ell | w$. By [**KRLT4**, Proposition 4.8], some power $h$ of $g_\infty$ has central order $\ell$. Now, $h$ normalizes $Q$, which can be viewed as an elementary abelian of $\mathrm{Sp}_{2n}(q)$. By Lemma 10.2.1, $Q = 1$, a contradiction.

(f) Next assume that $S = \mathrm{PSU}_n(q)$ with $q = p^f$, $2 \nmid n \geq 3$. As $D \geq 29$, by Theorem 3.1.5 we have that $L$ is a quotient of $\mathrm{SU}_n(q)$, $D = (q^n - q)/(q+1)$ or $D = (q^n + 1)/(q+1)$, and $H/\mathbf{Z}(H) \cong \mathrm{PGU}_n(q)$ by Theorem 3.1.8.

Suppose $D = (q^n - q)/(q+1)$. As $p \nmid A$, we must have $A = D + 1 = (q^n + 1)/(q+1)$ and $\chi = \mathbb{1}$, leading to (ii).

Suppose $D = (q^n + 1)/(q+1)$. If $\chi \neq \mathbb{1}$, then $A = D$, $w = (q^n - q)/(q+1)$, and $q_0 = q$. Now, the case $\chi^{q+1} = \mathbb{1}$ is included in (ii), whereas $\chi^{q+1} \neq \mathbb{1}$ is impossible since it would yield a scalar multiple of a complex reflection in $H$ by Theorem 10.1.12. Assume now that $\chi = \mathbb{1}$, so that $w = (q^n + 1)/(q+1)$. As $p \nmid D$, $p \nmid |\mathbf{Z}(H)|$ by [**KT5**, Proposition 4.8(iv)], whence $Q$ embeds in $S$. Since $n \geq 3$ and $D \geq 29$, by [**Zs**] we can find a primitive prime divisor $\ell$ of $p^{2nf} - 1$, so that $\ell | w$ and $\ell$ is coprime to $q + 1$ and $|H/\mathbf{Z}(H)L|$. By [**KRLT4**, Proposition 4.8], some power $h$ of $g_\infty$ has central order $\ell$, and so $h$ belongs to $\mathbf{Z}(H)L$. Now, $h$ normalizes $Q$, which can be viewed as an elementary abelian of $\mathrm{SU}_n(q)$. By Lemma 10.2.1, $Q = 1$, a contradiction.

(g) Now we consider the case $S = \mathrm{PSU}_n(q)$ with $q = p^f$, $2 \mid n \geq 4$. As $D \geq 29$, by Theorem 3.1.5 we have that $L$ is a quotient of $\mathrm{SU}_n(q)$, $D = (q^n - 1)/(q+1)$ or $D = (q^n + q)/(q+1)$, and $H/\mathbf{Z}(H) \cong \mathrm{PGU}_n(q)$ by Theorem 3.1.8.

Suppose $D = (q^n-1)/(q+1)$. As $p \nmid A$, we must have $A = D$, $\chi \neq \mathbb{1}$, and $\bar{\mathsf{o}}(g_0) = D$. This is however impossible by [**KT5**, Theorem 9.17].

Suppose $D = (q^n+q)/(q+1)$. As $p \nmid A$, we must have that $A = D+1$ and $\chi = \mathbb{1}$. By Proposition 2.4.3(i), $g_0$ is an $\mathsf{ssp}$-element of central order $D+1$. Applying [**KT5**, Theorem 8.13], we must have that $D+1 = (q^a+1)(q^b+1)/(q+1)$ for some $a,b \geq 1$ with $n = a+b$, which is impossible.

(h) Finally, we consider the case $S = \mathsf{A}_n$ for some $n \geq 5$. In fact, the assumption $D \geq 29$ together with Theorem 10.3.5 and [**KT5**, Lemma 9.1] show that $n \geq 10$, $D = n-1$ and $L = S = \mathsf{A}_n$ acts on $V$ as on the deleted permutation module $\mathbb{C}^{n-1}$; in particular, $\mathrm{Aut}(S) \cong \mathsf{S}_n$.

(h1) First suppose that $\chi \neq \mathbb{1}$, so that $p \nmid A = D = n-1$. Consider the case $2 \nmid n$, whence $p > 2$ and $Q \leq \mathbf{Z}(H)S$. In fact, as $p \nmid D$, $p \nmid |\mathbf{Z}(H)|$ by [**KT5**, Proposition 4.8(iv)], whence $Q \leq S$ and so the $Q$-module $V$, which is $\mathsf{Wild} \oplus \mathsf{Tame}$, is self-dual. It follows that $\mathsf{Wild}$, of odd dimension $n-2$, is self-dual over $Q$, contradicting Lemma 10.1.16. Hence $2|n$. Now, the spectrum of $g_0$ on $\mathbb{C}^{n-1}$ is just $\mu_{n-1}$, which shows by Theorem 10.3.5 that $g_0$ induces an $(n-1)$-cycle in $\mathsf{S}_n$. As $2|n$, Theorem 1.2.2 that $H = \mathbf{Z}(H)S$. Again using $p \nmid D$ we get $p \nmid |\mathbf{Z}(H)|$, and so $Q \leq S$. Recalling $\dim \mathsf{Tame} = 1$, we see in that case that the $p$-subgroup $Q < \mathsf{A}_n$ acting on the natural permutation module $\mathbb{C}^n$ has 2-dimensional fixed point subspace, which means that $Q$ has precisely two orbits while acting on $\Omega := \{1,2,\ldots,n\}$ and so, using $n > 2$ and $p \nmid (n-1)$,

$$n = p^a + p^b \text{ with } a \geq b \geq 1.$$

Suppose that $a > b$. Then $\mathbf{N}_{\mathsf{S}_n}(Q)$ must preserve these two orbits of length $p^a$ and $p^b$ on $\Omega$, and so it acts on $\mathbb{C}^{n-1}$ with at least 3 simple summands. On the other hand, the image $J$ of $I(\infty)$ acts irreducibly on both $\mathsf{Wild}$ and $\mathsf{Tame}$, a contradiction. We have shown that

$$n = 2p^a. \tag{10.2.6.2}$$

Assume in addition that $p \nmid w = n-2$, so that $q_0 = 1$ and $p > 2$. If $\chi \neq \chi_2$, then Theorem 10.1.12 implies that $H$ contains a scalar multiple of a complex reflection of order $> 2$, whereas $H$ can contain only a scalar multiple of a true reflection, a contradiction. Hence $\chi = \chi_2$, and we can use (10.2.6.2). If $a = b$ we arrive at (iii).

Now suppose that $w = n-2 = w_0p^e$ with $p \nmid w_0$ and $e \geq 1$, whence $p = 2$ by (10.2.6.2). Then $g_\infty$ has odd order but still normalizes $Q$, so it stabilizes each of the two $Q$-orbits on $\Omega$. This again contradicts the prescribed action of $J = Q \rtimes \langle g_\infty \rangle$ on $V$.

(h2) Finally, we consider the case $\chi = \mathbb{1}$, so that $A = n$. If $2 \nmid n$, then $\mathcal{H}$ is symplectic, cf. [**Ka-MMP**, 3.10.2-3], whereas the $S$-module $V$ is orthogonal, a contradiction. So $2|n$ and $p > 2$. Assume in addition that $p \nmid (n-1) = D$. Then we again have $p \nmid |\mathbf{Z}(H)|$, and so $Q \leq S$ and the $Q$-module $V = \mathsf{Wild}$ is self-dual of odd dimension $n-1$, contradicting Lemma 10.1.16. Hence $p|(n-1)$; write $w = n-1 = w_0p^e$ with $p \nmid w_0$ and $e \geq 1$. By Proposition 2.4.3 (and [**KRLT4**, Proposition 4.9]), $g_\infty$ is an $\mathsf{ssp}$-element of central order $w_0(p^e+1) \leq (4/3)(n-1)$. Now, if $w_0 = 1$, then we arrive at (iv). Suppose $w_0 \geq 2$. Then $w_0(p^e+1) = n-1+w_0 > n$, so the permutation $\pi \in \mathsf{S}_n$ induced by $g_\infty$ cannot be an $n$-cycle or an $(n-1)$-cycle. Hence $\bar{\mathsf{o}}(g_\infty) = k(n-k)$ for some $1 < k < n/2$ coprime to $n$, by Theorem 10.3.5. It follows that $\bar{\mathsf{o}}(g_\infty) \geq 2(n-2) > (4/3)(n-1)$, a contradiction. □

The next result determines the geometric monodromy group of $\mathcal{F}(A,1,\chi)$ when it is finite (recall the infinite case has been treated in Theorem 10.2.4).

THEOREM 10.2.7. *Let $p$ be a prime and let $A \in \mathbb{Z}_{\geq 2}$ be coprime to $p$. Consider the local system $\mathcal{F}(A,1,\chi)$ in characteristic $p$ of rank $D \geq 2$ with geometric monodromy group $G = G_{\mathrm{geom}}$. Then, in the cases where $G$ is finite, as listed in Theorem 10.2.6, $G$ is as follows.*

(i) *Suppose that $p > 2$, $A = (q+1)/2$ for some power $q = p^f$, and $\chi = \mathbb{1}$ or $\chi = \chi_2$. Then $G$ is the image of $\mathrm{SL}_2(q)$ in a Weil representation of degree $D = A-1$ when $\chi = \mathbb{1}$ and of degree $D = A$ when $\chi = \chi_2$.*

(ii) *Suppose $p$ arbitrary, $q = p^f$, $A = (q^n+1)/(q+1)$ for some odd integer $n \geq 3$, and $\chi^{q+1} = \mathbb{1}$. If $(n,q) \neq (3,2)$, then $G$ is the image of $\mathrm{SU}_n(q)$ in a Weil representation of degree $D = A-1$ when $\chi = \mathbb{1}$ and of degree $D = A$ when $\chi \neq \mathbb{1}$. If $(n,q) = (3,2)$, then $G \cong 2^{1+2}_-$ if $\chi = \mathbb{1}$ and $G \cong 3^{1+2}_+ \rtimes 2^{1+2}_-$ if $\chi \neq \mathbb{1}$.*

(iii) *Suppose $p > 2$, $A = 2q-1$ for some power $q = p^f$, and $\chi = \chi_2$. Then $G = \mathsf{A}_{2q}$ in the deleted permutation module of dimension $2q-1$.*

(iv) *Suppose $q = p^f$, $A = q+1$, and $\chi = \mathbb{1}$. If $p > 2$, $G$ is the Heisenberg group $p^{1+2f}_+$ of order $pq^2$ and exponent $p$. If $p = 2$, $G$ is the extraspecial 2-group $2^{1+2f}_-$.*

(v) *Suppose $p = 3$, $A = 23$ and $\chi = \chi_2$. Then $G = \mathsf{Co}_3$.*

(vi) *Suppose $p = 5$, $A = 7$, and $\chi = \mathbb{1}$. Then $G = 2.\mathrm{J}_2$.*

PROOF. (i) This is [**KT1**, Theorem 17.2] when $q > 3$; note that $G$ is $\mathrm{SL}_2(q)$ when $2|D$, and $\mathrm{PSL}_2(q)$ when $2 \nmid D$. Suppose that $q = 3$, and so $\chi = \chi_2$ as $D \geq 2$. By Lemma 10.1.7, $\mathcal{H} = \mathcal{H}_{big,3,1,\chi}$ is $(\mathbf{S}+)$, and has traces in $\mathbb{Q}(\zeta_{12})$. We can apply Lemma 1.1.3 to its geometric monodromy group $H$ and use [**HM**] to rule out the case $H$ is almost quasisimple. So $H$ contains a normal subgroup $R \cong 2^{1+2}_{\epsilon}$ for some $\epsilon = \pm$. As the image $Q \cong C_3$ of $P(\infty)$ in both $G$ and $H$ injects in $H/\mathbf{Z}(H)$ by [**KT5**, Proposition 4.8(i)], we have that $\epsilon = -$, and thus $H/\mathbf{Z}(H) \leq \mathrm{Aut}(R)$ has order 3 or 6. In particular, $G = \mathbf{O}^{3'}(G) \leq \mathbf{O}^{3'}(H) \leq \mathbf{Z}(H)R \cdot C_3$. Since $Q \leq G$, we have that $\mathbf{Z}(H)GR = \mathbf{Z}(H)R \cdot C_3$. Note that $Q$ acts irreducibly on $R/\mathbf{Z}(R)$ and $\mathbf{Z}(H) \leq \mathbf{Z}(G) \leq \mathbf{Z}(H)$. Now, if $\mathbf{Z}(H)G \not\geq R$, then $\mathbf{Z}(H)G = \mathbf{Z}(H) \cdot C_3$ and so by Ito's theorem [**Is**, (6.15)] cannot act irreducibly on $\mathcal{H}$. So $\mathbf{Z}(H)G = \mathbf{Z}(H)R \cdot C_3$. Comparing the order and using $\mathbf{Z}(H) \cap G = \mathbf{Z}(G)$, we then have that $|G| = 3|\mathbf{Z}(G)| \cdot |R|/2 = 12|\mathbf{Z}(G)|$. On the other hand, any $z \in \mathbf{Z}(G)$ acts on $\mathcal{F}(2,1,\chi_2)$ as $\zeta \cdot \mathrm{Id}$, with trace belonging to $\mathbb{Q}(\zeta_3)$, so $\zeta^6 = 1$ and so $a := |\mathbf{Z}(G)|$ divides 6. Also, $b := |H/G| \leq 2$, so we see that $|H|$ divides 144. Now, some element $1 \neq h \in Q$ acts as $\mathrm{diag}(1,\zeta_3)$ and a generator $g_0$ of the image of $I(0)$ in $H$ acts as $\mathrm{diag}(1,-1)$. As $H$ is generated by the normal closure of $g_0$ and $h$, see [**KRLT4**, Theorems 4.2 and 4.3], it follows that $H$ is generated by (and contain) complex reflections of order 2 and 3, and primitive. Using the classification result of [**ST**], we then see that $|H| = 48$ or 144, in fact it is either $C_4 * \mathrm{SL}_2(3)$, $C_{12} * \mathrm{SL}_2(3)$, or $C_6 * 2\mathsf{S}_4$.

Solving the equation $|H| = 12ab$, we obtain $b = 2$ and $a = 2$ or 6. Since $G = \mathbf{O}^{3'}(G)$ and $b = 2$, we get $G = \mathrm{SL}_2(3)$ or $C_3 \times \mathrm{SL}_2(3)$. We will show that in fact $G = \mathrm{SL}_2(3)$ as follows. A computation using $\mathsf{Magma}$ over $\mathbb{F}_9$ shows that $\mathsf{Frob}_{0,\mathbb{F}_9}$ has trace 2 (using the clearing factor $3^f$ over $\mathbb{F}_{9^f}$), and hence by Lemma 10.1.17 we have $G := G_{\mathrm{geom}} = G_{\mathrm{arith}}$. A second computation using $\mathsf{Magma}$ over $\mathbb{F}_{9^4}$ shows, by Lemma 2.5.4, whose $S_\infty = 2$, that

$$\Big|\frac{1}{|G|} - \frac{253}{9^4}\Big| \leq \frac{1}{3^4},$$

hence $\frac{1}{|G|}$ lies in the interval $[\frac{253}{9^4}-\frac{1}{3^4}, \frac{253}{9^4}+\frac{1}{3^4}] = [0.0262\ldots, 0.0509\ldots]$, and hence

$$19.6 \leq |G| \leq 38.2,$$

hence $G = \mathrm{SL}_2(3)$. Note that $\mathrm{SL}_2(3)$ has three irreducible representations of degree 2, two non-self-dual Weil representations and one self-dual. Since $\mathcal{F}$ is not self-dual, $G$ acts on $\mathcal{F}$ via a Weil representation.

(ii) For $2 \nmid q$, this is [**KT3**, Theorem 4.4].

Suppose $2|q$ and $A = (q^n+1)/(q+1) > 3$; in particular, $\mathcal{F}$ has rank $D \geq 10$. Then, as mentioned in part (a) of the proof of Theorem 10.2.6, the geometric monodromy group $H$ of the corresponding hypergeometric sheaf $\mathcal{H}$ is $(\mathbf{S}+)$, and we can apply Lemma 1.1.3 to the finite group $H$. Now, if $H$ is an extraspecial normalizer, then $p = 2$ forces $D$ to be a 2-power, a contradiction. Hence, $H$ is almost quasisimple. Let $S$ denote the unique non-abelian composition factor of $H$, which is also for $G$. Note that the case $A = 13$, i.e. $(n,q) = (3,4)$ is [**KT1**, Theorem 19.1]. Assume in addition that $(n,q) \neq (5,2)$, so that $D \geq 42$. By Theorems 10.3.5, 3.1.3, and 3.1.5, $S = \mathsf{A}_{D+1}$ in the deleted permutation module, or else $S$ is of Lie type in characteristic $r$, in which case $r = 2$ by Theorem 3.1.10. Now Theorem 10.2.6 and its proof rules out the former case, and shows that in the latter case $S = \mathrm{PSU}_m(q')$ for some odd $m \geq 3$ and some 2-power $s$, and $A = (s^m+1)/(s+1)$; in particular, the 2-part of $A-1$ is $s$. Since we also have $A = (q^n+1)/(q+1)$, the 2-part of $A-1$ is $q$, hence $s = q$ and $m = n$. By Theorem 3.1.5(iii), $E(H)$ is the image of $\mathrm{SU}_n(q)$ in a Weil representation of degree $D$. Moreover, $H/\mathbf{Z}(H) \cong \mathrm{PGU}_n(q)$ by [**KT5**, Corollary 8.4]. Now, as $H/G$ is cyclic and $G$ is generated by its Sylow $p$-subgroups but $[\mathrm{PGU}_n(q) : S]$ is $p'$, we have that $G/\mathbf{Z}(G) \cong S$ and that $G = \mathbf{Z}(G)E(G)$ with $E(G) = E(H)$. If $\chi \neq \mathbb{1}$, then $D = A$ is $p'$, and so $p \nmid |\mathbf{Z}(G)|$, so $G = \mathbf{O}^{p'}(G)$ forces $G = E(G)$. Suppose $\chi = \mathbb{1}$; in particular $E(G) = E(H) = S$. Then $\mathcal{H}$ is of symplectic type [**Ka-ESDE**, 8.8.1–2], implying $\mathbf{Z}(H) \leq C_2$. If $\mathbf{Z}(G) = 1$, then $G = E(G)$ as stated. Otherwise we have $\mathbf{Z}(H) = \mathbf{Z}(G) \cong C_2$. In such a case,

$$(H/S)/(\mathbf{Z}(H)S/S) \cong H/\mathbf{Z}(H)S \cong (H/\mathbf{Z}(H))/(\mathbf{Z}(H)S/\mathbf{Z}(H)) \cong \mathrm{PGU}_n(q)/S$$

is cyclic of $2'$-order $e := \gcd(n, q+1)$ and $\mathbf{Z}(H/S) \geq \mathbf{Z}(H)S \cong C_2$, whence $H/S$ is abelian of order $2e$ and so $H$ has a normal subgroup $H_1$ of index 2. But note that a generator $g_0$ of the image of $I(0)$ in $H$ has odd order, so $h_0 \in H_1$, and Theorem 1.2.2 shows that $H = H_1$, a contradiction.

Consider the case $A = 11$. If $S = \mathrm{SU}_5(2)$, then the above arguments show that $G \cong \mathrm{SU}_5(2)$ in a Weil representation. Suppose $S \neq \mathrm{SU}_5(2)$. The proof of Theorem 10.2.6 already showed that $S$ is not an alternating group or a group of Lie type. Applying [**HM**] and using the symplectic type of $\mathcal{F}(11,1,\mathbb{1})$, we see $S = \mathrm{SU}_5(2)$ when $\chi = \mathbb{1}$. So $\chi \neq \mathbb{1}$, of order 3, and $E(H) = S \cong \mathrm{M}_{11}$ or $E(H) = S \cong \mathrm{M}_{12}$ by [**HM**]. Using [**CCNPW**], we also see that $H = S \times \mathbf{Z}(H)$. Since $D = 11$ is $2'$, $2 \nmid |\mathbf{Z}(H)|$. Recalling that $H/G$ is cyclic and $G = \mathbf{O}^{2'}(G)$, we must have that $G = S$. Since the 11-dimensional representations of $S$ are self-dual, this means that $\mathcal{F}$ is self-dual, which is however not the case.

Now we consider the case $A = 3$. If $\chi = \mathbb{1}$, then it is (iv). Suppose $\chi \neq \mathbb{1}$. We still know that $\mathcal{H} = \mathcal{H}_{big,3,1,\chi}$ is still $(\mathbf{S}+)$ and has traces in $\mathbb{Q}(\zeta_3)$. Using [**HM**] we can rule out the case $H$ is almost quasisimple. Hence, by Lemma 1.1.3, $H$ contains a normal subgroup $R \cong 3^{1+2}_\epsilon$ acting irreducibly on $\mathcal{H}$, with $\epsilon = \pm$. Since $D = 3$, we we have $2 \nmid |\mathbf{Z}(H)|$. But $\mathbf{Z}(H) \geq \mathbf{Z}(R)$ and has traces in $\mathbb{Q}(\zeta_3)$, so $\mathbf{Z}(H) = \mathbf{Z}(R)$. In turn, this implies that

$H/R \hookrightarrow \mathrm{Aut}_0(R)/\mathrm{Inn}(R) \leq \mathrm{SL}_2(3) \cong Q_8 \rtimes C_3$, in particular, a Sylow 2-subgroup $T$ of $H$ has order $\leq 8$. As $w = 2$, the image $Q$ of $P(\infty)$ is non-abelian, forcing $|T| = 8$. Hence $H \cong R \rtimes Q_8$ or $R \rtimes \mathrm{SL}_2(3)$; in particular, $\mathbf{O}^{2'}(H) = R \times Q_8$ has index 1 or 3 in $H$. Now $G = \mathbf{O}^{2'}(G) \leq \mathbf{O}^{2'}(H)$ and $H/G \hookrightarrow C_3$, and we readily check that $G = R \rtimes Q_8$, which implies $\epsilon = +$ by [**Wi**].

(iii) is [**GKT**, Theorem 3.1], (v) is [**KRLT1**, Theorem 4.2], and (vi) is [**KRL**, Theorem 3.4].

(iv) The case $p > 2$ is [**KT1**, Theorem 21.1]. Assume $p = 2$. Then $G$ is a 2-group and $G/\mathbf{Z}(G)$ is elementary abelian of order $q^2$ by [**KT1**, Corollary 20.3]; in particular, $\mathbf{Z}(G) \neq 1$. Next, $\mathcal{F}$ is of symplectic type [**Ka-MMP**, 3.10.1–3], implying $\mathbf{Z}(G) \cong C_2$. It follows that $\Phi(G) = [G, G] = \mathbf{Z}(G)$, and so $G$ is extraspecial. Finally, $\mathcal{F}$ being symplectic implies that $G \cong 2^{1+2f}_{-}$. □

## 10.3. The $(A, B)$-case

The first result of the section shows that the main results of [**KT6**] can in fact be extended to cover all possible parameters $n > m \geq 1$, subject only to the natural condition $\gcd(n, m) = 1$ and thus removing the condition $m < n/2$ made therein. Referring the reader to §§9, 10 of [**KT6**] for precise formulations of the results alluded to, we restrict ourselves to the following statement, which is needed for our intended treatment of the $(A, B)$ exponential sums.

Recalling the sheaf $\mathcal{F}_{nngcd}(A, B, \mathbb{1})$ defined in Definition 7.3.1, for which we have the following fact, which follows from [**KT6**, Lemma 2.3].

Lemma 10.3.1. *Suppose $A > B > 0$ with $p \nmid AB$. Let $D := \gcd(A, B)$. Then on $\mathbb{A}^1/\mathbb{F}_p(\mu_D)$ we have a direct sum decomposition*

$$\mathcal{F}_{nngcd}(A, B, \mathbb{1}) \cong \bigoplus_{\chi:\chi^D=\mathbb{1}} \mathcal{F}(A/D, B/D, \chi)$$

*as the direct sum of $D$ geometrically irreducible constituents which are pairwise geometrically nonisomorphic.*

Next we recall the following well-known facts:

Lemma 10.3.2. *Let $t, k \in \mathbb{Z}_{\geq 2}$, and let $n_1, \dots, n_k \geq 0$ be integers such that* $\gcd(n_1, \dots, n_k) = 1$.

(i) $\gcd(t^{n_1} + 1, \dots, t^{n_k} + 1) = 1$ *if and only if* $2|t$ *and* $2|n_1 \dots n_k$.
(ii) *Suppose* $2 \nmid t$. *Then* $\gcd\big((t^{n_1} + 1)/2, \dots, (t^{n_k} + 1)/2\big) = 1$ *if and only if* $2|n_1 \dots n_k$.
(iii) *Suppose* $2 \nmid n_1 \dots n_k$. *Then* $\gcd\big((t^{n_1} + 1)/(t + 1), \dots, (t^{n_k} + 1)/(t + 1)\big) = 1$.

Proof. (i) Write $d := \gcd(t^{n_1} + 1, \dots, t^{n_k} + 1)$. If $2 \nmid t$ then $2|d$, and if $2 \nmid n_1 \dots n_k$ then $(t + 1)|d$. Assume now that $2|t$ and $2|n_1 \dots n_k$, say $2|n_1$. Note that $d$ divides

$$\gcd(t^{2n_1} - 1, \dots, t^{2n_k} - 1) = t^{\gcd(2n_1,\dots,2n_k)} - 1 = t^2 - 1.$$

As $2|n_1$, we have $(t^2 - 1)|(t^{n_1} - 1)$, and so $d = \gcd(d, t^{n_1} + 1) = \gcd(d, 2) = 1$.

(ii) In the notation of (i) we have $\gcd\big((t^{n_1} + 1)/2, \dots, (t^{n_k} + 1)/2\big) = d/2$. If $2 \nmid n_1 \dots n_k$, then $(t+1)|d$. Assume now that $2|n_1 \dots n_k$, say $2|n_1$. As noted above, $d$ divides $t^2 - 1$. Since $2|n_1$, we have $(t^2 - 1)|(t^{n_1} - 1)$, and so $d = \gcd(d, t^{n_1} + 1) = \gcd(d, 2) = 2$.

(iii) In the notation of (i) we have $\gcd\big((t^{n_1}+1)/(t+1), \dots, (t^{n_k}+1)/(t+1)\big) = d/(t+1)$. As noted above, we again have $d|(t^2-1)$. Since $2 \nmid n_1$, we have $(t^2-1)|(t^{n_1-1}-1)$, and so $d = \gcd(d, t^{n_1}+1) = \gcd(d, t+1) = t+1$. □

The next result completes the extraspecial normalizer case.

THEOREM 10.3.3. *Let $A > B \geq 3$ be odd integers, $\gcd(A, B) = 1$, and let $A > 9$. Suppose that the system $\mathcal{F}(A, B, \theta)$ in characteristic $p = 2$ has finite geometric monodromy group $G$, which is in the extraspecial normalizer case of Lemma 1.1.3. Then $\theta = \mathbb{1}$ and $A = 2^a + 1$ and $B = 2^b + 1$ for some integers $a > b \geq 1$ such that*

$$2\Big|\left(\frac{a}{\gcd(a,b)} \cdot \frac{b}{\gcd(a,b)}\right). \tag{10.3.3.1}$$

PROOF. Let $\mathcal{H} = \mathcal{H}_{small,A,B}$ or $\mathcal{H}_{big,A,B,\chi}$, as defined in (8.5.4.1), (8.5.4.2), be the hypergeometric sheaf corresponding to $\mathcal{F}(A, B, \theta)$. By Corollary 10.1.9, $\mathcal{H}$ has finite geometric monodromy group $H \rhd G$ which satisfies $(\mathbf{S}+)$. Hence $H$ is also in the extraspecial normalizer case of Lemma 1.1.3. By [**KT5**, Theorem 7.4], the characteristic of $H$ is 2 and the rank of $\mathcal{H}$ is a power of 2. As $2 \nmid A$, this implies that $\theta = \mathbb{1}$ and $A = 2^a + 1$ for some $a \geq 4$. In particular, $\mathcal{H} = \mathcal{H}_{small,A,B}$ and so by [**Ka-ESDE**, Thm. 8.12.2] has trivial geometric determinant. Suppose for the moment that $B = 2^b + 1$ for some $b \in \mathbb{Z}_{\geq 1}$. Applying Lemma 10.3.2 to $t := 2^c$ with $c := \gcd(a, b)$, we see that the condition $\gcd(A, B) = 1$ is equivalent to $2|(ab/c^2)$, i.e. to (10.3.3.1).

The rest of the proof is to show that we indeed have $B = 2^b + 1$ for some $b \geq 1$.

Write the dimension $w := A - B$ of the wild part as $2^e w_0$ with $1 \leq e \leq a$ and $2 \nmid w_0$, and let $g_\infty$ be a $2'$-element that generates the image of $I(\infty)$ in $H$ modulo the image of $P(\infty)$. By Proposition 2.4.3(ii), $\bar{\mathsf{o}}(g_\infty)$ is divisible by $C := w_0(2^e + 1)$ on $\mathsf{Wild}$, and by $B$ on $\mathsf{Tame}$ (since it has spectrum $\mu_B \smallsetminus \{1\}$ on $\mathsf{Tame}$ and $B \geq 3$), and so $\bar{\mathsf{o}}(g_\infty)$ is divisible by $\mathrm{lcm}(B, C)$. On the other hand, by Lemma 1.1.3(c), $g_\infty$ is an odd-order element in $\mathbf{N}_{\mathrm{GL}_{2^a}(\mathbb{C})}(R) \leq \mathbf{Z}(\mathrm{GL}_{2^a}(\mathbb{C}))R \cdot \mathrm{Sp}_{2a}(2)$. Hence, using [**GMPS**, Theorem 2.16] we have

$$\bar{\mathsf{o}}(g_\infty) \leq \mathrm{meo}(\mathrm{Sp}_{2a}(2)) \leq 2^{a+1} = 2A - 2.$$

Writing $d := \gcd(B, C)$, we then have

$$BC/d = \mathrm{lcm}(B, C) \leq \bar{\mathsf{o}}(g_\infty) \leq 2A - 2 < 2A = 2w + 2B < 2(B + C).$$

Thus $BC < 2d(B + C)$, and so $(B - 2d)(C - 2d) < 4d^2$. Recall that $d|B, C$, and $2 \nmid B, C$, in particular, either $B = d$ or $B \geq 3d$, and either $C = d$ or $C \geq 3d$. Assuming in addition that neither $B|C$ nor $C|B$, we have $4d > \min(B, C) \geq 3d$ and thus $\{B, C\} = \{3d, 5d\}$. Thus we have one of the following three cases.

*Case 1:* $B|C = w_0(2^e + 1)$. Note that $\gcd(B, w_0)$ divides $\gcd(B, w) = \gcd(B, A - B) = 1$, so in fact $B|(2^e + 1)$. Now, $2^e w_0 = w = A - B = 2^a + 1 - B$, hence $B - 1 = 2^a - 2^e w_0$ is divisible by $2^e$. As $2 \nmid B \geq 3$, we conclude that $B = 2^e + 1$, as stated.

*Case 2:* $\{B, C\} = \{3d, 5d\}$. As before, $\gcd(B, w_0) = 1$. Hence, $d = \gcd(B, C) = \gcd(B, 2^e + 1)$, and so $5d \geq C = w_0(2^e + 1) \geq w_0 d$, i.e. $w_0 \leq 5$.

Suppose $w_0 = 5$. As $\gcd(B, w_0) = 1$, we must have $B = 3d$, $5(2^e + 1) = C = 5d$, whence $d = 2^e + 1$, and $w = 5 \cdot 2^e$. Now $2^a + 1 = A = B + w = 8 \cdot 2^e + 3$, i.e. $2 = 2^{e+3} - 2^a$, a contradiction since $a \geq 4$.

Suppose $w_0 = 3$. As $\gcd(B, w_0) = 1$, we must have $B = 5d$, $3(2^e + 1) = C = 3d$, whence $d = 2^e + 1$, and $w = 3 \cdot 2^e$. Now $2^a + 1 = A = B + w = 8 \cdot 2^e + 5$, i.e. $4 = 2^{e+3} - 2^a$, again a contradiction since $a \geq 4$.

The remaining case is that $w_0 = 1$, i.e. $B = A - w = 2^a + 1 - 2^e = 2^{a-e} + 1$, as stated.

*Case 3: $C|B$ but $B \nmid C$.* Using $\gcd(B, w_0) = 1$ again, we see that $w_0 = 1$, so $w = 2^e$ and $B = 2^a - 2^e + 1$. Also, $(2^e + 1)|(2^a + 2) = 2(2^{a-1} + 1)$ implies $(a - 1)/e$ is an odd integer. If $e = a - 1$, then $B = 2^{a-1} + 1 = C$. We will assume now that $(a - 1)/e \geq 3$, so that $e \leq a - 3$. By [**KRLT4**, Proposition 4.9], there is some $\xi \in \mathbb{C}^\times$ such that $\mathrm{Spec}\,(g_\infty)$ on $\mathsf{Wild}$ is $\xi\big(\mu_{2^e+1} \smallsetminus \{1\}\big)$ and on $\mathsf{Tame}$ is $\mu_B \smallsetminus \{1\}$; in particular, $1 = \det(g_\infty) = \xi^{2^e}$. But $2 \nmid \mathsf{o}(g_\infty)$, so $\xi = 1$, and thus

$$\mathsf{o}(g_\infty) = \bar{\mathsf{o}}(g_\infty) = B = 2^a - 2^e + 1 > 7 \cdot 2^{a-3} > 2^{a-1}. \tag{10.3.3.2}$$

Also,

$$\text{the total multiplicity of repeated eigenvalues of } g_\infty \text{ is at most } 2^{e+1} \leq 2^{a-2}. \tag{10.3.3.3}$$

We will now explore the conditions (10.3.3.2) and (10.3.3.3). Recall that by [**Ka-ESDE**, Theorems 8.8.1-2], $\mathcal{H}$ is symplectic, so Lemma 1.1.3(c) shows that $\mathbf{Z}(E) = \mathbf{Z}(H) = \mathbf{C}_H(E)$ and thus $E \lhd H \leq E \cdot \mathrm{O}^-_{2a}(2)$, where $E = 2^{1+2a}_-$. Now $L = \mathsf{o}(g_\infty)$ is the same as the order of its image $\bar{g}_\infty$ in $\mathrm{O}^-_{2a}(2)$. As in [**GMPS**, §2], we can find

$$1 \leq k_1 \leq k_2 \leq \ldots \leq k_r,\ 1 \leq k_{r+1} \leq \ldots \leq k_{r+s},\ \text{with } a = \sum_{i=1}^{r+s} k_i,$$

such that

$$\begin{aligned} \bar{g}_\infty = \mathrm{diag}\big(h_1, \ldots, h_{r+s}\big) &\in \mathrm{O}^-_{2k_1}(2) \times \ldots \times \mathrm{O}^-_{2k_r}(2) \times \mathrm{O}^+_{2k_{r+1}}(2) \times \ldots \times \mathrm{O}^+_{2k_{r+s}}(2),\\ \mathsf{o}(\bar{g}_\infty) \text{ divides } L &:= \mathrm{lcm}(2^{k_1} + 1, \ldots, 2^{k_r} + 1, 2^{k_{r+1}} - 1, \ldots, 2^{k_{r+s}} - 1). \end{aligned}$$

Set $\epsilon_i := -1$ if $i \leq r$ and $\epsilon_i := +1$ if $i > r$. Note that the element $h_{r+i}$, $1 \leq i \leq s$, has order dividing $2^{k_{r+i}} - 1$ and so its odd-order preimage in $\mathbf{N}_{\mathrm{GL}_{2^{k_{r+i}}}(\mathbb{C})}(2^{1+2k_{r+i}}_+)$ admits some eigenvalue $\alpha_{r+i}$ with multiplicity $\geq 2$. "Grouping" those eigenvalues together, we see that if $s \geq 2$ then some eigenvalue of $g_\infty$ has multiplicity $\geq 2^s \geq 4$, whereas $g_\infty$ is $\mathsf{m2sp}$ by Proposition 2.4.3(ii), a contradiction. So $s \leq 1$. On the other hand, since $E$ has type $-$, we must have that $2 \nmid r \geq 1$.

Suppose that $k_i = k_j > 1$ for some $i < j \leq r$. By [**GMPS**, Lemma 2.9] we then have $L \leq 2^{a+1-k_i} \leq 2^{a-1}$, contrary to (10.3.3.2). Similarly, if $k_1 = k_2 = k_3 = 1$, then we again have by [**GMPS**, Lemma 2.9] that $L \leq 2^{a+1-k_1-k_2} \leq 2^{a-1}$, a contradiction.

Suppose $k_1 = k_2 = 1 < k_3 < \ldots < k_r$. Then the odd-order preimage in $\mathbf{N}_{\mathrm{GL}_{2^{k_i}}(\mathbb{C})}(2^{1+2k_i}_-)$ of $h_i$, $1 \leq i \leq 2$, has spectrum $\{\omega_i, \omega_i^{-1}\}$ with $\omega_i^3 = 1$, and so the product of these two preimages admits eigenvalue 1 with multiplicity $\geq 2$. If $s \geq 1$, then "grouping" this eigenvalue 1 with $\alpha_{r+1}$, we see that some eigenvalue of $g_\infty$ has multiplicity $\geq 4$, again a contradiction. Suppose $s = 0$. Again "grouping" this eigenvalue 1 with other eigenvalues coming from $h_j$ with $j \geq 3$, we see that the repeated eigenvalues of $g_\infty$ have total multiplicity at least half of $2^a = \mathrm{rank}(\mathcal{H})$, violating (10.3.3.3).

We have shown that $k_1 < k_2 < \ldots < k_r$. Now, if the order of some $h_i$ is less than $2^{k_i} - \epsilon_i$, then it is at most $(2^{k_i} - \epsilon_i)/3$, and so

$$\mathsf{o}(g_\infty) \le \frac{1}{3} \cdot \prod_{i=1}^{r}(2^{k_i}+1) \cdot \prod_{j=r+1}^{r+s}(2^{k_j}-1) < \frac{2.4}{3} \cdot 2^{\sum_{i=1}^r k_i} \cdot 2^{\sum_{j=r+1}^{r+s} k_j} = \frac{4}{5} \cdot 2^a,$$

contrary to (10.3.3.2). Thus each $h_i$ has order $2^{k_i} - \epsilon_i$. The same estimate shows that $\mathsf{o}(g_\infty) < (4/5)2^a$ if $2^{k_i} - \epsilon_i$, $1 \le i \le r+s$, are not pairwise coprime. Thus

$$\mathsf{o}(g_\infty) = \prod_{i=1}^{r}(2^{k_i}+1) \cdot \prod_{j=r+1}^{r+s}(2^{k_j}-1).$$

Now, if $s = 0$, then $\mathsf{o}(g_\infty) > 2^a$, violating (10.3.3.2). So $s = 1$. If $k_{r+1} = 1$, then $h_{r+1} = 1$, and so all eigenvalues of $g_\infty$ are repeated, contradicting (10.3.3.3). Hence $k_{r+1} \ge 2$. Now

$$2^a - 2^e + 1 = \mathsf{o}(g_\infty) \ge (2^{\sum_{i=1}^r k_i} + 1)(2^{k_{r+1}} - 1) \ge 2^a - 2^{\sum_{i=1}^r k_i} + 3,$$

and so $2^e < 2^{\sum_{i=1}^r k_i}$, whence $e < \sum_{i=1}^r k_i$. Now, the repeated eigenvalue $\alpha_{r+1}$ shows that the total multiplicity of repeated eigenvalues of $g_\infty$ is at least $2 \cdot 2^{\sum_{i=1}^r k_i} \ge 2^{e+2}$, again contradicting (10.3.3.3). □

Next we turn our attention to the alternating case. We will need the following result on permutation groups.

LEMMA 10.3.4. *Let $X = Q \rtimes C \le \mathsf{S}_n$ is a double transitive subgroup, where $Q \neq 1$ is a $p$-group acting transitively and $C$ is a cyclic $p'$-group. Then $n = p^a$, and $C$ is generated by an $(n-1)$-cycle.*

PROOF. Since $X$ is solvable, by Burnside's theorem [**Cam**, Proposition 5.2], we have that $X$ has a unique minimal normal subgroup $R$, in particular, $R \le Q$ and so $R$ is elementary abelian of order $p^a$. As shown in [**Cam**, Remark 1], one can identity $\{1, 2, \ldots, n\}$ with the point set of $W := \mathbb{F}_p^a$, $R$ with the subgroup of all translations on $W$, and $X$ with $R \rtimes X_0$, where $X_0 \le \mathrm{GL}_a(p)$ is a subgroup that acts transitively on $W \smallsetminus \{0\}$ and fixes 0. Now we have $Q = R \rtimes (X_0 \cap Q)$, and the $p$-subgroup $X_0 \cap Q$ acts semi-transitively (i.e. with orbits of same length) on $W \smallsetminus \{0\}$, hence trivially, and thus $Q = R$. Now $|X_0| = |X/Q| = |C|$ is coprime to $|Q$, and so the complement $C$ to $Q$ is conjugate to $X_0$ by the Schur-Zassenhaus theorem, and so without loss we may assume $X_0 = C = \langle x \rangle$. It follows that $x$ fixes 0 and acts transitively on $W \smallsetminus \{0\}$, i.e. it is an $(n-1)$-cycle. □

THEOREM 10.3.5. *Let $A, B \in \mathbb{Z}_{\ge 2}$ be integers and $p$ a prime with $p \nmid AB$ and* $\gcd(A,B) =$ 1*. Suppose* $2 \le B \le A-2$ *and* $A \ge 12$*. Then no local system $\mathcal{F}(A,B,\theta)$ in characteristic $p$ can have finite, almost quasisimple, geometric monodromy group $G$ which has $S = \mathsf{A}_n$ with $n \ge 5$ as a non-abelian composition factor.*

PROOF. (a) We argue by contradiction.

Let $\mathcal{H}$ be a hypergeometric sheaf giving rise to $\mathcal{F}(A,B,\theta)$. More precisely, if $\theta = \mathbb{1}$, take $\mathcal{H} := \mathcal{H}_{small,A,B}$. If $\theta \neq \mathbb{1}$, take $\mathcal{H} := \mathcal{H}_{big,A,B,\chi}$ for any choice of $\chi$ with $\chi^A = \theta$. Thus $\mathcal{H}$ has rank $D = A - \delta_{\theta,\mathbb{1}} \ge 11$. By Corollary 10.1.9, $\mathcal{H}$ has finite geometric monodromy group $H \rhd G$ which satisfies (**S**+). Applying Lemma 1.1.3 to $H \rhd G$, we see that $S$ is the unique non-abelian composition factor, and, as usual, $S \lhd H/\mathbf{Z}(H) \leq \mathrm{Aut}(S)$. Let $g_0$ be a generator of the image of $I(0)$ in $H$, $Q$ the image of $P(\infty)$ in $H$, and let $g_\infty$ be a $p'$-generator for the image $J$ of $I(\infty)$ in $H$ modulo $Q$. By Proposition 2.4.3, $g_0$ is $\mathsf{ssp}$, and $g_\infty$ is $\mathsf{m2sp}$. In particular, $11 \leq A = \bar{\mathsf{o}}(g_0) \leq \mathrm{meo}(\mathrm{Aut}(S))$, ruling out the case $n \leq 6$. If $n = 7$, then Theorem 3.1.3 shows that $D \leq 6$, a contradiction. Hence $n \geq 8$, and we can apply Theorem 3.1.2 to find possible candidates for $(V, g_0)$, where $V = V_{\mathcal{H}}$ is the underlying representation for $\mathcal{H}$. Using the condition $D \geq 10$ and [**KT5**, Lemma 9.1], we can rule out the spin cases and obtain that $E(G) = S$.

Suppose we are in case (i)(b) of Theorem 3.1.2, i.e. $S = \mathsf{A}_8$, $D = 14$, and $\bar{\mathsf{o}}(g_0) = 15$. Then $A = 15$ and $\theta = \mathbb{1}$; moreover, $H = \mathbf{Z}(H)S$ by Theorem 1.2.2. Recall from Proposition 2.4.3(ii) that $g_\infty$ has simple spectrum on $\mathsf{Wild}$ and simple spectrum $\mu_B \smallsetminus \{1\}$ on $\mathsf{Tame}$. Checking [**GAP**] for $\mathsf{m2sp}$-elements in $S$, we see that $\bar{\mathsf{o}}(g_\infty) = 15$ or $\bar{\mathsf{o}}(g_\infty) = 7$. As $I(\infty)$ is irreducible on $\mathsf{Wild}$ of dimension $w := A - B$ and $|S|$ is coprime to 11 and 13, we see that $w \neq 11, 13$, i.e. $B \neq 2, 4$. Also, $B$ is coprime to $A = 15$, $B|\bar{\mathsf{o}}(g_\infty)$ and $\bar{\mathsf{o}}(g_\infty)$ is again to coprime to 11 and 13, so we have $B \in \{7, 8\}$. Since $\mu_B \smallsetminus \{1\}$ is contained in $\mathrm{Spec}\,(g_\infty)$, we see that $\bar{\mathsf{o}}(g_\infty) \neq 15$, so $\bar{\mathsf{o}}(g_\infty) = 7$ and $B = 7$. Writing $g_\infty = zh$ with $z \in \mathbf{Z}(H)$ and $h \in S$ (of order 7), we have that $\mathrm{Spec}\,(g_\infty) = \alpha\mu_7 \sqcup \alpha\mu_7$ (as a multiset), for some $\alpha \in \mathbb{C}^\times$. Again, it contains $\mu_7 \smallsetminus \{1\}$, so $\alpha \in \mu_7$ and we can take $\alpha = 1$. This shows that $g_\infty$ has 1 as a repeated eigenvalue on $\mathsf{Tame}$, a contradiction.

We have therefore shown that Theorem 3.1.2(i)(a) holds, i.e. $S = \mathsf{A}_n$ with $n = D + 1$ and $S$ acts on $V$ via its deleted permutation representation. Moreover, either $\theta = \mathbb{1}$ and $g_0$ is a multiple of an $n$-cycle, or $\theta \neq \mathbb{1}$ and $g_0$ is a multiple of an $(n-1)$-cycle (this can be seen by inspecting the spectrum on $V$ of any disjoint product of a $k$-cycle and an $(n-k)$-cycle with $1 \leq k \leq n-1$ coprime to $n$). Let $\rho$ denote the natural permutation character (of degree $n$) of $\mathsf{S}_n$, and let $\varphi$ denote the character of the $H$-module $V$, so that $\varphi|_S = \rho|_S - 1_S$.

(b) Note by [**KT5**, Proposition 4.8(i)] that $Q \cap \mathbf{Z}(H) = 1$. Next we aim to show that $Q$ is contained in $S = \mathsf{A}_n$. First consider the case $p \nmid D$. Then $p \nmid \mathbf{Z}(H)$ by [**KT5**, Proposition 4.8(iv)]; also, $\mathsf{A}_n \lhd H/\mathbf{Z}(H) \leq \mathsf{S}_n$. If $p > 2$, then the $p$-subgroup $Q$ is contained in $\mathbf{O}^{p'}(\mathbf{Z}(H)S) = S$, as desired. Suppose $p = 2$. Then the $2'$-element $g_0$ is contained in $\mathbf{Z}(H)S$, and so $H = \mathbf{Z}(H)S$ by Theorem 1.2.2, and we again have $Q \leq S$ as in the previous case.

It remains to consider the case $p|D$. As $p \nmid A$, we must have that $n = A = D + 1$, and $\mathcal{H} = \mathcal{H}_{small,A,B}$. If $2 \nmid AB$, then $\mathcal{H}$ is symplectic by [**Ka-ESDE**, Theorems 8.8.1-2], whereas $V|_S$ is orthogonal, a contradiction. Hence $2|AB$, and so $p > 2$ and $Q$ is contained in $\mathbf{Z}(H)S = \mathbf{Z}(H) \times S$. In particular, any element $x \in Q$ is uniquely written as $x = z(x)h(x)$ with $z(x) \in \mathbf{Z}(H)$ and $h(x) \in S$. The map $x \mapsto h(x)$ is a group homomorphism $Q \to S$, with image $R := \{h(x) \mid x \in Q\}$, a $p$-subgroup, and $Q \leq \mathbf{Z}(H)Q = \mathbf{Z}(H)R$. As $Q \not\leq \mathbf{Z}(H)$, we have $R \neq 1$. By assumption, $p \nmid A = n$, hence the nontrivial $p$-subgroup $R$ cannot act transitively on $n$ points and so $[\rho|_R, 1_R]_R \geq 2$. It follows that the subspace $U$ of $R$-fixed points on $V$ is nonzero. Note that $J \leq \mathbf{N}_H(Q)$ normalizes each of the subgroups $Q$, $\mathbf{Z}(H)$, and $\mathbf{Z}(H)Q \cap S = \mathbf{Z}(H)R \cap S = R$. Hence $U$ is $J$-invariant. On the other hand, $x \in Q$ acts on $U$ via the scalar action of $z(x) \in \mathbf{Z}(H)$. Thus the $Q$-module $U$ affords the character $e\lambda$ for some linear character $\lambda \in \mathrm{Irr}(Q)$ and with $e := \dim U$, and $\lambda$ is $J$-invariant. If $\lambda$ occurs in $\mathsf{Wild}$, then the $J$-invariance of $\lambda$ and the irreducibility of $J$ on $\mathsf{Wild}$ imply by Clifford's theorem that $Q$ acts on $\mathsf{Wild}$ via the character $w\lambda$, which in turn show $w = A-B = 1$ by Propositions 4.8 and 4.9 of [**KRLT4**], a contradiction. Hence $\lambda$ occurs in $\mathsf{Tame}$, i.e. $z(x) \in \mathbf{Z}(H)$ acts trivially on $U$ for all $x \in Q$. It follows that $z(x)$ acts trivially on $V$ as well (as $\mathbf{Z}(H)$ acts via scalars on $V$), and so $z(x) = 1$ for all $x \in Q$. Thus $Q = R \leq S$, as stated.

(c) Recall that $\mathsf{A}_n \leq H/\mathbf{Z}(H) \leq \mathsf{S}_n$ and $S = \mathsf{A}_n$ acts on $V$ via the character $\rho|_S - 1_S$. Working in $\mathbf{N}_{\mathrm{GL}(V)}(S) = \mathbf{Z}(\mathrm{GL}(V))\mathsf{S}_n$, we can write (the action on $V$ of) $g_\infty$ as $\gamma h_\infty$, with $h_\infty \in \mathsf{S}_n$ having trace $\rho(h_\infty) - 1$ on $V$ and $\gamma \in \mathbb{C}^\times$. (In general, the action of $S$ on $V$ extends to $\mathsf{S}_n$ in two ways different from each other by the sign character sgn; changing $\gamma$ to $-\gamma$ in the case $g_\infty \notin \mathbf{Z}(H)S$, we achieve the designated trace for $h_\infty$.) Defining

$$\tilde{J} := \langle Q, h_\infty \rangle \leq \mathbf{N}_{\mathsf{S}_n}(Q).$$

we can extend $\varphi$ to $\tilde{J}$ by setting $\varphi(h_\infty) = \rho(h_\infty) - 1$, and thus $\varphi|_{\tilde{J}} = \rho|_{\tilde{J}} - 1_{\tilde{J}}$. Write $m := \dim \mathsf{Tame}$. We know that $J$ acts irreducibly on $\mathsf{Wild}$ of dimension $w = A - B = D - m$ (and wild on $Q$), and the $J$-module $\mathsf{Tame}$ is the sum of $m$ distinct 1-dimensional submodules (tame on $Q$). By its construction, $\tilde{J}$ still acts irreducibly on $\mathsf{Wild}$ (which is wild on $Q$), and the $\tilde{J}$-module $\mathsf{Tame}$ is the sum of $m$ distinct 1-dimensional submodules (tame on $Q$). It follows that

$$m + 1 = [\varphi|_J, \varphi|_J]_J = [\varphi|_{\tilde{J}}, \varphi|_{\tilde{J}}]_{\tilde{J}} = [\rho|_{\tilde{J}} - 1_{\tilde{J}}, \rho|_{\tilde{J}} - 1_{\tilde{J}}]_{\tilde{J}}. \tag{10.3.5.1}$$

Also, $[\varphi|_{\tilde{J}}, 1_{\tilde{J}}]_{\tilde{J}} \leq 1$, so $[\rho|_{\tilde{J}}, 1_{\tilde{J}}]_{\tilde{J}} \leq 2$, and thus $\tilde{J}$ has at most 2 orbits on $\{1, 2, \ldots, n\}$. Write the number of $\tilde{J}$-orbits as $1 + r$, with $r \in \{0, 1\}$.

(d) Now we may assume $\tilde{J} = Q \rtimes \langle h_\infty \rangle$ has $1 + r$ orbits, $\Delta$, and $\Omega$ if $r = 1$, on $n$ points $1, 2, \ldots, n$. Since $Q \neq 1$ acts nontrivially on $\{1, 2, \ldots, n\}$, we may assume that $\Delta$ consists of $k \geq 1$ $Q$-orbits of length $p^a > 1$ each, and $\Omega$ consists of $l$ $Q$-orbits of length $p^b$ each with $p^b \leq p^a$ if $r = 1$. Let $\alpha$ and $\beta$ denote the permutation character of $\tilde{J}$ on $\Delta$ and on $\Omega$, with the convention $\beta = 0$ if $r = 0$. Then

$$[\alpha, 1_{\tilde{J}}]_{\tilde{J}} = 1, \quad \text{and } [\beta, 1_{\tilde{J}}]_{\tilde{J}} \text{ if } r = 1, \text{ hence } [\alpha, \beta]_{\tilde{J}} \geq r. \tag{10.3.5.2}$$

Next, the $k$ orbits $\Delta_i$, $1 \leq i \leq k$, of $Q$ on $\Delta$ are cyclically permuted by $h_\infty$, so $h_\infty^k$ fixes each $\Delta_i$. Say $1 \in \Delta_1$. Then $\tilde{J}_1 := \mathrm{Stab}_{\tilde{J}}(1)$ fixes $\Delta_1$; also is contained in $\langle Q, h_\infty^k \rangle$ and thus fixing each $\Delta_i$ as well. As $|\Delta_1| = p^a > 1$, $\tilde{J}_1$ fixes $\{1\}$, and has at least one more orbit on $\Delta_1 \smallsetminus \{1\}$ and at least one orbit on each $\Delta_i$ with $2 \leq i \leq k$. It follows that $\mathrm{Stab}_J(1)$ has at least $k+1$ orbits on $\Delta$, i.e.

$$[\alpha, \alpha]_{\tilde{J}} = k + s \text{ with } s \geq 1. \tag{10.3.5.3}$$

If $r = 1$ and $p^b > 1$, then the same argument applied to $\Omega$ shows $[\beta, \beta]_{\tilde{J}} \geq l + 1$. If $p^b = 1$ and $r = 1$, i.e. $Q$ acts trivially on $\Omega$, then $l = |\Omega|$ and $\beta$ is the sum of $l$ linear characters, and so $[\beta, \beta]_{\tilde{J}} \geq l$. Thus we always have $[\beta, \beta]_{\tilde{J}} = lr + t$, where $t \geq 0$, and in fact $t \geq 1$ if $p^b > 1$ and $r = 1$.

From (10.3.5.2), and (10.3.5.3) and its variant for $\Omega$ we now obtain

$$[\rho|_{\tilde{J}}, \rho_{\tilde{J}}]_{\tilde{J}} = [\alpha + \beta, \alpha + \beta]_{\tilde{J}} \geq k + s + lr + t + 2r.$$

Also,

$$m = \dim \mathsf{Tame} = [\rho_Q - 1_Q, 1_Q]_Q = k + lr - 1. \tag{10.3.5.4}$$

Now using (10.3.5.1), we get

$$\begin{aligned} m+1 &= [\rho|_{\tilde{J}} - 1_{\tilde{J}}, \rho|_{\tilde{J}} - 1_{\tilde{J}}]_{\tilde{J}} \\ &= [\rho|_{\tilde{J}}, \rho_{\tilde{J}}]_{\tilde{J}} + 1 - 2[\rho|_{\tilde{J}}, 1_{\tilde{J}}]_{\tilde{J}} \\ &\geq (k+s+lr+t+2r) + 1 - 2(r+1) \\ &= k+s+t+lr-1 \\ &= m+s+t. \end{aligned}$$

It follows that $s=1$, i.e. $[\alpha,\alpha]_{\tilde{J}} = k+1$, and $t=0$, i.e. $p^b = 1$ if $r=1$. Thus $\tilde{J}_1$ has exactly $k+1$ orbits on $\Delta$, so they must be $\{1\}$, $\Delta_1 \smallsetminus \{1\}$, and $\Delta_i$, $2 \leq i \leq k$. As $\mathrm{Stab}_J(1) \leq \langle Q, h_\infty^k \rangle$, we see that $\langle Q, h_\infty^k \rangle$ acts doubly transitively on $\Delta_1$. Applying Lemma 10.3.4 to the image of $\langle Q, h_\infty^k \rangle$ in $\mathrm{Sym}(\Delta_1)$, we see that $h_\infty^k$ acts on $\Delta_1$ as a $(p^a-1)$-cycle, and hence we may assume that $h_\infty^k$ has orbits $\{1\}$, $\Delta_1 \smallsetminus \{1\}$ on $\Delta_1$. But $h_\infty$ commutes with $h_\infty^k$ and permutes $\Delta_1, \ldots, \Delta_k$ cyclically. Also, as $Q$ acts trivially on $\Omega$, $\Omega$ is a single $h_\infty$-orbit if $r=1$. So we have shown that $h_\infty$ has $2+r$ orbits, one of length

$$k(p^a-1) = w = A-B,$$

another of length $k$, and one more of length $l$ if $r=1$, on $\{1,2,\ldots,n\}$.

Returning to $g_\infty = \gamma h_\infty$, we see that $\mathrm{Spec}\,(g_\infty)$ on $V$ is

$$\gamma \cdot \mu_w \sqcup \gamma \cdot \bigl(\mu_k \smallsetminus \{1\}\bigr) \sqcup \underbrace{\gamma \cdot \mu_l}_{r}, \tag{10.3.5.5}$$

as a multiset. Now, if $p|w = p(k^a-1)$, then since $p^a > 1$ we have $p|k$, and so $\bar{\mathsf{o}}(g_\infty)$ is divisible by $k$ (see (10.3.5.5)) and by $p$, a contradiction. Hence $p \nmid w$.

(e) Suppose $\mathcal{H} = \mathcal{H}_{big,A,B,\chi}$, so that $m=B$, and $k+lr = B+1$ by (10.3.5.4). By [**KRLT4**, Proposition 4.8], $\mathrm{Spec}\,(g_\infty)$ on $V$ is

$$\delta \cdot \mu_w \sqcup \nu \cdot \mu_B \tag{10.3.5.6}$$

for some $\delta, \mu \in \mathbb{C}^\times$. This should of course match up with (10.3.5.5).

Assume first that $\delta \in \gamma \cdot \mu_w$. Then the two sets $\gamma \cdot \mu_w$ and $\delta \cdot \mu_w$ are identically the same. Matching up (10.3.5.5) with (10.3.5.6), we obtain

$$\gamma \cdot \bigl(\mu_k \smallsetminus \{1\}\bigr) \sqcup \underbrace{\gamma \cdot \mu_l}_{r} = \nu \cdot \mu_B.$$

If $r=0$, then since $B \geq 2$ we have $k = B+1 \geq 3$ by (10.3.5.4), and the left-hand-side contains two roots with ratio $\zeta_{B+1}$, a contradiction. [Note that the case $(B,r)=(1,0)$ led to Theorem 10.2.7(iii).] So $r=1$. Now, if $k \geq 2$ then the left-hand-side contains two roots with ratio $\zeta_k$, and the right-hand-side then shows that $k|B$. But $k$ divides $k(p^a-1) = A-B$, so $\gcd(A,B) > 1$, a contradiction. Hence $k=1$, $l=B$, $A = p^a-1+B$. Now if $p=2$ then, as $p^a > 1$, $2|AB$, a contradiction. If $p>2$, then $\gcd(A,B)=1$ implies that both $A,B$ are odd. Here, $D = A = n-1$, and $g_0$ is a multiple of an $A$-cycle, so Theorem 1.2.2 implies that $H = \mathbf{Z}(H)S$. On the other hand, $g_\infty$ is a multiple of a disjoint product of an $(A-B)$-cycle and a $B$-cycle, showing $g_\infty \notin \mathbf{Z}(H)S$, a contradiction.

Assume now that $\gamma \cdot \mu_w$ and $\delta \cdot \mu_w$ are disjoint. Then $\gamma \cdot \mu_w$ is contained in $\nu \cdot \mu_B$. The former contains two roots with ratio $\zeta_w$, so $w = A - B$ divides $B$, and thus $1 < w | \gcd(A,B)$, again a contradiction.

(f) Finally we consider the case $\mathcal{H} = \mathcal{H}_{small,A,B}$, so that $m = B-1$, and $k + lr = B$ by (10.3.5.4). If $r = 0$, then $A = n = kp^a$ is divisible by $p$, a contradiction. Hence $r = 1$. By [**KRLT4**, Proposition 4.8], Spec $(g_\infty)$ on $V$ is

$$\delta \cdot \mu_w \sqcup \big(\mu_B \smallsetminus \{1\}\big) \qquad (10.3.5.7)$$

for some $\delta \in \mathbb{C}^\times$. We will now match this up with (10.3.5.5).

Assume first that $\delta \in \gamma \cdot \mu_w$. Then the two sets $\gamma \cdot \mu_w$ and $\delta \cdot \mu_w$ are identically the same. Matching up (10.3.5.7) with (10.3.5.6), we obtain

$$\gamma \cdot \mu_k \cup \gamma \cdot \mu_l = \mu_B \smallsetminus \{1\}.$$

(noting that we now have a union of two sets in the left-hand-side). In particular, if $k \geq 2$ then the left-hand-side contains two roots with ratio $\zeta_k$, and the right-hand-side then shows that $k|B$. But $k$ divides $k(p^a-1) = A - B$, so $\gcd(A,B) > 1$, a contradiction. Hence $k = 1$, $l = B-1$, $\mu_B \smallsetminus \{1\} = \gamma \cdot \mu_l$, which is possible only when $B = 2$. But in this case, $p \nmid B$ implies $p > 2$, so $A = p^a + 1$ and $B = 2$ are both even, a contradiction.

Assume now that $\gamma \cdot \mu_w$ and $\delta \cdot \mu_w$ are disjoint. Then $\gamma \cdot \mu_w$ is contained in $\mu_B$. The former contains two roots with ratio $\zeta_w$, so $w = A - B$ divides $B$, and thus $1 < w | \gcd(A,B)$, again a contradiction. □

Next we classify semisimple m2sp-elements of finite general linear groups:

PROPOSITION 10.3.6. *Let $n \in \mathbb{Z}_{\geq 2}$, $q$ a power of a prime $p$, $(n,q) \neq (2,2)$, and let $G$ be a finite group with $\mathrm{PSL}_n(q) \lhd G/\mathbf{Z}(G) \cong \mathrm{PGL}_n(q)$. Suppose $G$ admits an irreducible $\mathbb{C}G$-module $V$ of dimension $D \geq (q^n - q)/(q-1)$ on which a $p'$-element $g \in G$ acts as an* m2sp*-element. Then one of the following statements holds for the image $\bar{g}$ of $g$ in $\mathrm{PGL}_n(q)$.*

(i) *$\langle \bar{g} \rangle$ is a subgroup of index at most 2 in a cyclic maximal torus $\bar{T}_n \cong C_{(q^n-1)/(q-1)}$ of $\mathrm{PGL}_n(q)$.*
(ii) *$n = a + b$ with $a, b \in \mathbb{Z}_{\geq 1}$, $\gcd(a,b) = 1$, and $\langle \bar{g} \rangle$ is a cyclic maximal torus $\bar{T}_{a,b}$ of order $(q^a-1)(q^b-1)/(q-1)$ of $\mathrm{PGL}_n(q)$.*

PROOF. Since $g$ is m2sp on $V$,

$$\bar{\mathsf{o}}(g) \geq D/2 \geq (q^n - q)/2(q-1). \qquad (10.3.6.1)$$

We may assume that $\bar{g}$ is the image of a semisimple element $h \in \mathrm{GL}_n(q)$ in $\mathrm{PGL}_n(q)$. We may decompose $W := \mathbb{F}_q^n$ into a direct sum $\oplus_{i=1}^s W_i$ of irreducible $\langle h \rangle$-submodules $V_i \cong \mathbb{F}_q^{n_i}$, with $n_1 \geq \ldots \geq n_s \geq 1$, and write $h = \mathrm{diag}(h_1, \ldots, h_s)$ with $h_i \in \mathrm{GL}(W_i)$. Note that $\mathsf{o}(h_i) | (q^{n_i} - 1)$; in fact, $h_i^{(q^{n_i}-1)/(q-1)} \in \mathbf{Z}(\mathrm{GL}(W_i))$, and so $\bar{\mathsf{o}}(g) = \mathsf{o}(\bar{g})$ divides $(q-1)L$, where

$$L := \mathrm{lcm}\bigg(\frac{q^{n_1}-1}{q-1}, \ldots, \frac{q^{n_s}-1}{q-1}\bigg).$$

Now, if $s = 1$, then $h = h_1$, and (10.3.6.1) implies that $\bar{\mathsf{o}}(g) > (q^n - 1)/3(q - 1)$ but $\bar{\mathsf{o}}(g)$ divides $(q^n - 1)/(q - 1)$, and so we arrive at (i). If $s \geq 3$ and $q \geq 3$, then

$$L \leq \prod_{i=4}^{s} \frac{q^{n_i} - 1}{q - 1} \cdot \frac{(q^{n_1} - 1)(q^{n_2} - 1)(q^{n_3} - 1)}{(q - 1)^3} \leq \frac{(q^{n-n_1} - 1)(q^{n_1} - 1)}{(q - 1)^3} < \frac{q^n - q}{(q - 1)^3},$$

and so $\bar{\mathsf{o}}(g) < (q^n - q)/2(q - 1)$, contrary to (10.3.6.1).

In the cases $(n, q) = (3, 2)$, respectively $(4, 2)$, (10.3.6.1) and [**GAP**] imply that $\mathsf{o}(h) \in \{3, 7\}$, respectively $\mathsf{o}(h) \in \{7, 15\}$, and we arrive at (i) or (ii). So we may assume $n \geq 5$ when $q = 2$. Suppose $s \geq 3$ and $q = 2$. Since $\bar{\mathsf{o}}(g) \leq \mathrm{meo}(\mathrm{SL}_n(2)) = 2^n - 1$ by [**GMPS**, Theorem 2.16], (10.3.6.1) implies $D \leq 2(2^n - 1)$. As $V$ yields an irreducible projective representation of $\mathrm{SL}_n(2)$, applying [**TZ1**, Theorem 3.1] we see that $D = 2^n - 2$ and $V$ yields a Weil representation of $S := \mathrm{SL}_n(2)$, whose character $\tau$ is the permutation character of $\mathrm{SL}_n(2)$ on $\mathbb{F}_2^n$ minus $2 \cdot 1_S$. One can now check that the restriction of $\tau$ to $X := \mathrm{SL}_{n_1}(2) \times \mathrm{SL}_{n_2}(2) \times \mathrm{SL}_{n-n_1-n_2}(2)$ contains $6 \cdot 1_X$. As $h \in X$, it follows that 1 is an $h$-eigenvalue with multiplicity $\geq 6$, a contradiction.

Finally, suppose $s = 2$. If $d := \gcd(n_1, n_2) \geq 2$, then

$$\bar{\mathsf{o}}(g) \leq (q - 1)L \leq (q - 1)\frac{(q^{n_1} - 1)(q^{n_2} - 1)}{(q^d - 1)(q - 1)} \leq \frac{q^n - q}{q^d - 1} \leq \frac{q^n - q}{q^2 - 1},$$

contradicting (10.3.6.1). Thus $\gcd(n_1, n_2) = 1$, and so $\bar{\mathsf{o}}(h)$ divides $(q-1)L = (q^{n_1} - 1)(q^{n_2} - 1)/(q - 1)$. Note that $(q - 1)L/2 < (q^n - q)/2(q - 1)$, so (10.3.6.1) forces $\bar{\mathsf{o}}(h) = (q - 1)L$, and we arrive at (ii). □

THEOREM 10.3.7. *Let $A, B \in \mathbb{Z}_{\geq 2}$ be integers with $p \nmid AB$ and* $\gcd(A, B) = 1$. *Suppose $A \geq 12$ and $2 \leq B \leq A - 2$. Then no local system $\mathcal{F}(A, B, \theta)$ in characteristic $p$ can have finite, almost quasisimple, geometric monodromy group $G$ which has a non-abelian composition factor $S = \mathrm{PSL}_n(q)$ with $n \geq 2$.*

PROOF. (a) We argue by contradiction. Let $\mathcal{H} = \mathcal{H}_{small,A,B}$ or $\mathcal{H}_{big,A,B,\chi}$ be a hypergeometric sheaf giving rise to $\mathcal{F}(A, B, \theta)$. Then $\mathcal{H}$ has rank $D \geq A - 1 \geq 11$. By Corollary 10.1.9, $\mathcal{H}$ has finite geometric monodromy group $H \rhd G$ which satisfies (**S**+). Applying Lemma 1.1.3 to $H \rhd G$, we see that $S$ is the unique non-abelian composition factor of $H$, and, as usual, $S \lhd H/\mathbf{Z}(H) \leq \mathrm{Aut}(S)$. Let $g_0$ be a generator of the image of $I(0)$ in $H$, $Q$ the image of $P(\infty)$ in $H$, and let $g_\infty$ be a $p'$-generator for the image $J$ of $I(\infty)$ in $H$ modulo $Q$. By Proposition 2.4.3, $g_0$ is $\mathsf{ssp}$, and $g_\infty$ is $\mathsf{m2sp}$. Furthermore, since $D \geq 11$, Theorem 3.1.10 implies that $q = p^f$ is a power of $p$.

(b) First we consider the case $n \geq 3$. The assumption $D \geq 11$ rules out the cases where either $(n, q) = (3, 2)$, or $(n, q) = (3, 4)$ but the representation does not come from a Weil representation of $\mathrm{SL}_n(q)$, by [**KT5**, Theorem 6.6]. Applying [**KT5**, Theorem 8.1] when $(n, q) \neq (3, 3)$, and using [**GAP**] when $(n, q) = (3, 3)$, we see that $\bar{\mathsf{o}}(g_0) = (q^n - 1)/(q - 1)$ and $E(H)$ is the image of $\mathrm{SL}_n(q)$ in a Weil representation of dimension $D$; in particular, the latter representation extends to $\mathrm{GL}_n(q)$. Moreover, $w = A - B \geq 2$, so [**KT5**, Corollary 8.4] shows that $H/\mathbf{Z}(H) \cong \mathrm{PGL}_n(q)$ and thus, up to scalar matrices, the image of $H$ in $\mathrm{GL}_D(\mathbb{C})$ is the same as the image of $\mathrm{GL}_n(q)$ in a Weil representation of dimension $D$. Hence, if $D = (q^n - 1)/(q - 1)$, then these images realize imprimitive subgroups of $\mathrm{GL}_D(\mathbb{C})$, contrary to $H$ being $(\mathbf{S}+)$. So we must have that $D = (q^n - q)/(q-1)$, $A = D+1$, and $\mathcal{H} = \mathcal{H}_{small,A,B}$. Now we apply Proposition 10.3.6 to $g_\infty$ and arrive at one of the following two possibilities.

(b1) $\bar{\mathsf{o}}(g_\infty)$ is either $A$ or $A/2$. If $B > 2$, then $B|\bar{\mathsf{o}}(g_\infty)$ by Lemma 10.1.15, and so $\gcd(A,B) = B > 1$, a contradiction. So $B = 2$, whence $2 < w = A - B \equiv 1 (\bmod\ p)$. Now we have $A - B$ divides $\bar{\mathsf{o}}(g_\infty)$ by Lemma 10.1.15(i), and so $\gcd(A,B) \geq w > 2$, again a contradiction.

(b2) The image of $g_\infty$ in $\mathrm{PGL}_n(q)$ generates a cyclic maximal torus of order $(q^a-1)(q^b-1)/(q-1)$, where $a > b \geq 1$, $n = a+b$, and $\gcd(a,b) = 1$. Say, this torus is generated by the image of $h \in \mathrm{GL}_a(q) \times \mathrm{GL}_b(q)$ in $\mathrm{GL}_n(q)$. Then the action of $g_\infty$ is a scalar multiple of the action of $h$ in the unipotent Weil representation (of degree $(q^n-q)/(q-1)$) of $\mathrm{GL}_n(q)$. Restricting this representation to $\mathrm{GL}_a(q) \times \mathrm{GL}_b(q)$, one sees that the spectrum of $h$ contains all elements of $\mu_{(q^a-1)/(q-1)} \sqcup \big(\mu_{(q^b-1)/(q-1)} \smallsetminus \{1\}\big)$ as repeated eigenvalues. It follows that the total $N$ of multiplicities of eigenvalues of $g_\infty$ is

$$N \geq 2\big((q^a-1)/(q-1) + (q^b-1)/(q-1) - 1\big) > 2,$$

hence $p|w = A - B$ by Lemma 10.1.15. In particular, $B > 2$ as otherwise $p \nmid (A-B)$. The proof of Lemma 10.1.15 shows that the ratio between two distinct repeated eigenvalues of $g_\infty$ is a $d^{\text{th}}$ root of unity. Applying this to repeated eigenvalues $1, \zeta_{(q^a-1)/(q-1)}$ and $1, \zeta_{(q^b-1)/(q-1)}$ of $h$, we see that $d$ is divisible by

$$\mathrm{lcm}\big(\frac{q^a-1}{q-1}, \frac{q^b-1}{q-1}\big) = \frac{(q^a-1)(q^b-1)}{(q-1)^2} =: M.$$

Thus, in the notation of Lemma 10.1.15(ii), $M$ divides both $B$ and $C/w_0 = p^e+1$, hence also $B + C = B + w + w_0 = A + w_0$. Thefefore,

$$M|(A+w_0) \text{ but } w_0 = \frac{C}{p^e+1} \leq \frac{\bar{\mathsf{o}}(g_\infty)}{M} = q-1. \qquad (10.3.7.1)$$

Suppose $b = 1$. Then $A - 1 = (q^n-q)/(q-1) = qM$, so (10.3.7.1) implies that

$$w_0 \geq M - 1 \geq (q^2-1)/(q-1) - 1 = q,$$

and this violates (10.3.7.1). Hence $a > b \geq 2$, and we now have $A - (q^a+q^b-2)/(q-1) = M(q-1)$. So (10.3.7.1) implies that

$$w_0 \geq M - \frac{q^a+q^b-2}{q-1} = \frac{(q^a-1)(q^b-1)}{(q-1)^2} - \frac{q^a+q^b-2}{q-1} > \frac{q^a-1}{q-1} \cdot \big((q+1)-2\big) = q^a - 1 > q,$$

and this again violates (10.3.7.1).

(c) Now we consider the case $S = \mathrm{PSL}_2(q)$. The bound $11 \leq D \leq \mathrm{meo}(\mathrm{Aut}(S))$ implies that $q \geq 11$, whence the image of $g_0$ lies in $\mathrm{PGL}_2(q)$ by Theorem 3.1.5(i). Since $w > 1$, Theorem 1.2.2 then shows that $S \lhd H/\mathbf{Z}(H) \leq \mathrm{PGL}_2(q)$. By [**KT5**, Proposition 4.8(i)], $Q \cap \mathbf{Z}(H) = 1$, hence $Q$ embeds in $H/\mathbf{Z}(H)$ and so $Q$ is abelian. This implies by [**KRLT4**, Proposition 4.8] that $p \nmid w$.

Suppose that $D \geq q-1$. If $\mathcal{H} \neq \mathcal{H}_{small,A,2}$, then Lemma 10.1.15 implies that

$$\bar{\mathsf{o}}(g_\infty) \geq B(A-B) \geq 2(A-2) \geq 2(q-3) > q+1 = \mathrm{meo}(\mathrm{Aut}(S)),$$

a contradiction. Hence $\mathcal{H} = \mathcal{H}_{small,A,2}$, in which case $A = D+1 \geq q$ and $p > 2$. But $p \nmid A$ and $A \leq \bar{\mathsf{o}}(g_0) \leq q+1$, hence $A = q+1$. Thus both $A$ and $B$ are even, again a contradiction.

Now consider the case $p > 2$ and $D = (q \pm 1)/2$. Since Weil representations of $\mathrm{SL}_2(q)$ fuse under diagonal automorphisms of $S$, this implies that $H/\mathbf{Z}(H) = \mathrm{PSL}_2(q)$, and so $\bar{\mathsf{o}}(g_\infty)$ divides $(q+1)/2$ or $(q-1)/2$; also $q \geq 23$ as $D \geq 11$. If $\mathcal{H} \neq \mathcal{H}_{small,A,2}$, then Lemma 10.1.15 implies that

$$\bar{\mathsf{o}}(g_\infty) \geq B(A-B) \geq 2(A-2) \geq 2((q-1)/2-2) = q-5 > (q+1)/2,$$

a contradiction. Hence $\mathcal{H} = \mathcal{H}_{small,A,2}$, in which case $A = D+1 = (q+1)/2$ or $(q+3)/2$. As $A = \bar{\mathsf{o}}(g_0) \leq (q+1)/2$, we must have that $A = (q+1)/2$. But then $w = A-2 = (q-3)/2$ cannot divide $\bar{\mathsf{o}}(g_\infty)$, again a contradiction. □

The following result classifies semisimple $\mathsf{m2sp}$-elements of finite symplectic groups:

Proposition 10.3.8. *Let $n \in \mathbb{Z}_{\geq 2}$, $q$ a power of a prime $p > 2$, and let $G$ be a finite group with $G/\mathbf{Z}(G) \cong \mathrm{PSp}_{2n}(q)$. Suppose $G$ admits an irreducible $\mathbb{C}G$-module $V$ of dimension $D \geq (q^n-1)/2$ on which a $p'$-element $g \in G$ acts as an $\mathsf{m2sp}$-element. Then one of the following statements holds for the image $\bar{g}$ of $g$ in $S := \mathrm{PSp}_{2n}(q)$.*

(i) *$\langle \bar{g} \rangle$ is of index at most 2 in a cyclic maximal torus $\bar{T}_n^{\pm} \cong C_{(q^n \pm 1)/2}$ of $\mathrm{PSp}_2(q^n) \hookrightarrow S$.*

(ii) *$n = a+b$ with $a,b \in \mathbb{Z}_{\geq 1}$, $\epsilon_a, \epsilon_b = \pm 1$, and $\bar{g}$ is contained in the image in $S$ of a maximal torus $T_{a,b}^{\epsilon_a,\epsilon_b} \cong C_{q^a-\epsilon_a} \times C_{q^b-\epsilon_b} < \mathrm{Sp}_{2a}(q) \times \mathrm{Sp}_{2b}(q)$ of $\mathrm{Sp}_{2n}(q)$.*

(iii) *$n = a+b+c$ with $a,b,c \in \mathbb{Z}_{\geq 1}$, $\epsilon_a, \epsilon_b, \epsilon_c = \pm 1$, and $\bar{g}$ is contained in the image in $S$ of a maximal torus $T_{a,b,c}^{\epsilon_a,\epsilon_b,\epsilon_c} \cong C_{q^a-\epsilon_a} \times C_{q^b-\epsilon_b} \times C_{q^c-\epsilon_c} < \mathrm{Sp}_{2a}(q) \times \mathrm{Sp}_{2b}(q) \times \mathrm{Sp}_{2c}(q)$ of $\mathrm{Sp}_{2n}(q)$. Moreover, $\bar{\mathsf{o}}(g) < 1.65q^n/4$.*

Proof. Since $g$ is $\mathsf{m2sp}$ on $V$,

$$\bar{\mathsf{o}}(g) \geq D/2 \geq (q^n-1)/4. \tag{10.3.8.1}$$

We may assume that $\bar{g}$ is the image of a semisimple element $h \in \mathrm{Sp}_{2n}(q)$ in $S$. As described on [**GMPS**, p. 7673], we may decompose $W := \mathbb{F}_q^{2n}$ into an orthogonal sum $\oplus_{i=1}^s W_i$ of $h$-stable non-degenerate subspaces $V_i \cong \mathbb{F}_q^{2n_i}$, with $n_1, \ldots, n_s \geq 1$, and write $h = \mathrm{diag}(h_1, \ldots, h_s)$ with $h_i$ contained in a cyclic maximal torus $C_{q^{n_i}-\epsilon_i} < \mathrm{Sp}_2(q^{n_i}) \hookrightarrow \mathrm{Sp}(W_i)$ for some $\epsilon_i = \pm 1$. Note that $h_i^{(q^{n_i}-\epsilon_i)/2} = \pm \mathrm{Id}_{W_i}$ for all $i$. Hence, $\bar{\mathsf{o}}(g) = \mathsf{o}(\bar{g})$ divides $2L$, where

$$L := \mathrm{lcm}\left(\frac{q^{n_1}-\epsilon_1}{2}, \ldots, \frac{q^{n_s}-\epsilon_s}{2}\right).$$

Now, if $s = 1$, then $h = h_1$, and (10.3.8.1) implies that $\bar{\mathsf{o}}(g) > (q^n+1)/6$ but $\bar{\mathsf{o}}(g)$ divides $(q^n \pm 1)/2$, and so we arrive at (i). The case $s = 2$ is recorded in (ii), so we will now assume $s \geq 3$.

Rewrite the sequence $(n_1, n_2, \ldots, n_s)$ so that the first $r$ terms $n_1 \leq n_2 \leq \ldots \leq n_r$ have $\epsilon_i = +$ and the last $t$ terms $n_{r+1} \leq n_{r+2} \leq \ldots \leq n_{r+t}$ have $\epsilon_i = -$, with $s = r+t$, so that

$$L := \mathrm{lcm}\left(\frac{q^{n_1}-1}{2}, \ldots, \frac{q^{n_r}-1}{2}, \frac{q^{n_{r+1}}+1}{2}, \ldots, \frac{q^{n_{r+s}}+1}{2}\right).$$

Suppose the sequence $(n_1, \ldots, n_r)$ contains exactly $r_0$ distinct terms, and denote the sum of these terms as $\sum_i' n_i$. Then

$$\mathrm{lcm}\left(\frac{q^{n_1}-1}{2}, \ldots, \frac{q^{n_r}-1}{2}\right) < \frac{q^{\sum_i' n_i}}{2^{r_0}}. \tag{10.3.8.2}$$

Next, if $1 \le a_1 < a_2 < \ldots < a_m$ are integers, then

$$\log\biggl(\prod_{i=1}^{m}(1+q^{-a_i})\biggr) < \log\biggl(\prod_{k=1}^{\infty}(1+q^{-k})\biggr) < \sum_{k=1}^{\infty} q^{-k} = 1/(q-1) \le 1/2,$$

whence $\prod_i(1+q^{-a_i}) < \exp(1/2) < 1.65$ and so $\prod_i(q^{a_i}+1) < (1.65)q^{\sum_i a_i}$. Now, suppose the sequence $(n_{r+1}, \ldots, n_{r+s})$ contains exactly $t_0$ distinct terms, and denote the sum of these terms as $\sum''_j n_j$, and correspondingly, $\prod''_j(q^{n_j}+1)$ denotes the product over only those terms. Then

$$\mathrm{lcm}\biggl(\frac{q^{n_{r+1}}+1}{2}, \ldots, \frac{q^{n_{r+s}}+1}{2}\biggr) \le \prod_j{}'' \frac{q^{n_j}+1}{2} < \frac{(1.65)q^{\sum''_j n_j}}{2^{t_0}}. \qquad (10.3.8.3)$$

Writing $s_0 := r_0 + t_0$, note that $\sum'_i n_i + \sum''_j n_j$ misses the $s - s_0$ repeated terms of the sequence $(n_1, \ldots, n_s)$, hence $\sum'_i n_i + \sum''_j n_j \le n - (s - s_0)$. Together with (10.3.8.2) and (10.3.8.3), this implies that

$$L < \frac{(1.65)q^{\sum'_i n_i + \sum''_j n_j}}{2^{s_0}} \le \frac{(1.65)q^{n-(s-s_0)}}{2^{s_0}} \le \frac{(1.65)q^n}{2^s}.$$

Now, if $s \ge 4$, then $\bar{\mathsf{o}}(g) \le 2L < (1.65q^n)/8 < (q^n-1)/4$, contradicting (10.3.8.1). Hence $s = 3$, $(n_1, n_2, n_3) = (a, b, c)$, and we arrive at (iii). $\square$

Theorem 10.3.9. *Let $p > 2$ be a prime, $A, B \in \mathbb{Z}_{\ge 2}$ be integers with $p \nmid AB$ and $\gcd(A, B) = 1$. Suppose $A \ge 12$, $2 \le B \le A - 2$, and that the local system $\mathcal{F}(A, B, \theta)$ in characteristic $p$ has a finite, almost quasisimple, geometric monodromy group $G$ which has a non-abelian composition factor $S = \mathrm{PSp}_{2n}(q)$ with $n \ge 2$. Then $q = p^f$, $\mathsf{o}(\theta) \le 2$, and we can find $r, s \in \mathbb{Z}_{\ge 1}$ with*

$$2 \Bigl| \biggl(\frac{r}{\gcd(r,s)} \cdot \frac{s}{\gcd(r,s)}\biggr) \qquad (10.3.9.1)$$

*such that $A = (p^r+1)/2$ and $B = (p^s+1)/2$.*

Proof. (a) Let $\mathcal{H} = \mathcal{H}_{small,A,B}$ or $\mathcal{H}_{big,A,B,\chi}$ be a hypergeometric sheaf giving rise to $\mathcal{F}(A, B, \theta)$. Then $\mathcal{H}$ has rank $D \ge A - 1 \ge 11$. By Corollary 10.1.9, $\mathcal{H}$ has finite geometric monodromy group $H \rhd G$ which satisfies (**S**+). Applying Lemma 1.1.3 to $H \rhd G$, we see that $S$ is the unique non-abelian composition factor of $H$. Let $g_0$ be a generator of the image of $I(0)$ in $H$, $Q$ the image of $P(\infty)$ in $H$, and let $g_\infty$ be a $p'$-generator for the image $J$ of $I(\infty)$ in $H$ modulo $Q$. By Proposition 2.4.3, $g_0$ is $\mathsf{ssp}$, and $g_\infty$ is $\mathsf{m2sp}$. Furthermore, since $D \ge 11$, Theorem 3.1.10 implies that $q = p^f$ is a power of $p$. Next, applying Theorems 3.1.5 and 3.1.8, we have that $H/\mathbf{Z}(H) \cong S$ and $D = (q^n \pm 1)/2$; in particular,

$$q^n \ge 23. \qquad (10.3.9.2)$$

Recalling $\bar{\mathsf{o}}(g_0) = A \in \{D, D+1\}$ and applying Theorems 8.2 and 9.11 of [**KT5**], we obtain that $A = (q^n+1)/2$. (Note that the assumption $(n, q) \ne (3, 3)$ in [**KT5**, Theorem 9.11] was used only to ensure that $p|q$, which is guaranteed by Theorem 3.1.10.) Thus $A = (p^r+1)/2$ with $r := nf$.

(b) Suppose for the moment that $B = (p^s+1)/2$ for some $s \in \mathbb{Z}_{\ge 1}$. Applying Lemma 10.3.2 to $t := p^v$ with $v := \gcd(r, s)$, we see that the assumption $\gcd(A, B) = 1$ is equivalent to $2|(rs/v^2)$, i.e. to to (10.3.9.1). We now show that $\mathsf{o}(\theta) \leq 2$. Recall that $D = (q^n \pm 1)/2$ is coprime to $p$, hence $p \nmid |\mathbf{Z}(H)|$ by [**KT5**, Proposition 4.8(iv)]. On the other hand, $H/\mathbf{Z}(H) \cong S$ and moreover $E(H)$ is the image of $\mathrm{Sp}_{2n}(q)$ in a Weil representation. It follows that $H = \mathbf{Z}(H)E(H)$ and $\mathbf{O}^{p'}(H) = E(H) = [H,H]$. Next, $\mathcal{F}$ is the $[A]^\star$ Kummer pullback of $\mathcal{H}$ and $\mathcal{F}$ lives on $\mathbb{A}^1$. Hence $G = \mathbf{O}^{p'}(G)$ and $H/G$ is a cyclic $p'$-group. This implies that $G = E(H)$, and so the field of traces of $\mathcal{F}$ is contained in the field of values for a Weil character of $\mathrm{Sp}_{2n}(q)$, which is contained in $\mathbb{Q}(\zeta_p)$. In view of Theorem 10.1.2, we may apply Theorem 10.1.18 to $\mathcal{F}$ to conclude that $\theta$ takes values in $\mathbb{Q}(\zeta_p)$. But $\mathsf{o}(\theta)$ is coprime to $p$, so we conclude that $\mathsf{o}(\theta) \leq 2$, as claimed.

The rest of the proof is to show that we indeed have $B = (p^s+1)/2$ for some $s \in \mathbb{Z}_{\geq 1}$.

(c) Suppose $B = 2$. If $p = 3$, then $B = (p^s+1)/2$ with $s := 1$, and so we are done. Suppose $p \neq 3$, so that $w := A - B = (q^n-3)/2$ is coprime to $p$. By [**KRLT4**, Proposition 4.8], $\bar{\mathsf{o}}(g_\infty)$ is divisible by $w$. The possibilities for $g_\infty$ are listed in Proposition 10.3.8. Since $1.65q^n/4 < (q^n-3)/2$ by (10.3.9.2), we are in case (i) or (ii) of Proposition 10.3.8. In case (i), $\bar{\mathsf{o}}(g_\infty)$ divides $(q^n \pm 1)/2$, which is however not divisible by $w$, a contradiction. In case (ii), we have

$$\bar{\mathsf{o}}(g_\infty) \leq 2 \cdot \frac{q^a - \epsilon_a}{2} \cdot \frac{q^b - \epsilon_b}{2} \leq 2 \cdot \frac{q^a+1}{2} \cdot \frac{q^b+1}{2} < q^n - 4 < 2w$$

again because of (10.3.9.2). So the condition $w|\bar{\mathsf{o}}(g_\infty)$ implies that

$$(q^{a+b}-3)/2 = w = \bar{\mathsf{o}}(g_\infty) = (q^a - \epsilon_a)(q^b - \epsilon_b)/2.$$

This is however impossible for any $\epsilon_a, \epsilon_b = \pm 1$.

(d) From now we may assume that $3 \leq B \leq A - 2$. Hence, by Lemma 10.1.15, $\bar{\mathsf{o}}(g_\infty)$ is divisible by $\mathrm{lcm}(B,C)$, where we set $C := w$ if $p \nmid w$ and $C = w_0(p^e+1)$ if $p|w = w_0p^e$. On the other hand, note that

(10.3.9.3)
$$\bar{\mathsf{o}}(g_\infty) < (3/4)(q^n+1) = 3A/2; \text{ in fact, } \bar{\mathsf{o}}(g_\infty) < (5/7)(q^n+1) = 10A/7 \text{ unless } q^n = 27.$$

Indeed, we can apply Proposition 10.3.8. In cases (i) and (iii), $\bar{\mathsf{o}}(g_\infty) \leq A$. In case (ii),

$$\bar{\mathsf{o}}(g_\infty) \leq (q^a+1)(q^b+1)/2 \leq (q^{n-1}+1)(q+1)/2,$$

and the latter is less than $(3/4)(q^n+1)$ if $q^n = 27$ and less than $(5/7)(q^n+1)$ if $23 \leq q^n \neq 27$.

Write $d := \gcd(B,C)$. Now, if $p \nmid w$, then $\bar{\mathsf{o}}(g_\infty) \geq B(A-B) \geq 2(A-2) > (3/2)A$, contrary to (10.3.9.3). So we must have that

$$p|w, \text{ and } d|(p^e+1), \tag{10.3.9.4}$$

where the second claim follows from $\gcd(w_0,B)|\gcd(w,B) = 1$. We also have

$$BC/d = \mathrm{lcm}(B,C) \leq \bar{\mathsf{o}}(g_\infty) < (3/2)A = (3/2)(w+B) < (3/2)(B+C).$$

Thus $2BC < 3d(B+C)$, and so $(2B-3d)(2C-3d) < 9d^2$. Recall that $d|B,C$; in particular, either $B = d$, or $B \geq 2d$ in which case $2B - 3d \geq d$ and so $2C - 3d \leq 8d$ and thus $C \leq 5d$. The same argument applies to $C$. Assuming in addition that neither $B|C$ nor $C|B$, we have $\{B,C\} = \{2d,3d\}$ or $\{2d,5d\}$. Thus we have one of the following three cases.

*Case 1:* $\{B, C\} = \{2d, 5d\}$. In this case, $\bar{\mathsf{o}}(g_\infty) \geq \mathrm{lcm}(B, C) = 10d = (10/7)(B + C) \geq (10/7)A$, hence $q^n = 27$ by (10.3.9.3), and so $A = 14$. By (10.3.9.4), $3 = p|w$, $7d = B + C = w_0 + A > 14$, i.e. $d \geq 3$. Now we have

$$21 \leq 7d = B + C = B + w_0(3^e + 1) < (4/3)(B + w_0 3^e) = (4/3)A = 56/3,$$

a contradiction.

*Case 2:* $\{B, C\} = \{2d, 3d\}$. In this case, $\bar{\mathsf{o}}(g_\infty) \geq \mathrm{lcm}(B, C) = 6d = (6/5)(B + C) \geq (6/5)A$. Hence, we must be in case (ii) of Proposition 10.3.8. If in addition $q \geq 11$ or $q = 7$ but $q^n \geq 7^3$, then

$$\bar{\mathsf{o}}(g_\infty) \leq (q^{n-1} + 1)(q + 1)/2 < (3/5)(q^n + 1) = (6/5)A,$$

a contradiction. Suppose $q = 7$ and $q^n < 7^3$, i.e. $S = \mathrm{PSp}_4(7)$, whence $A = 25$. By (10.3.9.4), $7 = p|w$, $5d = B + C = w_0 + A > 25$, i.e. $d \geq 6$. Now we have

$$30 \leq 5d = B + C = B + w_0(7^e + 1) < (8/7)(B + w_0 7^e) = (8/7)A = 200/7,$$

a contradiction.

We have shown that $q \leq 5$. On the other hand, both $B$ and $C = w_0(p^e + 1)$ are coprime to $p$, so $p \neq 3$ and thus $p = q = 5$. Now,

$$10d = 2(B + C) = 2(w_0 + A) = 2w_0 + 5^n + 1,$$

showing $w_0 \equiv 2 (\mathrm{mod}\ 5)$. By (10.3.9.4) we also have

$$3d \geq C = w_0(p^e + 1) \geq w_0 d.$$

Hence $w_0 = 2$, $2d \leq C = 2(p^e + 1)$, and thus $d = p^e + 1$, $C = 2d$, $B = 3d$. Now

$$(5^n + 1)/2 = A = B + w = 3(5^e + 1) + 2 \cdot 5^e,$$

yielding $5^n - 2 \cdot 5^{e+1} = 5$, a contradiction.

*Case 3:* $d = B|C = w_0(p^e + 1)$. Note that $w_0 p^e = w < A < q^n$, so $e < nf$. On the other hand, $2B - 1 = (2A - 1) - 2w = q^n - 2w_0 p^e$, so $p^e$ divides $2B - 1$. Writing $2B - 1 = bp^e$ for some odd integer $b \geq 1$, we see from (10.3.9.4) that $2(p^e + 1)$ is a multiple of $2d = 2B = 1 + bp^e$, which is possible only when $b = 1$. We conclude that $B = (p^e + 1)/2$, as stated.

*Case 4:* $w_0(p^e + 1) = C = d|B$. Then $w_0 = 1$ and $d = p^e + 1$ by (10.3.9.4). As $B = (q^n + 1)/2 - p^e$ is divisible by $d$, we see that

$$2(p^e + 1)|(q^n + 3); \tag{10.3.9.5}$$

in particular, $e \leq nf$. Write $nf = ke + l$, where $k \in \mathbb{Z}_{\geq 1}$ and $0 \leq l < e$. Then

$$q^n = p^{nf} \equiv (-1)^k p^l (\mathrm{mod}\ (p^e + 1)),$$

and so

$$(p^e + 1)|\big((-1)^k p^l + 3\big). \tag{10.3.9.6}$$

*Case 4a:* $(-1)^k p^l + 3 = 0$. Then we have $2 \nmid k$ and $p = 3$. However, in this case, $q^n + 3 = 3(3^{ke} + 1)$ is however not divisible by $2(3^e + 1)$, contrary to (10.3.9.5).

*Case 4b:* $(-1)^k p^l + 3 \neq 0$. If $2 \nmid k$, then $|(-1)^k p^l + 3| = p^l - 3 < p^{l+1} + 1 \leq p^e + 1$, contradicting (10.3.9.6). So $2|k$, and (10.3.9.6) implies $p^l + 3 \geq p^e + 1 \geq p^{l+1} + 1$, which is possible only when $(l,e) = (0,1)$ and $p = 3$. However, in this case $q^n + 3 = 3^k + 3$ is not divisible by $2(3^e + 1) = 8$, contrary to (10.3.9.5). □

Next we classify semisimple m2sp-elements of finite unitary groups:

Proposition 10.3.10. *Let $n \in \mathbb{Z}_{\geq 3}$, $q$ a power of a prime $p$, $(n,q) \neq (3,2)$, $(3,3)$, $(4,2)$, and let $G$ be a finite group with $\mathrm{PSU}_n(q) \lhd G/\mathbf{Z}(G) \cong \mathrm{PGU}_n(q)$. Suppose $G$ admits an irreducible $\mathbb{C}G$-module $V$ of dimension $D \geq (q^n - q)/(q+1)$ on which a $p'$-element $g \in G$ acts as an* m2sp*-element. Then one of the following statements holds for the image $\bar{g}$ of $g$ in* $\mathrm{PGU}_n(q)$.

(i) *$\langle \bar{g} \rangle$ is of index at most 2 in a cyclic maximal torus $\bar{T}_n \cong C_{(q^n-(-1)^n)/(q+1)}$ of* $\mathrm{PGU}_n(q)$.

(ii) *$n = a + b$ with $a, b \in \mathbb{Z}_{\geq 1}$, $a \neq b$, and $\bar{g}$ is contained in the image in $\mathrm{PGU}_n(q)$ of a maximal torus $T_{a,b} \cong C_{q^a-(-1)^a} \times C_{q^b-(-1)^b} < \mathrm{GU}_a(q) \times \mathrm{GU}_b(q)$ of $\mathrm{GU}_n(q)$. Moreover, $\bar{\mathsf{o}}(g) < 1.69q^n/(q+1)$ if $2 \nmid ab$ and $\bar{\mathsf{o}}(g) < q^{n-1} \leq 1.5q^n/(q+1)$ if $2|ab$.*

(iii) *$n = a+b+c$ with $a, b, c \in \mathbb{Z}_{\geq 1}$, $2 \nmid ab$, $q \leq 3$, and $\bar{g}$ is contained in the image in $\mathrm{GU}_n(q)$ of a maximal torus $T_{a,b,c} \cong C_{q^a+1} \times C_{q^b+1} \times C_{q^c-(-1)^c} < \mathrm{GU}_a(q) \times \mathrm{GU}_b(q) \times \mathrm{GU}_c(q)$ of $\mathrm{GU}_n(q)$. Moreover, $|\{a,b,c\}| \geq 2$, and $\bar{\mathsf{o}}(g) < 1.95q^{n-1}/(q+1)$. If $a < b < c$, then $\bar{\mathsf{o}}(g) < 1.95q^n/(q+1)^2$.*

Proof. (a) Since $g$ is m2sp on $V$,

$$\bar{\mathsf{o}}(g) \geq D/2 \geq (q^n - q)/2(q+1). \tag{10.3.10.1}$$

We may assume that $\bar{g}$ is the image of a semisimple element $h \in \mathrm{GU}_n(q)$ in $S$. As described on [**GMPS**, p. 7673], we may decompose $W := \mathbb{F}_{q^2}^n$ into an orthogonal sum $\oplus_{i=1}^s W_i$ of $h$-stable non-degenerate subspaces $V_i \cong \mathbb{F}_{q^2}^{n_i}$, with $n_1, \ldots, n_s \geq 1$, and write $h = \mathrm{diag}(h_1, \ldots, h_s)$ with $h_i$ contained in a cyclic maximal torus $C_{q^{n_i}-(-1)^{n_i}} \leq \mathrm{GU}(W_i)$. Note that $h_i^{(q^{n_i}-(-1)^{n_i})/(q+1)}$ acts as a scalar on $W_i$ of order dividing $q+1$ for all $i$. Hence, $\bar{\mathsf{o}}(g) = \mathsf{o}(\bar{g})$ divides $(q+1)L$, where

$$L := \mathrm{lcm}\biggl(\frac{q^{n_1} - (-1)^{n_1}}{2}, \ldots, \frac{q^{n_s} - (-1)^{n_s}}{q+1}\biggr).$$

If $s = 1$, then $h = h_1$, and (10.3.10.1) implies that $\bar{\mathsf{o}}(g) > (q^n+1)/3(q+1)$ (as $q^n > 4q$) but $\bar{\mathsf{o}}(g)$ divides $(q^n - (-1)^n)/(q+1)$, and so we arrive at (i). We will henceforth assume that $s \geq 2$.

(b) Rewrite the sequence $(n_1, n_2, \ldots, n_s)$ so that the first $r$ terms $n_1 \leq n_2 \leq \ldots \leq n_r$ are odd and the last $t$ terms $n_{r+1} \leq n_{r+2} \leq \ldots \leq n_{r+t}$ are even, with $s = r + t$, so that

$$L := \mathrm{lcm}\biggl(\frac{q^{n_1}+1}{q+1}, \ldots, \frac{q^{n_r}+1}{q+1}, \frac{q^{n_{r+1}}-1}{q+1}, \ldots, \frac{q^{n_{r+s}}-1}{q+1}\biggr).$$

Suppose the sequence $(n_{r+1}, \ldots, n_{r+t})$ contains exactly $t_0$ distinct terms, and denote the sum of these terms as $\sum_j'' n_j$. Then

$$\mathrm{lcm}\biggl(\frac{q^{n_{r+1}}-1}{q+1}, \ldots, \frac{q^{n_{r+t}}-1}{q+1}\biggr) < \frac{q^{\sum_j'' n_j}}{(q+1)^{t_0}}. \tag{10.3.10.2}$$

Next, if $1 \leq a_1 < a_2 < \ldots < a_m$ are odd integers, then

$$\log\Bigl(\prod_{i=1}^{m}(1+q^{-a_i})\Bigr) < \log\Bigl(\prod_{k=1}^{\infty}(1+q^{-(2k-1)})\Bigr) < \sum_{k=1}^{\infty} q^{-(2k-1)} = q/(q^2-1) \leq 2/3,$$

whence $\prod_i(1+q^{-a_i}) < \exp(2/3) < 1.95$ and so $\prod_i(q^{a_i}+1) < (1.95)q^{\sum_i a_i}$. Now, suppose the sequence $(n_1, \ldots, n_r)$ contains exactly $r_0$ distinct terms, and denote the sum of these terms as $\sum_i' n_i$, and correspondingly, $\prod_i'(q^{n_i}+1)$ denotes the product over only those terms. Then

$$\text{(10.3.10.3)} \qquad \mathrm{lcm}\Bigl(\frac{q^{n_1}+1}{q+1}, \ldots, \frac{q^{n_r}+1}{q+1}\Bigr) \leq \prod_i{}' \frac{q^{n_i}+1}{q+1} < \frac{(1.95)q^{\sum_i' n_i}}{(q+1)^{r_0}}.$$

Write $s_0 := r_0 + t_0 \geq 1$. First we consider the case $s_0 = 1$, i.e $n_1 = \ldots = n_s = n/s$, $L = (q^{n_1} - (-1)^{n_1})/(q+1)$. If $n = 3$ or $5$, then $n_i = 1$, $\bar{\mathsf{o}}(g) \leq q+1 < (q^n - q)/2(q+1)$ (as $(n, q) \neq (3, 2)$, $(3, 3)$), contradicting (10.3.10.1). If $n = 4$, then $q > 2$, and either

$$n_i = 1,\ \bar{\mathsf{o}}(g) \leq q+1 < (q^4-q)/2(q+1),$$

or

$$n_i = 2,\ \bar{\mathsf{o}}(g) \leq q^2-1 < (q^4-q)/2(q+1),$$

contrary to (10.3.10.1). If $n \geq 6$, then $\bar{\mathsf{o}}(g) \leq q^{n/2}+1 \leq q^{n-3}+1 < (q^n-q)/2(q+1)$, again contradicting (10.3.10.1).

We have shown that $s_0 \geq 2$. Note that $\sum_i' n_i + \sum_j'' n_j$ misses the $s - s_0$ repeated terms of the sequence $(n_1, \ldots, n_s)$, hence $\sum_i' n_i + \sum_j'' n_j \leq n - (s - s_0)$. Together with (10.3.10.2) and (10.3.10.3), this implies that

$$L < \frac{1.95q^{\sum_i' n_i + \sum_j'' n_j}}{(q+1)^{s_0}} \leq \frac{1.95q^{n-(s-s_0)}}{(q+1)^{s_0}} = \frac{1.95q^n}{(q+1)^s} \cdot \bigl(\frac{q+1}{q}\bigr)^{s-s_0} \leq \frac{1.95q^n}{(q+1)^s} \cdot \bigl(\frac{q+1}{q}\bigr)^{s-2} = \frac{1.95q^n}{q^{s-2}(q+1)^2}.$$

Suppose $s \geq 4$; in particular $n \geq 4$. If $q \geq 3$, or $s \geq 5$, or $(s, q) = (4, 2)$ but $n \geq 7$, then

$$\bar{\mathsf{o}}(g) \leq (q+1)L < \frac{1.95q^n}{q^{s-2}(q+1)} < \frac{q^n-q}{2(q+1)},$$

contradicting (10.3.10.1). If $(s, q, n) = (4, 2, 6)$, then $D \geq 21$, and we still have

$$\bar{\mathsf{o}}(g) \leq (q+1)L < 1.95q^n/q^2(q+1) < D/2,$$

a contradiction. If $(s, q, n) = (4, 2, 5)$, then $(n_1, \ldots, n_s) = (1, 1, 1, 2)$, $L = 1$, $D \geq 10$, and again $\bar{\mathsf{o}}(g) \leq 3 < D/2$.

(c) Suppose $s = 3$; in particular, $n \geq 3$. If $q \geq 5$, or $q = 4$ but $n \geq 4$, then

$$\bar{\mathsf{o}}(g) \leq (q+1)L < \frac{1.95q^n}{q(q+1)} < \frac{q^n-q}{2(q+1)},$$

contradicting (10.3.10.1). If $(n, q) = (3, 4)$, then $(n_1, \ldots, n_s) = (1, 1, 1)$, $L = 1$, $D \geq 12$, and we still have $\bar{\mathsf{o}}(g) \leq q+1 < D/2$. Hence $q \leq 3$, and $\bar{\mathsf{o}}(g) \leq (q+1)L < 1.95q^{n-1}/(q+1)$. If moreover $s_0 = 3$, then $\bar{\mathsf{o}}(g) \leq (q+1)L < 1.95q^n/(q+1)^2$, as stated in (iii).

Next suppose that $s = s_0 = 2$, i.e. $\{n_1, n_2\} = \{a, b\}$ with $a \neq b$, and

$$\bar{\mathsf{o}}(g) \leq (q+1)L \leq (q^a-(-1)a)(q^b-(-1)^b)/(q+1).$$

Now, instead of (10.3.10.2) and (10.3.10.3), we note that

$$\frac{(q^a+1)(q^b+1)}{q+1} \leq \frac{q^n}{q+1} \cdot \big(1+\frac{1}{q}\big) \cdot \big(1+\frac{1}{q^3}\big) < \frac{1.69q^n}{q+1}$$

if $2 \nmid ab$, and

$$\frac{(q^a+1)(q^b-1)}{q+1} < \frac{q^n}{q+1} \cdot \big(1+\frac{1}{q}\big) \leq \frac{1.5q^n}{q+1}$$

if $2|a$, yielding (ii).

It remains to show that when $s = 3$ the sequence $(n_1, \ldots, n_s)$ contains at most one even member. Suppose for instance that $a := n_i \leq n_j =: b$ and $a, b$ are even; in particular, $n = 5$ or $n \geq 7$ (since $s_0 \geq 2$). We have shown above that $D \leq 2\bar{\mathsf{o}}(g) < 3.9q^{n-1}/(q+1) < 2q^n/(q+1)$. This upper bound on $D$ now implies by [**TZ1**, Theorem 4.1] that $D \in \{(q^n + (-1)^n q)/(q+1), (q^n-(-1)^n)/(q+1)\}$, $E(G)$ is a quotient of $\mathrm{SU}_n(q)$ and acts on $V$ via a Weil representation, which extends to $\mathrm{GU}_n(q)$. Hence, by Gallagher's theorem [**Is**, (6.17)], the action of $g$ on $V$ is a scalar multiple of the action of $h$ on a Weil representation of $\mathrm{GU}_n(q)$. Arguing as in part (B2) of the proof of [**KT5**, Theorem 8.3], we see that the restriction of the latter to the subgroup $\mathrm{GU}_a(q) \times \mathrm{GU}_b(q)$ contains the tensor product $A \otimes B$, where $A$ is a Weil module for $\mathrm{GU}_a(q)$ of dimension $(q^a+q)/(q+1) > \bar{\mathsf{o}}(h_i)$ and $B$ is a Weil module for $\mathrm{GU}_b(q)$ of dimension $(q^b+q)/(q+1) > \bar{\mathsf{o}}(h_j)$. In particular, $h_i$ has a repeated eigenvalue $\alpha$ on $A$ and $h_j$ has a repeated eigenvalue $\beta$ on $B$. It follows that $\alpha\beta$ is an eigenvalue of multiplicity $\geq 4$ for $\mathrm{diag}(h_i, h_j)$ on $A \otimes B$. Hence $h$ has an eigenvalue with multiplicity at least 4 on $V$, and so does $g$, a contradiction. □

We will also need an application of the Borel-Tits theorem:

Lemma 10.3.11. *Let $n \geq 3$ be an odd integer, $q$ a power of a prime $p$, and let $Q$ be a $p$-subgroup of* $\mathrm{SU}_n(q)$. *If $n \geq 5$, let $\ell$ be a primitive prime divisor of $(-q)^{n-1} - 1$,* (which is a primitive prime divisor of $q^{n-1} - 1$ if $4|n$ and a primitive prime divisor of $q^{(n-1)/2} - 1$ if $n \equiv 2(\mathrm{mod}\ 4)$, cf. [**Zs**]), *and assume in addition that $Q$ is normalized by an element $s \in$* $\mathrm{SU}_n(q)$ *of order $\ell$. Then $Q$ is contained in the unipotent radical of a Siegel parabolic subgroup of* $\mathrm{SU}_n(q)$*, and the dimension of any simple $Q$-module in any Weil representation of* $\mathrm{SU}_n(q)$ *is at most $q$.*

Proof. The conclusion is vacuously true if $Q = 1$, so we will assume $Q \neq 1$. If $n = 3$, then the radical $R$ of a (Siegel) parabolic subgroup $P$ of $\mathrm{SU}_3(q)$ is a Sylow $p$-subgroup, and so we may assume that $Q \leq R$. Consider the case $n \geq 5$. By assumption, the spectrum of $s$ on the natural space $W = \mathbb{F}_{q^2}^n$ of $\mathrm{SU}_n(q)$ contains a primitive $\ell^{\mathrm{th}}$ root of unity. The condition on $\ell$ implies that the $\langle s \rangle$-module $W$ is the direct sum of three irreducible submodules $W_0 \oplus W_1 \oplus W_2$, where $W_0$ is non-degenerate of dimension 1, acted on trivially by $s$, and $W_1$ and $W_2$ are totally singular of dimension $(n-1)/2$.

Since $Q \neq 1$ is a $p$-subgroup, its fixed point subspace $U := \mathbf{C}_W(Q)$ is nonzero and proper in $W$. $Q$ also acts on $U^\perp \neq 0$ and has nonzero fixed points on it. It follows that $U_1 := U \cap U^\perp$ is nonzero and totally singular, of dimension $d \leq (n-1)/2$. As $s$ normalizes $Q$, it also acts on $U_1$, and the above described structure of $W$ forces $d = (n-1)/2$ and, say, $U_1 = W_1$. Hence $Q$ is contained in $P := \mathrm{Stab}_{\mathrm{SU}_n(q)}(W_1)$, which is a Siegel parabolic subgroup. The radical $R$ of $P$ is precisely $\{x \in P \mid x|_{W_1} = \mathrm{Id}_{W_1}\}$, and so it contains $Q$.

We have shown that $Q \leq R$. Now, as shown in the proofs of Lemmas 12.5 and 12.6 of [**GMST**], the restriction of any Weil module of $\mathrm{SU}_n(q)$ to $R$ is the sum of $(q^{n-1}-1)/(q+1)$ irreducible modules of dimension $q$ each, and possibly one more 1-dimensional module. Hence the statements follow. □

THEOREM 10.3.12. *Let $p$ be a prime, $A, B \in \mathbb{Z}_{\geq 2}$ be integers with $p \nmid AB$ and* $\gcd(A,B) = 1$. *Suppose $A \geq 12$, $2 \leq B \leq A-2$, and that the local system $\mathcal{F}(A,B,\theta)$ in characteristic $p$ has a finite, almost quasisimple, geometric monodromy group $G$ which has a non-abelian composition factor $S = \mathrm{PSU}_n(q)$ with $n \geq 3$. Then $q = p^f$, $2 \nmid n$, $\mathsf{o}(\theta)|(q+1)$, and we can find an odd integer $m \geq 1$ with $\gcd(n,m) = 1$ such that $A = (q^n+1)/(q+1)$ and $B = (q^m+1)/(q+1)$.*

PROOF. (a) Let $\mathcal{H} = \mathcal{H}_{small,A,B}$ or $\mathcal{H}_{big,A,B,\chi}$ be a hypergeometric sheaf giving rise to $\mathcal{F}(A,B,\theta)$. Then $\mathcal{H}$ has rank $D \geq A-1 \geq 11$. By Corollary 10.1.9, $\mathcal{H}$ has finite geometric monodromy group $H \rhd G$ which satisfies $(\mathbf{S}+)$. Applying Lemma 1.1.3 to $H \rhd G$, we see that $S$ is the unique non-abelian composition factor of $H$. Let $g_0$ be a generator of the image of $I(0)$ in $H$, $Q$ the image of $P(\infty)$ in $H$, and let $g_\infty$ be a $p'$-generator for the image $J$ of $I(\infty)$ in $H$ modulo $Q$. By Proposition 2.4.3, $g_0$ is $\mathsf{ssp}$, and $g_\infty$ is $\mathsf{m2sp}$. Furthermore, since $D \geq 11$, Theorem 3.1.10 implies that $q = p^f$ is a power of $p$, unless possibly when $S = \mathrm{SU}_3(4)$, $D = 12$ and $p = 5$ or 13. We now show that this exception cannot occur. First suppose that $p = 13$. Using [**GAP**] we see that any element $x \in Q \smallsetminus \mathbf{Z}(H)$ has eigenvalues of dimension at most 1, which shows that $\dim \mathsf{Tame} \leq 1$, whence $A - B = w \geq 11$, which is impossible since $A \leq D+1 = 13$, $p \nmid A$, and $B \geq 2$. Next suppose that $p = 5$. Using [**GAP**] we see that any element $x \in Q \smallsetminus \mathbf{Z}(H)$ has eigenvalues of dimension at most 4, whence $w \geq 8$. As $D = 12$, we can apply [**KT5**, Proposition 4.8(iv)] to see that $p \nmid |\mathbf{Z}(H)|$, which in turn implies that $Q \leq S$ since $p \nmid |\mathrm{Out}(S)|$; in particular, $Q \cong C_5$ or $C_5^2$. But $w \geq 8$ rules out $Q \cong C_5$ and thus $Q \cong C_5^2$. As the trace of any element $x \in Q \smallsetminus \{1\}$ is $-3$ or 2, we can apply (3.1.10.2) with $\alpha := 1/4$ to get $w \geq 9$, and $w = A - B \leq (D+1) - 2 = 11$. Now, $w \neq 9, 11$ because otherwise $g_\infty$ yields an element of order 9 or 11 in $\mathrm{Aut}(S)$ by [**KRLT4**, Proposition 4.8], which is impossible. We also rule out $w = 10$ since $Q$ is abelian.

(b) We have shown that $q = p^f$. Next, applying Theorems 3.1.5 and 3.1.8 (and using the condition $D \geq 11$), we have that $H/\mathbf{Z}(H) \cong \mathrm{PGU}_n(q)$ and $E(G)$ acts as the image of $\mathrm{SU}_n(q)$ in a Weil representation of dimension $D = (q^n + (-1)^n q)/(q+1)$ or $(q^n - (-1)^n)/(q+1)$; in particular,

$$(n,q) \neq (3,2),\ (3,3),\ (4,2),\ (5,2). \tag{10.3.12.1}$$

(Note that if $(n,q) = (5,2)$, then $A \geq 12$ and $D \in \{10, 11\}$ imply that $A = 12$, which is impossible since $p = 2 \nmid A$.) Recalling the assumption $\bar{\mathsf{o}}(g_0) = A \in \{D, D+1\}$ and using Theorems 8.3 and 9.17 of [**KT5**], we obtain that $2 \nmid n$ and that $A = (q^n+1)/(q+1)$. Note that the assumption $(n,q) \neq (4,3)$, $(6,2)$ in [**KT5**, Theorem 9.17] was used only to ensure that $p|q$, which is guaranteed by Theorem 3.1.10, and that $w \neq 1$, which is automatic since $w = A - B \geq 2$.

(c) Suppose for the moment that $B = (q^m+1)/(q+1)$ for some integer $m \geq 1$. Then $2 \nmid m$, and the assumption $\gcd(A,B) = 1$ then implies that $\gcd(m,n) = 1$.

We now show that $\mathsf{o}(\theta)|(q+1)$. Recall that $H/\mathbf{Z}(H) \cong \mathrm{PGU}_n(q)$ and moreover $E(H)$ is the image of $\mathrm{SU}_n(q)$ in a Weil representation. It follows that $E(H) \lhd \mathbf{O}^{p'}(H) \leq E(H)\mathbf{Z}(H)$

and in fact $\mathbf{O}^{p'}(H) = E(H)$ unless $p|\mathbf{Z}(H)|$. Next, $\mathcal{F}$ is the $[A]^\star$ Kummer pullback of $\mathcal{H}$ and $\mathcal{F}$ lives on $\mathbb{A}^1$. Hence $G = \mathbf{O}^{p'}(G)$ and $H/G$ is a cyclic $p'$-group. Unless $p||\mathbf{Z}(H)|$, we then have that $G = E(H)$, and so the field of traces of $\mathcal{F}$ is contained in the field of values for a Weil character of $\mathrm{SU}_n(q)$, which is contained in $\mathbb{Q}(\zeta_{q+1})$.

If $D = (q^n+1)/(q+1)$, then $p \nmid D$, hence $p \nmid |\mathbf{Z}(H)|$ by [**KT5**, Proposition 4.8(iv)]. Suppose $D = (q^n-q)/(q+1)$, so that $\mathcal{H} = \mathcal{H}_{small,A,B}$. As $2 \nmid AB$, $\mathcal{H}$ is symplectic by [**Ka-ESDE**, 8.8.1-2], and hence $|\mathbf{Z}(H)| \leq 2$; in particular, $p \nmid |\mathbf{Z}(H)|$ if $p > 2$. In the exceptional case where $p = 2$ and $D = (q^n-q)/(q+1)$, we still have $S \lhd G \leq C_2 \times S$, and so the field of traces of $\mathcal{F}$ is also contained in the field of values for a Weil character of $\mathrm{SU}_n(q)$, which in this case is $\mathbb{Q}$. In view of Theorem 10.1.2, we may now apply Theorem 10.1.18 to $\mathcal{F}$ to conclude that $\theta$ takes values in $\mathbb{Q}(\zeta_p, \zeta_{q+1})$. But $\mathsf{o}(\theta)$ is coprime to $p$, so we conclude that $\mathsf{o}(\theta)|(q+1)$, as claimed.

The rest of the proof is to show that we indeed have $B = (q^m+1)/(q+1)$ for some $m \in \mathbb{Z}_{\geq 1}$. Using (10.3.12.1), we can apply Proposition 10.3.10 to identify $g_\infty$; note that since $2 \nmid n$, we have $2 \nmid a$ and $2|b$ in case (ii) and $2 \nmid abc$ in case (iii) of Proposition 10.3.10.

(d) Suppose $B = 2$; in particular, $p > 2$. Then $w := A - B = (q^n-q)/(q+1) - 1$ is coprime to $p$. By Lemma 10.1.15(i), $\bar{\mathsf{o}}(g_\infty)$ is divisible by $w$. As mentioned above, the possibilities for $g_\infty$ are listed in Proposition 10.3.10; in particular, $\bar{\mathsf{o}}(g_\infty) < 1.5A < 2w$, and so $\bar{\mathsf{o}}(g_\infty) = w = A-2$. As $(A-2) \nmid A$, this rules out case (i) of Proposition 10.3.10. Case (iii) is also impossible, since in this case we have $q = 3$ and so $\bar{\mathsf{o}}(g_\infty) < 1.95q^{n-1}/(q+1) < 0.65A < A-2$. In case (ii), we have $w = \bar{\mathsf{o}}(g_\infty)$ divides $(q^a+1)(q^b-1)/(q+1)$ which is at most $q^{n-1}-1 < 1.5w$, hence

$$\frac{q^{a+b}+1}{q+1} - 2 = w = \bar{\mathsf{o}}(g_\infty) = \frac{(q^a+1)(q^b-1)}{q+1}.$$

It follows that $q^a = q^b + 2q$, where $2|b > 0$ and $2 \nmid a$, which is possible only when $p = 2$ and so $p|B$, a contradiction.

(e) From now we may assume that $3 \leq B \leq A-2$. Hence, by Lemma 10.1.15,

$$\bar{\mathsf{o}}(g_\infty) \text{ is divisible by } \mathrm{lcm}(B,C), \tag{10.3.12.2}$$

where we set $C := w$ if $p \nmid w$ and $C = w_0(p^e+1)$ if $p|w = w_0p^e$. By Proposition 10.3.10,

$$\bar{\mathsf{o}}(g_\infty) < q^{n-1} < 3A/2. \tag{10.3.12.3}$$

Write $d := \gcd(B,C)$. Now, if $p \nmid w$, then $\bar{\mathsf{o}}(g_\infty) \geq B(A-B) \geq 2(A-2) > (3/2)A$, contrary to (10.3.12.3). So we must have that

$$p|w = w_0p^e,\ p \nmid BC, \text{ and } d|(p^e+1), \tag{10.3.12.4}$$

where the third claim follows from $\gcd(w_0,B)|\gcd(w,B) = 1$. We also have

$$BC/d = \mathrm{lcm}(B,C) \leq \bar{\mathsf{o}}(g_\infty) < (3/2)A = (3/2)(w+B) < (3/2)(B+C).$$

Thus $2BC < 3d(B+C)$, and so $(2B-3d)(2C-3d) < 9d^2$. Recall that $d|B,C$; in particular, either $B = d$, or $B \geq 2d$ in which case $2B - 3d \geq d$ and so $2C - 3d \leq 8d$ and thus $C \leq 5d$. The same argument applies to $C$. Assuming in addition that neither $B|C$ nor $C|B$, we have $\{B,C\} = \{2d,3d\}$ or $\{2d,5d\}$. First we rule out these two cases.

(e1) Suppose $\{B, C\} = \{2d, 5d\}$. In this case, $p \geq 3$ by (10.3.12.4), hence (10.3.12.3) yields

$$\bar{\mathsf{o}}(g_\infty) < (4/3)A < (4/3)(B + C) = 28d/3 < 10d = \mathrm{lcm}(B, C),$$

contradicting (10.3.12.2).

(e2) Suppose $\{B, C\} = \{2d, 3d\}$. In this case, $p \geq 5$ by (10.3.12.4), hence (10.3.12.3) yields

$$\bar{\mathsf{o}}(g_\infty) < (6/5)A < (6/5)(B + C) = 6d = \mathrm{lcm}(B, C),$$

again a contradiction.

(f) Here we consider the case $w_0(p^e+1) = C = d|B$. Then $w_0 = 1$, $w = p^e$, and $d = p^e+1$ by (10.3.12.4). As $B = (q^n + 1)/(q + 1) - p^e$ is divisible by $d$, we see from (10.3.12.2) that

(10.3.12.5) $$\bar{\mathsf{o}}(g_\infty) \text{ if divisible by } B > A/2.$$

We again identify $g_\infty$ using Proposition 10.3.10. In case (i) of it, we then have $\bar{\mathsf{o}}(g_\infty)|A$ and so $B|A$, a contradiction.

(f1) Suppose we are in case (ii) of Proposition 10.3.10. Then $\bar{\mathsf{o}}(g_\infty)$ divides $(q^a + 1)(q^b - 1)/(q + 1)$, which is less than $q^{n-1} < (3/2)A < 3B$, so (10.3.12.5) implies that $(q^a + 1)(q^b - 1)/(q + 1)$ is either $B$ or $2B$.

(f11) Suppose $(q^a + 1)(q^b - 1)/(q + 1) = B$, i.e. $(q^a + 1)(q^b - 1) = q^{a+b} + 1 - p^e(q + 1)$. Then

(10.3.12.6) $$p^e(q + 1) = q^a - q^b + 2.$$

Recall that $2 \nmid a$ and $2|b > 0$, but $e \geq 1$. Since $p|(q^a - q^b + 2)$ by (10.3.12.6), we have $p = 2$. Now, if $a = 1$, then $q^a - q^b + 2 \leq q^2 - q^b \leq 0$, contradicting (10.3.12.6). Hence $a \geq 3$. In this case, $q^a - q^b + 2 \equiv 2(\mathrm{mod}\ 4)$, and so (10.3.12.6) shows $e = 1$, whence $2q + q^b = q^a$. If moreover $b \geq 4$, then $2q = q^a - q^b$ is divisible by $q^3$, a contradiction. So $b = 2$, $2q + q^2 = q^a$, yielding $(q, a) = (2, 3)$ and thus $(n, q) = (5, 2)$, which is ruled out by (10.3.12.1).

(f12) Suppose $(q^a+1)(q^b-1)/(q+1) = 2B$, i.e. $(q^a+1)(q^b-1) = 2q^{a+b}+2-2p^e(q+1)$. Then

(10.3.12.7) $$2p^e(q + 1) = q^{a+b} + q^a - q^b + 3.$$

Recall that $2 \nmid a$ and $2|b > 0$, but $e \geq 1$. Since $p|(q^n + q^a - q^b + 3)$ by (10.3.12.6), we have $p = 3$. Now, note that the 3-part of $q^n + q^a - q^b + 3$ is 3. So (10.3.12.7) implies that $e = 1$, whence $0 < q^n - q^b = -q^a + 6q + 3$, and so $a = 1$. In this case, $q^3 > 5q + 3 = q^n - q^b$ is divisible by $q^b$, showing $b = 2$, $q^n = q^2 + 5q + 3$, and thus $(n, q) = (3, 3)$, which is ruled out by (10.3.12.1). (Note that if we allow $A < 12$, then this exception is realized by $\mathcal{H}_{small,7,4}$ which has geometric monodromy group $6_1 \cdot \mathrm{PSU}_4(3)$ by [**KRLT4**, Theorem 20.4]. Furthermore, $\mathcal{H}_{small,7,2}$ also has geometric monodromy group $6_1 \cdot \mathrm{PSU}_4(3)$ by [**KRLT4**, Theorem 20.2].)

(f2) Suppose we are in case (iii) of Proposition 10.3.10. First we consider the case $q \geq 3$. If $a < b < c$, then $\bar{\mathsf{o}}(g_\infty) < 2q^n/(q + 1)^2 < A/2$, contrary to (10.3.12.5). Hence we may assume that $a < b$ and $c \in \{a, b\}$. In the notation of the proof of Proposition 10.3.10,

(10.3.12.8) $$\bar{\mathsf{o}}(g_\infty) \leq (q + 1)L \leq (q^a + 1)(q^b + 1)/(q + 1) \leq q^{n-2} + 1$$

(since $a + b \leq n - 1$). Now, (10.3.12.1) shows that either $n \geq 5$, or $n = 3$ but $q \geq 4$, whence $q^{n-2} + 1 < A/2$ and thus $\bar{\mathsf{o}}(g_\infty) < A/2$, contradicting (10.3.12.5).

So we must have that $q = 2$. In the notation of the proof of Proposition 10.3.10, $\mathsf{\bar{o}}(g_\infty)$ divides $3L$, and $3L|M$ with

(10.3.12.9)

$$M := \frac{(2^a+1)(2^b+1)(2^c+1)}{9} \leq \frac{2^n}{9}\big(1+\frac{1}{2}\big)\cdot\big(1+\frac{1}{2}\big)\cdot\big(1+\frac{1}{2^3}\big) < \frac{2.54\cdot 2^n}{9} < 0.85A < 1.7B.$$

In fact, if $a \geq 3$, then

$$M \leq \frac{2^n}{9}\big(1+\frac{1}{2^3}\big)\cdot\big(1+\frac{1}{2^3}\big)\cdot\big(1+\frac{1}{2^5}\big) < \frac{1.31\cdot 2^n}{9} < 0.44A < 0.88B,$$

and thus $\mathsf{\bar{o}}(g_\infty) < B$, contrary to (10.3.12.5). So $a = 1$, and (10.3.12.5) and (10.3.12.9) imply

$$(2^n+1)/3 - 2^e = B = \mathsf{\bar{o}}(g_\infty) = M = (2^b+1)(2^c+1)/3,$$

and thus

$$2^b + 2^c + 2^{e+1} + 2^e = 2^{b+c}, \text{ where } b < c \text{ and } 2 \nmid bc. \tag{10.3.12.10}$$

We claim that the only solution to (10.3.12.10) is that $(b, c, e) = (1, 3, 1)$. Indeed, if $e \leq b-1$, then the 2-part of $N := 2^b+2^c+2^{e+1}+2^e$ is $2^e$, hence $N \neq 2^{b+c}$. If $e \geq b+1$, then the 2-part of $N$ is $2^b$, and so $N \neq 2^{b+c}$. So we get $e = b$, $2^{b+c} = 2^c + 2^{b+2}$, whence $c = b+2$ and $b = 1$, as stated.) It follows that $(n, q) = (5, 2)$, which is ruled out by (10.3.12.1).

(g) Finally, we consider the case $d = B|C = w_0(p^e+1)$. Note that $w_0p^e = w < A < q^{n-1}$, so $e < (n-1)f$.

(g1) First assume that $q = 2$. Then $3B - 1 = 3A - 3w - 1 = 2^n - 3\cdot 2^e$ is divisible by $2^e$, so we can write $3B = 1 + 2^ek$, where $k \in \mathbb{Z}_{\geq 1}$. Next, $3B = 1 + 2^ek$ divides $3(2^e+1)$ by (10.3.12.4), so either $(k, e) = (4, 1)$ or $k \leq 3$. If $k = 1$, then $B = (2^e+1)/3$, as desired. Also $3B = 1 + 2^ek$ shows that $k \neq 3$.

Suppose $(k, e) = (4, 1)$, i.e. $B = 3$. Then $w = A - 3 = (2^n - 8)/3$, and so $e = 3$, a contradiction.

Suppose $k = 2$. Then $B = (2^{e+1}+1)/3 > (2^e+1)/2$ divides $2^e+1$, so $(2^{e+1}+1)/3 = 2^e+1$, and so $2^e = -2$, again a contradiction.

(g2) From now on we may assume $q \geq 3$. Now, in case (i) of Proposition 10.3.10, $\mathsf{\bar{o}}(g_\infty)|A$, so $B|A$, a contradiction. We also note that, since $B \leq C$ and $B + C = A + w_0$ we have from (10.3.12.2) that

$$\mathsf{\bar{o}}(g_\infty) \text{ is divisible by } C > A/2. \tag{10.3.12.11}$$

Suppose we are in case (iii) of Proposition 10.3.10. If $a < b < c$, then $\mathsf{\bar{o}}(g_\infty) < 2q^n/(q+1)^2 < A/2$, contradicting (10.3.12.11). If $a < b$ and $c \in \{a, b\}$, then (10.3.12.8) holds, and again we can use (10.3.12.1) to deduce that $\mathsf{\bar{o}}(g_\infty) < A/2$, again a contradiction.

Hence case (ii) of Proposition 10.3.10 must hold, and thus the image of $g_\infty$ in $\mathrm{PGU}_n(q)$ is the image of some element $h = \mathrm{diag}(h_1, h_2)$ of the torus $T_{a,b} \cong C_{Q_a} \times C_{Q_b} < \mathrm{GU}_a(q) \times \mathrm{GU}_b(q)$ in $\mathrm{PGU}_n(q)$, $n = a+b$, $2 \nmid a$, $2|b$, where we set $Q_a := (q^a+1)/(q+1)$ and $Q_b := (q^b-1)/(q+1)$.

(g3) Here we consider the case $a \geq 3$; in particular, $Q_a \geq q^2 - q + 1 \geq 7$. Arguing as in part (c) of the proof of Proposition 10.3.10, we see that $E(H)$ is a quotient of $\mathrm{SU}_n(q)$ and acts on the underlying representation $V = V_{\mathcal{H}}$ via a Weil representation, and the action of $g$ on $V$ is a scalar multiple of the action of $h$ on a Weil representation of $\mathrm{GU}_n(q)$. Furthermore, the restriction of the latter to the subgroup $\mathrm{GU}_a(q) \times \mathrm{GU}_b(q)$ contains the tensor product

$V_1 \otimes V_2$, where $V_1$ is a Weil module for $\mathrm{GU}_a(q)$ and $V_2$ is a Weil module for $\mathrm{GU}_b(q)$ of dimension $Q_b + 1 > \bar{\mathsf{o}}(h_2)$. In particular, $h_2$ has a repeated eigenvalue $\beta$ on $V_2$. On the other hand, the central order $\bar{\mathsf{o}}(h_1)$ of $h_1$ in $\mathrm{GU}_a(q)$ divides $Q_a$, which is odd. If $\bar{\mathsf{o}}(h_1) < Q_a$, then arguing as in part (b) of the proof of Proposition 10.3.10 we have

$$\bar{\mathsf{o}}(g_\infty) \leq \frac{1}{3} \cdot \frac{(q^a+1)(q^b-1)}{q+1} \leq (q^{n-1}-1)/3 < A/2,$$

contradicting (10.3.12.11). We have shown that $\bar{\mathsf{o}}(h_1) = Q_a$. Similarly, if $e_1 := \gcd(a,b) > 1$, then $e_1 \geq 3$, and so

$$\bar{\mathsf{o}}(g_\infty) \leq (q+1) \cdot \frac{(q^a+1)(q^b-1)}{(q^{e_1}+1)(q+1)} \leq \frac{(q^a+1)(q^b-1)}{q^3+1} < A/2,$$

again contradicting (10.3.12.11). Hence

$$\gcd(a,b) = 1. \qquad (10.3.12.12)$$

Now, a direct calculation shows that the spectrum of $h_1$ on $V_1$ is $\alpha \cdot \mu_{Q_a}$ if $\dim(V_1) = Q_a$, and $\alpha \cdot \big(\mu_{Q_a} \smallsetminus \{1\}\big)$ if $\dim(V_1) = Q_a - 1$, for some $\alpha \in \mathbb{C}^\times$. Hence, $g$ admits repeated eigenvalues on $V$ whose ratio is $\zeta_{Q_a}$. Applying Lemma 10.1.15(ii), we get that

$$Q_a | B. \qquad (10.3.12.13)$$

Recall that $q = p^f > 2$ and $a \geq 3$. Hence $q^{2a} - 1 = p^{2af} - 1$ admits a primitive prime divisor $\ell$ by [**Zs**], which then divides $Q_a$. Since $B|(p^e+1)$, (10.3.12.13) implies that $\ell|(p^{2e}-1)$, so $af|e$ by the choice of $\ell$. Suppose that $e > af$. Then $p^{2e}-1$ admits a primitive prime divisor $\ell'$ by [**Zs**], which then divides $p^e+1$ but not $Q_a$ nor $q+1$. By (10.3.12.2), $\ell'$ divides $\bar{\mathsf{o}}(g_\infty)$. On the other hand, $\bar{\mathsf{o}}(g_\infty)$ divides $(q^a+1)(q^b-1)/(q+1) = (q+1)Q_aQ_b$. Hence $\ell'|Q_b$, and so $e|b$ by the choice of $\ell'$. It follows that $af|b$, contrary to (10.3.12.12). Hence $e = af$. Using (10.3.12.13) and $B|(p^e+1) = (q+1)Q_a$, we can now write $B = b_0 Q_a$ with

$$b_0 | (q+1). \qquad (10.3.12.14)$$

We also have

$$w_0 q^a = w_0 p^e = w = A - B = \frac{q^{a+b}+1}{q+1} - b_0 \frac{q^a+1}{q+1} = (q^b - b_0)Q_a - Q_b,$$

and so

$$w_0(q^a+1) + Q_b - w_0 = (q^b - b_0)Q_a \qquad (10.3.12.15)$$

is divisible by $Q_a$. Thus we can write $w_0 = Q_b - vQ_a$ for some $v \in \mathbb{Z}$. Substituting this in (10.3.12.15), we obtain that $b_0 - 1 = vq^a$. But $|b_0 - 1| = b_0 - 1 \leq q$ by (10.3.12.14) and $a \geq 3$. So we conclude that $v = 0$, $b_0 = 1$, and thus $B = (q^a+1)/(q+1)$, as desired.

(g4) Finally, we consider the case $a = 1$, and thus $b = n-1$ and so $g_\infty$ has central order dividing $q^{n-1}-1$. We first show that

$$p^e \leq q. \qquad (10.3.12.16)$$

Since $H/\mathbf{Z}(H) \cong \mathrm{PGU}_n(q)$ has $p'$-index over $S$, we see that $Q$ is contained in $\mathbf{Z}(H)E(H)$. Thus $\mathbf{Z}(H)Q = \mathbf{Z}(H)Q_1$ with $Q_1 := \mathbf{Z}(H)Q \cap E(H)$. Since $Q$ is nilpotent, $Q_1$ is nilpotent, and so we can write $Q_1 = Q_2 \times Q_3$, where $Q_2 = \mathbf{O}_p(Q_1)$ and $Q_3 = \mathbf{O}_{p'}(Q_1)$. We also note that for any $x \in Q_3$, $x^{|Q|} \in \mathbf{Z}(E(H))$ but $x$ is a $p'$-element, so $x \in \mathbf{Z}(E(H))$ and thus

$Q_3 \le \mathbf{Z}(E(H)) \le \mathbf{Z}(H)$. Recall that $E(H)$ acts on $V$ via a Weill representation of $\mathrm{SU}_n(q)$; in particular, $\mathbf{Z}(E(H))$ is a $p'$-group, and so $Q_2 \cap \mathbf{Z}(H) = Q_2 \cap \mathbf{Z}(E(H)) = 1$. It follows that

$$\mathbf{Z}(H)Q = \mathbf{Z}(H)Q_1 = \mathbf{Z}(H)Q_3Q_2 = \mathbf{Z}(H)Q_2 = \mathbf{Z}(H) \times Q_2.$$

Recall from [**KRLT4**, Proposition 4.9] that the irreducible summands of the $Q$-module $\mathsf{Wild}$ all have dimension $p^e$. Hence it suffices to show that the dimension of any simple $Q_2$-submodule of $V$ is at most $q$. If $n = 3$, then the claim for $Q_2$ follows from Lemma 10.3.11. Consider the case $n \ge 5$ and let $\ell$ be a primitive prime divisor of $(-q)^{n-1} - 1$; note that $\ell \ge 5$ and is coprime to $q+1$. Since $q^{n-1} - 1 < (4/3)A < (8/3)C$, (10.3.12.11) implies that $\bar{\mathsf{o}}(g_\infty)$ is either $(q^{n-1} - 1)$ or $(q^{n-1} - 1)/2$; in particular it is divisible by $\ell$. Let $g_2$ denote a power of $g_\infty$, which has central order $\ell$. Since the index of $H/\mathbf{Z}(H)$ over $S$ is $\gcd(n, q+1)$, we see that $g_2 \in \mathbf{Z}(H)E(H)$ and thus $g_2 = z_2h_2$ for some $z_2 \in \mathbf{Z}(H)$ and $h_2 \in E(H)$ of central order $\ell$. Since $g$ normalizes $Q$ and $E(H)$, $g_2$ normalizes $Q_1 = \mathbf{Z}(H)Q \cap E(H)$ and also $Q_2 = \mathbf{O}_p(Q_1)$. Hence $h_2$ normalizes $Q_2$, and the claim for $Q_2$ follows from Lemma 10.3.11. Thus we have established (10.3.12.16).

Now we have

$$w_0p^e = w = A - B = q\frac{q^{n-1} - 1}{q+1} + 1 - B,$$

hence (10.3.12.16) implies that $p^e|(B - 1)$. On the other hand, $B \ge 2$ and $B|(p^e + 1)$ by (10.3.12.4), so $1 \le B - 1 \le p^e$. It follows that $B = p^e + 1$, and so

$$w_0 = p^{f-e}Q_{n-1} - 1, \tag{10.3.12.17}$$

where $Q_{n-1} = (q^{n-1} - 1)/(q + 1)$ as before. On the other hand, by (10.3.12.1) we have that $w_0$ divides $\bar{\mathsf{o}}(g_\infty)$, which divides

$$p^{f-e}\big(q^{n-1} - 1\big) = (q + 1)p^{f-e}Q_{n-1} = (q + 1)w_0 + (q + 1).$$

Hence, $w_0|(q + 1)$. Now, if $n \ge 5$ then $w_0 > (q^4 - 1)/(q + 1) - 1 > q + 1$ by (10.3.12.17), a contradiction. Thus $n = 3$. If $f = e$, then (10.3.12.17) yields $w_0 = q-2$ divides $q+1$, so $q = 5$ (as $q > 3$ by (10.3.12.1)). But in this case $C = w_0(p^e+1) = 18$ does not divide $q^{n-1}-1 = 24$, contrary to (10.3.12.11). If $p^{f-e} \ge 3$, then (10.3.12.17) yields $w_0 \ge 3(q - 1) - 1 > q + 1$, a contradiction.

If $p^{f-e} = 2$, then (10.3.12.17) yields $q + 1 \ge w_0 \ge 2(q - 1) - 1$, and so

$$q = 4,\ B = 3,\ A = 13,\ w = 10,\ p^e = 2.$$

In this case, $V$, as a module over $Q$ or $Q_2$, is a direct sum of five 2-dimensional simple submodules $X_i$, $1 \le i \le 5$, and at most three submodules of dimension 1, and $H = \mathbf{Z}(H)S$. We again apply (the proof of) Lemma 10.3.11 to the subgroup $Q_2$ which may be viewed as a subgroup of $R \in \mathrm{Syl}_2(S)$, and $\mathbf{N}_S(R) = R \rtimes C_{15}$. As shown above, $\bar{\mathsf{o}}(g_\infty) = 15$ and $g_\infty$ normalizes $Q_2 \ne 1$. Arguing as in the proof of Lemma 10.3.11, we again see that $Q_2 \ne 1$ fixes a unique singular line in $\mathbb{F}_{16}^3$ (if it fixed two distinct lines, then the two lines would generated a non-degenerate plane acted on trivially by $Q_2$ and so $Q_2 = 1$) whose stabilizer is $\mathbf{N}_S(R)$. Hence $g_\infty \in \mathbf{Z}(H)\mathbf{N}_S(R)$ and thus we may assume that $g_\infty = z_3h_3$ with $z_3 \in \mathbf{Z}(H)$ and $\mathbf{N}_S(R) = R \rtimes \langle h_3\rangle$. Now the $R$-module $V$ is a direct sum of three 4-dimensional submodules $Y_j$, $1 \le j \le 3$, transitively permuted by $h_3$, and possibly a 1-dimensional submodule. We may assume that $Y_1 = X_1 \oplus X_2$. As $h_3$ normalizes $Q_2$, we have similar decompositions for

$Y_2$ and $Y_3$, which means that the $Q_2$-module $V$ is a direct sum of six 2-dimensional simple submodules and possible one 1-dimensional. This contradiction completes the proof of the theorem.

Here is an alternate way of attaining this last contradiction. By [**KRLT4**, Theorem 24.2], the sheaf $\mathcal{F}(13,3,\mathbb{1})$ in characteristic $p=2$ has geometric monodromy group $2\cdot G_2(4)$. By Theorem 10.1.14, if $\mathcal{F}(13,3,\theta)$ in characteristic $p=2$ has finite geometric monodromy group, then $\theta^3$ has order 1 or 3 (it cannot have order 2 as it has order prime to $p=2$). But for $\theta$ of order 3 or 9, the $V$-test shows that $G_{\rm geom}$ is not finite, so it is only for $\theta=\mathbb{1}$ that $\mathcal{F}(13,3,\theta)$ in characteristic $p=2$ has finite geometric monodromy group, and this group is $2\cdot G_2(4)$. □

Now we can prove the main result of this section, which determines which $\mathcal{F}(A,B,\theta)$ have finite monodromy when $A>B>1$; see Theorem 10.2.6 for the case $B=1$.

THEOREM 10.3.13. *Let $p$ be a prime and let $A>B\geq 2$ be integers with $\gcd(A,B)=1$ and $p\nmid AB$. Consider the local system $\mathcal{F}(A,B,\theta)$ in characteristic $p$, of rank $D=A-1$ if $\theta=\mathbb{1}$ and $D=A$ otherwise, see Definition 7.3.1, with geometric monodromy group $G=G_{\rm geom}$. Then $G$ is finite if and only if one of the following conditions holds.*

(i) *$p>2$, $q=p^f$, $A=(q^n+1)/2$ and $B=(q^m+1)/2$ for some integers $n>m\geq 1$ with $2|nm$, $\gcd(m,n)=1$, and $\theta=\mathbb{1}$ or $\theta=\chi_2$. Moreover, $G$ is the image of $\mathrm{Sp}_{2n}(q)$ in a Weil representation of degree $D$.*

(ii) *$p$ arbitrary, $q=p^f$, $A=(q^n+1)/(q+1)$ and $B=(q^m+1)/(q+1)$ for some odd integers $n>m\geq 3$, $\gcd(m,n)=1$, and $\theta^{q+1}=\mathbb{1}$. Moreover, $G$ is the image of $\mathrm{SU}_n(q)$ in a Weil representation of degree $D$.*

(iii) *$p=2$, $q=2^f$, $A=q^n+1$ and $B=q^m+1$ for some integers $n>m\geq 1$ with $2|nm$, $\gcd(m,n)=1$, $\theta=\mathbb{1}$. If $nf\geq 4$ in addition, then $G=2^{1+2nf}_{-}\cdot\Omega^{-}_{2n}(q)$.*

(iv) *$p=2$, $A=13$, $B=3$, $\theta=\mathbb{1}$, and $G=2\cdot G_2(4)$.*

(v) *$p=3$, $A=23$, $B=5$, $\theta=\chi_2$, and $G=\mathsf{Co}_3$.*

(vi) *$p=3$, $A=7$, $B=5$, $\theta=\chi_2$, and $G=\mathrm{Sp}_6(2)$.*

(vii) *$p=3$, $A=7$, $B=4$ or $B=2$, $\theta=\mathbb{1}$, and $G=6_1\cdot\mathrm{PSU}_4(3)$.*

(viii) *$p=3$, $A=5$, $B=4$, $\theta=\mathbb{1}$, and $G=\mathrm{Sp}_4(3)\times 3$.*

(ix) *$p=5$, $A=7$, $B=3$, $\theta=\chi_2$, and $G=\mathrm{Sp}_6(2)$.*

(x) *$p=5$, $A=3$, $B=2$, $\theta=\mathbb{1}$, and $G=\mathrm{SL}_2(5)\times 5$.*

(xi) *$p=7$, $A=5$, $B=2$, $\theta=\mathbb{1}$, and $G=2\mathsf{A}_7$.*

PROOF. (a) First suppose that $(A,B,\theta)$ is one of the listed triples. In cases (i) and (ii), we apply Lemma 10.3.1 to see that $\mathcal{F}(A,B,\theta)$ is an irreducible summand of $\mathcal{F}_{nngcd}(q^n+1,q^m+1,\mathbb{1})$, hence the statement follows from Theorem 7.3.11, except for the structure of $G$ in case (ii) when $p=2$, which will be determined at the end of (c) (below). In case (iii), finiteness of $G$ follows immediately from the supersingularity statement of [**vdG-vdV**, Corollary 5.4] and $G$ is identified in Theorem 8.5.5.

In case (v), $G$ is determined in [**KRLT1**, Theorem 4.2(v)]. In cases (iv) and (vi)–(xi), finiteness of $G$ and its identification follow from Theorems 25.2, 31.6, 21.2 and 21.4, 30.7(iv), 31.2, 30.7(v), and 31.9 of [**KRLT4**], respectively.

(b) In the rest of the proof, we will assume $G$ is finite, and show that $(A,B,\theta)$ must be one of the listed triples. Let $\mathcal{H}=\mathcal{H}_{small,A,B}$ or $\mathcal{H}_{big,A,B,\chi}$ be a hypergeometric sheaf whose $[A]^\star$

Kummer pullback is $\mathcal{F}(A,B,\theta)$. Then $\mathcal{H}$ has finite monodromy group $H \rhd G$. By Corollary 4.1.3, finiteness of $H$ implies $A \leq 5$ in the case $B = A-1$.

More generally, here we explain how to handle the case $A \leq 29$. In all cases, $\mathcal{H}$ is primitive by Lemma 10.1.8. Note that $w := A - B \geq 1$ and $D \geq A-1 \geq 2$. If $(w,p,D) = (1,5,2)$, then $(A,B,\theta) = (3,2,\mathbb{1})$, leading to (x). So we will assume $(w,p,D) \neq (1,5,2)$. Applying Theorem 2.4.4 and using primitivity of $\mathcal{H}$, we conclude that $p \leq 2w+1$. Theorem 10.1.14 allows us to bound $\mathsf{o}(\theta)$ from above. Thus we have a (short) finite list of cases of $(A,B,\theta)$ with $A \leq 29$ and $p \leq 59$ for which $\mathcal{F}(A,B,\theta)$ in characteristic $p$ can possibly have finite $G_{\mathrm{geom}}$. We eliminate those not on the list given in the theorem by showing that they fail the $V$-test for finiteness, done using $\mathsf{Mathematica}$. Thus the only finite monodromy cases with $A \leq 29$ are those listed.

(c) Now we may assume that $A \geq 30$ and $2 \leq B \leq A-2$. As $A \geq 11$, $H$ satisfies $(\mathbf{S}+)$ by Corollary 10.1.9. By Lemma 1.1.3, $H$ is either almost quasisimple, with a unique non-abelian composition factor $S$, or an extraspecial normalizer. In the latter case, $p=2$ by [**KT5**, Theorem 9.19]; hence, applying Theorem 10.3.3 we arrive at (iii). Suppose we are in the almost quasisimple case. In this case, $S$ is also the unique non-abelian composition factor of $G$. By Theorem 10.3.5, $S \not\cong \mathsf{A}_n$ for any $n \geq 5$. Let $g_0$ be a generator of the image of $I(0)$ in $H$. Then $g_0$ is an $\mathsf{ssp}$-element by Proposition 2.4.3, and so we can apply Theorems 3.1.3 and 3.1.5 to identify $S$ and the underlying representation $V = V_{\mathcal{H}}$ for $G$, which is of dimension $D \geq A-1 \geq 29$. The bound $D \geq 29$ rules out all the sporadic simple groups, so $S = \mathrm{PSL}_n(q)$ with $n \geq 2$, $\mathrm{PSp}_{2n}(q)$ with $n \geq 2$, or $\mathrm{PSU}_n(q)$ with $n \geq 3$. Now, the case $S = \mathrm{PSL}_n(q)$ is ruled out by Theorem 10.3.7. The case $S = \mathrm{PSp}_{2n}(q)$ leads to (i) by Theorem 10.3.9, and the case $S = \mathrm{PSU}_n(q)$ leads to (ii) by Theorem 10.3.12.

As promised, we now return to case (ii) and determine the structure of $G$ when $p=2$. In this case, $A = (q^n+1)/(q+1)$, so $A$ is odd and the 2-part of $A-1$ is exactly $q$ and smaller than $A-1 \geq 29$. Hence this case is disjoint from all other possibilities (i) and (iii)–(xi). Therefore, our preceding analysis shows that $G$ is almost quasisimple, with $S = \mathrm{PSU}_m(r)$ and $A = (r^m+1)/(r+1)$ for some 2-power $r$ and $2 \nmid r \geq 3$. Since $q$ is the 2-part of $A-1$, we get $r = q$ and so $m = n$. Again using Theorem 3.1.5 and [**KT5**, Corollary 8.4], we get $H/\mathbf{Z}(H) \cong \mathrm{PGU}_n(q)$ and moreover $E(G) = E(H)$ is the image of $\mathrm{SU}_n(q)$ in a Weil representation of degree $D$. If $D = A$, then, since $A - B \geq 2$, by [**KT5**, Proposition 4.8(iv)] we have $p \nmid |\mathbf{Z}(H)|$ and so $H/E(H)$ is a $p'$-group. As $H/G$ is a cyclic $p'$-group and $G = \mathbf{O}^{p'}(G)$, we have $G = E(G)$ in this case. Finally, assume that $D = A-1$, and so $\mathcal{H} = \mathcal{H}_{small,A,B}$. In this case, as $2 \nmid AB$, $\mathcal{H}$ is symplectic by [**Ka-ESDE**, 8.8.1-2], and hence $|\mathbf{Z}(H)| \leq 2$. Also, $H/E(H)$ has a central subgroup $\mathbf{Z}(H)E(H)/E(H)$, with quotient $H/\mathbf{Z}(H)E(H) \cong \mathrm{PGU}_n(q)/S$ being cyclic of order $\gcd(n,q+1)$. Hence $H/E(H)$ is abelian, of order dividing $2\gcd(n,q+1)$. On the other hand, $H = \mathbf{O}^2(H)$ by Theorem 1.2.2. It follows that $H/E(H)$ has order dividing $\gcd(n,q+1)$, and hence $G = E(H)$ as stated in (ii). □

Note that Theorems 10.2.6 and 10.3.13 only deal with $\mathcal{F}(A,B,\theta)$ when $\gcd(A,B) = 1$. Next we will remove this condition.

Theorem 10.3.14. *Let $p$ be a prime and let $A > B \geq 1$ be integers with $p \nmid AB$ and $d := \gcd(A,B)$. Consider the local system $\mathcal{F}_{nngcd}(A,B,\theta)$ in characteristic $p$, of rank $D = A-1$ if $\theta = \mathbb{1}$ and $D = A$ otherwise, see Definition 7.3.1, with geometric monodromy group*

$G = G_{\mathrm{geom}}$. *Assume in addition that* $D \geq 2$. *Then* $G$ *is finite if and only if one of the following conditions holds.*

(a) $p > 2$, $q = p^f$, $d|2$, $A = (q^n + 1)/e$ *and* $B = (q^m + 1)/e$ *for some integers* $n > m \geq 0$ *with* $2|nm$, $\gcd(n, m) = 1$, $e := 2/d$, *and* $\theta^e = \mathbb{1}$.
(b) $p$ *arbitrary,* $q = p^f$, $d|(q + 1)$, $A = (q^n + 1)/e$ *and* $B = (q^m + 1)/e$ *for some odd integers* $n > m \geq 1$, $\gcd(n, m) = 1$, $e := (q + 1)/d$, *and* $\theta^e = \mathbb{1}$.
(c) $d = B = 1$, *and one of the possibilities* (iii), (iv) *of Theorem 10.2.6 occurs.*
(d) $d = 1 < B$, *and case* (iii) *of Theorem 10.3.13 occurs.*
(e) $d = B = 1$, *and one of the possibilities* (v), (vi) *of Theorem 10.2.6 occurs.*
(f) $d = 1 < B$, *and one of the possibilities* (iv)–(xi) *of Theorem 10.3.13 occurs.*

PROOF. If $d = 1$, then the statement follows from Theorems 10.2.6 and 10.3.13. So we will assume that $d > 1$ and fix a character $\sigma$ such that $\sigma^d = \theta$. By [**KT6**, Proposition 2.6],

$$\mathcal{F}_{nngcd}(A, B, \theta) \cong \oplus_{\chi \in \mathsf{Char}(d)} \mathcal{F}(A/d, B/d, \chi\sigma), \tag{10.3.14.1}$$

where the sheaves $\mathcal{F}(A/d, B/d, \chi\sigma)$ are geometrically irreducible and pairwise non-isomorphic. Working over fields over which all $\chi\sigma$ are defined and using Lemma 2.2.5, we see that the finiteness of $G_{\mathrm{geom}}$ implies that each of the $d$ sheaves $\mathcal{F}(A/d, B/d, \chi\sigma)$ also has finite $G_{\mathrm{geom}}$. They all share the same exponents $A/d$ and $B/d$, but have the characters $\chi\sigma$ that differ by a character of order dividing $d$.

First we consider the case $B/d \geq 2$. The above observations then show by Theorem 10.3.13 that none of the possibilities (iii)–(xi) listed therein cannot occur since $d > 1$. Note that in 10.3.13(i) we have $p > 2$ and $A/d \equiv (p + 1)/2 (\mathrm{mod}\ p)$, whereas $A/d \equiv 1 (\mathrm{mod}\ p)$ in 10.3.13(ii). Hence, either all the sheaves $\mathcal{F}(A/d, B/d, \chi\sigma)$ satisfy 10.3.13(i), or all of them satisfy 10.3.13(ii). In the former case of 10.3.13(i), we must have that $p > 2$, $d = 2$, $A/d = (q^n + 1)/2$, $B/d = (q^m + 1)/2$ for some power $q = p^f$ and some coprime $n > m \geq 1$ with $2|nm$, and $\mathbb{1} = (\chi\sigma)^2 = \theta$, and thus we arrive at (a). Suppose we are in the latter case of 10.3.13(ii). Then there is some power $q = p^f$ such that $A/d = (q^n + 1)/(q + 1)$, $B/d = (q^m + 1)/(q + 1)$ for some coprime $n > m \geq 1$ with $2 \nmid nm$, and $(\chi\sigma)^{q+1} = \mathbb{1}$ for all $\chi \in \mathsf{Char}(d)$. In particular, taking $\chi = \mathbb{1}$ we get $\sigma^{q+1} = \mathbb{1}$. Now taking $\chi \in \mathsf{Char}(d)$ of order $d$, we get $\chi^{q+1} = \mathbb{1}$, and so $d|(q + 1)$, $\mathbb{1} = \sigma^{q+1} = \theta^{(q+1)/d}$, and we arrive at (b).

Now we consider the case $B = d$. In the case $A = 2d$, assume in addition that $\theta \neq \mathbb{1}$, so that $(\chi\sigma)^d \neq \mathbb{1}$ and so $\chi\sigma \neq \mathbb{1}$ for all $\chi \in \mathsf{Char}(d)$. The above observations then show by Theorem 10.2.6 that none of the possibilities (iii)–(vi) listed therein can occur since $d > 1$. In the case of 10.2.6(i), we must have that $p > 2$, $d = 2$, $A/d = (q + 1)/2$ for some power $q = p^f$, and $\mathbb{1} = (\chi\sigma)^2 = \theta$, and thus we arrive at (a) with $(n, m) = (1, 0)$. Suppose we are in the case of 10.2.6(ii). Then there is some power $q = p^f$ such that $A/d = (q^n + 1)/(q + 1)$ for some odd $n > 1$, and $(\chi\sigma)^{q+1} = \mathbb{1}$ for all $\chi \in \mathsf{Char}(d)$. Arguing as above, we obtain $d|(q+1)$, $\mathbb{1} = \sigma^{q+1} = \theta^{(q+1)/d}$, and we arrive at (b) with $m = 1$.

Finally, assume that $(A, B, \theta) = (2B, B, \theta)$. Here we can take $\sigma = \mathbb{1}$. Since $D \geq 2$, we have $B \geq 2$. Applying Theorem 10.2.6 to any summand $\mathcal{F}(2, 1, \chi)$ in (10.3.14.1) with $\chi \neq \mathbb{1}$, we see that $p = 3$ and $\chi^2 = \mathbb{1}$. Thus $B = d = 2$, $A/2 = (3 + 1)/2$, and we arrive at (a) with $(p, q, n, m) = (3, 3, 1, 0)$. □

The finite geometric monodromy groups occurring in Theorem 10.3.14 are determined in Theorems 10.2.6 and 10.3.13 when $d = 1$, and will be determined in Theorem 11.2.4(ii), (iii) when $d > 1$.

Next we determine $G_{\mathrm{geom}}$ for $\mathcal{F}(A, B, \theta)$ when it is infinite.

Lemma 10.3.15. *There exists no local system $\mathcal{F}(A, B, \theta)$ in characteristic $p \nmid AB$ such that $G^{\circ}_{\mathrm{geom}}$ is the image of $\mathrm{SL}(V) \cong \mathrm{SL}_6$ acting on the irreducible representation $\wedge^k(V)$ with $k = 2$ or $k = 3$.*

Proof. (a) Assume the contrary, and consider the corresponding hypergeometric sheaf $\mathcal{H}$, with geometric monodromy group $H$. Since $\mathcal{H}$ satisfies (**S**+) by Lemma 10.1.7 and Corollary 10.1.9 and $H \rhd G_{\mathrm{geom}}$, we have that $H^{\circ} = G^{\circ}_{\mathrm{geom}}$ is the image of $\mathrm{SL}_6$. Applying Theorem 6.2.14, we have that $2 \leq p \leq k$.

First we consider the case $k = 2$, so $p = 2$ and $\mathcal{H}$ has rank $D = 15$. As $p \nmid A$, we must then have $A = 15$, $\mathcal{H} = \mathcal{H}_{big,15,B,\chi}$. But this is impossible by Lemma 6.1.18.

(b) Hence $k = 3$ and $\mathcal{H}$ has rank $D = 20$. Consider the case $p = 3$. As $p \nmid A$, we have $A = 20$, $\mathcal{H} = \mathcal{H}_{big,20,B,\chi}$. Since the $\mathrm{SL}_6$-module $\wedge^3(V)$ is self-dual, Corollary 2.4.8 implies that $\mathcal{F}(A, B, \theta)$ is geometrically self-dual. But this contradicts Theorem 10.1.6(i), as $A$ is even.

We have shown that $p = 2$. As $p \nmid A$, we have $A = 21$, $\mathcal{H} = \mathcal{H}_{small,21,B}$, $2 \nmid B$, $w := A - B \geq 2$. Let $g_0$ be a generator of the image of $I(0)$ in $H$. Then $g_0$ has spectrum $\mu_{21} \smallsetminus \{1\}$ on the underlying module $V_{\mathcal{H}}$; in particular, $\mathsf{o}(g_0) = 21$. Note that $\mathcal{H}$ is symplectically self-dual by [**Ka-ESDE**, 8.8.1-2], so $\mathbf{Z}(H) \leq C_2$. On the other hand, $H^{\circ}$ is the image of $\mathrm{SL}_6$ on $\wedge^3(V)$, so its center is $C_2$ and thus $\mathbf{Z}(H) = \mathbf{Z}(H^{\circ})$. It follows that $[H : H^{\circ}] \leq 2$, and so $g_0 \in H^{\circ}$. Theorem 1.2.2 then implies that $H = H^{\circ} = \mathrm{SL}_6/C_3$.

Since $\mathrm{SL}_6 \twoheadrightarrow H$ with kernel $C_3$, [**KT5**, Theorem 4.14] implies that $w := A - B \leq 6$, hence $B \geq 15$. But $p \nmid B$ and the irreducibility of $\mathcal{F}(A, B, \theta)$ implies by [**KT6**, Corollary 2.7] that $\gcd(A, B) = 1$. It follows that $B = 17$ or $19$, respectively $w = 4$ or $2$.

(c) Now we will deduce a contradiction by looking at the action of $g_{\infty}$, a $p'$-element that generates the image of $I(\infty)$ in $H$ modulo the image of $P(\infty)$. By [**KRLT4**, Proposition 4.9], $g_{\infty}$ acts on $\mathsf{Wild}$ with spectrum $\alpha \cdot \big(\mu_{w+1} \smallsetminus \{1\}\big)$, and on $\mathsf{Tame}$ with spectrum $\mu_B \smallsetminus \{1\}$. In particular, $1 = \det(g_{\infty}) = \alpha^w$ and so $\alpha \in \mu_4$. But $g_{\infty}$ has odd order, so in fact $\alpha = 1$. Thus $g_{\infty}^B = \wedge^3(X)$ has spectrum

$$\big(\mu_{w+1} \smallsetminus \{1\}\big) \sqcup \{1^{[B-1]}\} \tag{10.3.15.1}$$

on $V_{\mathcal{H}}$, where $X = \mathrm{diag}(a_1, \ldots, a_6) \in \mathrm{SL}_6$. Without any loss, we may assume by (10.3.15.1) that

$$a_1a_2a_3 = \beta, \text{ whence } a_4a_5a_6 = \beta^{-1}$$

for some $1 \neq \beta \in \mu_{w+1}$ (because $\det(X) = 1$). If $w = 2$, then no other triple products differ from 1. If $w = 4$, then two more triple products are not 1. Since the roles of $\{1, 2, 3\}$ and $\{4, 5, 6\}$ are symmetric, we may assume that either

$$a_1a_2a_4 = \gamma, \text{ whence } a_3a_5a_6 = \gamma^{-1},$$

with $1 \neq \gamma \in \mu_{w+1}$. All other triple products are 1.

Hence, for both $w = 2$ and $w = 4$, $a_i a_j a_k = 1$ (at least) for the following triples $ijk$:

$$125, 126, 134, 135, 136, 145, 146, 156, 234, 235, 236, 245, 246, 256, 345, 346.$$

Comparing the products for triples $134, 135, 136$, we get $a_4 = a_5 = a_6$. Using the triples $145, 245, 345$, we get $a_1 = a_2 = a_3$. Using the triples $134, 145$, we get $a_3 = a_5$. Thus $X = a_1 \cdot \mathrm{Id}$, $g_\infty^B = a_1^3 \cdot \mathrm{Id}$, contrary to (10.3.15.1). □

Lemma 10.3.16. *Let $n \in \{5, 6, 8\}$. There exists no local system $\mathcal{F}(A, B, \theta)$ in characteristic $p = 2 \nmid AB$ such that $G_{\mathrm{geom}}^\circ$ is $\mathrm{HSpin}_{2n}$ acting on a half-spin representation.*

Proof. Assume the contrary. Since $p \nmid AB$ and $D = 2^{n-1}$, we have that $B \leq A - 2$, $A = 2^{n-1} + 1$, $B$ is odd, and $\theta = \mathbb{1}$. Hence, by Theorem 10.1.6(iii), the underlying module $V$ for $G_{\mathrm{geom}}$ is symplectically self-dual. On the other hand, by [**Bour**, Table I, p. 213], the $G_{\mathrm{geom}}^\circ$-module $V$ is not self-dual if $n = 5$, symplectically self-dual if $n = 6$ and orthogonally self-dual if $n = 8$. This takes care of the cases $n = 5, 8$. It remains to treat the case $n = 6$.

Consider the corresponding hypergeometric sheaf $\mathcal{H} = \mathcal{H}_{small,33,B}$ and let $H$ denote its geometric monodromy group. Then $\mathcal{H}$ satisfies $(\mathbf{S}+)$ by Lemma 10.1.7 and Corollary 10.1.9. Since $\mathcal{H}$ is symplectic by [**Ka-ESDE**, 8.8.1-2], we have that $|\mathbf{Z}(H)| \leq 2$. On the other hand, $H \rhd G_{\mathrm{geom}}^\circ$, $G_{\mathrm{geom}}^\circ \cong \mathrm{HSpin}_{12}$ has center of order 2, and any outer automorphism of $\mathrm{HSpin}_{12}$ fuses the two half-spin representations (each of degree $32 = A - 1$). Hence $H = G_{\mathrm{geom}} = \mathrm{HSpin}_{12}$. Consider a generator $g_0$ of the image of $I(0)$ in $H$ and let $h := g_0^{11}$. Then $h$ has order 3 and its spectrum on $V$ is

$$\{1^{[10]}, \zeta^{[11]}, \bar{\zeta}^{[11]}\}, \tag{10.3.16.1}$$

where $\zeta := \zeta_3$. Embed $h$ in a maximal torus $\mathcal{T}$, and let

$$\Omega := \left\{ \frac{1}{2} \sum_{i=1}^{6} \epsilon_i e_i \mid \epsilon_i = \pm 1, \prod_{i=1}^{6} \epsilon_i = 1 \right\}$$

be the set of $\mathcal{T}$-weights on $V$, where $\{e_1, \ldots, e_6\}$ is an orthonormal basis of $\mathbb{R}^6$.

Suppose for instance that $e_1(h) = e_2(h) = 1$. Then, for any $\alpha = \pm 1$ and for any $\delta = \sum_{i=3}^6 \epsilon_i e_i$ with $\prod_{i=3}^6 \epsilon_i = \alpha$, the weights $(e_1 + \alpha e_2 + \delta)/2$ and $(-e_1 - \alpha e_2 + \delta)/2$ belong to $\Omega$ and take the same value at $h$. It follows that the multiplicity of any eigenvalue of $h$ on $V$ is even, contrary to (10.3.16.1).

We have shown that $e_i(h) = 1$ for at most one index $i$. It is well known, see e.g. [**TZ3**, Proposition 3.1(ii)] that any semisimple element of $H$ is real. Applying this to $h$, we see that $e_i(h) \neq 1$ for all $i$, and so we may assume that $e_1(h) = e_2(h) = e_3(h) = \zeta$ and $e_4(h) = e_5(h) = e_6(h) = \bar{\zeta}$. Hence, the spectrum of $h$ on $V$ is $\{1^{[20]}, \zeta^{[6]}, \bar{\zeta}^{[6]}\}$, again contradicting (10.3.16.1). □

Lemma 10.3.17. *There exists no local system $\mathcal{F}(A, B, \theta)$ in characteristic $p \nmid AB$ such that $G_{\mathrm{geom}}^\circ$ is $E_6$, acting on an irreducible representation of degree 27.*

Proof. Assume the contrary, and consider the corresponding hypergeometric sheaf $\mathcal{H}$, with geometric monodromy group $H$. Since $\mathcal{H}$ satisfies $(\mathbf{S}+)$ by Lemma 10.1.7 and Corollary 10.1.9 and $H \rhd G_{\mathrm{geom}}$, we have that $H^\circ = G_{\mathrm{geom}}^\circ = E_6$. Applying Theorem 6.2.14, we have that $p = 2$ or $p = 3$. Also, since any outer automorphism of $H^\circ$ fuses the two irreducible representations of $H^\circ$ of degree 27, we have $H = \mathbf{Z}(H)H^\circ$. Let $g_0$ be a generator of the image of $I(0)$ in $H$.

Suppose $p = 3$. Then $A = 28$ since $p \nmid A$, and $\mathcal{H} = \mathcal{H}_{small,28,B}$. Note that $g_0$ has spectrum $\mu_{28} \smallsetminus \{1\}$ on the underlying $H$-module $V_{\mathcal{H}}$. It follows that $g_0^7$ has order 4 and spectrum $\{1^{[6]}, \zeta^{[7]}, (-1)^{[7]}, \bar{\zeta}^{[7]}\}$, where $\zeta := \zeta_4$. Now write $g_0^7 = zh$, where $z \in \mathbf{Z}(H)$ and $h \in H^\circ$. Then $\mathrm{Id} = g_0^{28} = z^4h^4$, whence

$$z^4 = h^{-4} \in \mathbf{Z}(H) \cap H^\circ \leq \mathbf{Z}(H^\circ) \cong C_3$$

and so $z^{12} = \mathrm{Id}$. We also note that $\det(h) = 1$ as $H^\circ$ is perfect, and $-1 = \det(g_0^7) = \det(z)\det(h)$, so $\det(z) = -1$. It follows that $z$ acts as a scalar $\xi \in \mathbb{C}^\times$ on $V_{\mathcal{H}}$, where $\xi^{12} = 1$ and $-1 = \det(z) = \xi^{27}$; in particular, $\xi^6 = 1$ and $z^6 = \mathrm{Id}$. Therefore, $g_0^{42} = z^6h^6 = h^6$ is an element of $H^\circ$ that has spectrum $\{1^{[13]}, (-1)^{[14]}\}$ on $V_{\mathcal{H}}$ (and so is of order 2). However, according to [**CW**, Table 2], $H^\circ$ contains no such element, a contradiction.

We have shown that $p = 2$, so $A = 27$, and $\theta \neq \mathbb{1}$. Then $g_0$ has spectrum $\mu_{27}$ on $V_{\mathcal{H}}$. Write $g_0 = zh$ with $z \in \mathbf{Z}(H)$ and $h \in H^\circ$. Then $1 = \det(g_0) = \det(z)\det(h)$, but $\det(h) = 1$ since $H^\circ$ is perfect. So, $z$ acts as a scalar $\xi \in \mathbb{C}^\times$ on $V_{\mathcal{H}}$, where $1 = \det(z) = \xi^{27}$, and thus $\xi \in \mu_{27}$. It follows that the element $h \in H^\circ$ also has spectrum $\mu_{27}$ on $V_{\mathcal{H}}$. Now we put $h$ in a maximal torus $\mathcal{T}$ of $H^\circ$, and again adopt the realization of the set $\Omega$ of the $\mathcal{T}$-weights on $V_{\mathcal{H}}$ that was used in the proof of Theorem 6.2.13. Then the eigenvalues of $h$ on $V_{\mathcal{H}}$ are

$$(e_i \pm f)(h),\ (-e_i - e_j)(h),\ 1 \leq i < j \leq 6.$$

In particular, $e_1(h)^2 = (e_1 + f)(h) \cdot (e_1 - f)(h) \in \mu_{27}$. Hence we can write $e_1(h) = \epsilon\alpha_1 = \epsilon\zeta_{27}^{a_1}$ for some $a_1 \in \mathbb{Z}/27\mathbb{Z}$ and some $\epsilon = \pm$. Writing $e_j(h) = \epsilon\alpha_j$ and $f(h) = \epsilon\beta$ with $\alpha_j, \beta \in \mathbb{C}^\times$ for $2 \leq j \leq 6$, we then have that

$$\mu_{27} \ni (-e_1 - e_j)(h) = (\alpha_1\alpha_j)^{-1},\ \mu_{27} \ni (e_1 + f)(h) = \alpha_1\beta,$$

and so $\alpha_j = \zeta_{27}^{a_j}$ and $\beta = \zeta_{27}^{b}$ for some $a_j, b \in \mathbb{Z}/27\mathbb{Z}$. Keeping in mind (6.2.13.1), we then see that $1 = \prod_{i=1}^6 e_i(h) = \zeta_{27}^{\sum_{i=1}^6 a_i}$ and thus

$$\sum_{i=1}^{6} a_i = 0 \tag{10.3.17.1}$$

and

$$\{a_i \pm b, -a_i - a_j \mid 1 \leq i < j \leq 6\} = \mathbb{Z}/27\mathbb{Z}. \tag{10.3.17.2}$$

Note that (10.3.17.2) shows that $a_1, \ldots, a_6$ are pairwise distinct. A Magma calculation (see Appendix A2) shows however that there is no $(a_1, \ldots, a_6, b) \in (\mathbb{Z}/27\mathbb{Z})^7$ that satisfies both (10.3.17.1) and (10.3.17.2), again a contradiction. □

LEMMA 10.3.18. *There exists no local system $\mathcal{F}(A, B, \theta)$ in characteristic $p \nmid AB$ such that $G_{\mathrm{geom}}^\circ$ is $E_7$, acting on an irreducible representation of degree* 56.

PROOF. Assume the contrary, and consider the corresponding hypergeometric sheaf $\mathcal{H}$, with geometric monodromy group $H$. Since $\mathcal{H}$ satisfies ($\mathbf{S}+$) by Lemma 10.1.7 and Corollary 10.1.9 and $H \rhd G_{\mathrm{geom}}$, we have that $H^\circ = G_{\mathrm{geom}}^\circ = E_7$. Applying Theorem 6.2.14, we have that $p = 2$ or $p = 3$. If $p = 2$, then $A = 57$ since $p \nmid A$, and this case is ruled out by Lemma 10.2.2. So $p = 3$, $A = 56$, and $\theta \neq \mathbb{1}$. Since the irreducible 56-dimensional $E_7$-module

$V_{\mathcal{H}}$ is self-dual, Corollary 2.4.8 implies that $\mathcal{F}(A,B,\theta)$ is geometrically self-dual. But this contradicts Theorem 10.1.6(i), as $A$ is even. □

LEMMA 10.3.19. *Consider the subgroup $S = \mathrm{SL}_2 \otimes \mathrm{SL}_2 \otimes \mathrm{SL}_2 < \mathrm{SL}_8$ and suppose that $h \in S$ has $1$ as an eigenvalue with multiplicity $m \geq 4$. Then the following statements hold.*

(i) *All eigenvalues of $h$ have multiplicity $\geq 2$.*

(ii) *If $m > 4$, then $1$ is the only eigenvalue of $h$.*

PROOF. Write $h = X \otimes Y \otimes Z$, with $X \in \mathrm{SL}_2$ with spectrum $\{x, x^{-1}\}$, $Y \in \mathrm{SL}_2$ with spectrum $\{y, y^{-1}\}$, and $Z \in \mathrm{SL}_2$ with spectrum $\{z, z^{-1}\}$. As 1 is an eigenvalue of $h$, replacing $x$ or $y$ or $z$ by their inverses if necessary, we may assume $z = xy$. Then the spectrum of $h$ is $\{1^{[2]}, x^2, x^{-2}, y^2, y^{-2}, (xy)^2, (xy)^{-2}\}$. It follows that $x^2$ or $y^2$ or $(xy)^2$ is 1. Using the symmetry of $x, y, z$, we may assume that $z = \pm 1$. Replacing $(X, Z)$ by $(-X, -Z)$, we may assume that $z = 1$. Now the spectrum of $h$ is $\{xy^{[2]}, (xy^{-1})^{[2]}, (xy^{-1})^{[2]}, (x^{-1}y^{-1})^{[2]}\}$, yielding (i).

In the case of (ii), replacing $x$ by $x^{-1}$ if necessary, we may assume $x = y$, and so the spectrum of $h$ is $\{1^{[4]}, (x^2)^{[2]}, (x^{-2})^{[2]}\}$. As $m > 4$, we must have that $x^2 = 1$ and thus 1 is the only eigenvalue of $h$. □

LEMMA 10.3.20. *The system $\mathcal{F}(5, 3, \mathbb{1})$ in any characteristic $p > 5$ has geometric monodromy group $G = G_{\mathrm{geom}} = \mathrm{Sp}_4$.*

PROOF. Consider the corresponding hypergeometric sheaf $\mathcal{H} = \mathcal{H}_{small,5,3}$, with geometric monodromy group $H$. By [**Ka-ESDE**, 8.8.1-2], $\mathcal{H}$ is symplectically self-dual, so $G \lhd H \leq \mathrm{Sp}_4$ and $\mathbf{Z}(H) \leq C_2$. By Lemma 10.1.8, $H$ is primitive, hence, for any $N \lhd H$, the underlying module $V_{\mathcal{H}}$ is homogeneous over $N$, i.e. a direct sum of some copies of a simple $N$-module. Since $w = 2$ and $p \geq 7$, $H$ is infinite by Theorem 2.4.4, and thus $G^\circ = H^\circ \neq 1$.

By Grothendieck's result "the radical is unipotent" [**De2**, 1.3.8, 1.3.9], one knows that $H^0$ is a semisimple algebraic group. Thus $H^\circ$ is a (connected) semisimple subgroup of $\mathrm{Sp}_4$, so it has rank 1 or 2. Suppose it has rank 2. If $H^\circ$ is of type $C_2$, then we are done. Otherwise it has type $2A_1$, and so $H^\circ$ is a quotient of $\mathrm{SL}_2 \times \mathrm{SL}_2$. But $H^\circ$ acts faithfully and homogeneously on $V_{\mathcal{H}}$ of dimension 4, so $H^\circ = \mathrm{SL}(V_1) \otimes \mathrm{SL}(V_2) \cong \mathrm{SL}_2 * \mathrm{SL}_2$ and $V_{\mathcal{H}} \cong V_1 \otimes V_2$ as an (irreducible) $H^\circ$-module. It follows that $V$ is orthogonally self-dual as an $H^\circ$-module, a contradiction.

Finally, consider the case $H^\circ$ is of type $A_1$, i.e. $H^\circ$ is a quotient of $\mathrm{SL}(U) \cong \mathrm{SL}_2$. As above, the $H^\circ$-module is the sum of $t$ copies of a simple $H^\circ$-module $M$. The faithful action of $H^\circ$ shows that $\dim(M) > 1$, and so $\dim(M) = 4$ or $\dim(M) = 2$. If $\dim(M) = 4$, then $H^\circ$ is irreducible on $V_{\mathcal{H}} \cong \mathrm{Sym}^3(U)$, contrary to Theorem 6.1.5.

Hence $\dim(M) = 2$, $H^\circ = \mathrm{SL}(U)$ and it has no outer automorphism, whence $H = C * H^\circ$ with $C := \mathbf{C}_H(H^\circ)$. Here, $C^\circ \leq C \cap H^\circ = \mathbf{Z}(H^\circ) = C_2$, so $C$ is a finite group. As $H = C * H^\circ$ is irreducible on $V_{\mathcal{H}}$ and $M \cong U$, $V_{\mathcal{H}}$ decomposes as $R \otimes U$, where $R$ is an irreducible $C$-module of dimension 2. Since $H$ is primitive, $R$ is primitive, whence it is (**S**+). Now we can apply Lemma 1.1.3 to see that the image of $C$ in $\mathrm{PGL}(R) \cong \mathrm{PSL}_2$ is either $\mathsf{A}_5 \cong \mathrm{PSL}_2(5)$ or $\mathrm{Aut}(E) \leq \mathsf{S}_4$ for $E \in \{D_8, Q_8, D_8 * C_4\}$. We will therefore achieve a contradiction by showing that the image of $C$ in $\mathrm{PGL}(R)$ contains an element of order $p > 5$. To do this, we consider some element $g$ of order $p$ in the image $Q$ of $P(\infty)$ in $H$. Then we may assume that $g$ has an eigenvalue $\zeta = \zeta_p$ on $\mathsf{Wild}$. But $g \in \mathrm{Sp}_4$ and $w = 2$, so $g$ has spectrum

$$\{\zeta, \bar{\zeta}, 1^{[2]}\} \qquad (10.3.20.1)$$

on $R \otimes U$. Now write $g = X \otimes Y$, where $X = \mathrm{diag}(x, x^{-1}) \in \mathrm{SL}(U)$, and $Y = \mathrm{diag}(y, z)$ in the image of $C$ on $R$. As 1 is an eigenvalue of $g$, we may assume $y = x$ and thus $g$ has spectrum $\{1, x^2, xz, x^{-1}z\}$. If $x^2 = 1$, then $g$ has spectrum $\{1^{[2]}, z^{[2]}\}$, contrary to (10.3.20.1). If $x^{-1}z = 1$, then $g$ has spectrum $\{1^{[2]}, (x^2)^{[2]}\}$, again contradicting (10.3.20.1). We conclude that $xz = 1$, so $\{x^2, x^{-2}\} = \{\zeta, \bar{\zeta}\}$ and so $\mathsf{o}(x^2) = p$. Thus $y/z = x^2$ has order $p$, and so $Y$ has central order $p$. As $Y$ lies in the image of $C$ on $R$, this shows that the image of $C$ in $\mathrm{PGL}(R)$ contains an element order $p$, as desired. □

Now we can prove the $B > 1$ counterpart of Theorem 10.2.4.

THEOREM 10.3.21. *Let $p$ be a prime and let $A > B \geq 2$ be integers coprime to $p$ with $\gcd(A, B) = 1$. Consider the local system $\mathcal{F}(A, B, \theta)$ in characteristic $p$, of rank $D = A - 1$ if $\theta = \mathbb{1}$ and $D = A$ otherwise, with geometric monodromy group $G_{\mathrm{geom}}$. Assume that $G_{\mathrm{geom}}$ is infinite. Then we have the following results.*

(i) *If $AB$ is even, then for every $\theta$, $\mathcal{F}(A, B, \theta)$ has $G^{\circ}_{\mathrm{geom}} = \mathrm{SL}_D$. Moreover, if $B \neq A - 1$, then $G_{\mathrm{geom}} = \mathrm{SL}_D$. If $B = A - 1$, then $G_{\mathrm{geom}} = \{x \in \mathrm{GL}_D \mid \det(x)^p = 1\}$.*
(ii) *If $AB$ is odd and $\theta \neq \mathbb{1}, \chi_2$, then $G_{\mathrm{geom}} = \mathrm{SL}_D$.*
(iii) *If $AB$ is odd and $\chi = \mathbb{1}$, then $G_{\mathrm{geom}} = \mathrm{Sp}_D$.*
(iv) *If $AB$ is odd and $\chi = \chi_2$, then $G_{\mathrm{geom}} = \mathrm{SO}_D$.*

PROOF. (a) Consider $\mathcal{H} = \mathcal{H}_{small,A,B}$ if $\theta = \mathbb{1}$ and consider $\mathcal{H} = \mathcal{H}_{big,A,B,\chi}$ with $\chi^A = \theta$ if $\theta \neq \mathbb{1}$. Let $H$ denote the geometric monodromy group of $\mathcal{H}$. By Theorem 10.1.1, $G := G_{\mathrm{geom}}$ is finite if and only if $H$ is finite; indeed, $G$ has index dividing $A$ in $H$. By our assumption, both $G$ and $H$ are infinite.

First we consider the $B = A - 1$ case; in particular, $p > 2$. If $A = 3$, then we even have $p \geq 5$. If, in addition $p \geq 7$ or $\theta \neq \mathbb{1}$, then we arrive at (i) by Corollary 4.1.3 and Remark 2.4.11. On the other hand, when $p = 5$ the sheaf $\mathcal{F}(3, 2, \mathbb{1})$ has finite monodromy by Theorem 10.3.13(x). So we may assume that either $A \geq 5$, or $A = 4$ but $p \geq 5$ (as $p \nmid AB$). Note that when $p = 3$ the sheaf $\mathcal{F}(5, 4, \mathbb{1})$ has finite monodromy by Theorem 10.3.13(viii), so when $A = 5$ we may also assume $p \geq 5$. Applying Corollary 4.1.3 and Remark 2.4.11, we again arrive at (i).

(b) Henceforth we will assume that $2 \leq B \leq A - 2$. Since $\gcd(A, B) = 1$, this rules out the case $A = 4$. Next, $H$ is primitive by Lemma 10.1.8. Furthermore, if $D \neq 4$, then $H$ is tensor indecomposable by [**KT5**, Lemma 2.4]. If $D = 4$, then since $A \geq 5$, we have $A = 5$ and $\theta = \mathbb{1}$. In this case, either $B = 2$ and so $H$ is (**S**+) by Corollary 10.1.9, or $(B, p) = (3, 2)$, in which case $H$ is finite by Theorem 10.3.13(iii), or $B = 3$ and $p > 5$, in which case $G = \mathrm{Sp}_4$ by Lemma 10.3.20. Thus we may assume henceforth that $H$ is tensor indecomposable, and hence that $H$ satisfies (**S**−).

Recall that $H$ is infinite and $H/G$ is a finite cyclic group. Applying Lemma 1.1.9, we have that $G^{\circ} = H^{\circ}$ is a central product $L_1 * \ldots * L_t$ of $t \geq 1$ simple algebraic groups that are transitively permuted by $H$, and $G^{\circ}$ is irreducible on the underlying representation $V_{\mathcal{H}}$. By Corollary 10.1.9, if $D \neq 4, 8, 9$ then $\mathcal{H}$ satisfies (**S**+), and so $t = 1$ by Lemma 1.1.3. By Proposition 2.4.3(i), a generator $g_0$ of the image of $I(0)$ is an $\mathsf{ssp}$-element on the underlying representation $V$ of $\mathcal{H}$; more precisely, its spectrum is $\mu_A \smallsetminus \{1\}$ if $\theta = \mathbb{1}$ and $\mu_A$ otherwise, and so $\bar{\mathsf{o}}(g_0) = A$.

(c) Here we consider the case $t = 1$, i.e. $G^\circ = H^\circ$ is a simple algebraic group. Then we can apply Theorem 6.2.14 and arrive at one of the following possibilities for the irreducible action of $H^\circ$ on the underlying representation $V_{\mathcal{H}}$.

(c1) $H^\circ$ is a classical group $\mathrm{SL}_D$, $\mathrm{Sp}_D$, or $\mathrm{SO}_D$, acting on $V_{\mathcal{H}}$ via the natural representation or its dual, or $G_2$ with $D = 7$. Here, if $2|AB$, or if $2 \nmid AB$ but $\theta \neq \mathbb{1}, \chi_2$, then $\mathcal{F}(A,B,\theta)$ is not self-dual by Theorem 10.1.6. In this case, Lemma 10.1.3 implies that the $H^\circ$-module $V_{\mathcal{H}}$ is not self-dual, so $G^\circ = H^\circ = \mathrm{SL}_D$. If moreover $B \neq A-1$, then the wild part has dimension $w = A - B \geq 2$, and Corollary 2.4.10 implies that $G = \mathrm{SL}_D$, leading to (i), respectively (ii). If $B = A - 1$, then we arrive at (i) using Remark 2.4.11.

Assume now that $2 \nmid AB$ and $\mathsf{o}(\theta) \leq 2$. If $\theta = \mathbb{1}$, then $\mathcal{F}(A,B,\theta)$ is symplectically self-dual by Theorem 10.1.6, whence Lemma 10.1.3 implies that the $H^\circ$-module $V_{\mathcal{H}}$ is symplectic, so $G = H^\circ = \mathrm{Sp}_D$, leading to (iii). Suppose $p > 2$ and $\theta = \chi_2$. Then $\mathcal{F}(A,B,\theta)$ is orthogonally self-dual by Theorem 10.1.6, whence Lemma 10.1.3 implies that the $H^\circ$-module $V_{\mathcal{H}}$ is orthogonal; also $G \leq \mathrm{O}_D$. In this case, we must have that $G^\circ = \mathrm{SO}_D$, or $D = 7$ and $G^\circ = G_2$. We will see below that this last case does not occur. We also note that $g_0$ has determinant 1 (as $2 \nmid A$), and $w = A - B \geq 2$. Hence $H \leq \mathrm{SL}_D$ by Theorem 1.2.2, and $\mathbf{Z}(G) \leq \mathbf{Z}(H) \cap \mathrm{O}_D = 1$ (as $D = A$ is odd). If $G^\circ = \mathrm{SO}_D$, then we have $G = \mathrm{SO}_D$, as stated in (iv). Suppose $D = 7$ and $G^\circ = G_2$, whence $H^\circ = G_2$. As $\mathcal{H}$ is of type $(7,B)$ with $B$ odd and $G_2$ has no outer automorphism, we apply Lemma 6.2.2 to infer that some tame twist $\mathcal{L}_\chi \otimes \mathcal{H}$ has $G_{\mathrm{geom},\mathcal{L}_\chi\otimes\mathcal{H}} = G_2$. But this twist, $\mathcal{L}_\chi \otimes \mathcal{H}$, is still of type $(7,B)$. As $B > 1$, this contradicts [**Ka-G2**, Theorem 3.1], according to which the only hypergeometric sheaves in any odd characteristic with $G_{\mathrm{geom}} = G_2$ are of type $(7,1)$.

(c2) One of (a)–(d) listed in Lemma 10.2.3, and so they are all ruled out.

(c3) One of the cases (viii)–(x) of Theorem 6.2.14. These cases are ruled out by Lemmas 10.3.15, 10.3.16, 10.3.17, and 10.3.18, respectively.

(d) The rest of the proof is to deal with the case $t > 1$. By Lemma 1.1.3, in this case $H$ is tensor induced. By Corollary 10.1.9, $D \in \{4,8,9\}$. In fact, as mentioned above, $D = 4$ would imply $(A,B) = (5,2)$ and $\theta = \mathbb{1}$, and so $H$ is (**S**+) and $t = 1$. So we have one of the following possibilities.

(d1) $D = A = 8$ and so $\theta \neq \mathbb{1}$. Here, if $B = 3$ then $H$ is again (**S**+) by Corollary 10.1.9. As $2 \leq B \leq A-2$ and $\gcd(A,B) = 1$, we are left with $B = 5$. Since $H$ is tensor induced and $t > 1$, we must have that $t = 3$ and $H^\circ = \mathrm{SL}_2 * \mathrm{SL}_2 * \mathrm{SL}_2$, whence the $H^\circ$-module $V_{\mathcal{H}}$ is self-dual. But this contradicts Lemma 10.1.3, since $\mathcal{F}$ is not self-dual by Theorem 10.1.6.

(d2) $D = 8$ and $(A,\theta) = (9,\mathbb{1})$. Here, if $B = 2$ or 4, then $H$ is again (**S**+) by Corollary 10.1.9. As $2 \leq B \leq A-2$ and $\gcd(A,B) = 1$, we are left with $B = 5$ and $B = 7$. In both cases, $\mathcal{H}$ is symplectically self-dual by [**Ka-ESDE**, 8.8.1-2], so $|\mathbf{Z}(H)| \leq 2$. Since $t > 1$ and $\mathcal{H}$ is tensor induced, we must have that $t = 3$ and $H^\circ = \mathrm{SL}_2 * \mathrm{SL}_2 * \mathrm{SL}_2$, so in fact $\mathbf{Z}(H) = \mathbf{C}_H(H^\circ) = C_2$, and

$$H/H^\circ \hookrightarrow \mathsf{S}_3. \tag{10.3.21.1}$$

Suppose $(A,B) = (9,5)$. Note that when $p = 2$, the sheaf $\mathcal{F}(9,5,\mathbb{1})$ has finite monodromy by Theorem 10.3.13(iii), so we have $p > 2$. Now we consider a $p'$-element $g_\infty \in H$ that generates the image of $I(\infty)$ in $H$ modulo the image of $P(\infty)$. Since $w = 4$, by [**KRLT4**, Proposition 4.8], $g_\infty$ permutes the 4 simple $P(\infty)$-summands on $\mathsf{Wild}$ transitively, and has spectrum $\mu_5 \smallsetminus \{1\}$ on $\mathsf{Tame}$. It follows from (10.3.21.1) that $g_\infty^{12}$ belongs to $H^\circ$ and has spectrum $\{\epsilon^{[4]}\} \sqcup \big(\mu_5 \smallsetminus \{1\}\big)$ for some $\epsilon \in \mathbb{C}^\times$. As $g_\infty^{12} \in \mathrm{Sp}_8$ is real, $\epsilon = \epsilon^{-1}$. Hence $g_\infty^{24} \in H^\circ$ has spectrum $\{1^{[4]}\} \sqcup \big(\mu_5 \smallsetminus \{1\}\big)$. Applying Lemma 10.3.19 to $g_\infty^{24}$, we get a contradiction.

Suppose $(A, B) = (9, 7)$. First assume that $p > 2$, in which case we have $p > 3$, which implies by (10.3.21.1) that the image $Q$ of $P(\infty)$ lies in $H^\circ = \mathrm{SL}_2 * \mathrm{SL}_2 * \mathrm{SL}_2$. Now any $p$-element $1 \neq h \in Q$ has 1 as an eigenvalue with multiplicity $\geq 6$. Applying Lemma 10.3.19 to $h$, we again get a contradiction. Assume now that $p = 2$. As $Q$ is irreducible on $\mathsf{Wild}$ of dimension 2, $Q$ is non-abelian, and so it contains an element $g$ of order 4. Again (10.3.21.1) implies that $g^2 \in H^\circ$. Now applying Lemma 10.3.19 to $g^2$, we see that the (semisimple) element $g^2$ is trivial, a contradiction.

(d3) $D = A = 9$ and so $\theta \neq \mathbb{1}$. Here, if $B = 2$, then $H$ is again ($\mathbf{S}+$) by Corollary 10.1.9. As $2 \leq B \leq A - 2$ and $\gcd(A, B) = 1$, we are left with $B \in \{4, 5, 7\}$. Since $H$ is tensor induced, we must have that $\mathcal{H}$ is 2-tensor induced. Now, if $B = 4$, then $p > 2$ and $w = 5$, so $\mathcal{H}$ is not 2-tensor induced by Proposition 5.1.9. Similarly, if $B = 5$ or 7 and $p > 2$, then $\mathcal{H}$ is not 2-tensor induced by Proposition 5.1.10. If $B = 5$ or 7 and $p = 2$, then $\mathcal{H}$ is not 2-tensor induced by Lemma 5.1.4. In all cases, we arrive at a contradiction.

(d4) $D = 9$ and $(A, \theta) = (10, \mathbb{1})$. Here, if $B = 3$, then $H$ is again ($\mathbf{S}+$) by Corollary 10.1.9. As $2 \leq B \leq A - 2$ and $\gcd(A, B) = 1$, we are left with $B = 7$, in which case $p > 2$, $w = 3$, so $\mathcal{H}$ is not 2-tensor induced by Proposition 5.1.9. As $D = 9$, this implies that $\mathcal{H}$ is ($\mathbf{S}+$) and $t = 1$, a contradiction. □

In the general case of local systems $\mathcal{F}_{nngcd}(A, B, \theta)$ in characteristic $p$ where $A, B$ are not necessarily coprime, Theorem 10.3.14 already determines all the possibilities of $(p, A, B, \theta)$ that give rise to finite geometric monodromy groups.

We also note the following immediate consequence of Theorems 10.2.6 and 10.3.13 (compare to Theorem 2.4.4).

Corollary 10.3.22. *Let $p$ be a prime and let $A > B \geq 1$ be integers with $\gcd(A, B) = 1$ and $p \nmid AB$. Consider the local system $\mathcal{F}(A, B, \theta)$ in characteristic $p$, of rank $D = A - 1$ if $\theta = \mathbb{1}$ and $D = A$ otherwise, see Definition 7.3.1, with geometric monodromy group $G = G_{\mathrm{geom}}$. Suppose $D \geq 2$ and $G$ is finite. Then $p \leq 2A - 1$, and one of the following statements holds.*

(i) *$p|(A - 1)(2A - 1)$ and $p|(B - 1)(2B - 1)$.*
(ii) *$\theta = \chi_2$, $A = 2p^f - 1$, and $B = 1$. In particular, $p|(A + 1)/2$ and $p|(B - 1)$.*
(iii) *$(p, A, B, \theta) = (7, 5, 2, \mathbb{1})$, $(5, 7, 1, \mathbb{1})$, $(5, 3, 2, \mathbb{1})$, or $(5, 7, 3, \chi_2)$. In particular, $p|(2A - 1)(3A - 1)$.*

CHAPTER 11

# Multi-parameter families of exponential sums

## 11.1. Preliminaries

The results in this chapter determine the geometric monodromy groups for some "van der Geer-van der Vlugt" local systems on $\mathbb{A}^k$, which generalize various results of [**KT1, KT3, KT6**]. First we need some preliminary statements.

LEMMA 11.1.1. *Let $p$ be a prime, $k \geq 2$, and let $A > B_1 > \ldots > B_k \geq 1$ be integers with $p \nmid AB_1 \ldots B_k$. Consider the arithmetically semisimple local system $\mathcal{F}(A, B_1, \ldots, B_k, \theta)$ over $\mathbb{A}^k$ with trace function*

$$(t_1, \ldots, t_k) \mapsto -\sum_x \psi\big(x^A + t_1 x^{B_1} + \ldots + t_k x^{B_k}\big)\theta(x),$$

*in characteristic $p$, of rank $D = A - 1$ if $\theta = \mathbb{1}$ and $D = A$ otherwise, cf.* (0.0.0.2). *Then $\mathcal{F}(A, B_1, \ldots, B_k, \theta)$ is geometrically irreducible if and only if* $\gcd(A, B_1, \ldots, B_k) = 1$.

PROOF. This is a consequence of [**KT6**, Corollary 2.7]. □

We will need the following number-theoretic fact, which is a special case of a result due to Erdös and György, cf. [**Erd**], [**Gy**]:

LEMMA 11.1.2. *For integers $n > m \geq 1$, $\binom{n}{m}$ can be a prime power $p^a$ exactly when $n = p^a$ and $m = 1, n-1$.*

PROOF. Suppose that $\binom{n}{m} = p^a$ for some prime $p$ and $2 \leq m \leq n-2$. Without any loss we may assume $2 \leq m \leq n/2$. By Sylvester's theorem [**Syl2**], at least one of the $m$ integers $n, n-1, \ldots, n-m+1$ is divisible by a prime $\ell > m$, say $\ell | (n-i)$ for some $0 \leq i \leq m-1$. In this case, $\ell$ divides $\binom{n}{m}$, so $p = \ell$. If $\ell$ also divides $n-j$ for another $0 \leq j \leq m-1$, then $\ell$ divides $i-j$, but $|i-j| < m < \ell$, a contradiction. As $\ell^a(m!) = \prod_{j=0}^{m-1}(n-j)$, it follows that $n-i$ is divisible by $\ell^a$. But this is impossible, since $0 < n-i \leq n$ and $\ell^a = \binom{n}{m} \geq \binom{n}{2} > n$. □

PROPOSITION 11.1.3. *Let $q = p^f$ be a power of an odd prime $p$, $n \in \mathbb{Z}_{\geq 1}$, $D = (q^n \pm 1)/2$, and let $q^n \geq 5$. Let $G < \mathrm{GL}_D$ be a Zariski closed subgroup such that $G/\mathbf{Z}(G)$ is infinite and $G$ contains a subgroup $G_1$ which is the image of $\mathrm{Sp}_{2n}(q)$ in an irreducible Weil representation of degree $D$. Then $[G, G]^\circ$ is a simple algebraic group acting irreducibly on $\mathbb{C}^D$. Assume in addition that $D$ is an odd prime power. Then one of the following statements holds.*

(i) *$[G, G] = \mathrm{SL}_D$.*

(ii) *$q \equiv 1 \pmod 4$, $D = (q^n + 1)/2$, and $[G, G]^\circ = \mathrm{SO}_D$.*

(iii) *$q^n = 13$, $D = 7$, and $[G, G]^\circ = G_2$.*

PROOF. (i) By assumption, $G \geq G_1$ acts irreducibly on $V := \mathbb{C}^D$. It is well known that the Weil representation of $G_1 = E(G_1)$ on $V$ admits an $\mathsf{ssp}$-element $g_1$. Next, the smallest index $P(G_1)$ of proper subgroups of $G_1$ is $\geq (q^n+3)/2 > D$, see [**KlL**, Table 5.2.A]. It follows that $G_1$, and hence $G$, cannot fix any imprimitive decomposition $V = \oplus_{i=1}^m V_i$ with $m > 1$. Next suppose that $G$ fixes a tensor decomposition $V = V_1 \otimes V_2$ with $\dim V_i > 1$. Certainly $\mathbf{Z}(G_1)$ acts via scalars on both $V_1$ and $V_2$. Hence $G_1/\mathbf{Z}(G_1) \cong \mathrm{PSp}_{2n}(q)$ admits a nontrivial projective representation on some $V_i$, of dimension $\leq D/2 \leq (q^n+1)/4$. On the other hand, according to [**KlL**, Table 5.3.A], the degree of any such representation is at least $(q^n-1)/2$ if $q^n \neq 9$ and 3 if $(q,n) = (9,1)$, a contradiction. Finally, if $G$ fixes a tensor induced decomposition $V = V_1 \otimes \ldots \otimes V_m \cong V_1^{\otimes m}$ with $m \geq 2$, then

$$m \leq \log_2(q^n+1)/2 < P(G_1).$$

In such a case, $G_1$ must fix every tensor factor $V_i$, and hence $V|_{G_1}$ is tensor decomposable, contrary to the preceding result.

We have shown that $(V,G)$ satisfies condition (**S**). [When $D \neq 4,6$, this statement also follows from Theorem 3.1.6.] Applying [**GT3**, Proposition 2.8], for the subgroup $H = \mathrm{SL}(V) \cap ZG$, where $Z := \mathbf{Z}(\mathrm{GL}(V))$, we have that $ZG = ZH$ and either $H^\circ$ is a simple algebraic group or $H$ is finite. In the latter case, $G \leq ZH$ and $Z \cap G = \mathbf{Z}(G)$, and so $G/\mathbf{Z}(G)$ is finite, contrary to the hypothesis. So $H^\circ$ is a simple algebraic group. Next, $H \lhd ZH = ZG$ and $ZG$ satisfies (**S**), so by [**GT3**, Lemma 2.5], either $H^\circ$ is irreducible on $V$ or $H^\circ \leq Z$. As $H/H^\circ$ is finite, we again see that

$$G/\mathbf{Z}(G) \cong ZG/Z = ZH/Z = ZH/ZH^\circ$$

is finite, a contradiction. Thus $H^\circ$ acts irreducibly on $V$ and $H^\circ = [H^\circ, H^\circ]$. Now

$$H^\circ \leq [H,H] = [ZH,ZH] = [ZG,ZG] = [G,G],$$

and hence $H^\circ \leq [G,G]^\circ$. But we also have that $[G,G]^\circ = [H,H]^\circ \leq H^\circ$. Therefore, $[G,G]^\circ = H^\circ$ is a simple algebraic group acting irreducibly on $V$.

By Schur's lemma, $\mathbf{C}_G([G,G]^\circ) = \mathbf{Z}(G)$ is cyclic. Furthermore, $\mathrm{Out}([G,G]^\circ)$ is a subgroup of $\mathsf{S}_3$, hence solvable. It follows that $G/[G,G]^\circ$ is solvable. But $G_1$ is perfect, so $G_1 \leq [G,G]^\circ$. In particular, $[G,G]^\circ$ contains the $\mathsf{ssp}$-element $g_1$. Hence we can apply Theorem 3.3.4(A) to the action of $[G,G]^\circ$ on $V$.

(ii) Under the further assumption that $D = p^a$ is a power of an odd prime $r$, we now arrive at one of the following cases of Theorem 3.3.4(A).

(a) $[G,G]^\circ$ is of type $A_r$ with $r \geq 1$, and $V|_{[G,G]^\circ} = L(a\varpi_1)$ with $a \geq 1$ or $L(a\varpi_r)$, or $L(\varpi_i)$ with $2 \leq i \leq r-1$. Now, if $V|_{[G,G]^\circ} = L(\varpi_1)$ or $L(\varpi_r)$, then $r+1 = D$ and $[G,G]^\circ = \mathrm{SL}_D$. Since $G \leq \mathrm{GL}_D$, in such a case we have $[G,G] = \mathrm{SL}_D$. In all other cases, $D = \dim V$ is a binomial coefficient $\binom{N}{m}$ for some $2 \leq m \leq N-2$, and so $D \neq p^a$ by Lemma 11.1.2.

(b) $[G,G]^\circ$ is of type $B_r$ with $r \geq 1$, and $V|_{[G,G]^\circ} = L(\varpi_1)$, the natural representation of degree $2r+1$. In this case, $[G,G]^\circ \cong \mathrm{SO}_D$; moreover, $V|_{[G,G]^\circ}$ is self-dual of type $+$, and the same holds for $V|_{G_1}$. This implies that $q \equiv 1 \pmod 4$, and as $2 \nmid D$, we must have that $D = (q^n+1)/2$.

(c) $([G,G]^\circ, \dim(V)) = (G_2, 7)$, or $(E_6, 27)$. In the former case, since $(q^n \pm 1)/2 = D = 7$ we must have that $q^n = 13$. In the latter case, since $(q^n \pm 1)/2 = D = 27$ we must have that $q^n = 53$. It follows that $\mathrm{PSL}_2(53)$ projectively embeds in $E_6$, which is impossible by the main result of [**GrR**].

□

LEMMA 11.1.4. *The following statements hold.*

(i) *The local system* $\mathcal{F}(5,4,2,1,\mathbb{1})$ *of* (0.0.0.2) *in characteristic* $p=3$ *has geometric monodromy group* $\tilde{G}_{\rm geom} = \mathrm{Sp}_4(3)\times 3$*, with* $\mathrm{Sp}_4(3)$ *acting in a Weil representation of degree* 4.

(ii) *The local system* $\mathcal{F}(5,2,1,\mathbb{1})$ *of* (0.0.0.2) *in characteristic* $p=3$ *has geometric monodromy group* $G_{\rm geom,1} = \mathrm{Sp}_4(3)$ *in a Weil representation of degree* 4*.*

(iii) *The local system* $\mathcal{F}(5,2,1,\chi_2)$ *of* (0.0.0.2) *in characteristic* $p=3$ *has geometric monodromy group* $G_{\rm geom,2} = \mathrm{PSp}_4(3)$ *in a Weil representation of degree* 5*.*

(iv) *The local system* $\mathcal{F}(10,4,2,\mathbb{1})$ *of* (0.0.0.2) *in characteristic* $p=3$ *has geometric monodromy group* $G_{\rm geom} = \mathrm{Sp}_4(3)$ *in a total Weil representation.*

PROOF. (i) is [**KRLT4**, Theorem 32.6].

(ii) Since the system $\mathcal{F}(5,2,1,\mathbb{1})$ on $\mathbb{A}^2$, with trace function

$$(t_1,t_2)\mapsto -\sum_x \psi\big(x^5+t_1x^2+t_2x\big),$$

is obtained from the system $\mathcal{F}(5,4,2,1,\mathbb{1})$ on $\mathbb{A}^3$, with trace function

$$(t_0,t_1,t_2)\mapsto -\sum_x \psi\big(x^5+t_0x^4+t_1x^2+t_2x\big),$$

by the specialization $t_0=0$, we have $G_{\rm geom,1}\le \mathrm{Sp}_4(3)\times 3$. Applying [**KT3**, Theorem 10.7] to the specialization $t_2=0$ of $\mathcal{F}(5,2,1,\mathbb{1})$, we get $G_{\rm geom,1}\ge \mathrm{Sp}_4(3)$. Moreover, $G_{\rm geom,1}$ has trivial determinant by Corollary 2.3.4, which shows that $\mathbf{Z}(G_{\rm geom,1})\not\geq C_3$, and so $G_{\rm geom,1}\ne \mathrm{Sp}_4(3)\times 3$. Hence $G_{\rm geom,1}=\mathrm{Sp}_4(3)$.

(iii) Note by [**KT6**, Corollary 2.7] that the system $\mathcal{F}(10,4,2,\mathbb{1})$ is the direct sum of the two systems $\mathcal{F}(5,2,1,\mathbb{1})$ and $\mathcal{F}(5,2,1,\chi_2)$, the latter with trace function

$$(t_1,t_2)\mapsto -\sum_x \psi\big(x^5+t_1x^2+t_2x\big)\chi_2(x),$$

and has finite geometric monodromy group by [**KT6**, Theorem 2.9]. It follows from Lemmas 2.2.5 and 11.1.1 that $G := G_{\rm geom,2}$ is a finite irreducible subgroup of $\mathrm{GL}_5$. Applying [**KT3**, Theorem 10.7] to the specialization $t_2=0$ of $\mathcal{F}(5,2,1,\chi_2)$, we get that $G$ contains $\mathrm{PSp}_4(3)$ in a Weil representation of degree 5; in particular, $G$ satisfies (**S**+) (as its subgroup $\mathrm{PSp}_4(3)$ does). Next, the field of traces of elements in $G$ is contained in $\mathbb{Q}(\zeta_3)$ by [**KT6**, Theorem 2.8(ii)], whence $\mathbf{Z}(G)\le C_6$ by Schur's lemma. Furthermore, by Corollary 2.3.4, both $\mathcal{F}(10,4,2,\mathbb{1})$ and $\mathcal{F}(5,2,1,\mathbb{1})$ have geometrically trivial determinant. It follows that $\mathcal{F}(5,2,1,\chi_2)$ also has geometrically trivial determinant. Since it has rank 5, this implies that

$$\mathbf{Z}(G)=1. \tag{11.1.4.1}$$

Applying Lemma 1.1.3 to $G$ and using (11.1.4.1), we now see that the extraspecial normalizer case is ruled out, and $G$ is almost simple: $S\lhd G\le \mathrm{Aut}(S)$ for some finite simple group $S$, which itself is an irreducible subgroup of $\mathrm{GL}_5$ and still contains $\mathrm{PSp}_4(3)$. Using the classification result of [**HM**], we can check that $S=\mathrm{PSp}_4(3)$. But $\mathrm{Aut}(S)=S\cdot 2$ does not have irreducible representations of degree 5. So we conclude that $G=S$, acting in a Weil representation of degree 5.

(iv) As mentioned above, $\mathcal{F}(10,4,2,\mathbb{1}) \cong \mathcal{F}(5,2,1,\mathbb{1}) \oplus \mathcal{F}(5,2,1,\chi_2)$. Using the results of (ii) and (iii) and arguing by Goursat's lemma, we can finish as in the proof of Lemma 7.3.2. □

Next we prove a low-dimensional analogue of Theorem 7.2.2:

PROPOSITION 11.1.5. *Let $p$ be an odd prime, $n \in \mathbb{Z}_{\geq 1}$, and let $p^n \leq 9$. Let $G < \mathrm{GL}(V) \cong \mathrm{GL}_{p^n}(\mathbb{C})$ be a finite irreducible subgroup that contains a subgroup $G_1 \cong \mathrm{Sp}_{2n}(p)$ that acts via a total Weil representation, with the convention in Lemma 7.3.3 for $p = 3$. If $p^n = 3$, assume in addition that the field of traces of elements in $G$ is contained in $\mathbb{Q}(\zeta_3)$. Then there exist an irreducible Heisenberg subgroup $E \cong p_+^{1+2n} < \mathrm{GL}(V)$ normalized by $G_1$ such that*

$$G = \mathbf{Z}(G)(E \rtimes G_1).$$

PROOF. (i) By assumption, $G \geq G_1$ acts irreducibly on $V = \mathbb{C}^{p^n}$. Next, the smallest index $P(G_1)$ of proper subgroups of $G_1$ is 27 if $p^n = 9$, and $p$ otherwise, see [**CCNPW**]. Suppose that $G$ fixes an imprimitive decomposition $V = \oplus_{i=1}^m V_i$ with $m > 1$. If $m < P(G_1)$, then $G_1$ has to fix each of the $V_i$'s. As $\dim(V_i)$ is a proper divisor of $\dim(V) = p^n$, we have $\dim(V_i) \leq p^{n-1} \leq (p^n-1)/2$. On the other hand, $G_1$ acts on $V$ with two simple submodules of dimensions $(p^n-1)/2$ and $(p^n+1)/2$, a contradiction. Thus $m \geq P(G_1)$, and so $p^n \leq 7$, $n = 1$, $m = p$, and $\dim(V_i) = 1$. We have also shown that $G_1 = \mathrm{Sp}_2(p)$ permutes the $p$ subspaces $V_i$ transitively. Let $G_{11}$ denote the stabilizer of $V_1$ in $G_1$. According to [**GAP**], $G_{11}$ is a subgroup of type $2 \cdot \mathsf{S}_4$ if $p = 7$, $\mathrm{SL}_2(3)$ if $p = 5$, and $Q_8 = 2_-^{1+2}$ if $p = 3$. In fact, since $G_1$ has only one involution, namely the central involution $\boldsymbol{j}$, we must have that $\boldsymbol{j} \in G_{11}$. Now the action of $G_{11}$ on the 1-dimensional space $V_1$ must be trivial on $\boldsymbol{j}$. As $G_1$ permutes the $V_i$'s transitively and $\boldsymbol{j} \in \mathbf{Z}(G_1)$, $\boldsymbol{j}$ acts trivially on every $V_i$ and so on $V$, contradicting the faithfulness.

We have shown that $G$ acts primitively on $V$. It follows that $G$ satisfies ($\mathbf{S}+$) if $p^n \neq 9$. Suppose that $p^n = 9$ and $G$ fixes a tensor decomposition $V = A \otimes_{\mathbb{C}} B$, that is, $G \leq \mathrm{GL}(A) \otimes \mathrm{GL}(B)$, with $1 < \dim(A), \dim(B)$. This induces projective representations of $G_1 = \mathrm{Sp}_4(3)$ on $A$ and $B$, which have dimensions at most $p^n/3 = 3$. By [**CCNPW**], this is possible only when these projective representations are trivial, that is, $G_1$ acts via scalars on $A$ and on $B$. This implies that $G_1$ acts via scalars on $V$, whence this action is trivial since $G_1$ is perfect, again contradiction. Assume now that $G$ fixes a tensor induced decomposition $V = U^{\otimes m}$ for some $m > 1$. Then $m = 2$, and so the action of $G_1$ on the 2 tensor factors is trivial, i.e. $G_1$ fixes a tensor decomposition $V = U_1 \otimes U_2$ with $\dim(U_i) = \dim(U)$. But this is impossible by the preceding case.

(ii) We have shown that the finite group $G$ satisfies condition ($\mathbf{S}+$) and so can apply Lemmas 1.1.3 and 1.1.6 to conclude that either

(a) $G$ is almost quasisimple with $G^{(\infty)}$ acting irreducibly on $V$, or
(b) $E \lhd G < \mathbf{N}_{\mathrm{GL}(V)}(E)$ for some extraspecial $p$-group $E$ of order $p^{1+2n}$ acting irreducibly on $V$.

Here we consider the second possibility (b). First we note that

$$G_1 \cap \mathbf{Z}(\mathrm{GL}(V))E = 1. \tag{11.1.5.1}$$

Indeed, $G_1 = \mathrm{Sp}_{2n}(p)$ normalizes the nilpotent subgroup $X := G_1 \cap \mathbf{Z}(\mathrm{GL}(V))E$. If $p^n > 3$, then $G_1$ is quasisimple, whence $X = 1$ or $X = \mathbf{Z}(G_1) = \langle \boldsymbol{j} \rangle$. The same holds when $p^n = 3$ as we have $G_1 = \mathrm{SL}_2(3) = Q_8 \rtimes 3$. Suppose $X \neq 1$. Now, if $\boldsymbol{j} \notin \mathbf{Z}(\mathrm{GL}(V))$, then it is a scalar multiple of a non-central element in $E$, whence it has trace 0 on $V$. On the other hand, the involution $\boldsymbol{j}$ has only eigenvalues 1 and $-1$ on $V = \mathbb{C}^{p^n}$ of odd dimension, and so its trace must be nonzero, a contradiction. So $\boldsymbol{j} \in \mathbf{Z}(\mathrm{GL}(V))$, whence it acts as scalar $-1$ and so has determinant $-1$ on $V$. This is again a contradiction, as $\boldsymbol{j} \in [G_1, G_1]$ and so it lies in $\mathrm{SL}(V)$.

Next, consider the conjugation action of $G_1$ on $E$. The kernel of this action is $G_1 \cap \mathbf{Z}(\mathrm{GL}(V)) = 1$ by (11.1.5.1), so the action embeds $G_1$ in the group $\mathrm{Aut}_1(E)$ of all automorphisms of $E$ that act trivially on $\mathbf{Z}(E)$, which is equal to $\mathbb{F}_p^{2n} \rtimes \mathrm{Sp}_{2n}(p)$ if $\exp(E) = p$ and $\mathbb{F}_p^{2n} \rtimes (p_+^{2n-1} \rtimes \mathrm{Sp}_{2n-2}(p))$ if $\exp(E) > p$, see [**Wi**, Theorem 1]. Note that $G_1 \cong \mathrm{Sp}_{2n}(p)$ cannot embed in the subgroup $\mathbb{F}_p^{2n} \rtimes (p_+^{2n-1} \rtimes \mathrm{Sp}_{2n-2}(p))$ of $\mathrm{Aut}_1(E)$. This implies that $\exp(E_1) = p$, i.e. $E \cong p_+^{1+2n}$, and $\Gamma(p,n) := \mathbf{N}_{\mathrm{GL}(V)}(E) = \mathbf{Z}(\mathrm{GL}(V))(E \rtimes \mathrm{Sp}_{2n}(p))$. By (11.1.5.1), $G_1 \cong \mathrm{Sp}_{2n}(p)$ embeds in $G/\mathbf{Z}(G)E \hookrightarrow \Gamma(p,n)/\mathbf{Z}(\mathrm{GL}(V))E \cong \mathrm{Sp}_{2n}(p)$, and so $G = \mathbf{Z}(G)EG_1 = \mathbf{Z}(G)(E \rtimes G_1)$ as stated.

(iii) Now we handle the possibility (a), and recall that $L := G^{(\infty)}$ acts irreducibly on $V$. As $G$ is almost quasisimple, $L$ is a cover of a simple group $S$, and the list of such groups is given in [**HM**].

First suppose that $p^n > 3$. Then $L \geq G_1 = \mathrm{Sp}_{2n}(p)$ as $G_1$ is perfect. If $p^n = 9$, no such group $L$ can contain $\mathrm{Sp}_4(3)$.

If $p^n = 7$, then $L$ contains $G_1 = \mathrm{Sp}_2(7)$ acting in a total Weil representation of degree 7, so the field of traces of its elements contains $\mathbb{Q}(\sqrt{-7})$. However, $L = \mathsf{A}_8$, $\mathrm{SU}_3(3)$, $\mathrm{Sp}_6(2)$, $\mathrm{PSL}_2(13)$, $\mathrm{SL}_2(8)$, or $\mathrm{PSL}_2(7)$ [**HM**]. The first four groups have fields of traces $\mathbb{Q}$, $\subseteq \mathbb{Q}(i)$, $\mathbb{Q}$, and $\mathbb{Q}(\sqrt{13})$, a contradiction. The last two groups cannot contain $\mathrm{SL}_2(7)$, again a contradiction.

If $p^n = 5$, then $L$ contains $G_1 = \mathrm{Sp}_2(5)$ acting in a total Weil representation of degree 5, so the field of traces of its elements contains $\mathbb{Q}(\sqrt{5})$. However, $L = \mathsf{A}_5$, $\mathsf{A}_6$, $\mathrm{PSp}_4(3)$, or $\mathrm{PSL}_2(11)$, with fields of traces $\mathbb{Q}$, $\mathbb{Q}$, $\mathbb{Q}$,$\mathbb{Q}(\sqrt{-3})$, and $\mathbb{Q}(\sqrt{-11})$, a contradiction.

Finally, assume that $p^n = 3$, in which case $L = \mathsf{A}_5$, $3 \cdot \mathsf{A}_6$, or $\mathrm{PSL}_2(7)$. Since the fields of traces are $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{-3}, \sqrt{5})$, and $\mathbb{Q}(\sqrt{-7})$, none of these cases is possible. □

PROPOSITION 11.1.6. (i) *For $p = 3$, $5$, and $7$, the local system $\mathcal{F}(p+1, 2, 1, \mathbb{1})$ of* (0.0.0.2) *in characteristic $p$ has geometric monodromy group $G_{\mathrm{geom}} = p_+^{1+2} \rtimes \mathrm{Sp}_2(p)$.*

(ii) *The local systems $\mathcal{F}(10, 4, 2, 1, \mathbb{1})$ and $\mathcal{F}(10, 4, 1, \mathbb{1})$ of* (0.0.0.2) *in characteristic $p = 3$ each have geometric monodromy group $G_{\mathrm{geom}} = 3_+^{1+4} \rtimes \mathrm{Sp}_4(3)$.*

(iii) *The local system $\mathcal{F}(10, 2, 1, \mathbb{1})$ of* (0.0.0.2) *in characteristic $p = 3$ has geometric monodromy group $G_{\mathrm{geom}} = 3_+^{1+4} \rtimes \mathrm{SL}_2(9)$.*

PROOF. (i) Let $G$ denote $G_{\mathrm{geom}}$ for the system $\mathcal{F}(p+1, 2, 1, \mathbb{1})$, which has trace function

$$(t_1, t_2) \mapsto -\sum_x \psi\big(x^{p+1} + t_1 x^2 + t_2 x\big).$$

Specializing $t_2 = 0$, we obtain the system $\mathcal{F}(p+1, 2, \mathbb{1})$ which has geometric monodromy group $G_1 = \mathrm{Sp}_2(p)$ acting in a total Weil representation, by Lemmas 7.3.2 and 7.3.3. Thus $G$ is an irreducible subgroup of $\mathrm{GL}_p(\mathbb{C})$ containing $G_1$. By Theorem 7.1.1, $G$ is finite, with field of traces contained in $\mathbb{Q}(\zeta_p)$. Now we can apply Proposition 11.1.5 to see that $G = \mathbf{Z}(G)(E \rtimes G_1)$, with $E = p_+^{1+2}$. To finish the proof, it suffices to show that $\mathbf{Z}(G) = \mathbf{Z}(E) \cong C_p$.

The constraint on the field of traces shows that if $\mathbf{Z}(G) \neq \mathbf{Z}(E)$ then $\mathbf{Z}(G) = C_2 \times \mathbf{Z}(E)$ and so $\mathbf{Z}(G)$ contains an element $z$ with determinant $(-1)^p = -1$. However, if $p > 3$, then $G$ has trivial determinant by Corollary 2.3.4. Even when $p = 3$, since the system lives over $\mathbb{A}^2$, we can still say that its geometric determinant, a system of rank 1 over $\mathbb{A}^2$, has order dividing $p$, cf. Lemma 2.3.9, ruling out the existence of such $z$.

(ii) Let $G$ denote $G_{\mathrm{geom}}$ for the system $\mathcal{F}(10, 4, 2, 1, \mathbb{1})$, which has trace function

$$(t_1, t_2, t_3) \mapsto -\sum_x \psi\big(x^{10} + t_1x^4 + t_2x^2 + t_3x\big).$$

Specializing $t_3 = 0$, we obtain the system $\mathcal{F}(10, 4, 2, \mathbb{1})$ which has geometric monodromy group $G_1 = \mathrm{Sp}_4(3)$ acting in a total Weil representation, by Lemma 11.1.4(iv). Thus $G$ is an irreducible subgroup of $\mathrm{GL}_9(\mathbb{C})$ containing $G_1$. As before, $G$ is finite, with field of traces contained in $\mathbb{Q}(\zeta_3)$. Applying Proposition 11.1.5 we obtain $G = \mathbf{Z}(G)(E \rtimes G_1)$, with $E = 3^{1+4}_+$. Moreover, $G$ has trivial determinant by Corollary 2.3.4, so we can conclude $\mathbf{Z}(G) = \mathbf{Z}(E)$ and $G = E \rtimes G_1$ as above.

The same arguments apply to the system $\mathcal{F}(10, 4, 1, \mathbb{1})$, which has trace function

$$(t_1, t_2) \mapsto -\sum_x \psi\big(x^{10} + t_1x^4 + t_2x\big),$$

since its specialization $t_2 = 0$ has geometric monodromy group $\mathrm{Sp}_4(3)$ acting in a total Weil representation by [**KT3**, Theorem 10.6].

(iii) Let $H$ denote $G_{\mathrm{geom}}$ for the system $\mathcal{F}(10, 2, 1, \mathbb{1})$, which has trace function

$$(t_2, t_3) \mapsto -\sum_x \psi\big(x^{10} + t_2x^2 + t_3x\big).$$

This is the specialization $t_1 = 0$ of the system $\mathcal{F}(10, 4, 2, 1, \mathbb{1})$, so $H \leq E \rtimes G_1 = 3^{1+4}_+ \rtimes \mathrm{Sp}_4(3)$ by the result of (ii); in particular $H \leq \mathrm{SL}_9(\mathbb{C})$ and $\mathbf{Z}(H) \leq \mathbf{Z}(G) = \mathbf{Z}(E)$ by irreducibility. Specializing $t_2 = 0$ we obtain the Pink–Sawin system $\mathcal{F}(10, 1, \mathbb{1})$ which has geometric monodromy group $E_1 \cong E$ by Theorem 7.3.8, whence $H \geq E_1$. As $\mathbf{Z}(E_1)$ and $\mathbf{Z}(E)$ are both central cyclic subgroups of order 3, we get

$$H \geq \mathbf{Z}(E_1) = \mathbf{Z}(E). \tag{11.1.6.1}$$

On the other hand, specializing $t_3 = 0$, we obtain the system $\mathcal{F}(10, 4, \mathbb{1})$ which has geometric monodromy group $H_1 = \mathrm{Sp}_2(9)$ acting in a total Weil representation by Lemma 7.3.2. Next, if $\varphi$ denotes the character of the underlying representation of $H$, then

$$|\varphi(h)|^2 = 0 \text{ or a power of 9 for all } h \in H \tag{11.1.6.2}$$

by Theorem 7.1.2. Also note that $E \cap H_1$ is a normal 3-subgroup of $H_1 = \mathrm{Sp}_2(9)$, so

$$E \cap H_1 = 1. \tag{11.1.6.3}$$

It follows that

$$H_1 \cong EH_1/E \leq EH/E \leq G/E = G_1 \cong \mathrm{Sp}_4(3).$$

Checking the list of maximal subgroups of $\mathrm{Sp}_4(3)$ [**CCNPW**], we see that

$$EH/E = \mathrm{Sp}_4(3),\ \mathrm{SL}_2(9) \cdot 2,\ \text{or } \mathrm{SL}_2(9). \tag{11.1.6.4}$$

In fact, the middle case of (11.1.6.4) is impossible, since $\mathcal{G}(10,2,1,\mathbb{1})$ lives over $\mathbb{A}^2$ and so $H = \mathbf{O}^{3'}(H)$.

Suppose that $H \geq E$. In the first case of (11.1.6.4), we obtain $H = G > G_1 = \mathrm{Sp}_4(3)$, and since $G_1$ acts via a total Weil representation, we get $|\varphi(h_1)| = \sqrt{3}$ for some $h_1 \in G_1$, in violation of (11.1.6.2). Hence $H/E = \mathrm{SL}_2(9) \cong H_1$, and so $H = E \rtimes H_1$ by (11.1.6.3).

It remains to consider the case $H \not\geq E$. We still have by (11.1.6.4) that $EH/E$ is a subgroup of $\mathrm{Sp}_4(3)$ that contains $EH_1/E \cong H_1$, which is unique up to conjugacy [**CCNPW**]; in particular it acts irreducibly on $E/\mathbf{Z}(E) \cong \mathbb{F}_3^4$. On the other hand, by (11.1.6.1) we see in this case that $(H \cap E)/\mathbf{Z}(E)$ is a proper subgroup of $E/\mathbf{Z}(E)$, so $H \cap E = \mathbf{Z}(E)$ by irreducibility. It follows from (11.1.6.4) that

$$H/\mathbf{Z}(E) = H/(H \cap E) \cong EH/E \hookrightarrow \mathrm{Sp}_4(3).$$

But $H/\mathbf{Z}(E) \geq E_1/\mathbf{Z}(E) \cong 3^4$, and we arrive at a contradiction since Sylow 3-subgroups of $\mathrm{Sp}_4(3)$ are non-abelian groups of order $3^4$. □

## 11.2. The general case

THEOREM 11.2.1. *Let $q = p^f$ be a power of a prime $p > 2$, $k \in \mathbb{Z}_{\geq 1}$, and consider the local system $\mathcal{G}(A, B_1, \dots, B_k)$ over $\mathbb{A}^k/\mathbb{F}_p$ of rank $A - 1$, with trace function*

$$(t_1, \dots, t_k) \in L^k \mapsto \frac{1}{\mathsf{Gauss}_L} \sum_x \psi_L\big(x^A + t_1 x^{B_1} + \dots + t_k x^{B_k}\big)$$

*for any finite extension $L/\mathbb{F}_p$ and with geometric monodromy group $G = G_{\mathrm{geom}}$. Then the following statements hold.*

(a) *Suppose $k \geq 2$, $A = q^n + 1$, $B_i = q^{m_i} + 1$ for $1 \leq i \leq k-1$ with $n > m_1 > \dots > m_{k-1} \geq 0$, $B_k = 1$, $\gcd(n, m_1, \dots, m_{k-1}) = 1$, and $2|nm_1 \dots m_{k-1}$. Then $G = p_+^{1+2nf} \rtimes \mathrm{Sp}_{2n}(q)$, where $p_+^{1+2nf}$ is the extraspecial $p$-group of order $p^{1+2nf}$ and exponent $p$, cf. §7.1.*

(b) *Suppose $A = q^n + 1$, $B_i = q^{m_i} + 1$ for $1 \leq i \leq k$ with $n > m_1 > \dots > m_k \geq 0$, $\gcd(n, m_1, \dots, m_k) = 1$, and $2|nm_1 \dots m_k$. Then $G = \mathrm{Sp}_{2n}(q)$ acting in a total Weil representation.*

PROOF. (a) is Theorem 7.3.5 if $q^n \geq 11$ and Proposition 11.1.6 if $q^n \leq 9$. The rest of the proof is to establish (b).

The case $k = 1$ is already handled in Lemmas 7.3.2 and 7.3.3 when $m_1 = 0$, and in Theorem 7.3.11 when $m_1 \geq 1$. So we will assume $k \geq 2$; in particular, $n > m_1 \geq 1$. If $q^n \leq 9$, then we must have that $(q, n) = (3, 2)$ and so $(k, m_1, m_2) = (2, 1, 0)$, in which case the statement follows from Lemma 11.1.4(iv). From now on we may assume that $q^n \geq 11$.

Note that $\mathcal{G}(A, B_1, \dots, B_k)$ is just the specialization $t_{k+1} = 0$ of the system $\mathcal{G}(A, B_1, \dots, B_k, 1)$ considered in (a). Hence $G$ embeds in $\Gamma := E \rtimes S$, where $E = p_+^{1+2nf}$ is irreducible, and $S = \mathrm{Sp}_{2n}(q)$ acts in a total Weil representation, see Theorem 7.2.2. Similarly to the action of $S$, by [**KT6**, Corollary 2.7], the underlying representation $V$ for $G$ on $\mathcal{G}(A, B_1, \dots, B_k)$ is also a direct sum of two irreducible summands, call them $V_1$ and $V_2$, which correspond to the two local systems, $\mathcal{G}_1$ of rank $(q^n - 1)/2$ with trace function

$$(t_1, \dots, t_k) \mapsto \frac{1}{\mathsf{Gauss}_L} \sum_x \psi_L\big(x^{(q^n+1)/2} + t_1 x^{(q^{m_1}+1)/2} + \dots + t_k x^{(q^{m_k}+1)/2}\big),$$

and $\mathcal{G}_2$ of rank $(q^n+1)/2$ with trace function

$$(t_1,\dots,t_k)\mapsto \frac{1}{\mathsf{Gauss}_L}\sum_x \psi_L\big(x^{(q^n+1)/2}+t_1x^{(q^{m_1}+1)/2}+\ldots+t_kx^{(q^{m_k}+1)/2}\big)\chi_2(x).$$

Since $1\le m_1\le n-1$ and $q^n\ge 11$, we have

$$A-2B_1=\frac{q^n+1}{2}-(q^{m_1}+1)\ge \frac{q^{n-1}(q-2)-1}{2}$$

is at least 7 if $q\ge 5$ and at least 4 if $q=3$; in particular $B_1\le A/2-2$ and so $B_1\le \lfloor A/2\rfloor-2$. Hence we can apply Corollary 2.3.4 to $\mathcal{G}_1$ to see that

$$\text{(11.2.1.1)}\qquad \mathcal{G}_1 \text{ has geometrically trivial determinant.}$$

This implies that

$$\text{(11.2.1.2)}\qquad G\cap \mathbf{Z}(E)=1.$$

Indeed, if $\mathbf{Z}(E)\cap G\ne 1$, then $G\ge \mathbf{Z}(E)=\langle \boldsymbol{z}\rangle$, with $\boldsymbol{z}$ acting on $\mathcal{G}(A,B_1,\dots,B_k)$ as the scalar $\zeta_p$. In this case, $\boldsymbol{z}\in G$ acts on $\mathcal{F}_1$ with determinant $\zeta_p^{(q^n-1)/2}\ne 1$, and this contradicts (11.2.1.1). Also, if $\varphi$ denotes the character of this representation $V$, then

$$\text{(11.2.1.3)}\qquad |\varphi(g)|^2 \text{ is either zero or a } q\text{-power}$$

for any $g\in G$, in fact for any $g\in\Gamma$ by Theorem 7.1.2(a).

For any $1\le j\le l$, write $d_j:=\gcd(n,m_j)$, so that $\gcd(n/d_j,m_j/d_j)=1$. By assumption, $(q^{d_j})^{n/d_j}=q^n=p^N\ge 11$; also, if $m_j>0$ then $d_j\le n/2$ as $m_j<n$. Note that $2|(nm_j/d_j^2)$ for at least one $j$. (Indeed, assume $2\nmid (nm_j/d_j^2)$ for all $j$. If $2|n$, then since $2\nmid (n/d_j)$, we have that $2|d_j$ and so $2|m_j$ for all $j$ and thus $2|\gcd(n,m_1,\dots,m_k)$, a contradiction. So $2\nmid n$, forcing $2\nmid d_j$, and so, as $2\nmid (m_j/d_j)$, we have $2\nmid m_j$ for all $j$ and thus $2\nmid nm_1\dots m_k$, again a contradiction.)

Fix some $j=j_0$ such that $2|(nm_j/d_j^2)$. Then the system $\mathcal{G}(A,B_1,\dots,B_k)$, where all $t_i$ with $i\ne j$ are specialized to be 0, is the local system $\mathcal{W}(\psi,n/d_j,m_j/d_j,q^{d_j})$ on $\mathbb{A}^1/\mathbb{F}_p$ defined in [**KT6**, (9.0.4)], whose geometric monodromy group is shown in [**KT6**, Theorem 9.2] to contain $L_{j_0}:=\mathrm{Sp}_{2n/d_{j_0}}(q^{d_{j_0}})$, acting in a total Weil representation. In particular, the $L$-module $V$ splits as a direct sum of two Weil modules, hence they must be $V_1$ and $V_2$ (restricted to $L_j$). Next, the central involution $\boldsymbol{j}$ of $L_{j_0}$ acts as 1 on the $V_i$ of odd dimension and as $-1$ on the $V_{3-i}$ of even dimension. Since $G$ stabilizes both $V_1$ and $V_2$, it follows that $G$ centralizes $\boldsymbol{j}$, and thus $G\le \mathbf{C}_\Gamma(\boldsymbol{j})$. We also see that the trace of $\boldsymbol{j}$ on $V$ is $\pm 1$, so [**GT1**, Lemma 2.4] implies that $\boldsymbol{j}$ acts without nonzero fixed point on $E/\mathbf{Z}(E)\cong \mathbb{F}_p^{2nf}$. The same is true for the central involution of $S$, and in fact this element and $\boldsymbol{j}$ belong to the same $E$-coset in $\Gamma$. Since $|E|$ is odd, it follows that these two elements are conjugate in $E\langle \boldsymbol{j}\rangle\cong E\cdot 2$. Conjugating $S$ suitably, we may therefore assume that $\boldsymbol{j}$ is the central involution of $S$. Since $\boldsymbol{j}$ centralizes $\mathbf{Z}(E)S$ and acts as inversion on $E/\mathbf{Z}(E)$, we now have that

$$\text{(11.2.1.4)}\qquad L_{j_0}\le G\le \mathbf{C}_\Gamma(\boldsymbol{j})=\mathbf{Z}(E)S$$

In particular, $G\cap E\le \mathbf{Z}(E)S\cap E=\mathbf{Z}(E)$. Hence

$$\text{(11.2.1.5)}\qquad G\cap E=G\cap\mathbf{Z}(E)=1$$

by (11.2.1.2). We next show that it suffices to show

$$|\mathrm{PSp}_{2n}(q)| \text{ divides } |G|. \tag{11.2.1.6}$$

Indeed, assuming (11.2.1.6), we see from (11.2.1.2) that $\mathbf{Z}(E)G$ has order divisible by $|\mathbf{Z}(E)| \cdot |S|/2 = |\mathbf{Z}(E)S|/2$. Since $\mathbf{Z}(E) \cong C_p$ and $S = \mathrm{Sp}_{2n}(q)$, any subgroup of $\mathbf{Z}(E)S$ of such order is equal to $\mathbf{Z}(E)S$. It follows from (11.2.1.4) that $\mathbf{Z}(E)G = \mathbf{Z}(E)S$, and so

$$G^{(\infty)} = (\mathbf{Z}(E)G)^{(\infty)} = (\mathbf{Z}(E)S)^{(\infty)} = S,$$

forcing $G = (\mathbf{Z}(E) \cap G)S$, and so $G = S$ by (11.2.1.2).

The rest of this proof is to prove (11.2.1.6). Now we apply Theorem 7.2.2 to the irreducible subgroup $EG > L_{j_0} = \mathrm{Sp}_{2n/d_{j_0}}(q^{d_{j_0}})$ to see that, modulo $\mathbf{Z}(\mathrm{GL}(V))$ the subgroup $EG$ is $E_1 \rtimes L$, with $E_1 \cong p_+^{1+2nf}$ and $\mathrm{Sp}_{2nf/e'}(p^{e'}) \lhd L \leq \mathrm{Sp}_{2nf/e'}(p^{e'}) \rtimes C_{e'}$ for some $e'|d_{j_0}f$. Since $\mathrm{Sp}_{2nf/e'}(p^{e'})$ is a standard subgroup of $\mathrm{Sp}_{2nf}(p)$ acting in a total Weil representation, $|\varphi(h)|^2 = p^{e'}$ for some $h \in \mathrm{Sp}_{2nf/e'}(p^{e'})$ by [**KT3**, Theorem 3.5]. It follows from (11.2.1.3) that $e' = ef$ for some $e|d_{j_0}$ and

$$\mathrm{Sp}_{2n/e}(q^e) \lhd L \leq \mathrm{Sp}_{2n/e}(q^e) \cdot C_{ef}.$$

This argument also shows that

$$e|d_j \text{ whenever } 2|(nm_j/d_j^2). \tag{11.2.1.7}$$

Suppose $e = 1$. Then $EG$ shares the non-abelian composition factor $\mathrm{PSp}_{2n}(q)$ with $E_1 \rtimes L$. As $E \cap G = 1$ by (11.2.1.5), $G$ admits $\mathrm{PSp}_{2n}(q)$ as a composition factor, proving (11.2.1.6).

So we will assume $e > 1$. Next we show that we may also assume that

$$e|d_j \text{ whenever } 2 \nmid (nm_j/d_j^2). \tag{11.2.1.8}$$

Consider any such $j$; in particular $d_j \leq n/3$ (since $m_j \geq 1$). Then, over $\mathbb{F}_{q^{2d_j}}$, the local system $\mathcal{G}(A, B_1, \ldots, B_k)$, where all $t_i$ are specialized to be 0, is the pullback by the map $t_j \mapsto -t_j$ of the local system $\mathcal{W}^{n/d_j, m_j/d_j}$ defined in [**KT6**, §10], whose geometric monodromy group is shown in [**KT6**, Theorem 10.2] to contain $\mathrm{SU}_{n/d_j}(q^{d_j})$ (acting in the total Weil representation), and hence contains a maximal torus of order

$$(q^{d_j})^{n/d_j-1} - 1 = q^{n-d_j} - 1 = p^{f(n-d_j)} - 1.$$

Note that $f(n - d_j) \geq 2nf/3 \geq 2$, with equality only when $(n, f) = (3, 1)$ and $d_j = 1$. Suppose we are in the latter case. If $m_i = 2$ for some $i$, then $d_i = 1$ and $e = 1$, and so we are done. Otherwise we must have $k = 2$, $(m_1, m_2) = (1, 0)$, and (11.2.1.7) (with $j = 2$) shows that $e|3$, whence $e = 3$ and $L \leq \mathrm{SL}_2(q^3) \cdot 3$. But in this case $E_1L$ and $EG$ cannot contain $\mathrm{SU}_3(q)$, a contradiction. Hence we may assume that $f(n-d_j) \geq 3$, and so $p^{f(n-d_j)}-1$ admits a primitive prime divisor $\ell_j \geq f(n - d_j) + 1 \geq 2nf/3 + 1$ by [**Zs**], and $G$ contains some non-scalar element $g_j$ of order $\ell_j$. As $g_j$ is non-scalar and of order coprime to $p$, $|g_j| = \ell_j$ divides $|L|$. We next note that $\ell_j$ in fact divides $|\mathrm{Sp}_{2n/e}(q^e)|$. (Indeed, if $\ell_j > 2nf/3$ divides $e' = ef$, then, as $e'|nf$ we must have $\ell_j = e' = nf$ is prime and so $d_j = 1$, $e = e'$ (as $e > 1$), and $f = 1$. In this case, $\mathrm{PSU}_n(p)$ embeds in $\mathbf{Z}(\mathrm{GL}(V))EG/(\mathbf{Z}(\mathrm{GL}(V))E) \cong L \leq \mathrm{Sp}_2(p^n) \rtimes C_n$, which is impossible since $n \geq 3$.) It therefore follows that, there is some $1 \leq c_j \leq n/e$ such that $\ell_j$ divides $q^{2ec_j}-1$. By the choice of $\ell_j$, we have that $(n-d_j)|2ec_j \leq 2n \leq 3(n-d_j)$. Hence,

$$\text{either } n-d_j = 2ec_j, \text{ or } n-d_j = ec_j, \text{ or } 3n-3d_j = 2ec_j = 2n \text{ and } d_j = n/3 = m_j.$$

Since $e|n$, (11.2.1.8) holds in the first two cases. So if $e \nmid d_j$, we must be in the third case. Then $\mathrm{PSU}_3(q^{n/3})$ embeds in $\mathbf{Z}(\mathrm{GL}(V))EG/(\mathbf{Z}(\mathrm{GL}(V))E) \cong L \leq \mathrm{Sp}_{2n/e}(q^e) \rtimes C_{e'}$. As mentioned above, a Sylow $\ell_j$-subgroup of $\mathrm{PSU}_3(q^{n/3})$ embeds in $\mathrm{Sp}_{2n/e}(q^e)$ for $\ell_j$ a primitive prime divisor of $p^{2nf/3}-1 = q^{2n/3}-1$, and this Sylow subgroup is non-cyclic. However, the Sylow $\ell_j$-subgroup of $C_{q^{2n}-1}$ is of course cyclic. So there exists another $1 \leq c'_j < n/e = c_j$ such that $\ell_j$ divides $q^{2ec'_j}-1$. Using $e \nmid d_j$ and repeating the previous argument for $c'_j$ in place of $c_j$, we obtain that $3n-3d_j = 2ec'_j = 2n$ and thus $c'_j = n/e = c_j$, a contradiction.

We have therefore shown in (11.2.1.7) and (11.2.1.8) that $e|d_j$ for all $j$, and thus $e|m_j$ for all $j$. As $e>1$ and $e|n$, we get $\gcd(n, m_1, \ldots, m_k) > 1$, a contradiction. □

The next result is the odd-$p$ analogue of Theorems 8.5.7 and Theorem 8.5.8.

Theorem 11.2.2. *Let $q = p^f$ be a power of a prime $p > 2$, $k \in \mathbb{Z}_{\geq 1}$, and consider the local system $\mathcal{G}(A, B_1, \ldots, B_k)$ over $\mathbb{A}^k/\mathbb{F}_p$ of rank $A-1$, with trace function*

$$(t_1, \ldots, t_k) \in L^k \mapsto \frac{1}{\mathsf{Gauss}_L} \sum_x \psi_L\big(x^A + t_1 x^{B_1} + \ldots + t_k x^{B_k}\big)$$

*for any finite extension $L/\mathbb{F}_p$ and with geometric monodromy group $G = G_{\mathrm{geom}}$. Then the following statements hold.*

(a) *Suppose $A = q^n+1$, $B_i = q^{m_i}+1$ for $1 \leq i \leq k$ with $n > m_1 > \ldots > m_k \geq 1$, $\gcd(n, m_1, \ldots, m_k) = 1$, and $2 \nmid nm_1 \ldots m_k$. Then $G = \mathrm{SU}_n(q)$ acting in the total Weil representation.*

(b) *Suppose $k \geq 2$, $A = q^n+1$, $B_i = q^{m_i}+1$ for $1 \leq i \leq k-1$ with $n > m_1 > \ldots > m_{k-1} \geq 1$, $B_k = 1$, $\gcd(n, m_1, \ldots, m_{k-1}) = 1$, and $2 \nmid nm_1 \ldots m_{k-1}$. Then $G = p_+^{1+2nf} \rtimes \mathrm{SU}_n(q)$.*

Proof. Note that the assumptions imply $q^n \geq 27$.

(a) The case $k=1$ is already handled in Theorem 7.3.11, so we will assume $k \geq 2$; in particular, $n > m_1 \geq 1$. Note that $\mathcal{G}(A, B_1, \ldots, B_k)$ is just the specialization $t_{k+1} = 0$ of the system $\mathcal{G}(A, B_1, \ldots, B_k, B_{k+1})$, with $B_{k+1} = q^2+1$. By Theorem 11.2.1(b), $G$ embeds in $S := \mathrm{Sp}_{2n}(q)$ acting in a total Weil representation. By [**KT6**, Corollary 2.7], $\mathcal{G}(A, B_1, \ldots, B_k)$ is the direct sum of $q+1$ irreducible subsheaves, one of rank $(q^n-q)/(q+1)$ and $q$ of rank $(q^n+1)/(q+1)$. Applying [**KT3**, Theorem 3.4] to the subgroup $G$ of $S$, we obtain that $\mathrm{SU}_n(q) \lhd G \leq \mathrm{GU}_n(q)$, with $\mathrm{SU}_n(q)$ a standard special unitary subgroup of $\mathrm{Sp}_{2n}(q)$. Since $\mathcal{G}(A, B_1, \ldots, B_k)$ lives over $\mathbb{A}^k$, $G$ has no nontrivial $p'$-quotient. Hence $G = \mathrm{SU}_n(q)$.

(b) Note that $\mathcal{G}(A, B_1, \ldots, B_k)$ is just the specialization $t_{k+1} = 0$ of the system $\mathcal{G}(A, B_1, \ldots, B_k, 0)$. By Theorem 11.2.1(a), $G$ embeds in $\Gamma = E \rtimes S$. On the other hand, the specialization $t_k = 0$ of $\mathcal{G}(A, B_1, \ldots, B_k)$ is the system $\mathcal{G}(A, B_1, \ldots, B_{k-1})$. Hence, by (a), $G$ contains $R = \mathrm{SU}_n(q)$ acting in its total Weil representation. Certainly $R \cap E = 1$, so $R$ injects in $S$. Also, $G$ is irreducible by Lemma 11.1.1.

We next observe that $R$ acts irreducibly on $E/\mathbf{Z}(E) \cong \mathbb{F}_p^{2nf}$. (Indeed, as $2 \nmid nm_1 \dots m_{k-1}$ and $k \geq 2$, we have $n \geq 3$. Therefore, $L$ contains an element of order a primitive prime divisor $\ell$ of $p^{2nf}-1$ [**Zs**], and any such element in $S$ acts irreducibly on $E/\mathbf{Z}(E)$.)

Now assume that $\mathbf{Z}(E)G \cap E = \mathbf{Z}(E)$. Then $\bar{G} := \mathbf{Z}(E)G/\mathbf{Z}(E)$ embeds in $\Gamma/E = S = \mathrm{Sp}_{2n}(q)$. Under this embedding, the image $\bar{R}$ of $R$ is the standard subgroup $\mathrm{SU}_n(q)$ in $S$. We claim that the only proper subgroups $X$ of $S$ that contain $\bar{R}$ are either between $\bar{R} \cong \mathrm{SU}_n(q)$ and $\mathbf{N}_S(\bar{R}) \cong \mathrm{GU}_n(q) \cdot 2$. (Indeed, any such $X$ has order divisible by $\ell$, and we can apply [**KT2**, Theorem 4.6] to determine the structure of $\mathbf{O}^{p'}(X)$. Using the facts that $X \geq \bar{R}$ and $X \leq S$ has a faithful irreducible representation of degree $\leq (q^n+1)/2$, and arguing as in the proof of [**KT3**, Theorem 3.4], we readily obtain that $\bar{R} \lhd X$.) Thus $\mathrm{SU}_n(q) \lhd \bar{G} \leq \mathrm{GU}_n(q) \cdot 2$, or $\bar{G} = S$. In the former case, $R^{(\infty)} = R \cong \mathrm{SU}_n(q)$ is contained in $G^{(\infty)}$ which is a central cover of $\mathrm{PSU}_n(q)$. It follows that $G^{(\infty)} = R$. By irreducibility of $G$, all $R$-irreducible summands in $\mathcal{G}(A, B_1, \dots, B_k)$ are of the same dimension that divides $q^n$, and this contradicts the action of $R$ on the sheaf. In the latter case, $G^{(\infty)}$ is a central over of $\mathrm{PSp}_{2n}(q)$ with $n \geq 3$, and this again contradicts the irreducible action of $G$ on $\mathcal{G}(A, B_1, \dots, B_k)$ of rank $q^n$.

We have shown that $\mathbf{Z}(E)G \cap E > \mathbf{Z}(E)$, which implies $\mathbf{Z}(E)G \geq E$ by the irreducible action of $R$ on $E/\mathbf{Z}(E)$. Now, $\mathbf{Z}(E)G/E$ is a subgroup of $S = \mathrm{Sp}_{2n}(q)$ that contains $ER/E \cong R$. As above, we have that $\mathbf{Z}(E)G/E = S$, or $\mathrm{SU}_n(q) \lhd \mathbf{Z}(E)G/E \leq \mathrm{GU}_n(q) \cdot 2$. In the former case, $\mathbf{Z}(E)G = ES = \Gamma$. Since $S$ acts via a total Weil representation, we get an element in $G$ with trace of absolute value $\sqrt{q}$. On the other hand, working over extensions of $\mathbb{F}_{q^2}$, we see by Theorem 7.1.2 that any such trace has absolute value 0 or a $q$-power, a contradiction. So we are in the latter case. Since $\mathcal{G}(A, B_1, \dots, B_k)$ lives over $\mathbb{A}^k$, $G = \mathbf{O}^{p'}(G)$, and so $\mathbf{Z}(E)G/E = \mathrm{SU}_n(q)$ and thus $\mathbf{Z}(E)G = E \rtimes \mathrm{SU}_n(q)$. As $G$ contains $G^{(\infty)} = (\mathbf{Z}(E)G)^{(\infty)} = E \rtimes \mathrm{SU}_n(q)$, we conclude that $G = E \rtimes \mathrm{SU}_n(q)$. □

THEOREM 11.2.3. *Let $p$ be a prime, $k \geq 2$, and let $A > B_1 > \dots > B_k \geq 1$ be integers with $\gcd(A, B_1, \dots, B_k) = 1$ and $p \nmid AB_1 \dots B_k$. Consider the local system $\mathcal{F}(A, B_1, \dots, B_k, \theta)$ over $\mathbb{A}^k$ with trace function for any finite extension $L/\mathbb{F}_p$*

$$(t_1, \dots, t_k) \in L^k \mapsto -\sum_x \psi_L\big(x^A + t_1 x^{B_1} + \dots + t_k x^{B_k}\big)\theta(x),$$

*in characteristic $p$, of rank $D = A-1$ if $\theta = \mathbb{1}$ and $D = A$ otherwise, with geometric monodromy group $G = G_{\mathrm{geom}}$. Then $G$ is finite if and only if one of the following conditions holds.*

(i) *$p > 2$, $q = p^f$, $A = (q^n+1)/2$, $B_i = (q^{m_i}+1)/2$, $1 \leq i \leq k$, where $n > m_1 > \dots > m_k \geq 0$ are integers with $2|nm_1 \dots m_k$, $\gcd(n, m_1, \dots, m_k) = 1$, and $\theta = \mathbb{1}$ or $\theta = \chi_2$. Moreover, $G$ is the image of $\mathrm{Sp}_{2n}(q)$ in a Weil representation of degree $D$.*

(i-bis) *$p > 2$, $q = p^f$, $A = q^n+1$, $B_i = q^{m_i}+1$, $1 \leq i \leq k-1$, where $n > m_1 > \dots > m_{k-1} \geq 0$ are integers with $\gcd(n, m_1, \dots, m_{k-1}) = 1$, $B_k = 1$, and $\theta = \mathbb{1}$. Moreover, $G$ is $p_+^{1+2nf} \rtimes \mathrm{Sp}_{2n}(q)$ if $2|nm_1 \dots m_{k-1}$, and $p_+^{1+2nf} \rtimes \mathrm{SU}_n(q)$ if $2 \nmid nm_1 \dots m_{k-1}$.*

(ii) *$p = 2$, $q = 2^f$, $A = q^n+1$, $B_i = q^{m_i}+1$, $1 \leq i \leq k-1$. Furthermore, $B_k = q^{m_k}+1$ with $m_k \geq 1$, or $B_k = 1$, in which case we set $m_k = 0$; $n > m_1 > \dots > m_k \geq 0$ are integers with $2|nm_1 \dots m_k$, $\gcd(n, m_1, \dots, m_k) = 1$, and $\theta = \mathbb{1}$. Assume in addition that $q^n > 8$. Then $G \cong 2_-^{1+2nf} \cdot \Omega_{2n}^-(q)$ if $m_k \geq 1$, or if $m_k = 0$ but $2|nm_1 \dots m_{k-1}$. If*

*$m_k = 0$ and $2 \nmid nm_1 \dots m_{k-1}$, then $G \cong 2_-^{1+2nf} \rtimes \mathrm{SU}_n(q)$, with $\mathrm{SU}_n(q)$ acting in its total Weil representation.*

(iii) *$p$ arbitrary, $q = p^f$, $A = (q^n + 1)/(q + 1)$, $B_i = (q^{m_i} + 1)/(q + 1)$, $1 \le i \le k$, where $n > m_1 > \dots > m_k \ge 1$ are odd integers with $\gcd(n, m_1, \dots, m_k) = 1$, and $\theta^{q+1} = \mathbb{1}$. Moreover, $G$ is the image of $\mathrm{SU}_n(q)$ in a Weil representation of degree $D$.*

(iv) *$p = 2$, $k = 2$, $A = 13$, $B_1 = 3$, $B_2 = 1$, $\theta = \mathbb{1}$, and $G = 2 \cdot G_2(4)$.*

(v) *$p = 3$, $k = 2$, $A = 23$, $B_1 = 5$, $B_2 = 1$, $\theta = \chi_2$, and $G = \mathsf{Co}_3$.*

(vi) *$p = 3$, $k = 2$, $A = 7$, $B_1 = 5$, $B_2 = 1$, $\theta = \chi_2$, and $G = \mathrm{Sp}_6(2)$.*

(vii) *$p = 3$, $k = 2, 3$, $A = 7$, $\{B_1, \dots, B_k\} \subseteq \{4, 2, 1\}$, $\theta = \mathbb{1}$, and $G = 6_1 \cdot \mathrm{PSU}_4(3)$.*

(viii) *$p = 3$, $k = 2, 3$, $A = 5$, $\{B_1, \dots, B_k\} \subseteq \{4, 2, 1\}$, $\theta = \mathbb{1}$. Furthermore, $G = \mathrm{Sp}_4(3) \times 3$ if some $B_i$ is 4, and $G = \mathrm{Sp}_4(3)$ otherwise.*

(ix) *$p = 5$, $A = 3$, $B_1 = 2$, $B_2 = 1$, $\theta = \mathbb{1}$, and $G = \mathrm{SL}_2(5) \times 5$.*

PROOF. (a) First we show that $G$ is finite and has the indicated identification in each of the listed cases.

Case (i-bis) follows from Theorems 11.2.1(a) and 11.2.2(b). Case (i) follows by applying Theorem 11.2.1(b) and projecting the geometric monodromy group of $\mathcal{G}(A, B_1, \dots, B_k)$ onto each of its two irreducible subsheaves. Similarly, when $p > 2$ case (iii) follows by applying Theorem 11.2.2(a) and projecting the geometric monodromy group of $\mathcal{G}(A, B_1, \dots, B_k)$ onto each of its $q + 1$ irreducible subsheaves. Case $p = 2$ of (iii) follows from Theorem 8.5.7 (note that here we have $q^n \ge 32$ since $k \ge 2$). Case (ii) is established in Theorem 8.5.9, respectively Theorem 8.5.8.

Case (iv) is [**KRLT4**, Theorem 32.4]. Case (v) is [**KRLT1**, Theorem 4.2(ii)]. Case (vi) is [**KRLT4**, Theorem 31.6(b)]. Suppose we are in case (vii). Then the case $k = 3$ is [**KRLT4**, Theorem 32.2], which also shows that $G_{\mathrm{geom}} \le 6_1 \cdot \mathrm{PSU}_4(3)$ when $k = 2$. On the other hand, we have that $G_{\mathrm{geom}}$ contains $6_1 \cdot \mathrm{PSU}_4(3)$ when some $B_i$ is 4 by [**KRLT4**, Theorem 21.4], and when some $B_i$ is 2 by [**KRLT4**, Theorem 21.4]. It follows that $G_{\mathrm{geom}} = 6_1 \cdot \mathrm{PSU}_4(3)$ when $k = 2$.

Next, suppose we are in case (viii). Then the case $k = 3$ is Lemma 11.1.4(i), which also shows that $G_{\mathrm{geom}} \le \mathrm{Sp}_4(3) \times 3$ when $k = 2$. On the other hand, we have that $G_{\mathrm{geom}}$ contains $\mathrm{Sp}_4(3) \times 3$ when some $B_i$ is 4 by [**KRLT4**, Theorem 30.7(iv)]. It remains to consider the case $k = 2$ and $(B_1, B_2) = (2, 1)$, in which case the statement is Lemma 11.1.4(ii).

Finally, case (ix) is [**KRLT4**, Theorem 32.8].

The rest of the proof is to show that the only local systems $\mathcal{F} = \mathcal{F}(A, B_1, \dots, B_k, \theta)$ that have finite geometric monodromy group $G = G_{\mathrm{geom}}$ are the ones listed in the theorem. The proof uses the fact that the systems on $\mathbb{A}^1$ obtained by specializing $k - 1$ parameters $t_i$ to be zero also have finite monodromy.

(b) Consider any $1 \le j \le k$. Specializing $t_j = 0$ for all $i \ne j$ and applying Theorem 10.3.14, we obtain the possibilities for $(p, A, B_j, \theta)$ listed in Theorem 10.3.14. First we assume that either the possibility (e) or (f) in Theorem 10.3.14 occurs for some $j$; in particular, $\gcd(A, B_j) = 1$ and $\theta$ is uniquely determined. Now we will make suitable specializations and again apply Theorem 10.3.14 to determine candidates for any $B_i$ with $i \ne j$. In the case of 10.3.13(iv) for $j$, $A = 13$, so $\gcd(A, B_i) = 1$ and Theorem 10.3.14 shows that $B_1 = 3$ and $B_2 = 1$, leading to conclusion (iv). Similarly, in the case of 10.3.13(v) or 10.2.6(v) for $j$, we have $A = 23$, $B_1 = 5$ and $B_2 = 1$, leading to conclusion (v). In the case of 10.3.13(vi) for $j$, we have $A = 7$, $B_1 = 5$ and $B_2 = 1$, leading to conclusion (vi). Cases 10.3.13(vii) for $j$ leads to conclusion (vii). Case 10.3.13(viii) for $j$ leads to conclusion (viii). Case 10.3.13(x) for $j$ leads to conclusion (ix). Cases 10.2.6(vi), 10.3.13(ix), and 10.3.13(xi) for $j$ do not give rise to any system with $k \geq 2$.

(c) Henceforth we will assume that, for any $i$, only one of (a)–(d) of Theorem 10.3.14 can hold for $(p, A, B_i, \theta)$. Write $d_i := \gcd(A, B_i)$.

Suppose we are in the case of 10.3.14(a) for $(A, B_j)$ for some $j$, so that $p > 2$, $d_j|2$, $\theta^{e_j} = \mathbb{1}$, and $A = (p^n + 1)/e_j$ and $B_j = (p^{m_j} + 1)/e_j$ for some $n > m_j \geq 0$ and $e_j := 2/d_j$. Consider any $B_i$ with $i \neq j$. Then we can apply Theorem 10.3.14 to $(A, B_i, \theta)$. Note that, whenever 10.3.14(c) occurs for some $i$, then $\theta$ is uniquely determined and $d_i = 1$. By our assumption, we arrive at one of the following possibilities.

(c1) For all $i \neq j$, $A = (p^{n_i} + 1)/e_i$ and $B_i = (p^{m_i} + 1)/e_i$ for some $0 \leq m_i < n_i$, $d_i|2$, and $e_i := 2/d_i$. In this case, if $e_i \neq e_j$ for some $i \neq j$, then either $(e_j, e_i) = (1, 2)$ and $2p^n - p^{n_i} = -1$, or $(e_j, e_i) = (2, 1)$ and $p^n - 2p^{n_i} = 1$, which both are impossible. So $e_i = e_j$ for all $i$. Since $p > 2$ and $\gcd(A, B_1, \ldots, B_k) = 1$, we have $e_j = 2$. Now, setting $d := \gcd(n, m_1, \ldots, m_k)$, $q := p^d$, and applying Lemma 10.3.2(ii), we arrive at conclusion (i).

(c2) For some $i \neq j$, $A = (q^s + 1)/e_i$ and $B_i = (q^t + 1)/e_i$ for some $q = p^f$, $d_i|(q + 1)$, $e_i := (q + 1)/d_i$, and some odd integers $s > t \geq 1$. Because of the preceding case (c1), we may assume $e_i > 2$. Since $s \geq 3$ and $p > 2$, $p^{2sf} - 1$ has a primitive prime divisor $\ell_1$ by [**Zs**], which will divide $A = (q^s + 1)/e_i$ and so divide $p^n + 1 = e_j A$ as well. It follows that $2n \geq 2sf$ and so $n \geq 3$. This in turn implies that $p^{2n} - 1$ has a primitive prime divisor $\ell_2$ by [**Zs**], which will divide $A = (p^n + 1)/e_j$ and so divide $q^s + 1 = e_i A$ as well. Hence $2sf \geq 2n$, and thus $p^n + 1 = q^s + 1$ and $e_i = e_j \leq 2$, a contradiction.

(c3) For some $i \neq j$, $d_i = 1$, $A = 2q - 1$, $B_i = 1$, for some $q = p^f$. In this case, if $e_j = 1$, then $p^n - 2q = -2$, a contradiction. Hence $e_j = 2$, $p^n - 4q = -3$, so $p = 3$. Now, $p^n - 3q = q - 3$ is divisible by $3^2$ since $n \geq 2$, hence $q = 3$, $A = 5$, going back to (i).

(c4) For some $i \neq j$, $d_i = 1$, $A = q + 1$, $B_i = 1$, for some $q = p^f$, and $\theta = \mathbb{1}$. In this case, if $e_j = 2$, then $p|(A - 1) = (p^n - 1)/2$, a contradiction. Hence $e_j = 1$, and $B_i = B_k = 1$ by our ordering. We have shown that for any $1 \leq l \leq k - 1$, $A = (p^{n_l} + 1)/e_l$ and $B_l = (p^{m_l} + 1)/e_l$ for some $0 \leq m_l < n_l$, $d_l|2$, and $e_l := 2/d_l$ as in (c1). The arguments in (c1) show that $e_l = e_j = 1$, and we arrive at (i-bis).

(d) Now we may assume that, for any $i$, only (b) or (c) or (d) of Theorem 10.3.14 can occur. Suppose we are in the case of 10.3.14(b) for $(A, B_j, \theta)$, so that $d_j|(q + 1)$, $\theta^{e_j} = \mathbb{1}$, $A = (q^n + 1)/e_j$ and $B_j = (q^{m_1} + 1)/e_j$ for some odd integers $n > m_j \geq 1$, $e_j := (q + 1)/d_j$, and some power $q = p^f$. By the result of (c), we may assume that $e_j \geq 2$ if $p > 2$. Consider any $B_i$ with $i \neq j$. Then we can apply Theorem 10.3.14 to $(A, B_i, \theta)$. By our assumption, we arrive at one of the following possibilities.

(d1) For all $i \neq j$, $A = (r_i^{n_i} + 1)/e_i$ and $B_i = (r_i^{m_i} + 1)/e_i$ for some $p$-power $r_i = p^{f_i}$, $d_i|(r_i + 1)$, $e_i := (r_i + 1)/d_i$, and some odd integers $n_i > m_i \geq 1$. Assume in addition that either $(q, n) \neq (2, 3)$ or $(r_i, n_i) \neq (2, 3)$, say $(q, n) \neq (2, 3)$. Then $p^{2nf} - 1$ has a primitive prime divisor $\ell_1$ by [**Zs**], which will divide $A = (q^n + 1)/e_j$ and so divide $r_i^{n_i} + 1 = e_i A$ as well. It follows that $2n_i f_i \geq 2nf$, and so $n_i f_i \geq 3$ and $(p, n_i f_i) \neq (2, 3)$. This in turn implies that $p^{2n_i f_i} - 1$ has a primitive prime divisor $\ell_2$ by [**Zs**], which will divide $A = (r_i^{n_i} + 1)/e_i$

and so divide $q^n + 1 = e_j A$ as well. Hence $2nf \geq 2n_i f_i$, and thus $q^n + 1 = r_i^{n_i} + 1$ and $e_i = e_j$. Changing the notation, we may now write $A = (q^n + 1)/e_j$ and $B_i = (q^{m_i} + 1)/e_j$ for all $i$, where $\gcd(n, m_1, \ldots, m_k) = 1$. Now, if $e_j > 2$, then, by Lemma 10.3.2(i), (ii) we have $2 \nmid nm_1 \ldots m_k$. The condition $\gcd(A, B_1, \ldots, B_k) = 1$ implies by Lemma 10.3.2(iii) that $e_j = q + 1$, and so we arrive at conclusion (iii). In particular, we are done if $p > 2$. If $p = 2$ and $e_j = 1$, then by Lemma 10.3.2(i), the condition $\gcd(A, B_1, \ldots, B_k) = 1$ implies that $2|nm_1 \ldots m_k$, and we arrive at (ii). Suppose now that $(q, n) = (r_i, n_i) = (2, 3)$. Then $n = n_i = 3$, $9/e_j = A = 9/e_i$, so $e_j = e_i$ and $B_j = 3/e_j = 3/e_i = B_i$, contrary to $i \neq j$.

(d2) $p > 2$, for some $i$ we have $d_i = 1$, $A = 2r - 1$, $B_i = 1$, for some $p$-power $r$. In this case,

$$2r - 1 = A = (q^n + 1)/e_j \geq q^2 - q + 1 \geq 2q + 1,$$

so $r > q$ and hence $r \geq pq$. Again using $2r - 1 = A = (q^n + 1)/e_j$, we see $e_j + 1 = 2e_j r - q^n$ is divisible by $pq$ and thus $e_j \geq pq - 1 > q + 1$, contrary to $e_j|(q + 1)$.

(d3) $p > 2$, for some $i$ we have $d_i = 1$, $A = r + 1$, $B_i = 1$, for some $p$-power $r$, and $\theta = \mathbb{1}$. In this case,

$$r + 1 = A = (q^n + 1)/e_j \geq q^2 - q + 1 \geq 2q + 1,$$

so $r > q$ and hence $r \geq pq$. Again using $r + 1 = A = (q^n + 1)/e_j$, we see $e_j - 1 = q^n - e_j r$ is divisible by $pq$ and thus $e_j = 1$, since $e_j|(q + 1)$. By our ordering, $B_i = B_k = 1$. We have therefore shown that for any $1 \leq l \leq k - 1$, $A = (r_l^{n_l} + 1)/e_l$ and $B_l = (r_l^{m_l} + 1)/e_l$ for some $p$-power $r_l = p^{f_l}$, $d_l|(r_l + 1)$, $e_l := (r_l + 1)/d_l$, and some odd integers $n_l > m_l \geq 1$. The arguments in (d1) show that in this case $e_l = e_j = 1$. Hence we arrive at (i-bis).

(d4) $p = 2$, for some $i \neq j$ we have $d_i = 1$, $A = r_i^{n_i} + 1$ for some power $r_i = 2^{f_i}$, $\theta = \mathbb{1}$, and either $B_i = r_i^{m_i} + 1$ for some some integers $n_i > m_i \geq 1$ with $2|n_i m_i$ and $\gcd(n_i, m_i) = 1$, or $B_i = 1$. First suppose that $(q, n) = (2, 3)$, so that $A = 9/e_j$. If $e_j = 3$, then $A = 3$ and so $k = 1$, a contradiction. So $e_j = 1$, $(A, B_j) = (9, 3)$, and either $B_i = 1$ or $B_i = 5$. By Theorem 10.3.13, no $B_{i'}$ can be 7. So $2 \leq k \leq 3$ and $(A, B_1, \ldots, B_k)$ is one of $(9, 3, 1)$, $(9, 5, 3)$, or $(9, 5, 3, 1)$, and we arrive at (ii). Now we may assume that $(q, n) \neq (2, 3)$. As $n > 1$ is odd, $2^{2nf} - 1$ has a primitive prime divisor $\ell_1$ by [**Zs**], which will divide $A = (q^n + 1)/e_j$ and so divide $r_i^{n_i} + 1 = A$ as well. It follows that $2n_i f_i \geq 2nf$, and so $n_i f_i > 3$. This in turn implies that $2^{2n_i f_i} - 1$ has a primitive prime divisor $\ell_2$ by [**Zs**], which will divide $A = r_i^{n_i} + 1$ and so divide $q^n + 1 = e_j A$ as well. Hence $2nf \geq 2n_i f_i$, and thus $q^n + 1 = r_i^{n_i} + 1$ and $e_j = 1$. We have therefore shown that for any $1 \leq l \leq k$, either this possibility (d4) occurs for $(A, B_l)$, or $A = (r_l^{n_l} + 1)/e_l$ and $B_l = (r_l^{m_l} + 1)/e_l$ for some 2-power $r_l = 2^{f_l}$, $d_l|(r_l + 1)$, $e_l := (r_l + 1)/d_l$, and some odd integers $n_l > m_l \geq 1$ as in (d1). The arguments in (a31) show that in the latter case $e_l = e_j = 1$. Changing the notation, we may now write $A = q^n + 1$ and $B_i = q^{m_i} + 1$ for all $1 \leq i \leq k - 1$, and either $B_k = q^{m_k} + 1$, or $(B_k, m_k) = (1, 0)$, where $q$ is a 2-power, and $\gcd(n, m_1, \ldots, m_k) = 1$. The condition $\gcd(A, B_1, \ldots, B_k) = 1$ implies by Lemma 10.3.2(i) that $2|nm_1 \ldots m_k$, and we arrive at (ii).

(e) Now we may assume that, for any $i$, only (c) or (d) of Theorem 10.3.14 can occur. Since $k > 1$, we see that $B_1 > 1$, and hence we are in the case of 10.3.13(ii) for $(A, B_1)$, so that $\theta = \mathbb{1}$, $p = 2$, $A = 2^n + 1$ and $B_1 = 2^m + 1$ for some integers $n > m_1 \geq 1$. Consider any $B_i$ with $i > 1$. Then we can apply Theorem 10.3.14 to $(A, B_i)$. Since $p > 2$, case (iii) of Theorem 10.2.6 cannot occur. By our assumption, for all $i > 1$, we have $d_i = 1$, and either $B_i = 2^{m_i} + 1$

for some $n > m_i \geq 1$, or $i = k$ and $(B_k, m_k) = (1, 0)$. Let $d := \gcd(n, m_1, \ldots, m_k)$, and let $t := 2^d$. Applying Lemma 10.3.2(i), we arrive at conclusion (ii). □

Note that the restriction $q^n > 8$ in Theorem 11.2.3(ii) has been relaxed in [**KT8**, Theorem 4.4].

The next result removes the assumption $\gcd(A, B_1, \ldots, B_k) = 1$ in Theorem 11.2.3 (and generalizes Theorem 10.3.14).

THEOREM 11.2.4. *Let $p$ be a prime, $k \geq 2$, and let $A > B_1 > \ldots > B_k \geq 1$ be integers with $p \nmid AB_1 \ldots B_k$. Consider the local system $\mathcal{F}(A, B_1, \ldots, B_k, \theta)$ over $\mathbb{A}^k$ with trace function for any finite extension $L/\mathbb{F}_p$*

$$(t_1, \ldots, t_k) \in L^k \mapsto -\sum_x \psi_L\big(x^A + t_1 x^{B_1} + \ldots + t_k x^{B_k}\big)\theta(x),$$

*in characteristic $p$, of rank $D = A - 1$ if $\theta = \mathbb{1}$ and $D = A$ otherwise, with geometric monodromy group $G = G_{\mathrm{geom}}$. Then $G$ is finite if and only if one of the following conditions holds.*

(i) $\gcd(A, B_1, \ldots, B_k) = 1$, *and one of the conclusions* (i)–(ix) *of Theorem 11.2.3 holds.*

(ii) *$p > 2$, $q = p^f$, $A = q^n + 1$, $B_i = q^{m_i} + 1$, $1 \leq i \leq k$, where $n > m_1 > \ldots > m_k \geq 0$ are integers with $2|nm_1 \ldots m_k$, $\gcd(n, m_1, \ldots, m_k) = 1$, and $\theta = \mathbb{1}$. Moreover, $G$ is $\mathrm{Sp}_{2n}(q)$ acting in a total Weil representation of degree $D = q^n$, and this identification of $G$ also holds in the case $k = 1$.*

(iii) *$p$ arbitrary, $q = p^f$, $1 < d \mid (q + 1)$ for $d := \gcd(A, B_1, \ldots, B_k)$, $A = d(q^n + 1)/(q + 1)$, $B_i = d(q^{m_i} + 1)/(q + 1)$, $1 \leq i \leq k$, where $n > m_1 > \ldots > m_k \geq 1$ are odd integers with $\gcd(n, m_1, \ldots, m_k) = 1$, and $\theta^{(q+1)/d} = \mathbb{1}$. Moreover, $G$ is the image of $\mathrm{SU}_n(q)$ in a sub-representation of degree $D$ of the total Weil representation, and this identification of $G$ also holds in the case $k = 1$.*

PROOF. In view of Theorem 11.2.3, we may assume that $\gcd(A, B_1, \ldots, B_k) =: d > 1$. Fix a character $\sigma$ with $\sigma^d = \theta$. By [**KT6**, Corollary 2.7], $\mathcal{F}$ is geometrically isomorphic to the direct sum $\oplus_{i=1}^d \mathcal{F}_i$ of geometrically irreducible and pairwise non-isomorphic sheaves $\mathcal{F}_i$, with trace function

$$(t_1, \ldots, t_k) \mapsto -\sum_x \psi\big(x^{A/d} + t_1 x^{B_1/d} + \ldots + t_k x^{B_k/d}\big)\chi_i(x)\sigma(x),$$

where $\chi_1, \ldots, \chi_d$ are the $d^{\mathrm{th}}$-roots of $\mathbb{1}$. Working over fields over which all $\chi_i\sigma$ are defined and using Lemma 2.2.5, we see that the finiteness of $G_{\mathrm{geom}}$ implies that each of the $d$ sheaves $\mathcal{F}_i$ also has finite geometric monodromy group $G_{\mathrm{geom},i}$. They all share the same exponents $A/d$ and $B_i/d$, but have the characters $\chi_i\sigma$ that differ by a character of order dividing $d$. Applying Theorem 11.2.3, we see that $\mathcal{F}_i$ must be in the case of 11.2.3(i) or 11.2.3(iii). Now arguing as in the second paragraph of the proof of Theorem 10.3.14, we arrive at (ii) or (iii).

It remains to identify $G$ in these two cases, for which we also allow the possibility $k = 1$. In the case of (ii), we can just apply Theorem 11.2.1(b). Assume we are in (iii). If $p > 2$, then $\mathcal{F}$ is a direct summand of the sheaf $\tilde{\mathcal{F}}$ considered in Theorem 11.2.2(a), which has $\mathrm{SU}_n(q)$ (in its total Weil representation) as its geometric monodromy group. By Lemma 2.2.5, $\mathrm{SU}_n(q)$ maps onto $G$, and in fact $G$ is the image of $\mathrm{SU}_n(q)$ in a sub-representation of degree $D$ of the total Weil representation. If $p = 2$, we can argue similarly, using Theorem 8.5.7. □

Using Lemma 8.5.1, we can now prove:

Corollary 11.2.5. *Let $q = p^f$ be a power of a prime $p > 2$, $k \in \mathbb{Z}_{\geq 2}$, $A = q^n + 1$, $B_i = q^{m_i} + 1$ for $1 \leq i \leq k-1$ with $n > m_1 > \ldots > m_{k-1} \geq 0$, $B_k = 1$, $\gcd(n, m_1, \ldots, m_{k-1}) = 1$, and $2|nm_1 \ldots m_{k-1}$.*

(i) *Consider the local system $\mathcal{H}^\sharp$ over $(\mathbb{G}_m \times \mathbb{A}^k)/\mathbb{F}_p$ of rank $A - 1$, with trace function*

$$(s, t_1, \ldots, t_k) \in L^\times \times L^k \mapsto \frac{1}{\mathsf{Gauss}_L} \sum_x \psi_L\big(sx^A + t_1 x^{B_1} + \ldots + t_k x^{B_k}\big)$$

*and with geometric monodromy group $H$. Then $H = p_+^{1+2nf} \rtimes \mathrm{Sp}_{2n}(q)$, where $p_+^{1+2nf}$ is the extraspecial $p$-group of order $p^{1+2nf}$ and exponent $p$.*

(ii) *Consider the local system $\mathcal{G}^\sharp$ over $(\mathbb{G}_m \times \mathbb{A}^{k-1})/\mathbb{F}_p$ of rank $A - 1$, with trace function*

$$(s, t_1, \ldots, t_{k-1}) \in L^\times \times L^{k-1} \mapsto \frac{1}{\mathsf{Gauss}_L} \sum_x \psi_L\big(sx^A + t_1 x^{B_1} + \ldots + t_{k-1} x^{B_{k-1}}\big)$$

*and with geometric monodromy group $K$. Then $K = \mathrm{Sp}_{2n}(q)$ acting in a total Weil representation.*

Proof. (i) By Theorem 11.2.1(a) and Lemma 8.5.1, $H$ contains the normal subgroup $G = E \rtimes S$, where $E = p_+^{1+2nf}$, acting irreducibly on the underlying representation $V$ of dimension $q^n$, $S \cong \mathrm{Sp}_{2n}(q)$, acting on $V$ via a total Weil representation, and $H/G \hookrightarrow C_{q^n+1}$. If $\varphi$ denotes the $H$-character afforded by $V$, then the trace formula shows that $\mathbb{Q}(\varphi) \subseteq \mathbb{Q}(\zeta_p)$, which in turn implies that $\mathbf{Z}(H) = \mathbf{Z}(G) = \mathbf{Z}(E) \cong C_p$. Next, since $E = \mathbf{O}_p(G)$ $\mathsf{char}$ $G \lhd H$, $E \lhd H$, and so

$$H \leq \mathbf{N}_{\mathrm{GL}(V)}(E) = \mathbf{Z}(\mathrm{GL}(V))E \rtimes R,$$

with $R \cong \mathrm{Sp}_{2nf}(p)$. Since $E$ acts irreducibly on $V$, $\mathbf{C}_H(E) = \mathbf{Z}(H) = \mathbf{Z}(E)$. It follows that $S \lhd H/E$ embeds in the image $R$ of $\mathbf{N}_{\mathrm{GL}(V)}(E)/E$ in $\mathrm{Out}(E)$. We also know that $S \cong \mathrm{Sp}_{2n}(q)$ is a standard subgroup inside $R$, and $\mathbf{N}_R(S) \cong S \rtimes C_f$, with $C_f$ induced by field automorphisms of $S$. Hence $H/E = S \cong C_e$ for some $e|f$. The proof of [**KT3**, Theorem 3.5] shows that $H/E$ contains an element which fixes exactly $q^{1/e}$ vectors while acting on $E/\mathbf{Z}(E) \cong \mathbb{F}_p^{2nf}$. It then follows from Lemma 7.2.1 that $H$ contains an element $h$ with $|\varphi(h)|^2 = q^{1/e}$. On the other hand, by Theorem 7.1.2, $|\varphi(h)|^2$ is either 0 or a power of $q$. Hence we conclude that $e = 1$ and $H/E = S$, whence $H = G$ as stated.

(ii) Keep the notation made in (i). By Theorem 11.2.1(b) and Lemma 8.5.1, $K$ contains the normal subgroup $S \cong \mathrm{Sp}_{2n}(q)$ acting on $V$ via a total Weil representation of dimension $q^n$, and $K/S \hookrightarrow C_{q^n+1}$. Note that $\mathcal{G}^\sharp$ is obtained from the sheaf $\mathcal{F}^\sharp$ by the specialization $t_k = 0$. Hence $K$ is a subgroup of $H = E \rtimes S$ by the result of (i). As $[K : S]$ is coprime to $p$ and $[H : K]$, which divides $[H : S] = |E|$, is a power of $p$, we conclude that $K = S$. □

More generally, we have

Corollary 11.2.6. *Let $p$ be a prime, $k \geq 2$, and let $A > B_1 > \ldots > B_k \geq 1$ be integers with $p \nmid AB_1 \ldots B_k$. Consider the local system $\mathcal{F}^\sharp(A, B_1, \ldots, B_k, \theta)$ over $\mathbb{G}_m \times \mathbb{A}^k$ with trace function for any finite extension $L/\mathbb{F}_p$*

$$(s, t_1, \ldots, t_k) \in L^k \mapsto -\sum_x \psi_L\big(sx^A + t_1 x^{B_1} + \ldots + t_k x^{B_k}\big)\theta(x),$$

*in characteristic $p$, of rank $D = A - 1$ if $\theta = \mathbb{1}$ and $D = A$ otherwise, with geometric monodromy group $G^\sharp$. Then $G^\sharp$ is finite if and only if one of the following conditions holds.*

(i) $\gcd(A, B_1, \dots, B_k) = 1$, *and one of the conclusions* (i)–(ix) *of Theorem 11.2.3 holds for* $\mathcal{F}(A, B_1, \dots, B_k, \theta)$.

(ii) *$p > 2$, $q = p^f$, $A = q^n + 1$, $B_i = q^{m_i} + 1$, $1 \le i \le k$, where $n > m_1 > \dots > m_k \ge 0$ are integers with $2|nm_1 \dots m_k$, $\gcd(n, m_1, \dots, m_k) = 1$, and $\theta = \mathbb{1}$.*

(iii) *$p$ arbitrary, $q = p^f$, $1 < d \mid (q+1)$ for $d := \gcd(A, B_1, \dots, B_k)$, $A = d(q^n+1)/(q+1)$, $B_i = d(q^{m_i}+1)/(q+1)$, $1 \le i \le k$, where $n > m_1 > \dots > m_k \ge 1$ are odd integers with $\gcd(n, m_1, \dots, m_k) = 1$, and $\theta^{(q+1)/d} = \mathbb{1}$.*

Proof. Denote by $N$ the order of $\theta$. In the notation of Theorem 11.2.4, consider the local system $\mathcal{F}(A, B_1, \dots, B_k, \theta)$ over $\mathbb{A}^k$, with geometric monodromy group $G$. By Lemma 8.5.1, $G$ injects in $G^\sharp$ as a normal subgroup with cyclic quotient of order dividing $AN$. Hence the statement follows from Theorem 11.2.4. □

When $\theta = \mathbb{1}$, for some local systems $\mathcal{F}^\sharp(A, B_1, \dots, B_k, \theta)$ with finite monodromy, the corresponding geometric monodromy group $G^\sharp_{\text{geom}}$ has been determined in Corollary 11.2.5. It would be of interest to determine $G^\sharp_{\text{geom}}$ in the remaining cases.

Next we prove a $p = 2$ analogue of Corollary 11.2.5:

Corollary 11.2.7. *Let $q = 2^f$ be a power of 2, $k \in \mathbb{Z}_{\ge 2}$, $A = q^n + 1$, $B_i = q^{m_i} + 1$ for $1 \le i \le k-1$. Furthermore, assume that $B_k = q^{m_k}+1$ with $m_k \ge 1$, or $B_k = 1$, in which case we set $m_k := 0$; $n > m_1 > \dots > m_k \ge 0$, $\gcd(n, m_1, \dots, m_k) = 1$, and $2|nm_1 \dots m_k$. Assume in addition that $2|nm_1 \dots m_{k-1}$ if $m_k = 0$. Consider the local system $\mathcal{H}^\sharp$ over $(\mathbb{G}_m \times \mathbb{A}^k)/\mathbb{F}_p$ of rank $A - 1$, with trace function*

$$(s, t_1, \dots, t_k) \in L^\times \times L^k \mapsto \frac{1}{\mathsf{Gauss}_L} \sum_x \psi_L\big(sx^A + t_1 x^{B_1} + \dots + t_k x^{B_k}\big)$$

*and with geometric monodromy group $H$. Then $H = 2^{1+2nf}_- \cdot \Omega^-_{2n}(q)$.*

Proof. The hypothesis implies that $m_1 \ge 1$ and so $n \ge 2$. By Theorem 11.2.3(ii) for $q^n > 8$ and [**KT8**, Theorem 4.4] for $q^n \le 8$, and Lemma 8.5.1, $H$ contains the normal subgroup

$$G = H_f^\circ = E \cdot S,$$

where $E = 2^{1+2nf}_-$, acting irreducibly on the underlying representation $V$ of dimension $q^n$, $S \cong \Omega^-_{2n}(q)$, and $H/G \hookrightarrow C_{q^n+1}$. Let $\varphi$ denotes the $H$-character afforded by $V$. By Corollary 8.1.2 and Remark 8.1.3, working over even-degree extensions of $\mathbb{F}_q$ we have

$$\forall h \in H,\ \varphi(h) \in \mathbb{Z} \text{ and either } \varphi(h) = 0 \text{ or } |\varphi(h)| \text{ is a power of } q. \qquad (11.2.7.1)$$

In particular, $\varphi$ is real-valued. But $\varphi|_E$ is of symplectic type and irreducible, hence $\varphi$ is of symplectic type. It follows from Theorem 8.2.5(iii) that

$$G \lhd H \le \mathbf{N}_{\mathrm{Sp}_{q^n}(\mathbb{C})}(G) = \langle G, s \rangle \cong G \cdot C_{2f}.$$

Recall that $a_1 := |H/G|$ is odd, in particular, $a_1|f$. If $H = G$, we are done. So we will assume that

$$f \ge a_1 \ge 3. \qquad (11.2.7.2)$$

Suppose $a_1 < f$. Applying Theorem 8.2.5(iii)(c) to $X := H$, we obtain an element $t \in H$ with $|\varphi(t)|^2 = q^{2/a_1}$. Since $a_1 \geq 3$, this contradicts (11.2.7.1).

Assume now that $a_1 = f$. Again applying Theorem 8.2.5(iii)(c) to $X := H$, we obtain an element $t \in H$ with $|\varphi(t)|^2 = 2^{2n}$. This implies by (11.2.7.1) that $2^n$ is a power of $q = 2^f$, so

$$f|n. \tag{11.2.7.3}$$

As $f = a_1 \geq 3$, we have $n \geq 3$. Again using Theorem 8.2.5(iii)(c), we obtain an element $t' \in H$ with $|\varphi(t')|^2 = 2^{2n-2}$, which implies by (11.2.7.1) that $2^{n-1}$ is a power of $q = 2^f$, whence

$$f|(n-1).$$

Using this and (11.2.7.3), we conclude that $f = 1$, and so $a_1 = 1$, contrary to (11.2.7.2). □

Next we prove extensions of Corollaries 11.2.5 and 11.2.7.

Corollary 11.2.8. *Let $p$ be any prime, $q := p^f$, $k \in \mathbb{Z}_{\geq 1}$, and*

$$n > m_1 > \ldots > m_k \geq 1$$

*with* $\gcd(n, m_1, \ldots, m_k) = 1$, $(n, q) \neq (3, 2)$, *and* $2 \nmid n \prod_i m_i$. *Define*

$$A := q^n + 1, \ B_i = q^{m_i} + 1.$$

*Consider the local system $\mathcal{G}^\sharp$ over $(\mathbb{G}_m \times \mathbb{A}^k)/\mathbb{F}_p$ of rank $A - 1$, with trace function*

$$(s, t_1, \ldots, t_k) \in L^\times \times L^{k-1} \mapsto -\sum_x \psi_L\big(sx^A + t_1 x^{B_1} + \ldots + t_k x^{B_k}\big)$$

*and with geometric monodromy group $K$. Then $K = \mathrm{GU}_n(q)$ acting in a total Weil representation.*

Proof. (a) Here we assume that $p > 2$, and recall from Corollary 11.2.5(ii) the local system $\mathcal{F}^\sharp$ over $(\mathbb{G}_m \times \mathbb{A}^{k+1})/\mathbb{F}_p$ of rank $A - 1$, with trace function

$$(s, t_1, \ldots, t_{k-1}) \in L^\times \times L^{k-1} \mapsto -\sum_x \psi_L\big(sx^A + t_1 x^{B_1} + \ldots + t_k x^{B_k} + t_{k+1} x^2\big)$$

constructed with the sequence $n > m_1 > \ldots > m_k > m_{k+1} = 0$ (so that $B_{k+1} = q^0 + 1 = 2$). It is proved there that $G_{\mathrm{geom},\mathcal{F}^\sharp}$ is $\mathrm{Sp}_{2n}(q)$ in a total Weil representation. The local system $\mathcal{G}^\sharp$ is the $t_{k+1} = 0$ pullback of $\mathcal{F}^\sharp$. Thus we have

$$K := G_{\mathrm{geom},\mathcal{G}^\sharp} \leq G_{\mathrm{geom},\mathcal{H}^\sharp} = \mathrm{Sp}_{2n}(q)$$

in a total Weil representation $\Phi$, and under the action of $G_{\mathrm{geom},\mathcal{G}^\sharp}$, we get a direct sum of $q+1$ distinct irreducibles, one of dimension $(q^n - q)/(q+1)$ and the other $q$ each of dimension $(q^n + 1)/(q + 1)$. Then one knows [**KT3**, Theorem 3.4] that

$$\mathrm{SU}_n(q) \leq K \leq \mathrm{GU}_n(q). \tag{11.2.8.1}$$

(b) Assume now that $p = 2$. Note that the specialization $s = 1$ of $\mathcal{G}^\sharp$ has geometric monodromy group $K_1 \cong \mathrm{SU}_n(q)$ in a total Weil representation by Theorem 8.5.7. Now we recall from Corollary 8.5.6 the local system $\mathcal{F}^\sharp$ over $(\mathbb{G}_m \times \mathbb{A}^{nf})/\mathbb{F}_p$ of rank $A-1$, with trace function

$$(s_0, s_1, \ldots, s_{nf}) \in L^\times \times L^{nf} \mapsto -\frac{1}{\sqrt{\#L}} \sum_x \psi_L\big(s_0 x^{2^{nf}+1} + s_1 x^{2^{nf-1}+1} + \ldots + s_{nf-1}x^3 + s_{nf}x\big).$$

Since $nf \geq 5$, it is proved there that $G_{\mathrm{geom},\mathcal{F}^\sharp}$ is $H_1^\circ \cong 2_-^{1+2nf} \cdot \Omega_{2nf}^-(2)$ in a faithful irreducible representation $\Phi$ of degree $2^{nf} = q^n$. The local system $\mathcal{G}^\sharp$ is again a pullback of $\mathcal{F}^\sharp$, and so we have

$$K := G_{\mathrm{geom},\mathcal{G}^\sharp} \leq G_{\mathrm{geom},\mathcal{H}^\sharp} = H_1^\circ$$

in the representation $\Phi$, and under the action of $G_{\mathrm{geom},\mathcal{G}^\sharp}$, we again get a direct sum of $q+1$ distinct irreducibles, one of dimension $(q^n - q)/(q+1)$ and the other $q$ each of dimension $(q^n+1)/(q+1)$. By Theorem 8.4.4, either

$$\mathrm{SU}_n(q) \lhd K \leq C_2 \times \mathrm{GU}_n(q) \qquad (11.2.8.2)$$

with $\Phi|_{\mathrm{GU}_n(q)}$ a total Weil representation, or $(n,q) = (5,2)$ and $K \rhd L_1$ with $L_1 \in \{\mathrm{PSL}_2(11), \mathrm{SL}_2(11)\}$. Suppose we are in the latter case. It follows that $K \geq K_1 L_1 \cong K_1 \times L_1$, where $K_1 \cong \mathrm{SU}_5(2)$, and hence $|H_1^\circ|$ has order divisible by $11^2$, which is absurd. We have therefore shown that (11.2.8.2) holds. In fact, by Lemma 8.5.1, $K/K_1$ is cyclic of order dividing $q^n+1$. Since $p=2$, it now follows from (11.2.8.2) that (11.2.8.1) holds in this case as well.

(c) Now we return to the general case and show that $K = G_{\mathrm{geom},\mathcal{G}^\sharp}$ is $\mathrm{GU}_n(q)$, using the fact that $\mathrm{SU}_n(q)$ is a perfect subgroup of index $q+1$ in $\mathrm{GU}_n(q)$. Choose a character $\chi$ of order $q+1$. The $\chi$-component of $\mathcal{G}^\sharp$ has trace function

$$(s, t_1, \ldots, t_k) \mapsto -\sum_x \psi(s x^{(q^n+1)/(q+1)} + \sum_{i=1}^k t_i x^{(q^{m_i}+1)/(q+1)})\chi(x).$$

The degree $(q^n+1)/(q+1)$ is odd, and is $> 2(q^{n-2}+1)/(q+1)$. It then results from Corollary 2.3.11 that this $\chi$-component has geometric determinant $\mathcal{L}_{\overline{\chi}(s)}$, of full order $q+1$. Moreover, its specialization $s=1$ has geometric monodromy group $K_1$, the image of $\mathrm{SU}_n(q)$ in an irreducible Weil representation of degree $(q^n+1)/(q+1)$. Note that $K_1$ is contained in the image of $K$ in the $\chi$-component of $\Phi$. It follows that the quotient $K/\mathrm{SU}_n(q)$ has order divisible by $q+1$. As $\mathrm{GU}_n(q)/\mathrm{SU}_n(q)$ has order $q+1$, it follows immediately from (11.2.8.1) (which has been shown to hold for any prime $p$) that $K = \mathrm{GU}_n(q)$. □

Corollary 11.2.9. *Let $p$ be any prime, $q := p^f$, $k \in \mathbb{Z}_{\geq 1}$, and*

$$n > m_1 > \ldots > m_k \geq 1$$

*with $\gcd(n, m_1, \ldots, m_k) = 1$, $(n,q) \neq (3,2)$, and $2 \nmid n \prod_i m_i$. Define*

$$A := q^n + 1,\ B_i = q^{m_i} + 1.$$

*Consider the local system $\mathcal{G}^\sharp$ over $(\mathbb{G}_m \times \mathbb{A}^{k+1})/\mathbb{F}_p$ of rank $A-1$, with trace function*

$$(s, t_1, \ldots, t_{k+1}) \in L^\times \times L^{k-1} \mapsto -\sum_x \psi_L\big(s x^A + t_1 x^{B_1} + \ldots + t_k x^{B_k} + t_{k+1}x\big)$$

*and with geometric monodromy group $M$. Then $M = E \rtimes K$, where $K = \mathrm{GU}_n(q)$ acting in a total Weil representation, and $E = p_+^{1+2nf}$ if $p > 2$, $K = 2_-^{1+2nf}$ if $p = 2$.*

PROOF. (a) Note that the specialization $t_{k+1} = 0$ of $\mathcal{G}^\sharp$ has geometric monodromy group $K \cong \mathrm{GU}_n(q)$ in a total Weil representation by Corollary 11.2.8 and hence $K \hookrightarrow M$.

Now we consider the local system $\mathcal{F}^\sharp$ over $(\mathbb{G}_m \times \mathbb{A}^{k+2})/\mathbb{F}_p$ of rank $A-1$, with trace function

$$(s, r, t_1, \dots, t_{k+1}) \in L^\times \times L^{nf} \mapsto -\sum_x \psi_L\big(sx^A + rx^{q^{n-1}+1} + t_1x^{B_1} + \ldots + t_kx^{B_k} + t_{k+1}x\big).$$

By Corollary 11.2.5(i) when $p > 2$ and Corollary 11.2.7 when $p = 2$, $\Gamma := G_{\mathrm{geom},\mathcal{F}^\sharp}$ has a normal subgroup $E$, where $E = p_+^{1+2nf}$ if $p > 2$ and $E = 2_-^{1+2nf}$ if $p = 2$, in both cases acting irreducibly in the underlying representation $\Phi$ of degree $q^n$. Furthermore, $\Gamma = E \rtimes R$ with $R = \mathrm{Sp}_{2n}(q)$ acting in a total Weil representation if $p > 2$, and $\Gamma/E \cong R := \Omega^-_{2n}(q)$ if $p = 2$. It follows that

$$K \leq M \leq \Gamma = ER;$$

in particular,

$$\mathbf{C}_\Gamma(E) = \mathbf{Z}(E) \cong C_p,\ \mathbf{C}_\Gamma(E/\mathbf{Z}(E)) = E. \tag{11.2.9.1}$$

On the other hand, by Theorem 11.2.3 (i-bis), (ii), the specialization $s = 1$ of $\mathcal{G}^\sharp$ has geometric monodromy group $G = E_1 \rtimes S$, where $E_1 \cong E$ and $S \cong \mathrm{SU}_n(q)$. By Lemma 8.5.1, $G \hookrightarrow M$ as a normal subgroup and

$$M/G \leq C_{q^n+1}. \tag{11.2.9.2}$$

We next show that

$$E_1 = E. \tag{11.2.9.3}$$

Indeed, by assumption, $n \geq 3$ is odd and $(n, q) \neq (3, 2)$. Hence by [**Zs**], $p^{nf} + 1$ admits a primitive prime divisor $\ell$ which then divides the order of $S$. Fix an element $g \in S$ of order $\ell$ and note that the choice of $\ell$ and (11.2.9.1) shows that $g$ acts irreducibly on $W := E/\mathbf{Z}(E) \cong \mathbb{F}_p^{2nf}$. Now we consider the action of $G = ES$ by conjugation on $E$. As $E_1$ acts irreducibly on $\Phi$, we may identify $\mathbf{Z}(E_1)$ with $\mathbf{Z}(E)$. As the $p$-group $E_1/\mathbf{Z}(E_1)$ acts on the $\mathbb{F}_p$-space $W$, it has a nonzero fixed point subspace $W_1$, which is then stabilized by $g$. But $g$ acts irreducibly on $W$, so $W_1 = W$ and thus $E_1$ centralizes $E/\mathbf{Z}(E)$. It then follows from (11.2.9.1) that $E_1 \leq E$, and hence (11.2.9.3) holds by order consideration.

We also note that $E \cap K \leq \mathbf{O}_p(K) = 1$ (as $K \cong \mathrm{GU}_n(q)$), and so $EK = E \rtimes K$. Since $G = E_1 \rtimes S \lhd M$, (11.2.9.2) now shows that

$$K \hookrightarrow M/E \leq R,\ S \lhd M/E \leq R.$$

Now the arguments in the proof of Proposition 8.4.1 show that

$$\mathbf{N}_R(S) \cong \mathrm{GU}_n(q) \cdot C_2. \tag{11.2.9.4}$$

Note that $M/E$ already contains $K \cong \mathrm{GU}_n(q)$. It follows from (11.2.9.2) that $M/EK$ has order dividing $(q^n + 1)/(q + 1)$, which is odd (since $2 \nmid n$). On the other hand, $M/EK$ has order dividing 2 by (11.2.9.4). We conclude that $M = EK = E \rtimes \mathrm{GU}_n(q)$, as stated. □

Remark 11.2.10. In fact, Corollary 11.2.9 also holds for $k = 0$. More precisely, for any power $q = p^f$ of any prime $p$, consider the local system $\mathcal{G}^\sharp$ over $(\mathbb{G}_m \times \mathbb{A}^1)/\mathbb{F}_p$ of rank $A - 1$, with trace function

$$(s,t) \in L^\times \times L \mapsto -\sum_x \psi_L\big(sx^{q+1} + tx\big).$$

Then $\mathcal{G}^\sharp$ has geometric monodromy group $P = E \rtimes C$, where $C \cong C_{q+1}$, $E \cong p_+^{1+2f}$ if $p > 2$ and $E \cong 2_-^{1+2f}$ if $p = 2$.

Indeed, the pullback $s = 0$ of $\mathcal{G}^\sharp$ is the Pink-Sawin sheaf which has geometric monodromy group $E$ by Theorem 7.3.8. By Lemma 8.5.1, $E \lhd P$ and $P/E \hookrightarrow C_{q+1}$. On the other hand, $C = C_{q+1} \hookrightarrow P$ by Lemma 12.3.9(i) (below). It follows that $P = E \rtimes C$.

We also record the following immediate consequence of Theorems 10.2.6, 10.3.13, and 11.2.3:

Corollary 11.2.11. *Let $p$ be a prime, $k \geq 1$, and let $A > B_1 > \ldots > B_k \geq 1$ be integers with $\gcd(A, B_1, \ldots, B_k) = 1$ and $p \nmid AB_1 \ldots B_k$. Suppose for some multiplicative character $\theta$ of order $d > 2$, the local system $\mathcal{F}(A, B_1, \ldots, B_k, \theta)$ over $\mathbb{A}^k$ in characteristic $p$ has finite geometric monodromy group $G_{\mathrm{geom}}$. Then the following statements hold.*

(i) *There is some power $q = p^f$ of $p$ and odd integers $n > m_1 > \ldots > m_k \geq 1$ such that $A = (q^n + 1)/(q + 1)$, $B_i = (q^{m_i} + 1)/(q + 1)$, $d|(q + 1)$, and $G_{\mathrm{geom}}$ is the image of $\mathrm{SU}_n(q)$ in an irreducible Weil representation of degree $A$. In particular, $p|(A - 1)$ and $2 \nmid AB_1 \ldots B_k$.*

(ii) *For any multiplicative character $\theta'$ of order dividing $d$, the local system $\mathcal{F}(A, B_1, \ldots, B_k, \theta')$ also has finite geometric monodromy group, which is the image of $\mathrm{SU}_n(q)$ in an irreducible Weil representation of degree $A - 1$ when $\theta' = \mathbb{1}$ and degree $A$ when $\theta' \neq \mathbb{1}$.*

CHAPTER 12

# Local systems with non-monomial coefficients

In this chapter, we consider some two-parameter families of exponential sums, some in characteristic 2 using Witt vectors and $\psi_2$, and some in arbitrary characteristic $p$, but only using $\psi$. The major novelty is that the polynomial coefficient for some parameter is **not** just a monomial.

## 12.1. Local systems of the first kind

We first look at the two-parameter family of polynomials in one variable $x$ of the form

$$sx + tf(x)$$

in which $f(x)$ is of van der Geer–van der Vlugt form over some finite extension $k/\mathbb{F}_p$. More precisely, $q$ is a power of $p$, $q_1 < q_2 < \ldots < q_n$ are $n \geq 1$ strictly positive powers of $q$, and

$$f(x) = xR(x) \text{ where } R(x) = \sum_{i=1}^{n} a_i x^{q_i}, \quad \text{with coefficients } a_i \in k^\times. \tag{12.1.0.1}$$

Thus $f(x)$ is not a monomial if $n \geq 2$. Once we have fixed a choice of $R$, we define the following finite (possibly empty) set of roots of unity in $\overline{\mathbb{F}_p}$:

$$\mu_{total}(R) := \bigcap_{1\leq i\leq n} \{\zeta \in \overline{\mathbb{F}_p} | \zeta^{q_i - 1} = (-1)^p\}. \tag{12.1.0.2}$$

In the special case of characteristic $p = 2$, we have $(-1)^p = 1$, and

$$\mu_{total}(R) = \mu_{\gcd_{i=1}^n (q_i - 1)}.$$

The following observation is helpful in computing $\mu_{total}(R)$ for $p > 2$.

Lemma 12.1.1. *Let $n \geq 2$, $p > 2$, $q_i = q^{m_i}$ for $1 \leq i \leq n$, and $m_1 < \ldots < m_n$. Also let $e := \gcd(m_1, \ldots, m_n)$. Then*

$$\#\mu_{total}(R) = \begin{cases} 0, & 2|(m_i/e) \text{ for some } i, \\ q^e - 1, & 2 \nmid (m_i/e) \text{ for all } i. \end{cases}$$

Proof. Replacing $q$ by $q^e$, we may assume that $\gcd(m_1, \ldots, m_n) = e = 1$. Suppose $2|m_i$, $2 \nmid m_j$, and $\zeta \in \mu_{total}(R)$. Since $\zeta^{q^{m_j}-1} = -1$ and $m_j$ is odd, we see that the 2-part $2^f$ of the order of $\zeta$ is $2(q^{m_j} - 1)_2 = 2(q-1)_2$, twice the 2-part of $q - 1$. As $p > 2$, $2^f$ divides $(q^2 - 1)_2$, which in turn divides $q^{m_i} - 1$ because $2|m_i$, and this contradicts the equality $\zeta^{q^{m_i}-1} = -1$.

Assume now that $2 \nmid m_i$ for all $i$, so that $2 \nmid (q^{m_i} - 1)/(q - 1)$, and choose a primitive $2(q-1)^{\text{th}}$ root of unity $\theta \in \overline{\mathbb{F}_p}$. Then $-1 = \theta^{q-1} = \theta^{q^{m_i}-1}$, and hence $\zeta \in \mu_{total}(R)$ if and only if $(\zeta\theta)^{q^{m_i}-1} = 1$ for all $i$. There are exactly

$$\gcd\big(q^{m_1} - 1, \ldots, q^{m_n} - 1\big) = q^{\gcd(m_1,\ldots,m_n)} - 1 = q - 1$$

possibilities for such $\zeta\theta$. □

We begin with a general irreducibility criterion for two-variable polynomials:

THEOREM 12.1.2. *Let $\mathbb{F}$ be an algebraically closed field and $u$, $v$ be two independent variables. Let $m \in \mathbb{Z}_{\geq 2}$ and let*

$$f(u,v) := \sum_{i=0}^{m} a_i(u)v^{n_i},$$

*where $n_i \in \mathbb{Z}_{\geq 0}$ and $a_i(u) \in \mathbb{F}[u]$ is a nonzero polynomials for $0 \leq i \leq m$. Suppose that*
(a) $\gcd\bigl(a_0(u), a_1(u), \ldots, a_m(u)\bigr) = 1$,
(b) *$a_m(u)$ has no multiple roots,*
(c) *$n_m/2 > n_{m-1} > \ldots > n_1 > n_0 = 0$, and*
(d) *$D := \deg_u a_m(u) > \max\bigl(\deg_u a_i(u), 0 \leq i \leq m-1\bigr)$.*
*Then $f$ viewed as a polynomial in $v$ with coefficients in $\mathbb{F}[u]$ is irreducible.*

PROOF. Assume the contrary:

$$f(u,v) = g(u,v)h(u,v), \tag{12.1.2.1}$$

where $g(u,v) = \sum_{i=0}^{r} b_i(u)v^i$ has degree $r$ and $h(u,v) = \sum_{i=0}^{s} c_i(u)v^i$ has degree $s$, with $r \geq s \geq 1$, $r+s = n_m$, $b_i(u), c_i(u) \in \mathbb{F}[u]$.

Let $Z \subset \mathbb{F}$ denote the set of $D$ roots of the leading coefficient $a_m(u)$, and consider any $\zeta \in Z$. By (a), there is some $0 \leq j < m$ such that $a_j(\zeta) \neq 0$; choose the largest such $j$. Then, after being reduced modulo $u - \zeta$, the polynomial $f$ in the variable $v$ now has degree $n_j < n_m/2 \leq r$ by (c). Hence (12.1.2.1) implies that $g$ modulo $u - \zeta$ has degree $< r$ (in $v$), which means that $\zeta$ is a root of the leading coefficient $b_r(u)$. This holds for all $\zeta \in Z$, so $b_r(u)$ is divisible by $a_m(u)$ by (b). In particular,

$$\deg_u b_r(u) \geq \deg_u a_m(u) = D. \tag{12.1.2.2}$$

On the other hand, $\deg_u f = D$ because of (d). Together with (12.1.2.1) and (12.1.2.2), this implies that $\deg_u h = 0$, i.e. all the coefficients $c_i(u)$ are constants and $h = h(v)$ is a polynomial of $v$ only. Now, again using (d) and equating the coefficient for $u^D$ in (12.1.2.1), we see that $h$ divides $v^{n_m}$. As $h = h(v) \in \mathbb{F}[v]$, it follows that $h = cv^s$, where $c := c_s(u)$; in particular, $v$ divides $h$, and so it divides $f$. But this is a contradiction, since $f \equiv a_0(u)$ (mod $v$) and $a_0(u) \neq 0$. □

THEOREM 12.1.3. *Consider the local system $\mathcal{F}$ on $(\mathbb{A}^1 \times \mathbb{G}_m)/k$, $k/\mathbb{F}_p$ a finite extension, of rank $q_n$, whose trace function, at a point $(s,t) \in L \times L^\times$ for $L/k$ a finite extension, given by*

$$\mathrm{Trace}\bigl(\mathsf{Frob}_{(s,t),L}|\mathcal{F}\bigr) = \frac{-1}{\sqrt{\#L}} \sum_{x \in L} \psi_L(sx + tf(x)),$$

*with $f(x) = xR(x)$ as in (12.1.0.1). Then*

$$M_{2,2}(\mathcal{F}) = \begin{cases} 2 + \#\mu_{total}(R), & \textit{if } n \geq 2, \\ 1 + \#\mu_{total}(R) = q_n, & \textit{if } n = 1. \end{cases}$$

Proof. The question is geometric, so we may assume that $k$ contains all roots of unity of order dividing $2\prod_i(q_i-1)$. Then $M_{2,2}$ is the large $L$ limit of the sums

$$\frac{1}{(\#L)^3(\#L-1)}\sum_{s\in L,\ t\in L^\times}\ \sum_{x,y,z,w\in L}\psi_L\big(s(x+y-z-w)+t(f(x)+f(y)-f(z)-f(w)\big).$$

The "missing" sums, over $(s,0)$, are just

$$\frac{1}{(\#L)^2(\#L-1)}\#\{(x,y,z,w)\in L^4 \mid x+y=z+w\}=\frac{\#L}{\#L-1},$$

with large $L$ limit 1. So $M_{2,2}+1$ is the large $L$ limit of the sums, but now extended over all $(s,t)\in L^2$. The large $L$ limit is unchanged if we replace the $1/((\#L)^3(\#L-1))$ factor by $1/(\#L)^4$. Thus $M_{2,2}+1$ is the large $L$ limit of

$$\frac{1}{(\#L)^2}\#\left\{(x,y,z,w)\in L^4 \mid x-z=w-y \ \text{ and } f(x)-f(z)=f(w)-f(y)\right\}.$$

The locus defined by the two equations $x-z=w-y$ and $f(x)-f(z)=f(w)-f(y)$ in the $(x,y,z,w)$-space is the locus in $\mathbb{A}^3$, coordinates $x,w,v$ with $v:=z-x=y-w$ defined by the single equation

$$f(x)-f(x+v)=f(w)-f(w+v).$$

This is now

$$xR(x)-(x+v)R(x+v)=wR(w)-(w+v)R(w+v).$$

Because $R$ is additive, this is just the equation

$$vR(x)+xR(v)=vR(w)+wR(v),$$

or equivalently

$$vR(x-w)+(x-w)R(v)=0.$$

So in the new variable $t:=x-w$, our locus is the product of $\mathbb{A}^1$ with the curve

$$vR(t)+tR(v)=0$$

in the $(t,v)$-space, and hence $M_{2,2}+1$ is the large $L$ limit of

$$\frac{1}{\#L}\#\{v,t\in L|vR(t)+tR(v)=0\}.$$

By Weil's estimates, this large $L$ limit is just the number of distinct irreducible factors (i.e., not counting multiplicities) of the polynomial $vR(t)+tR(v)$ in the polynomial ring $\overline{k}[t,v]$.

Recall that

$$R(x)=\sum_{i=1}^n a_ix^{q_i},\quad \text{with coefficients } a_i\in k^\times.$$

The polynomial $vR(t)+tR(v)$ visibly vanishes if $v=0$ or if $t=0$. Thus

$$M_{2,2}+1=2+\ \text{the number of irreducible factors different from } v,t.$$

Thus we are looking for the number of irreducible factors of $vR(t)+tR(v)$ in $\overline{k}[t,v,1/v,1/t]$. Here we may make the change of variable

$$u=t/v$$

and then factor the polynomial $vR(uv)+uvR(v)$ in $\overline{k}[u,v,1/v,1/u]$. Factoring out $v$, this is the same as factoring $R(uv)+uR(v)$. Both $R(uv)$ and $R(v)$ are divisible by $v^{q_1}$. So we must factor $R(uv)/(uv^{q_1})+R(v)/v^{q_1}$, i.e., we must factor

$$\sum_{i=1}^{n} a_i u^{q_i-1}v^{q_i-q_1}+\sum_{i=1}^{n} a_i v^{q_i-q_1}=\sum_{i=1}^{n} a_i(u^{q_i-1}+1)v^{q_i-q_1}.$$

The content $c(u)$ of this polynomial in $v$ is $c(u)=\prod_{\zeta\in\mu_{total}(R)}(u-\zeta)$. Thus

$$M_{2,2}(\mathcal{F})=1+\#\mu_{total}(R)+\text{ the number of irreducible factors of } P(v),$$

for $P(v)$ the polynomial

$$\frac{1}{c(u)}\sum_{i=1}^{n} a_i(u^{q_i-1}+1)v^{q_i-q_1}$$

in $\overline{\mathbb{F}_p}(u)[v]$. If $n\geq 2$, then by Theorem 12.1.2, $P$ is irreducible, and so the theorem follows. If $n=1$, $P(v)=1$, so has no irreducible factors, and, in this $n=1$ case, $\#\mu_{total}(R)=q_n-1$. □

We next examine the curve whose geometric irreducibility, established in Theorem 12.1.2, played the key role in the proof above of Theorem 12.1.3.

Lemma 12.1.4. *In the situation of* (12.1.0.1)*, with $R(x)=\sum_{i=1}^{n}a_ix^{q_i}$, suppose that $n\geq 2$ and that $\mu_{total}(R)=\varnothing$. Consider the geometrically irreducible curve $\mathcal{C}_0$ in $\mathbb{A}^2/\overline{\mathbb{F}_p}$, coordinates $(u,v)$, of equation*

$$\mathcal{C}_0:\sum_{i=1}^{n} a_i(u^{q_i-1}+1)v^{q_i-q_1}=0.$$

*Denote by $\mathcal{C}$ the complete nonsingular model of $\mathcal{C}_0$. View $\mathcal{C}$ over the projective $v$-line $\mathbb{P}^1_v$. Then $\mathcal{C}$ has degree $q^n-1$ over $\mathbb{P}^1_v$, and over the point $v=\infty$ of $\mathbb{P}^1_v$, $\mathcal{C}$ has $q^n-1$ distinct points $(\zeta,\infty)$, with $\zeta$ a root of $\zeta^{q_n-1}+1=0$. At each such point of $\mathcal{C}$, $v$ has a simple pole and the function $u-\zeta$ on $\mathcal{C}$ has a zero of order $q_n-q_{n-1}$.*

Proof. Write the equation of $\mathcal{C}_0$, first as

$$\sum_{i=1}^{n} a_i v^{q_i-q_1}u^{q_i-1}+\sum_{i=1}^{n} a_i v^{q_i-q_1},$$

then divide through by $v^{q_n-q_1}$ to obtain

$$a_nu^{q_n-1}+\sum_{i=1}^{n-1} a_i(1/v)^{q_n-q_i}u^{q_i-1}+\big(a_n+\sum_{i=1}^{n-1} a_i(1/v)^{q_n-q_i}\big).$$

Modulo $(1/v)^{q_n-q_1}$, this is just the equation $a_nu^{q_n-1}+a_n=0$. The iterative algorithm $(\alpha\mapsto -f(\alpha)/f'(\alpha))$ of Newton's lemma shows that indeed $u-\zeta$ on $\mathcal{C}$ has a zero of order $q_n-q_{n-1}$ at the point $(\zeta,\infty)$. Because $v=\infty$ has the full number $q_n-1$ of points lying over it, the curve $\mathcal{C}$ is finite etale over $\mathbb{P}^1_v$ near $v=\infty$, hence $v$ has a simple pole at each such point. □

Remark 12.1.5. In the previous Lemma 12.1.4, still with $n \geq 2$, we might consider the more general case when $\mu_{total}(R)$ is non-empty, in which case the content $c(u)$ has degree $\#\mu_{total}(R)$, and the equation for the geometrically irreducible curve $\mathcal{C}_0$ in $\mathbb{A}^2/\overline{\mathbb{F}_p}$, coordinates $(u, v)$, is

$$\mathcal{C}_0 : \frac{1}{c(u)} \sum_{i=1}^{n} a_i(u^{q_i-1} + 1)v^{q_i-q_1} = 0.$$

In this case, $\mathcal{C}$ has degree $q^n - 1 - \#\mu_{total}(R)$ over $\mathbb{P}^1_v$, and over the point $v = \infty$ of $\mathbb{P}^1_v$, $\mathcal{C}$ has $q^n - 1 - \#\mu_{total}(R)$ distinct points $(\zeta, \infty)$ with $\zeta$ a root of $\zeta^{q_n-1} + 1 = 0$ but $\zeta$ not in $\mu_{total}(R)$ . At each such point of $\mathcal{C}$, $v$ has a simple pole and the function $u - \zeta$ on $\mathcal{C}$ has a zero of order $q_n - q_{n-1}$.

Remark 12.1.6. Suppose that in the sequence $q_1 < q_2 < \ldots < q_n$ of powers of $q$, we allow the case $q_1 = 1$. If $p$ is odd, then $\mu_{total}(R)$ is empty, and Theorem 12.1.3 remains valid as stated, with the same proof.

If $p = 2$, then the polynomial equation $R(uv) + uR(v) = 0$ which occurs in the proof of Theorem 12.1.3 has its linear term in $v$ vanishing. In this $q_1 = 1$ case, we must assume $n \geq 3$, and define

$$\mu_{total}(R) := \bigcap_{2 \leq i \leq n} \{\zeta \in \overline{\mathbb{F}_p} | \zeta^{q_i - 1} = (-1)^p\}.$$

With this definition, Theorem 12.1.3 remains valid as stated, with the same proof.

In the next result, we determine, for the first time, the geometric monodromy groups of an infinite series of non-monomial local systems.

Theorem 12.1.7. *Let $q = p^f > 9$ be a power of a prime $p > 2$ and fix some constants $a, b \in \mathbb{F}_q^\times$. Consider the local system $\mathcal{F}$ on $(\mathbb{A}^1 \times \mathbb{G}_m)/k$, $k/\mathbb{F}_q$ a finite extension, of rank $q$, whose trace function, at a point $(s, t) \in L \times L^\times$ for $L/k$ a finite extension, given by*

$$\mathrm{Trace}\big(\mathsf{Frob}_{(s,t),L}|\mathcal{F}\big) = \frac{1}{\mathsf{Gauss}_L} \sum_{x \in L} \psi_L\big(sx + t(ax^2 + bx^{q+1})\big).$$

*Then the geometric monodromy group of $\mathcal{F}$ is $G = E \rtimes \mathrm{Sp}_2(q)$, where $E = p_+^{1+2f}$ is extraspecial of order $p^{1+2f}$ and exponent $p$.*

Proof. (a) By Theorem 12.1.3 and Remark 12.1.6, $G$ has $M_{2,2} = 2$ on the underlying representation $V$ of dimension $q$. Next, $\mathcal{F}$ is the specialization $u = t$ of the local system $\mathcal{F}^\sharp$ on $(\mathbb{A}^2 \times \mathbb{G}_m)/k$, $k/\mathbb{F}_q$ a finite extension, of rank $q$, whose trace function, at a point $(s, t, u) \in L \times L^\times$ for $L/k$ a finite extension, given by

$$\mathrm{Trace}\big(\mathsf{Frob}_{(s,t,u),L}|\mathcal{F}^\sharp\big) = \frac{1}{\mathsf{Gauss}_L} \sum_{x \in L} \psi_L(sx + tax^2 + ubx^{q+1}).$$

By Corollary 11.2.5(i), $\mathcal{F}^\sharp$ has geometric monodromy group $H = E \rtimes S$ with $S \cong \mathrm{Sp}_2(q)$.

(b) The aforementioned specialization implies that $G \leq H$. First we show that either $EG = H$, or $q = 11$ and $EG/E \cong \mathrm{SL}_2(5) < S$. Indeed, $2 \leq M_{2,2}(EG) \leq M_{2,2}(G) = 2$, so $M_{2,2}(EG) = 2$. Since $E \lhd EG$, it follows from [**GT2**, Theorem 1.5] and [**BNRT**, Theorem 3] that $EG$ acts transitively on the $q^2 - 1$ nonzero vectors of $E/\mathbf{Z}(E) \cong \mathbb{F}_p^{2f}$; in particular,

$EG/E$ is a subgroup of $H/E \cong \mathrm{Sp}_2(q)$ of order divisible by $q^2-1$. When $q \geq 13$, the largest order of proper subgroups in $\mathrm{Sp}_2(q)$ is $q(q-1)$, see e.g. [**TZ1**, Table VI], hence $EG = H$. (Alternatively, one can also apply [**BNRT**, Theorem 5].) If $q = 11$ and $EG < H$, then [**BNRT**, Theorem 5] shows that $EG/E \cong \mathrm{SL}_2(5)$.

In either case, we see that $R := EG/E$ is perfect and has trivial Schur multiplier.

(c) Next we show that $\mathbf{Z}(E)G = EG$. As mentioned above, $EG$ acts transitively on the set of $q^2-1$ nontrivial elements of $E/\mathbf{Z}(E)$ (via conjugation), but $E$ centralizes $E/\mathbf{Z}(E)$. So $\mathbf{Z}(E)G$ acts transitively on these $q^2-1$ elements, and hence it acts irreducibly on $E/\mathbf{Z}(E)$. It follows that $\mathbf{Z}(E)G \cap E$ is either $\mathbf{Z}(E)$ or $E$. Suppose we are in the former case. Then we have

$$R = EG/E = E(\mathbf{Z}(E)G)/E \cong \mathbf{Z}(E)G/(\mathbf{Z}(E)G \cap E) = \mathbf{Z}(E)G/\mathbf{Z}(E).$$

As $R$ is perfect and $\mathbf{Z}(E) \leq \mathbf{Z}(\mathbf{Z}(E)G) \geq R$, $(\mathbf{Z}(E)G)^{(\infty)}$ is a central cover of $R$ and hence equal to $R$, since $\mathrm{Mult}(R) = 1$. Thus $R$ embeds in $\mathbf{Z}(E)G$ as a normal subgroup; in particular, $\mathbf{Z}(R) \cong C_2$ is normal and hence central in $\mathbf{Z}(E)G$. On the other hand, $\mathbf{Z}(E)G$ acts irreducibly and faithfully on $V$ of odd dimension $q$. So we see that the central involution $\boldsymbol{z}$ of $\mathbf{Z}(R)$ acts as scalar $-1$ on $V$, which is impossible since $\det(V)$ is trivial on the perfect group $R$. Hence we must be in the latter case, i.e. $\mathbf{Z}(E)G \geq E$, whence $\mathbf{Z}(E)G = EG$.

As $\mathbf{Z}(E) < E < EG = \mathbf{Z}(E)G$, we can write $E = \mathbf{Z}(E)(E \cap G)$. Taking the derived subgroup, we get $\mathbf{Z}(E) = [E, E]$ is contained in $E \cap G$. Thus $G \geq \mathbf{Z}(E)$, and so $G = \mathbf{Z}(E)G = EG$, which means $E \lhd G$.

(d) Now, if $EG = H$, then we conclude that $G = H$; in particular we are done if $q \geq 13$.

The only remaining possibility is that $q = 11$ and $G/E = R = \mathrm{SL}_2(5)$. In addition to $G$, we also consider the arithmetic monodromy group $G_1 = G_{\mathrm{arith},\mathbb{F}_{11}}$ of $\mathcal{F}$ over $\mathbb{F}_{11}$. As $E = \mathbf{O}_{11}(G) \lhd G_1$, we have $E \lhd G_1$, and hence

$$G_1 \leq \mathbf{N}_{\mathrm{GL}_{11}(\mathbb{C})}(E) = T(E \rtimes \mathrm{SL}_2(11)),$$

where $T := \mathbf{Z}(\mathrm{GL}_{11}(\mathbb{C})$. In particular, $TG_1/TE$ embeds in $\mathrm{SL}_2(11)$. But $TG_1/TE$ contains the normal subgroup $TG/TE \cong R = \mathrm{SL}_2(5)$ and $\mathrm{SL}_2(5)$ is maximal in $\mathrm{SL}_2(11)$. It follows that $TG_1 = TG$. In particular, for any $h \in G_1$, we can write $h = \alpha g$ for some $g \in G$ and $\alpha \in \mathbb{C}^\times$. As $G_1$ and $G$ are finite, $\alpha$ is a root of unity, whence $|\varphi(h)| = |\varphi(g)|$ if $\varphi$ denotes the character of $G_1$ acting on $\mathcal{F}$.

Note that $R = \mathrm{SL}_2(5)$ acts on $E/\mathbf{Z}(E) \cong \mathbb{F}_{11}^2$ via its irreducible character of degree 2; in particular, the dimension of the fixed point subspace of any element in $R$ on $E/\mathbf{Z}(E)$ is either 0 or 2. This implies by Lemma 7.2.1 that $|\varphi(g)| \in \{0, 1, 11\}$ for any $g \in G$. The preceding statement then shows that $|\varphi(h)| \in \{0, 1, 11\}$ for any $h \in G$. However, a Magma computation shows that, for any choice of $a, b \in \mathbb{F}_{11}^\times$, there is a Frobenius $\mathsf{Frob}_{(s,t),\mathbb{F}_{11^4}}$ that has trace of absolute value $\sqrt{11}$, a contradiction. □

Next we prove a Witt analogue of Theorem 12.1.3:

THEOREM 12.1.8. *Consider the local system $\mathcal{F}$ on $(\mathbb{A}^1 \times \mathbb{G}_m)/k$, $k/\mathbb{F}_2$ a finite extension, whose trace function, at a point $(s,t) \in L \times L^\times$ for $L/k$ a finite extension, given by*

$$\mathrm{Trace}\big(\mathsf{Frob}_{(s,t),L}|\mathcal{F}\big) = \frac{-1}{\sqrt{\#L}} \sum_{x \in L} \psi_{2,L}([x, sx + tf(x)]),$$

*with* $f(x) = xR(x)$ *as in* (12.1.0.1)*. Then*

$$M_{2,2}(\mathcal{F}) = 2.$$

Proof. The question is geometric, so we may assume that $k$ contains all roots of unity of order dividing $\prod_i (q_i - 1)$. Then $M_{2,2}$ is the large $L$ limit of the sums

$$\frac{1}{(\#L)^3(\#L-1)} \sum_{\substack{s \in L, t \in L^\times \\ x,y,z,w \in L}} \psi_{2,L}([x+y+z+w, Q(x,y,z,w)+s(x+y+z+w)+t(f(x)+f(y)+f(z)+f(w)]),$$

with

$$Q = (x+y)(z+w) + xy + zw + z^2 + w^2.$$

The "missing" sum, over $(s, 0)$, contributes zero to the large $L$ limit. Indeed, it is

$$\begin{aligned}
&\frac{1}{(\#L)^2(\#L-1)} \sum_{x,y,z,w \in L, x+y=z+w} \psi_{2,L}([0, Q(x,y,z,w)]) \\
=&\frac{1}{(\#L)^2(\#L-1)} \sum_{x,y,z \in L} \psi_L((x+z)(y+z)) \\
=&\frac{1}{(\#L)(\#L-1)} \sum_{x,y \in L} \psi_L(xy) \\
=&\frac{\#L}{(\#L)(\#L-1)} = O(1/\#L).
\end{aligned}$$

[For a fixed $x \neq 0$, the sum of $\psi_L(xy)$ over $y$ vanishes, and for $x = 0$, this sum over $y$ is $\#L$.]

So $M_{2,2}$ is the large $L$ limit of the sums, but now extended over all $(s,t) \in L^2$. The large $L$ limit is unchanged if we replace the $1/((\#L)^3(\#L-1))$ factor by $1/(\#L)^4$. Thus $M_{2,2}$ is the large $L$ limit of

$$\frac{1}{(\#L)^2} \sum_{\substack{x,y,z,w \in L \\ x-z=w-y \\ f(x)-f(z)=f(w)-f(y)}} \psi_L(xy+zw).$$

Exactly as in the proof of Theorem 12.1.3, the locus defined by the two equations $x - z = w - y$ and $f(x) - f(z) = f(w) - f(y)$ in the $(x,y,z,w)$-space is the locus in $\mathbb{A}^3$, coordinates $x, w, v$ with $v := z - x = y - w$, defined by the single equation

$$vR(x-w) + (x-w)R(v) = 0.$$

On this locus,

$$Q = xy + zw = x(v+w) + (v+x)w = (x+w)v.$$

So in the new variable $t := x - w = x + w$ (remember we are in characteristic 2), our locus is the product of $\mathbb{A}^1$ with the curve

$$vR(t) + tR(v) = 0$$

and $M_{2,2}$ is the large $L$ limit of

$$\frac{1}{\#L} \sum_{\substack{v,t \in L \\ vR(t)+tR(v)=0}} \psi_L(tv).$$

The polynomial $vR(t)+tR(v)$ is visibly divisible by both $t$ and by $v$. The sum over each of the loci ($t=0, v$ free) and ($v=0, t$ free) contributes 1. Thus $M_{2,2}-2$ is the large $L$ limit of the sum

$$S(L) := \frac{1}{\#L}\sum_{\substack{v,t\in L^\times \\ vR(t)+tR(v)=0}} \psi_L(tv).$$

Because we require $v\neq 0$, we may make the substitution $t=uv$, after which the function being summed is $\psi(uv^2)$, and our equation becomes $vR(uv)+uvR(v)=0$. But both $u,v$ are to be invertible, so our equation becomes first $R(uv)+uR(v)=0$, then $R(uv)/u=R(v)$, then

$$R(uv)/(uv^{q_1}) = R(v)/v^{q_1}.$$

Writing this out explicitly, it is

$$\sum_{i=1}^{n} a_i(u^{q_i-1}-1)v^{q_i-q_1} = 0.$$

Viewed as a polynomial in $v$ with coefficients in $\overline{\mathbb{F}_2}[u]$, its content is

$$c(u) = \prod_{\zeta\in\mu_{total}(R)} (u-\zeta).$$

Over each locus $u=\zeta\in\mu_{total}(R), v$ free, the sum of $\psi_L(\zeta v^2)=\psi_L(\sqrt{\zeta}v)$ over $v$ vanishes.

In the case $n=1$, we are done. To treat the case $n\geq 2$, we work on the locus $\mathcal{C}$ defined

$$\frac{1}{c(u)}\sum_{i=1}^{n} a_i(u^{q_i-1}-1)v^{q_i-q_1} = 0.$$

By Theorem 12.1.2, $\mathcal{C}$ is geometrically irreducible. We must show that $\mathcal{L}_{\psi(uv^2)}$ is geometrically nontrivial on this curve. Because $n\geq 2$, $\#\mu_{total}(R) < q_n-1$. By Lemma 12.1.4 and Remark 12.1.5, at each point $\mathcal{P} := (\zeta,\infty)$ with $\zeta$ a root of $\zeta^{q_n-1}=1$ but $\zeta$ not in $\mu_{total}(R)$, the function $u-\zeta$ has a zero of order $q_n-q_1$. But $q_n-q_1\geq q_n-q_{n-1}\geq q_{n-1}\geq 2$, and thus

$$uv^2 = \zeta v^2 + \text{a holomorphic function at } \mathcal{P}.$$

Thus

$$\mathsf{Swan}_{\mathcal{P}}(\mathcal{L}_{\psi(uv^2)}) = \mathsf{Swan}_{\mathcal{P}}(\mathcal{L}_{\psi(\zeta v^2)}) = \mathsf{Swan}_{\mathcal{P}}(\mathcal{L}_{\psi(\sqrt{\zeta}v)}) = 1,$$

the penultimate equality because we are in characteristic 2. Hence $\mathcal{L}_{\psi(uv^2)}$ is geometrically nontrivial on $\mathcal{C}$, and thus the sum

$$\frac{1}{\#L}\sum_{(u,v)\in\mathcal{C}(L)} \psi_L(uv^2)$$

is $O((\#L)^{-1/2})$, as desired. □

Remark 12.1.9. Remark 12.1.6 applies here as well. When $q_1=1$ and $n\geq 3$, Theorem 12.1.8 remains valid, with the identical proof, but with $\mu_{total}(R)$ modified as in Remark 12.1.6.

## 12.2. Local systems of the second kind

Now we consider the case of a two-parameter family of polynomials in one variable $x$ of the form

$$sx + tf(x) + g(x)$$

in which both $f(x)$ and $g(x)$ are of van der Geer–van der Vlugt form over some finite extension $k/\mathbb{F}_p$. More precisely, $q$ and $Q$ are (not necessarily different) powers of $p$,

$$q_1 < q_2 < \ldots < q_n$$

are $n \geq 1$ non-negative powers of $q$,

$$Q_1 < Q_2 < \ldots < Q_m$$

are $m \geq 1$ non-negative powers of $Q$. We make the assumption that if $p = 2$, then both $q_1, Q_1$ are $\geq 2$. [In odd characteristic $p$, we allow either $q_1$ or $Q_1$ to be 1.] We assume that

$$(12.2.0.1) \qquad f(x) = xR(x) \text{ where } R(x) = \sum_{i=1}^{n} a_i x^{q_i}, \quad \text{with coefficients } a_i \in k^\times.$$

$$(12.2.0.2) \qquad g(x) = xS(x) \text{ where } S(x) = \sum_{i=1}^{m} b_i x^{Q_i}, \quad \text{with coefficients } b_i \in k^\times.$$

In what follows, we will assume that

$$(12.2.0.3) \qquad k = \mathbb{F}_{p^\kappa} \text{ is the smallest field that contains all } a_i \text{ and } b_j.$$

Once we have fixed choices of $R$ and $S$, we can define the finite, possibly empty, sets of roots of unity

$$\mu_{total}(R),\ \mu_{total}(S)$$

as in (12.1.0.2).

THEOREM 12.2.1. *Suppose that $Q_m > q_n$. Consider the two-parameter local system $\mathcal{F}$ on $\mathbb{A}^2/k$ of rank $Q_m$, whose trace function, at a point $(s,t) \in L^2$ for $L/k$ a finite extension, given by*

$$\mathrm{Trace}\big(\mathsf{Frob}_{(s,t),L}|\mathcal{F}\big) = \frac{-1}{\sqrt{\#L}} \sum_{x \in L} \psi_L(sx + tf(x) + g(x)),$$

*with $f(x) = xR(x)$ and $g(x) = xS(x)$ as in* (12.2.0.1) *and* (12.2.0.2)*. Then*

$$M_{2,2}(\mathcal{F}) = 2 + \#\big(\mu_{total}(R) \cap \mu_{total}(S)\big).$$

PROOF. As in the proof of Theorem 12.1.3, we readily calculate that $M_{2,2}$ is the large $L$ limit of the sums

$$\frac{1}{(\#L)^2} \sum_{\substack{x,y,z,w \in L \\ x-z=w-y \\ f(x)-f(z)=f(w)-f(y)}} \psi_L(g(x) - g(z) + g(y) - g(w)).$$

The locus defined by the two equations $x - z = w - y$ and $f(x) - f(z) = f(w) - f(y)$ in the $(x,y,z,w)$-space is the locus in $\mathbb{A}^3$, coordinates $x, w, v$ with $v := z - x = y - w$, defined by the single equation

$$vR(x-w) + (x-w)R(v) = 0.$$

On this locus,

$$g(x) - g(z) + g(y) - g(w) = vS(x - w) + (x - w)S(v).$$

So in the new variable $t := x - w$, our locus is the product of $\mathbb{A}^1$ with the curve

$$vR(t) + tR(v) = 0,$$

the function inside the $\psi_L$ is $vS(t) + tS(v)$, and $M_{2,2}$ is the large $L$ limit of

$$\frac{1}{\#L} \sum_{\substack{v,t \in L \\ vR(t)+tR(v)=0}} \psi_L(vS(t) + tS(v)).$$

The polynomial $vR(t) + tR(v)$ is visibly divisible by both $t$ and by $v$, as is the polynomial $vS(t) + tS(v)$. The sum over each of the loci ($t = 0, v$ free) and ($v = 0, t$ free) contributes 1. Thus $M_{2,2} - 2$ is the large $L$ limit of the sum

$$\Sigma(L) := \frac{1}{\#L} \sum_{\substack{v,t \in L^\times \\ vR(t)+tR(v)=0}} \psi_L(vS(t) + tS(v)).$$

On the locus $vS(t) + tS(v) = 0, tv \neq 0$, we may make the change of variable $t = uv$, and now the locus of summation is $vR(uv) + uvR(v) = 0, uv \neq 0$, or $R(uv)/(uv^{q_1}) + R(v)/v^{q_1} = 0, uv \neq 0$. Over the $L$-points of this locus, what we are summing is $\psi_L(vS(uv) + uvS(v))$. Written out explicitly,

$$vS(uv) + uvS(v) = \sum_{i=1}^{m} b_i u(u^{Q_i - 1} + 1)v^{1+Q_i}.$$

When we regard $R(uv)/(uv^{q_1}) + R(v)/v^{q_1}$ as a polynomial in $v$ with coefficients in $\overline{\mathbb{F}_p}[u]$, its content is

$$c(u) = \prod_{\zeta \in \mu_{total}(R)} (u - \zeta).$$

For fixed $\zeta \in \mu_{total}(R)$, on the locus $u = \zeta \neq 0, v$ free, the polynomial $vS(\zeta v) + \zeta vS(v))$ either vanishes identically, which happens precisely when $\zeta \in \mu_{total}(S)$ (in which case we get a contribution of 1 to $M_{2,2}$), or it is a sum of monomials in $v$ whose degrees are all coprime to $p$. In this second case, $\mathcal{L}_{\psi(vS(\zeta v)+\zeta vS(v))}$ is geometrically nontrivial (its $\mathsf{Swan}_\infty$ is the coprime to $p$ degree of $vS(\zeta v) + \zeta vS(v))$ and the sum over $v$ is $O((\#L)^{1/2})$. Thus the contribution of the content is $\#(\mu_{total}(R) \cap \mu_{total}(S))$.

In the case $n = 1$, we are done. To treat the case $n \geq 2$, it remains to show that the sum of $\psi_L(vS(uv) + uvS(v))$ over the curve $\mathcal{C}$ defined by

$$\frac{1}{c(u)} \sum_{i=1}^{n} a_i(u^{q_i - 1} + 1)v^{q_i - q_1} = 0$$

is $O((\#L)^{1/2})$.

Because $n \geq 2$, we may choose $\zeta$ with $\zeta^{q_n - 1} + 1 = 0$ but $\zeta$ not in $\mu_{total}(R)$. Then from Lemma 12.1.4 and Remark 12.1.5, we know that at the point $\mathcal{P} := (\zeta, \infty)$, the function $u - \zeta$ has a zero of order $q_n - q_1$. We must show that $\mathcal{L}_{\psi\left(\sum_{i=1}^{m} u(u^{Q_i-1}+1)b_i v^{1+Q_i}\right)}$ is geometrically nontrivial on $\mathcal{C}$. We will do this by showing that at the point $\mathcal{P}$, the function $\sum_{i=1}^{m} u(u^{Q_i - 1} +$

$1)b_iv^{1+Q_i}$ has a pole of order prime to $p$. Suppose first that $\zeta^{Q_m-1}+1 \neq 0$. Then the function $u(u^{Q_i-1}+1)$ is a unit at $\mathcal{P}$, and so the leading term has a pole of order $1+Q_m$, while all lower terms, if any, have poles of order $\leq 1+Q_{m-1} < 1+Q_m$.

Suppose next that $\zeta^{Q_m-1}+1=0$. Then the leading term has a pole of order $1+Q_m-q_n+q_1$ at $\mathcal{P}$. Notice that this pole order is prime to $p$ (either each of $Q_m, q_n, q_1$ is a strictly positive power of 1, or $p$ is odd, $q_1=1$, and each of $Q_m, q_n$ is a strictly positive power of $q$).

The lower terms, if $m \geq 2$, have poles of order $\leq 1+Q_{m-1}$. So it suffices to check that $1+Q_m-q_n+q_1 > 1+Q_{m-1}$, or equivalently that

$$Q_m - Q_{m-1} > q_m - q_1.$$

But $Q_{m-1} \leq (1/q)Q_m$, so $Q_m - Q_{m-1} \geq Q_m - (1/q)Q_m$, while $q_n - q_1 < q_n$. So it suffices to check that $Q_m(1-1/q) \geq q_n$, or equivalently $Q_m(1-1/q)/q_n \geq 1$. But $Q_m/q_n \geq q$, and trivially $q(1-1/q) = q-1 \geq 1$. So in this case as well, we have a pole of order prime to $p$. □

LEMMA 12.2.2. *Let $q = p^\nu > 1$ be a power of an odd prime $p$ and let $f(x)$ and $g(x)$ as in* (12.2.0.1) *and* (12.2.0.2), *with $q_i = q^{c_i}$ for $1 \leq i \leq n$, $Q_j = q^{d_j}$ for $1 \leq j \leq m$, and $k = \mathbb{F}_{p^\kappa}$ as in* (12.2.0.3). *Consider the two-parameter local system $\mathcal{F}$ on $\mathbb{A}^2/k$ of rank $Q_m = q^N$, whose trace function, at a point $(s,t) \in L^2$ for $L/k$ a finite extension, given by*

$$\mathrm{Trace}\big(\mathsf{Frob}_{(s,t),L}|\mathcal{F}\big) = \frac{-1}{\sqrt{\#L}} \sum_{x \in L} \psi_L(sx + tf(x) + g(x)).$$

*Suppose that for some $t \in k^\times$ we have*

$$\gcd(\Delta(x), x^{\kappa N}-1) = x-1, \tag{12.2.2.1}$$

*for*

$$\Delta(x) := \sum_{i=1}^{n} \big((ta_i)^{q^N} x^{N+c_i} + (ta_i)^{q^{N-c_i}} x^{N-c_i}\big) + \sum_{j=1}^{m} \big(b_j^{q^N} x^{d_j} + b_j^{q^{N-d_j}} x^{N-d_j}\big) \in k[x].$$

*Then $|\mathrm{Trace}\big(\mathsf{Frob}_{(0,t),\mathbb{F}_{q^{\kappa N}}}|\mathcal{F}\big)|^2 = q$.*

PROOF. We will follow the proof of Theorem 7.1.2 to compute the trace of $g := \mathsf{Frob}_{(0,t),\mathbb{F}_{q^{\kappa N}}}$ on $\mathcal{F}$ for the given $t \in k^\times$. Here, the relevant function $R(x)$ is

$$R(x) = t\sum_{i=1}^{n} a_i x^{q^{c_i}} + \sum_{j=1}^{m} b_j x^{q^{d_j}}.$$

Note that $\mathbb{F}_{q^{\kappa N}}$ contains $\mathbb{F}_{p^\kappa} = k$, so $t \in \mathbb{F}_{q^{\kappa N}}$. Now the corresponding subspace $W_R$ of $\mathbb{F}_{q^{\kappa N}}$ is the zero locus over $\mathbb{F}_{q^{\kappa N}}$ of the polynomial

$$\sum_{i=1}^{n} \big((ta_i)^{q^N} x^{q^{N+c_i}} + (ta_i)^{q^{N-c_i}} x^{q^{N-c_i}}\big) + \sum_{j=1}^{m} \big(b_j^{q^N} x^{q^{N+d_j}} + b_j^{q^{N-d_j}} x^{q^{N+d_j}}\big).$$

Denoting by $F$ the Frobenius map $x \mapsto x^q$ on $\overline{\mathbb{F}_q}$, we see that $W_R$ is the set of $x \in \overline{\mathbb{F}_q}$ that is annihilated by $F^{\kappa N}-1$ and by $\Delta(F)$, hence by $F-1$ because of (12.2.2.1). Thus $W_R = \mathbb{F}_q$. Now using Theorem 7.1.2(a) (and the fact that $q$ is odd), we conclude that $|\mathrm{Trace}(g)|^2 = \#W_R = q$. □

In Lemma 12.2.2, in the case $f(1) = \sum_{i=1}^{n} a_i \neq 0$ and $k \subseteq \mathbb{F}_q$, the natural choice for $t$ is $-\sum_{j=1}^{m} b_j / \sum_{i=1}^{n} a_i$ (since we want $\Delta(1) = 0$)).

Now we can prove a generalization of Theorem 12.1.7, which gives geometric monodromy groups of infinite series of (non-monomial if $n+m \geq 3$) local systems:

THEOREM 12.2.3. *Let $q = p^\nu > 1$ be a power of an odd prime $p$ and let $f(x) = xR(x)$ and $g(x) = xS(x)$ as in* (12.2.0.1) *and* (12.2.0.2), *with $q_i = q^{c_i}$ for $1 \leq i \leq n$, $Q_j = q^{d_j}$ for $1 \leq j \leq m$, and*

$$\gcd(c_1, \dots, c_n, d_1, \dots, d_m) = 1.$$

*Suppose that $Q_1 > q_1$, $Q_m > q_n$, and that $2|(c_1 \dots c_n d_1 \dots d_m)$. Consider the two-parameter local system $\mathcal{F}$ on $\mathbb{A}^2/k$ of rank $Q_m$, whose trace function, at a point $(s,t) \in L^2$ for $L/k$ a finite extension, given by*

$$\mathrm{Trace}\big(\mathsf{Frob}_{(s,t),L}|\mathcal{F}\big) = \frac{-1}{\sqrt{\#L}} \sum_{x \in L} \psi_L(sx + tf(x) + g(x))$$

*with geometric monodromy group $G = G_{\mathrm{geom}}$. Under the extra conditions that $p \nmid N$ for $N := d_m$, $q^N \neq 9$, and, in addition,* (12.2.2.1) *holds, we have $G = p_+^{1+2N\nu} \rtimes \mathrm{Sp}_{2N}(q)$.*

PROOF. First we note that when $N = 1$, both $f$ and $g$ are monomial, and hence we are done by Theorem 11.2.1(a). So in what follows we will assume $N > 1$. Since $q^N \neq 9$ and $1 < N$ is coprime to $p$, we now have that $q^N \geq 25$ and $q^N \neq 27$.

(a) Note that $\mu_{total}(R) \cap \mu_{total}(S) = \varnothing$ by Lemma 12.1.1. Hence by Theorem 12.2.1, $G$ has $M_{2,2} = 2$ on the underlying representation $V$ of dimension $Q_m = q^N$. Next, $\mathcal{F}$ is the specialization

$$t_1 = a_1 t,\ t_2 = a_2 t, \dots,\ t_n = a_n t,\ u_1 = b_1, \dots,\ u_m = b_m$$

of the local system $\mathcal{F}^\sharp$ on $(\mathbb{A}^{m+n} \times \mathbb{G}_m)/k$, $k/\mathbb{F}_q$ a finite extension, of rank $Q_m$, whose trace function, at a point

$$(s, t_1, \dots, t_n, u_1, \dots, u_m) \in L^{m+n} \times L^\times$$

for $L/k$ a finite extension, given by

$$\mathrm{Trace}\big(\mathsf{Frob}_{(s,t_1,\dots,t_n,u_1,\dots,u_m),L}|\mathcal{F}^\sharp\big) = \frac{-1}{\sqrt{\#L}} \sum_{x \in L} \psi_L\big(sx + \sum_{i=1}^{n} t_i x^{q^{c_i}+1} + \sum_{j=1}^{m} u_j x^{q^{d_j}+1}\big).$$

By Lemma 12.1.1(i), the condition $\mu_{total}(R) \cap \mu_{total}(S) = \varnothing$ is equivalent to $2|c_1 \dots c_n d_1 \dots d_m$. Hence by Corollary 11.2.5(ii), $\mathcal{F}^\sharp$ has geometric monodromy group $H = E \rtimes S$ with $E = p_+^{1+2N\nu}$ and $S \cong \mathrm{Sp}_{2N}(q)$. Moreover, by Corollary 2.3.8(ii), if we choose the clearing factor suitably, we can achieve that $\mathcal{F}^\sharp$ has trivial arithmetic determinant.

The aforementioned specialization implies that $G \leq H$. Note that

$$2 \leq M_{2,2}(EG) \leq M_{2,2}(G) = 2,$$

so $M_{2,2}(EG) = 2$. Since $E \lhd EG$, it follows from [**GT2**, Theorem 1.5] and [**BNRT**, Theorem 3] that $EG$ acts transitively on the $q^{2N}-1$ nonzero vectors of $E/\mathbf{Z}(E) \cong \mathbb{F}_p^{2N\nu}$. Now applying [**BNRT**, Theorem 5] and invoking the conditions $q^N \geq 25$ and $q^N \neq 27$, we see that there are some integers $b, e \geq 1$ such that $N\nu = be$ and

$$\mathrm{Sp}_{2b}(p^e) \lhd EG/E \leq \mathrm{Sp}_{2b}(p^e) \rtimes C_e \leq S = \mathrm{Sp}_{2N}(p^\nu).$$

Let $\varphi$ denote the $H$-character afforded by $V$. By Theorem 7.1.2(a), working over extensions $L$ that contain both $k$ and $\mathbb{F}_q$, we have that $|\varphi(h)|^2$ is 0 or a power of $q$ for any $h \in H$. On the other hand, choosing an element $g \in G$ such that the coset $Eg$ in $EG/E$ induces an element of $\mathrm{Sp}_{2b}(p^e)$ that has exactly $p^e$ fixed points on $\mathbb{F}_{p^e}^{2b}$, we see by Lemma 7.2.1 that the coset $Eg$ contains an element $g_1$ with $|\varphi(g_1)|^2 = p^e$. It follows that $\nu|e$. Writing $e = \nu e_1$ with $e_1 \in \mathbb{Z}_{\geq 1}$, we now have that $b = N/e_1$ and

$$\mathrm{Sp}_{2N/e_1}(q^{e_1}) \lhd EG/E \leq S = \mathrm{Sp}_{2N}(q).$$

Recall that $\mathrm{Sp}_{2N/e_1}(q^{e_1})$ is a standard subgroup of $S$, with normalizer $\mathrm{Sp}_{2N/e_1}(q^{e_1}) \rtimes C_{e_1}$ in $S$. It follows that

$$\mathrm{Sp}_{2N/e_1}(q^{e_1}) \lhd EG/E \leq \mathrm{Sp}_{2N/e_1}(q^{e_1}) \rtimes C_{e_1}.$$

We also have that $e_1$, being a divisor of $N$, is coprime to $p$. On the other hand, since $\mathcal{F}$ lives over $\mathbb{A}^2$, $G$ has no nontrivial $p'$-quotient. Hence $EG/E = \mathrm{Sp}_{2N/e_1}(q^{e_1})$, and so $EG = E \rtimes K$, for a suitable subgroup

$$K \cong \mathrm{Sp}_{2N/e_1}(q^{e_1})$$

of the subgroup $S$ of $H = E \rtimes S$.

(b) Next we show that $G = EK$. By the previous result, $EG$ acts transitively on the set of $q^{2N} - 1$ nontrivial elements of $E/\mathbf{Z}(E)$ (via conjugation), but $E$ centralizes $E/\mathbf{Z}(E)$. So $\mathbf{Z}(E)G$ acts transitively on these $q^{2N} - 1$ elements, and hence it acts irreducibly on $E/\mathbf{Z}(E)$. It follows that $\mathbf{Z}(E)G \cap E$ is either $\mathbf{Z}(E)$ or $E$. Suppose we are in the former case. Then $EG = EK$ implies that

$$K = EK/E = EG/E = E(\mathbf{Z}(E)G)/E \cong \mathbf{Z}(E)G/(\mathbf{Z}(E)G \cap E) = \mathbf{Z}(E)G/\mathbf{Z}(E).$$

As $K$ is perfect and $\mathbf{Z}(E) \leq \mathbf{Z}(\mathbf{Z}(E)G)$, $(\mathbf{Z}(E)G)^{(\infty)}$ is a central cover of $K$ and hence equal to $K$, since $\mathrm{Mult}(K) = 1$. Thus $K$ embeds in $\mathbf{Z}(E)G$ as a normal subgroup; in particular, $\mathbf{Z}(K) \cong C_2$ is normal and hence central in $\mathbf{Z}(E)G$. On the other hand, $\mathbf{Z}(E)G$ acts irreducibly and faithfully on $V$ of odd dimension $q^N$. So we see that the central involution $\boldsymbol{z}$ of $\mathbf{Z}(K)$ acts as scalar $-1$ on $V$, which is impossible since $\det(V)$ is trivial on the perfect group $K$. Hence we must be in the latter case, i.e. $\mathbf{Z}(E)G \geq E$, whence $\mathbf{Z}(E)G = EK$.

As $\mathbf{Z}(E) < E < \mathbf{Z}(E)G$, we can write $E = \mathbf{Z}(E)(E \cap G)$. Taking the derived subgroup, we get $\mathbf{Z}(E) = [E, E]$ is contained in $E \cap G$. Thus $G \geq \mathbf{Z}(E)$, and so $G = \mathbf{Z}(E)G = EK$.

(c) Recalling that $E = \mathbf{O}_p(G) \,\mathsf{char}\, G$ and $G$ is normal with cyclic quotient in the (necessarily finite by [**KT6**, Theorem 2.9]) arithmetic monodromy group $\tilde{G} := G_{\mathrm{arith},k}$ of $\mathcal{F}$ over $k = \mathbb{F}_{p^\kappa}$, we have

$$\tilde{G} \leq \mathbf{N}_{\mathrm{GL}(V)}(E) = \mathbf{Z}(\mathrm{GL}(V))E \cdot \mathrm{Sp}_{2N\nu}(p).$$

Here we assume that the clearing factor for $\mathcal{F}$ is the same one that makes the arithmetic determinant of $\mathcal{F}^\sharp$ trivial. As $E$ acts irreducibly on $V$, any element $z \in \mathbf{C}_{\tilde{G}}(E)$ acts as a scalar $\zeta$ on $V$ which is a root of unity, and its trace is in $\mathbb{Q}(\zeta_p)$. It follows that $\zeta = \epsilon\zeta_p^j$ for some $0 \leq j \leq p-1$ and $\epsilon = \pm 1$. But the arithmetic determinant of $\mathcal{F}^\sharp$ is trivial and the rank is $D = q^N$, we must have that $\epsilon = 1$ and hence $z \in \mathbf{Z}(E)$. This argument shows that $\tilde{G}/E$ embeds in the subgroup $\mathrm{Sp}_{2N\nu}(p)$ of outer automorphisms of $E$ induced by $\mathbf{N}_{\mathrm{GL}(V)}(E)$. It follows that

$$K = \mathrm{Sp}_{2N/e_1}(q^{e_1}) = G/E \lhd \tilde{G}/E \leq \mathrm{Sp}_{2N\nu}(p).$$

As the normalizer in $\mathrm{Sp}_{2N\nu}(p)$ of the standard subgroup $K$ is $K \rtimes C_{\nu e_1}$, we conclude that $\tilde{G}/G \hookrightarrow C_{\nu e_1}$. In particular, $G = G_{\mathrm{arith},\mathbb{F}_{q^{N\kappa}}}$.

Now, assuming (12.2.2.1), we can use Lemma 12.2.2 to get an element $g_2 = \mathsf{Frob}_{(0,t),\mathbb{F}_{q^{N\kappa}}} \in G$ with $|\varphi(g_2)|^2 = q$. On the other hand, Lemma 7.2.1 guarantees that $|\varphi(g_2)|^2$ is either 0 or a power of $q^{e_1}$. Hence $e_1 = 1$, $K = S$, and $G = ES$ as stated. □

Example 12.2.4. We offer some examples of non-monomial systems to which Theorem 12.2.3 applies. Let $a, b \in \mathbb{F}_p^\times$ and $q = p^\nu$.

(i) Let $1 \leq l < N$, and consider $\mathcal{F}$ as in Theorem 12.2.3, with $R(x) = ax + bx^{q^l}$ and $g(x) = x^{q^N}$. Assume in addition that $a + b \neq 0$, $p \nmid N$ and $\gcd(l, N) = 1$. Choose $t = -1/(a+b) \neq 0$. Modulo $x^N - 1$, the polynomial $\Delta(x)$ is $tb(x^{N-l} + x^l - 2)$, which in turn reduces to $tb(x^l - 1)^2$. The assumptions imply that $\gcd((x^l-1)^2, x^N - 1) = x - 1$, and so Theorem 12.2.3 applies to show that $G_{\mathrm{geom}} = p_+^{1+2N\nu} \rtimes \mathrm{Sp}_{2N}(q)$.

(ii) Assume $1 \leq l < N/2$, and consider $\mathcal{F}$ as in Theorem 12.2.3, with $R(x) = ax^{q^l} + bx^{q^{N-l}}$ and $g(x) = x^{q^N}$. Assume in addition that $a + b \neq 0$, $p \nmid N$ and $\gcd(l, N) = 1$. Again choose $t = -1/(a+b) \neq 0$. Modulo $x^N - 1$, the polynomial $\Delta(x)$ is $x^{N-l} + x^l - 2$, which in turn reduces to $(x^l - 1)^2$. The assumptions again imply that $\gcd((x^l-1)^2, x^N - 1) = x - 1$, and so Theorem 12.2.3 applies to show that $G_{\mathrm{geom}} = p_+^{1+2N\nu} \rtimes \mathrm{Sp}_{2N}(q)$.

(iii) Assume $1 \leq l < N/2$, and consider $\mathcal{F}$ as in Theorem 12.2.3, with $R(x) = a(x^{q^l} - x)$ and $g(x) = b(x^{q^N} - x^{q^{N-l}})$. Assume in addition that $p \nmid N$ and $\gcd(l, N) = 1$. Choose $t \in \mathbb{F}_p^\times$ such that $ta \neq b$. Modulo $x^N - 1$, the polynomial $\Delta(x)$ is $(ta-b)(x^{N-l} + x^l - 2)$, which in turn reduces to $(ta - b)(x^l - 1)^2$. The assumptions again imply that $\gcd((x^l-1)^2, x^N - 1) = x - 1$, and so Theorem 12.2.3 applies to show that $G_{\mathrm{geom}} = p_+^{1+2N\nu} \rtimes \mathrm{Sp}_{2N}(q)$.

Now we prove a Witt analogue of Theorem 12.2.1:

Theorem 12.2.5. *Suppose that $p = 2$ and $Q_m > q_n$. Consider the two-parameter local system $\mathcal{F}$ on $\mathbb{A}^2/k$ of rank $Q_m$, whose trace function, at a point $(s,t) \in L^2$ for $L/k$ a finite extension, given by*

$$\mathrm{Trace}\big(\mathsf{Frob}_{(s,t),L}|\mathcal{F}\big) = \frac{-1}{\sqrt{\#L}} \sum_{x \in L} \psi_{2,L}\big([x, sx + tf(x) + g(x)]\big),$$

*with $f(x) = xR(x)$ and $g(x) = xS(x)$ as in* (12.2.0.1) *and* (12.2.0.2). *Then*

$$M_{2,2}(\mathcal{F}) = 2.$$

Proof. Just as in the proof of Theorem 12.1.8, $M_{2,2} - 2$ is the large $L$ limit of the sum

$$\Sigma(L) := \frac{1}{\#L} \sum_{\substack{v,t \in L^\times \\ vR(t)+tR(v)=0}} \psi_L(vt + vS(t) + tS(v)).$$

Because $vt \neq 0$, we may make the change of variables $t = uv$, and we are looking at

$$\Sigma(L) = \frac{1}{\#L} \sum_{\substack{v,u \in L^\times \\ vR(uv)+uvR(v)=0}} \psi_L(uv^2 + vS(uv) + uvS(v)).$$

The content of $R(uv)/(uv^{q_1}) + R(v)/v^{q_1}$ contributes 0 to the large $L$ limit, because for any fixed $\zeta \neq 0$, the polynomial in $\overline{\mathbb{F}_2}[v]$ given by $\zeta v^2 + vS(\zeta v) + \zeta v S(v)$ is Artin-Schreier nontrivial, being equivalent to

$$\sqrt{\zeta}v + \text{ a polynomial, possibly zero, with all nonzero monomials of odd degree } \geq 3.$$

In the case $n = 1$, we are done. If $n \geq 2$, it suffices to show that $\mathcal{L}_{\psi\left(uv^2+vS(uv)+uvS(v)\right)}$ on $\mathcal{C}$ is geometrically nontrivial, so that its $H^2_c$ vanishes and $M_{2,2} = 2$. For this, we pick $\zeta$ with $\zeta^{q_n - 1} + 1 = 0$ but $\zeta$ not in $\mu_{total}(R)$. By Lemma 12.1.4 and Remark 12.1.5, at the point $\mathcal{P} := (\zeta, \infty)$, $v$ has a simple pole and the function $u - \zeta$ has a zero of order $q_n - q_1$ at $\mathcal{P}$. We again examine the poles of

$$uv^2 + vS(uv) + uvS(v) = uv^2 + \sum_{i=1}^{m} u(u^{Q_i - 1} + 1) b_i v^{Q_i + 1}$$

at the point $\mathcal{P}$. We will show that this function has a pole of order prime to $p$ at the point $\mathcal{P}$, which implies the needed geometric nontriviality.

At $\mathcal{P}$, the leading term $u(u^{Q_m - 1} + 1) b_m v^{Q_m + 1}$ either has a pole of order $Q_m + 1$, or a pole of order $Q_m + 1 - (q_n - q_1)$, and the lower terms, if $m \geq 2$ have poles of order $\leq 1 + Q_{m-1}$ (including the first term $uv^2$, with a pole of order $\leq 2 < 1 + Q_{m-1}$). If $m = 1$, the $uv^2$ term at $\mathcal{P}$ is Artin-Schreier equivalent to $\sqrt{\zeta}v +$ holomorphic. In the $m \geq 2$ case, we observe that $Q_m + 1 - (q_n - q_1) > 1 + Q_{m-1}$, exactly as at the end of the proof of Theorem 12.2.1. In the $m = 1$ case, we simply need $Q_m + 1 - (q_n - q_1) > 1$, which is obvious. □

Now we offer some Witt analogue of Theorem 12.2.3, which determines the geometric monodromy group of some local systems with non-monomial Witt vectors:

THEOREM 12.2.6. *Let $q = 2^f$, $n > m \geq 1$, $\gcd(n, m) = 1$, $a, b \in \mathbb{F}_q^\times$, and consider the local system $\mathcal{W}$ on $(\mathbb{A}^1)^2 \times \mathbb{G}_m$ with the trace function*

$$(r, s, t) \in L^2 \times L^\times \mapsto \sum_{x \in L} \psi_{2,L}\big([rx, sx + t(ax^{q^m+1} + bx^{q^n+1})]\big)$$

*for any finite extension $L/\mathbb{F}_q$. Then $\mathcal{W}$ has geometric monodromy group $G = (4 * 2^{1+2nf}_+) \cdot \mathrm{Sp}_{2n}(q)$.*

PROOF. Note that $\mathcal{F}$ is a specialization of the local system $\mathcal{W}^*(q^n + 1, q^m + 1, 1)$ in Theorem 9.3.9, with geometric monodromy group $H = R \cdot S$, where $R = 4 * 2^{1+2nf}_+$ and $S \cong \mathrm{Sp}_{2n}(q)$. It follows that $G \leq H$.

We now compute $G_{\mathrm{geom}}$ for a suitable pullback.

Rescaling $t$ by $t \mapsto t/b$, we reduce to the case $b = 1$. Then the $(r, s, t) \mapsto (r, s, t^{q^n+1})$ partial Kummer pullback of $\mathcal{F}$ has trace function

$$(r, s, t) \mapsto \sum_{x \in L} \psi_{2,L}\big([rx, sx + t^{q^n+1}(ax^{q^m+1} + x^{q^n+1})]\big),$$

which after the variable change $x \mapsto x/t$ becomes

$$(r, s, t) \mapsto \sum_{x \in L} \psi_{2,L}\big([rx/t, sx/t + t^{q^n - q^m} a x^{q^m+1} + x^{q^n+1}]\big).$$

Pulling back by the automorphism $(r,s,t) \mapsto (rt, st, t)$, the trace function becomes

$$(r,s,t) \mapsto \sum_{x \in L} \psi_{2,L}\big([rx, sx + t^{q^n - q^m} a x^{q^m+1} + x^{q^n+1}]\big).$$

This is the pullback, by the universal homeomorphism $(r,s,t) \mapsto (r,s,t^{q^m})$, of the local system whose trace function is

$$(r,s,t) \mapsto \sum_{x \in L} \psi_{2,L}\big([rx, sx + t^{q^{n-m}-1} a x^{q^m+1} + x^{q^n+1}]\big).$$

This is the $(r,s,t) \mapsto (r,s,t^{q^{n-m}-1})$ partial Kummer pullback of the local system whose trace function is

$$(r,s,t) \mapsto \sum_{x \in L} \psi_{2,L}\big([rx, sx + tax^{q^m+1} + x^{q^n+1}]\big),$$

which in turn is the pullback by the automorphism $(r,s,t) \mapsto (r,s,ta)$ of $\mathcal{W}(q^n+1, q^m+1, 1)$. By Theorem 9.3.9, $\mathcal{W}(q^n+1, q^m+1, 1)$ has geometric monodromy group $\cong H$. Thus $G$ contains a subgroup isomorphic to $H$, and hence $G = H$. $\square$

## 12.3. Local systems of the third kind

THEOREM 12.3.1. *Let $p > 2$, $k/\mathbb{F}_p$ a finite extension, and $a, b \in k^\times$. Consider the local system $\mathcal{F}$ on $(\mathbb{A}^1 \times \mathbb{G}_m)/k$ of rank $q = p^f$, whose trace function, at a point $(s,t) \in L \times L^\times$ for $L/k$ a finite extension, given by*

$$\mathrm{Trace}\big(\mathsf{Frob}_{(s,t),L}|\mathcal{F}\big) = \frac{-1}{\sqrt{\#L}} \sum_{x \in L} \psi_L(sx^2 + t(ax + bx^{q+1})).$$

*Then $M_{2,2}(\mathcal{F}) = 2$.*

PROOF. Define $\Sigma_m := x^m + y^m - z^m - w^m$ for any $m \in \mathbb{Z}_{\geq 1}$. First for any fixed $c \in L$ we show that

$$\#\{(x,y,z,w) \in L^4 \mid \Sigma_1 = c,\ \Sigma_2 = 0\} = \begin{cases} \#L(2\#L-1), & \text{if } c = 0, \\ \#L^2, & \text{if } c \neq 0. \end{cases} \tag{12.3.1.1}$$

Indeed, we can write $x = w + (z - y + c)$. Then $\Sigma_2 = 0$ yields

$$2w(z-y+c) + (z-y+c)^2 + y^2 - z^2 = 0.$$

Now, if $y \neq z + c$, then this equation completely determines $w$ (and $z$) in terms of $z$ and $y \neq z + c$, giving us $\#L^2 - \#L$ points. If $y = z + c$, then $z^2 = (z+c)^2$, i.e. $2cz + c^2 = 0$. If $c = 0$, there are no extra constraints aside from $y = z$, $x = w$, and so we get $\#L^2$ points. If $c \neq 0$, then $z = -c/2$, $y = c/2$, $x = w$, yielding $\#L$ points.

In particular, the quadric $\Sigma_2 = 0$ has

$$\#L(2\#L-1) + \#L^2(\#L-1) = \#L^3 + \#L^2 - \#L \tag{12.3.1.2}$$

points. [Here is another proof for the asymptotical bound $(1+o(1))\#L^3$. This quadric is the covering of the $(y,z,w)$-space $\mathbb{A}^3$ defined by taking the square root of $-y^2+z^2+w^2$, which is not a square. So the problematic cohomology group in question is the direct sum of

$$H^6_c(\mathbb{A}^3, \mathbb{Q}_\ell) \oplus H^6_c(\mathbb{A}^3, \mathcal{L}_{\chi_2(-y^2-z^2-w^2)}).$$

The first summand gives $\#L^3$, the second vanishes because $\mathcal{L}_{\chi_2(-y^2-z^2-w^2)}$ is geometrically nontrivial.]

As in the proof of Theorem 12.1.3, we have that $M_{2,2}$ is the large $L$ limit of the sums

$$\frac{1}{(\#L)^3(\#L-1)}\sum_{s\in L, t\in L^\times}\sum_{x,y,z,w\in L}\psi_L\big(s\Sigma_2+t(a\Sigma_1+b\Sigma_{q+1})\big),$$

where $\Sigma_m := x^m+y^m-z^m-w^m$ for any $m\in\mathbb{Z}_{\geq 1}$. The "missing" sums, over $(s,0)$, are just

$$\frac{1}{(\#L)^2(\#L-1)}\#\{(x,y,z,w)\in L^4 \mid \Sigma_2=0\}=\frac{\#L+1-1/\#L}{\#L-1}$$

by (12.3.1.2), with large $L$ limit 1. So $M_{2,2}+1$ is the large $L$ limit of the sums, but now extended over all $(s,t)\in L^2$. The large $L$ limit is unchanged if we replace the $1/((\#L)^3(\#L-1))$ factor by $1/(\#L)^4$. Thus $M_{2,2}+1$ is the large $L$ limit of

$$\frac{1}{(\#L)^2}\#\{(x,y,z,w)\in L^4 \mid \Sigma_2=0 \text{ and } a\Sigma_1+b\Sigma_{q+1}=0\}.$$

Let us denote the locus defined by these two equations $\Sigma_2=0$ and $a\Sigma_1+b\Sigma_{q+1}=0$ in the $(x,y,z,w)$-space $\mathbb{A}^4$ by $H$, and its set of points over $L$ by $H(L)$.

First we look at the intersection of $H(L)$ with the hyperplane $\Sigma_1=0$. Using (12.3.1.1) with $c=0$, we see that this intersection contributes at most 2 to the large $L$ limit.

Next, we look at the intersection of $H(L)$ with the complement $\Sigma_1\neq 0$. For any point $(x,y,z,w)$ in this intersection, we have $c:=x+y-z-w\neq 0$, so this point is $c(x_0,y_0,z_0,w_0)$ with

$$(x_0,y_0,z_0,w_0)\in H_1(L):=\{(x,y,z,w)\in L^4 \mid \Sigma_1=1,\ \Sigma_2=0\}.$$

The condition $a\Sigma_1+b\Sigma_{q+1}=0$ now becomes

$$ac+bc^{q+1}\big(x_0^{q+1}+y_0^{q+1}-z_0^{q+1}-w_0^{q+1}\big)=0.$$

Since $a,b,c\neq 0$, we must have that $x_0^{q+1}+y_0^{q+1}-z_0^{q+1}-w_0^{q+1}\neq 0$, and

$$c=\big(-a^{-1}b(x_0^{q+1}+y_0^{q+1}-z_0^{q+1}-w_0^{q+1})\big)^{-1/q}.$$

Thus $c$ is uniquely determined by the point $(x_0,y_0,z_0,w_0)\in H_1(L)$. We have shown that the ray defined by each point $(x_0,y_0,z_0,w_0)\in H_1(L)$ contains at most one point $(x,y,z,w)$ in $H(L)\cap\{\Sigma_1\neq 0\}$. Since $\#H_1(L)=\#L^2$ by (12.3.1.1), $H(L)\cap\{\Sigma_1\neq 0\}$ contains at most $\#L^2$ points, contributing at most 1 to the large $L$ limit. Hence $M_{2,2}+1\leq 3$. Since $M_{2,2}\geq 2$, we conclude that $M_{2,2}=2$. □

To generalize Theorem 12.3.1 from $x^2$ to $x^{q+1}$, we begin with an identity which will be used to calculate $M_{2,2}$. We consider the identities

$$x+y=z+w,\quad x^{1+q}+y^{1+q}=z^{1+q}+w^{1+q}.$$

We substitute $w=x+y-z$ into the second, to obtain

$$x^{1+q}+y^{1+q}-z^{1+q}=(x+y-z)^{1+q}.$$

For the $p=2$ case of the following lemma, cf. [**JW**, Theorem 4].

Lemma 12.3.2. *Let $p$ be a prime, $q \geq 1$ a power of $p$. If $q > 1$, then in $\mathbb{F}_{q^2}[x, y, z]$, we have the identity*

$$x^{1+q} + y^{1+q} - z^{1+q} - (x + y - z)^{1+q} = -(y - z) \prod_{A \in \mathbb{F}_{q^2},\ A^q = -A} (x + Ay - (A + 1)z).$$

*If $p$ is odd and $q = 1$, then in $\mathbb{F}_p[x, y, z]$, we have the identity*

$$x^{1+q} + y^{1+q} - z^{1+q} - (x + y - z)^{1+q} = -2(y - z)(x - z).$$

*In the special case $p = 2, q > 1$, we get the identity in $\mathbb{F}_q[x, y, z]$*

$$x^{1+q} + y^{1+q} - z^{1+q} - (x + y - z)^{1+q} = -(y - z) \prod_{A \in \mathbb{F}_q} (x + Ay - (A + 1)z).$$

Proof. In the case $p = 2$, the condition that $A \in \mathbb{F}_{q^2}$ satisfies $A^q = -A$ is just the condition that $\alpha \in \mathbb{F}_q$.

Suppose now that $p$ is odd. The $q = 1$ case is left to the reader. In the $q > 1$ case, we use the identity

$$\prod_{A \in \mathbb{F}_{q^2},\ A^q = -A} (T + A) = T^q + T.$$

Then we see that

$$\begin{aligned}\prod_{A \in \mathbb{F}_{q^2},\ A^q = -A} (x + Ay - (A + 1)z) &= \prod_{A \in \mathbb{F}_{q^2},\ A^q = -A} ((x - z) + A(y - z)) \\ &= (y - z)^q \prod_{A \in \mathbb{F}_{q^2},\ A^q = -A} ((x - z)/(y - z) + A) \\ &= (y - z)^q((x - z)^q/(y - z)^q + ((x - z)/(y - z)) \\ &= (x - z)^q + (y - z)^{q-1}(x - z).\end{aligned}$$

Thus

$$\begin{aligned}-(y - z) \prod_{A \in \mathbb{F}_{q^2},\ A^q = -A} (x + Ay - (A + 1)z) &= -(y - z)(x - z)^q - (y - z)^q(x - z) \\ &= -(y - z)(x^q - z^q) - (y^q - z^q)(x - z) \\ &= -yx^q + yz^q + zx^q - z^{q+1} - xy^q + zy^q + xz^q - z^{q+1}.\end{aligned}$$

But

$$\begin{aligned}x^{1+q} + y^{1+q} - z^{1+q} - (x + y - z)^{1+q} &= x^{1+q} + y^{1+q} - z^{1+q} - (x + y - z)(x^q + y^q - z^q) \\ &= -xy^q + xz^q - yx^q + yz^q + zx^q + zy^q - 2z^{1+q}.\end{aligned}$$

□

Corollary 12.3.3. *Let $q$ be a power of an odd prime $p$, let $0 \leq m \neq n$ be integers with* $\gcd(m, n) = 1$, *and let $Q_1 := q^m$, $Q_2 := q^n$. Suppose that $2|mn$. Then in $\overline{\mathbb{F}_p}[x, y, z]$, where each of*

$$f_{Q_1} := x^{1+Q_1} + y^{1+Q_1} - z^{1+Q_1} - (x + y - z)^{1+Q_1},\ f_{Q_2} := x^{1+Q_2} + y^{1+Q_2} - z^{1+Q_2} - (x + y - z)^{1+Q_2}$$

*is a product of pairwise distinct linear factors, their only factors in common are $y-z$ and $x-z$.*

Proof. If both $A^{q^m} = -A$ and $A^{q^n} = -A$ but $A \neq 0$, then $A^{q^m-1} = -1 = A^{q^n-1}$, which is impossible when $2|mn$ and $\gcd(m,n) = 1$, by Lemma 12.1.1(i). □

Theorem 12.3.4. *Let $q = p^f$ be a power of an odd prime, and let $m, n \in \mathbb{Z}_{\geq 0}$ be such that $m \neq n$, $\gcd(m,n) = 1$ and $2|mn$. Let $k/\mathbb{F}_p$ be a finite extension, and fix $a, b \in k^\times$. If $m < n$, consider the local system on $(\mathbb{A}^1 \times \mathbb{G}_m)/k$ whose trace function is given, for $L/k$ a finite extension and $s \in L, t \in L^\times$, by*

$$(12.3.4.1) \qquad (s,t) \mapsto \frac{1}{\mathsf{Gauss}_L} \sum_{x \in L} \psi_L\big(sx^{q^m+1} + t(ax + bx^{q^n+1})\big),$$

*If $m > n$, consider the local system on $(\mathbb{A}^1 \times \mathbb{G}_m)/k$ whose trace function is given, for $L/k$ a fintie extension and $s \in L, t \in L^\times$, by*

$$(12.3.4.2) \qquad (s,t) \mapsto \frac{1}{\mathsf{Gauss}_L} \sum_{x \in L} \psi_L\big(s(ax + bx^{q^n+1}) + tx^{q^m+1}\big).$$

*Each of these local systems has $M_{2,2} = 2$.*

Proof. We follow the proof of Theorem 12.3.1. Our first task is to show that the "missing sums" over $s \in L,\ t = 0$ in the $L$-approximation of $M_{2,2}$ contribute 1. Its contribution is the large $L$ limit of

$$\frac{1}{(\#L)^3(\#L-1)} \sum_{s \in L} \sum_{(x,y,z,w) \in L^4} \psi_L\big(s\Sigma_{q^m+1}(x,y,z,w)\big)$$

for the first local system, and the large $L$ limit of

$$\frac{1}{(\#L)^3(\#L-1)} \sum_{s \in L} \sum_{(x,y,z,w) \in L^4} \psi_L\big(s(a\Sigma_1(x,y,z,w) + b\Sigma_{q^n+1}(x,y,z,w))\big)$$

for the second local system.

In both of these sums, the $s = 0$ term is

$$\frac{(\#L)^4}{(\#L)^3(\#L-1)},$$

whose large $L$ limit is 1. The key observation now is that both of the polynomials $\Sigma_{q^m+1}(x,y,z,w)$ and $a\Sigma_1(x,y,z,w) + b\Sigma_{q^n+1}(x,y,z,w)$ are Deligne polynomials in four variables, cf. [**De2**, 8.4], of degrees $q^m+1$ and $q^n+1$ respectively. So for all $s \in L^\times$, we have the estimates

$$\Big|\sum_{(x,y,z,w) \in L^4} \psi_L\big(s\Sigma_{q^m+1}(x,y,z,w)\big)\Big| \leq q^{4m}(\#L)^2,$$

$$\Big|\sum_{(x,y,z,w) \in L^4} \psi_L\big(s(a\Sigma_1(x,y,z,w) + b\Sigma_{q^n+1}(x,y,z,w))\big)\Big| \leq q^{4n}(\#L)^2.$$

Then in each case the entire sum over $s \in L^\times$ of these Deligne polynomial summands is $O((\#L)^3)$, so contributes 0 to the large $L$ limit.

Exactly as in the previous proofs, $M_{2,2}+1$ is the number of geometrically irreducible components highest dimension 2 in the affine scheme $H$ in $\mathbb{A}^4$ defined by the two equations

$$a\Sigma_1 + b\Sigma_{Q_1+1} = 0,\ \Sigma_{Q_2+1} = 0,$$

where

$$Q_1 := q^n, \quad Q_2 := q^m.$$

We first show that $H_0 := H \cap (\Sigma_1 = 0)$ has $\#H_0(L) = 2(\#L)^2 + O(\#L)$. Indeed, here we are looking at the affine scheme $H_0$ in $\mathbb{A}^3$ defined by the two equations

$$f_{Q_1} = 0,\ f_{Q_2} = 0.$$

By Lemma 12.3.2 and Corollary 12.3.3, this locus is the union of the two planes $y = z$ and $x = z$, and at most $Q_1Q_2$ lines.

It remains to show that $H \smallsetminus H_0$ has $(\#L)^2 + O(\#L)$ points with values in each $L/\mathbb{F}_p$. Consider first, for each $c \in L$, the scheme $V_c$ in $\mathbb{A}^4$ defined by the two equations

$$\Sigma_1 = c,\ \Sigma_{Q_2+1} = 0.$$

We first show that $\#V_c(L) = (\#L)^2+O(\#L)$ for each $c \in L^\times$. To see this, first notice that by homothety, all the $V_c$ with $c \neq 0$ are isomorphic to each other. But the $V_c(L)$ with $c \in L$ form a partition of the $L$-points on the hypersurface $\Sigma_{Q_2+1} = 0$. This affine hypersurface, call it $X$, is the affine cone in $\mathbb{A}^4$ over a smooth hypersurface in $\mathbb{P}^3$. Hence $\#X(L) = (\#L)^3+O((\#L)^2)$. Thus

$$\#X(L) = \#V_0(L) + (\#L - 1)\#V_1(L).$$

By the factorization lemma 12.3.2 for $\mathbb{F}_{Q_2}$, we see that $\#V_0(L) \leq (Q_2 + 1)(\#L)^2$. Thus we have

$$(\#L - 1)\#V_1(L) = (\#L)^3 + O((\#L)^2),\ \text{hence } \#V_1(L) = (\#L)^2 + O(\#L).$$

Now partition the $L$-points of $H \smallsetminus H_0$ into the $L$-points of the subschemes $H_c := H \cap (\Sigma_1 = c)$ for $c \in L^\times$. Fix $c \in L^\times$. If $H_c(L)$ is non-empty, and $(x, y, z, w) \in H_c(L)$, then write $(x, y, z, w) = c(x_0, y_0, z_0, w_0)$. Then the point $P := (x_0, y_0, z_0, w_0)$ has $\Sigma_1(P) = 1$, $\Sigma_{Q_2+1}(P) = 0$, and

$$ac + bc^{Q_1+1}\Sigma_{Q_1+1}(P) = 0.$$

Since $a, b, c \neq 0$, $c$ is completely determined by $P$:

$$c^{Q_1} = -a/b\Sigma_{Q_1+1}(P).$$

This construction maps each nonempty $H_c(L)$ injectively to $V_1(L)$, where the images of two different non-empty $H_{c_1}(L)$ and $H_{c_2}(L)$ with $c_1 \neq c_2$, both nonzero, are disjoint in $V_1(L)$. In other words, we have a bijection between $H \smallsetminus H_0$ with the open set of $V_1$ on which $\Sigma_{Q_1+1}$ is invertible. So

$$\#(H \smallsetminus H_0)(L) \leq (\#L)^2 + O(\#L).$$

So we have shown that $M_{2,2} + 1 \leq 3$. Since $M_{2,2} \geq 2$ for any local system of rank $> 1$, it follows that $M_{2,2} = 2$. □

THEOREM 12.3.5. *Let $q = p^f > 9$ be a power of a prime $p > 2$ and fix some constants $a, b \in \mathbb{F}_q^\times$. Consider the local system $\mathcal{F}_1$ on $(\mathbb{A}^1 \times \mathbb{G}_m)/k$, $k/\mathbb{F}_q$ a finite extension, of rank $q$, whose trace function, at a point $(s,t) \in L \times L^\times$ for $L/k$ a finite extension, given by*

$$\mathrm{Trace}\big(\mathsf{Frob}_{(s,t),L}|\mathcal{F}\big) = \frac{1}{\mathsf{Gauss}_L}\sum_{x \in L} \psi_L\big(sx^2 + t(ax + bx^{q+1})\big),$$

*and the local system $\mathcal{F}_2$ on $(\mathbb{A}^1 \times \mathbb{G}_m)/k$, $k/\mathbb{F}_q$ a finite extension, of rank $q$, whose trace function, at a point $(s,t) \in L \times L^\times$ for $L/k$ a finite extension, given by*

$$\mathrm{Trace}\big(\mathsf{Frob}_{(s,t),L}|\mathcal{F}\big) = \frac{1}{\mathsf{Gauss}_L}\sum_{x \in L} \psi_L\big(s(ax + bx^2) + tx^{q+1}\big).$$

*Then the geometric monodromy groups of $\mathcal{F}_1$ and $\mathcal{F}_2$ are both equal to $G = E \rtimes \mathrm{Sp}_2(q)$, where $E = p_+^{1+2f}$ is extraspecial of order $p^{1+2f}$ and exponent $p$.*

PROOF. For each of the two systems and with $q = 11$, a Magma computation shows that, for any choice of $a, b \in \mathbb{F}_{11}^\times$, there is a Frobenius $\mathsf{Frob}_{(s,t),\mathbb{F}_{11^4}}$ that has trace of absolute value $\sqrt{11}$. Now we can repeat the proof of Theorem 12.1.7 verbatim. □

Next we extend Theorem 12.3.5:

THEOREM 12.3.6. *Let $p > 2$ be a prime, $q = p^\nu$, $m, n \in \mathbb{Z}_{\geq 0}$ with $m \neq n$, $\gcd(m,n) = 1$, $2|mn$, and let $\mathcal{F}$ be any of the sheaves defined in* (12.3.4.1) *and* (12.3.4.2)*. Then the geometric monodromy group $G = G_{\mathrm{geom},\mathcal{F}}$ of $\mathcal{F}$ is $E \rtimes \mathrm{Sp}_{2N}(q)$, where $N = \max(m,n)$ and $E = p_+^{1+2Nv}$ is the extraspecial $p$-group of exponent $p$ and order $pq^{2N}$.*

PROOF. (a) When $m < n$, $\mathcal{F}$ is the specialization

$$t_1 = at,\ t_2 = s,\ t_3 = bt$$

of the local system $\mathcal{F}^\sharp$ on $(\mathbb{A}^2 \times \mathbb{G}_m)/k$, $k/\mathbb{F}_q$ a finite extension, of rank $D$, whose trace function, at a point $(t_1, t_2, t_3) \in L^2 \times L^\times$ for $L/k$ a finite extension, given by

$$\mathrm{Trace}\big(\mathsf{Frob}_{(t_1,t_2,t_3),L}|\mathcal{F}^\sharp\big) = \frac{1}{\mathsf{Gauss}_L}\sum_{x \in L} \psi_L\big(t_1x + t_2x^{q^m+1} + t_3x^{q^n+1}\big).$$

When $n < m$, $\mathcal{F}$ is the specialization

$$t_1 = as,\ t_2 = bs,\ t_3 = t$$

of the local system $\mathcal{F}^\sharp$ on $(\mathbb{A}^2 \times \mathbb{G}_m)/k$, $k/\mathbb{F}_q$ a finite extension, of rank $D$, whose trace function, at a point $(t_1, t_2, t_3) \in L^2 \times L^\times$ for $L/k$ a finite extension, given by

$$\mathrm{Trace}\big(\mathsf{Frob}_{(t_1,t_2,t_3),L}|\mathcal{F}^\sharp\big) = \frac{1}{\mathsf{Gauss}_L}\sum_{x \in L} \psi_L\big(t_1x + t_2x^{q^n+1} + t_3x^{q^m+1}\big).$$

Since $\gcd(m,n) = 1$ and $2|mn$, by Corollary 11.2.5(ii), $\mathcal{F}^\sharp$ has geometric monodromy group $H = E \rtimes S$ with $E = p_+^{1+2N\nu}$ and $S \cong \mathrm{Sp}_{2N}(q)$.

The aforementioned specialization implies that $G \leq H$.

(b) Assume now that $m < n$. The idea is to compute $G_{\mathrm{geom}}$ for a suitable pullback.

Rescaling $t$ in (12.3.4.1) by $t \mapsto t/b$, we reduce to the case $b = 1$. Then the $(s,t) \mapsto (s, t^{q^n+1})$ partial Kummer pullback of $\mathcal{F}$ has trace function

$$(s,t) \mapsto \frac{1}{\mathsf{Gauss}_L} \sum_{x \in L} \psi_L\big(sx^{q^m+1} + t^{q^n+1}(ax + x^{q^n+1})\big),$$

which after the variable change $x \mapsto x/t$ becomes

$$(s,t) \mapsto \frac{1}{\mathsf{Gauss}_L} \sum_{x \in L} \psi_L\big(st^{-(q^m+1)}x^{q^m+1} + t^{q^n}ax + x^{q^n+1}\big).$$

Pulling back by the automorphism $(s,t) \mapsto (st^{q^m+1}, t)$, the trace function becomes

$$(s,t) \mapsto \frac{1}{\mathsf{Gauss}_L} \sum_{x \in L} \psi_L\big(sx^{q^m+1} + t^{q^n}ax + x^{q^n+1}\big).$$

This is the pullback, by the universal homeomorphism $(s,t) \mapsto (s, at^{q^n})$, of the local system whose trace function is

$$(s,t) \mapsto \frac{1}{\mathsf{Gauss}_L} \sum_{x \in L} \psi_L\big(sx^{q^m+1} + tx + x^{q^n+1}\big).$$

Because $G_{\mathrm{geom}}$ is unchanged by such pullback, it suffices to treat this case. The corresponding sheaf has geometric monodromy group $\cong H$ by Theorem 11.2.1(a). Thus $G$ contains a subgroup isomorphic to $H$, and hence $G = H$.

Similarly, assume that $n < m$. Rescaling $s$ in (12.3.4.2) by $s \mapsto s/b$, we reduce to the case $b = 1$. Then the $(s,t) \mapsto (s, t^{q^m+1})$ partial Kummer pullback of $\mathcal{F}$ has trace function

$$(s,t) \mapsto \frac{1}{\mathsf{Gauss}_L} \sum_{x \in L} \psi_L\big(s(ax + x^{q^n+1}) + t^{q^m+1}x^{q^m+1}\big),$$

which after the variable change $x \mapsto x/t$ becomes

$$(s,t) \mapsto \frac{1}{\mathsf{Gauss}_L} \sum_{x \in L} \psi_L\big(st^{-1}ax + st^{-(q^n+1)}x^{q^n+1} + x^{q^m+1}\big).$$

Pulling back by $(s,t) \mapsto (st, t)$, this becomes

$$(s,t) \mapsto \frac{1}{\mathsf{Gauss}_L} \sum_{x \in L} \psi_L\big(sax + st^{-q^n}x^{q^n+1} + x^{q^m+1}\big).$$

This is the pullback, by the automorphism $(s,t) \mapsto (st^{q^n}, t)$, of the local system whose trace function is

$$(s,t) \mapsto \frac{1}{\mathsf{Gauss}_L} \sum_{x \in L} \psi_L\big(st^{q^n}ax + sx^{q^n+1} + x^{q^m+1}\big).$$

This in turn is the pullback, by the universal homeomorphism $(s,t) \mapsto (s, t^{q^n})$, of the local system whose trace function is

$$(s,t) \mapsto \frac{1}{\mathsf{Gauss}_L} \sum_{x \in L} \psi_L\big(stax + sx^{q^n+1} + x^{q^m+1}\big),$$

which in turn is the pullback, by the automorphism $(s,t) \mapsto (s, t/as)$, of the local system whose trace function is

$$(s,t) \mapsto \frac{1}{\mathsf{Gauss}_L} \sum_{x \in L} \psi_L\big(tx + sx^{q^n+1} + x^{q^m+1}\big),$$

The corresponding sheaf has geometric monodromy group $\cong H$ by Theorem 11.2.1(a). Thus $G$ contains a subgroup isomorphic to $H$, and hence $G = H$. □

We also offer some twisted versions of Lemma 12.2.2, as well as some statements which are independent of Theorem 12.3.6.

LEMMA 12.3.7. *Under the notation and hypothesis of Theorem 12.3.4, assume that* $a, b \in \mathbb{F}_q^\times$ *and* $p \nmid N := \max(m,n)$. *If* $\mathcal{F}$ *is any of the local systems in Theorem 12.3.4, then*

$$|\mathrm{Trace}\big(\mathsf{Frob}_{(1/b,1),\mathbb{F}_{q^{2N}}}|\mathcal{F}\big)|^2 = q \text{ if } m > n,$$
$$|\mathrm{Trace}\big(\mathsf{Frob}_{(1,1/b),\mathbb{F}_{q^{2N}}}|\mathcal{F}\big)|^2 = q \text{ if } n > m.$$

PROOF. We will follow the proof of Theorem 7.1.2 to compute the trace of $g := \mathsf{Frob}_{(1/b,1),\mathbb{F}_{q^{2N}}}$ if $m > n$, and $g := \mathsf{Frob}_{(1,1/b),\mathbb{F}_{q^{2N}}}$ if $n > m$, on $\mathcal{F}$. Here, the relevant function $R(x)$ is $R(x) = x^{q^n} + x^{q^m}$. Then the corresponding subspace $W_R$ of $\mathbb{F}_{q^{2N}}$ is the zero locus over $\mathbb{F}_{q^{2N}}$ of the polynomial

$$x^{q^{N+n}} + x^{q^{N-n}} + x^{q^{N+m}} + x^{q^{N-m}}.$$

Denoting by $F$ the Frobenius map $x \mapsto x^q$ on $\overline{\mathbb{F}_q}$, we see that $W_R$ is the set of $x \in \overline{\mathbb{F}_q}$ that is annihilated by $F^{2N} - 1$ and by $\Delta(F) := F^{N+n} + F^{N-n} + F^{N+m} + F^{N-m}$.

Without loss of generality, we may assume $n > m$, so that $N = n$. Setting $l := n - m$ we have

$$\begin{aligned} \gcd(x^{2n} - 1, \Delta(x)) &= \gcd(x^{2n} - 1, x^{n+m} + x^{n-m} + 2) \\ &= \gcd(x^{2n} - 1, x^l(x^{n+m} + x^{n-m} + 2)) \\ &= \gcd(x^{2n} - 1, (x^l + 1)^2). \end{aligned}$$

By assumption, $\gcd(n,m) = 1$ and $l := n - m$ is odd and coprime to $n$. In this case we have $\gcd(x^{2n} - 1, x^{2l} - 1) = x^2 - 1$, but $x - 1$ does not divide $x^l + 1$. Also, $p \nmid N$ implies that $(x+1)^2$ does not divide $x^{2n} - 1$. Hence $\gcd(x^{2n} - 1, \Delta(x)) = x + 1$.

Thus $W_R = \{x \in \mathbb{F}_{q^{2N}} \mid x^q + x = 0\}$; in particular, $W_R \subset \mathbb{F}_{q^2}$ and $\#W_R = q$. For any $x \in W_R$, $R(x) = x^{q^n} + x^{q^m} = x^q + x = 0$ (because one of $n, m$ is even and the other is odd). So for any $x \in W_R$ and any $s \in \mathbb{F}_q$, we have

$$\begin{aligned} \mathrm{Trace}_{\mathbb{F}_{q^{2N}}/\mathbb{F}_q}(xR(x) + sax) &= \mathrm{Trace}_{\mathbb{F}_{q^{2N}}/\mathbb{F}_q}(sax) \\ &= \mathrm{Trace}_{\mathbb{F}_{q^2}/\mathbb{F}_q}\big(\mathrm{Trace}_{\mathbb{F}_{q^{2N}}/\mathbb{F}_{q^2}}(sax)\big) \\ &= \mathrm{Trace}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(Nsax) \\ &= Nsa(x^q + x) = 0. \end{aligned}$$

We conclude that $|\mathrm{Trace}(g)|^2 = \#W_R = q$. □

Next we deal with the case $p | \max(m,n)$.

LEMMA 12.3.8. *Under the notation and hypothesis of Theorem 12.3.4, assume that* $a, b \in \mathbb{F}_q^\times$ *and that* $p|N := \max(m,n)$. *If* $\mathcal{F}$ *is any of the local systems in Theorem 12.3.4, then there are* $s, t \in \mathbb{F}_{q^N}^\times$ *such that*

$$|\mathrm{Trace}\big(\mathsf{Frob}_{(s,t),\mathbb{F}_{q^N}}|\mathcal{F}\big)|^2 = q.$$

PROOF. (i) We again follow the proof of Theorem 7.1.2 to compute the trace of $g := \mathsf{Frob}_{(s,t),\mathbb{F}_{q^N}}$ on $\mathcal{F}$. Interchanging $s$ and $t$ if necessary, we may write the relevant function $R(x)$ as $R(x) = sbx^{q^n} + tx^{q^m}$. Then, for $s, t \in \mathbb{F}_{q^N}^\times$, the corresponding subspace $W_R$ of $\mathbb{F}_{q^N}$ is the zero locus over $\mathbb{F}_{q^N}$ of the polynomial

$$sbx^{q^{N+n}} + (sb)^{q^{N-n}}x^{q^{N-n}} + tx^{q^{N+m}} + t^{q^{N-m}}x^{q^{N-m}}.$$

Denoting by $F$ the Frobenius map $x \mapsto x^q$ on $\overline{\mathbb{F}_q}$, we see that $W_R$ is the set of $x \in \overline{\mathbb{F}_q}$ that is annihilated by $F^N - 1$ and by $\Delta(F)$, with

$$\Delta(x) := sbx^{N+n} + (sb)^{q^{N-n}}x^{N-n} + tx^{N+m} + t^{q^{N-m}}x^{N-m}.$$

(ii) As $p|N$, we have $N \geq 3$. Claim that, for any $1 \leq l \leq N-1$ coprime to $N$, we can find $\alpha \in \mathbb{F}_{q^N}^\times$ such that

$$\alpha^{q^l} + \alpha \neq 0,\ \alpha^{N(q^l-1)} \neq 1,\ \mathrm{Tr}_{\mathbb{F}_{q^N}/\mathbb{F}_q}(\alpha) = 0. \tag{12.3.8.1}$$

Indeed, there are $q^{N-1}$ solutions in $\mathbb{F}_{q^N}$ to the equation $\mathrm{Tr}_{\mathbb{F}_{q^N}/\mathbb{F}_q}(\alpha) = 0$. If $l \leq N-2$, then there are at most $q^{N-2}$ solutions to the equation $\alpha q^l + \alpha = 0$. If $l = N-1$, then any common solution $y$ to the equations $\mathrm{Tr}_{\mathbb{F}_{q^N}/\mathbb{F}_q}(\alpha) = 0$ and $\alpha^{q^l} + \alpha = 0$ also satisfies

$$\alpha^{q^{N-2}} + \alpha^{q^{N-3}} + \ldots + \alpha^q = 0,$$

and so there are most $q^{N-2}$ such common solutions. Thus there are at least $q^{N-1} - q^{N-2}$ elements $\alpha \in \mathbb{F}_{q^N}$ such that $\alpha^{q^l} + \alpha \neq 0$ and $\mathrm{Tr}_{\mathbb{F}_{q^N}/\mathbb{F}_q}(\alpha) = 0$.

Next suppose that $\alpha \in \mathbb{F}_{q^N}^\times$ and $\alpha^{N(q^l-1)} = 1$. As $\gcd(N, l) = 1$ and $p|N$, we have that the order of $\alpha$ divides

$$\gcd(q^N - 1, N(q^l - 1)) \text{ which divides } (N/p)\gcd(q^N - 1, q^l - 1) = (q-1)N/p.$$

Hence there are most $(q-1)N/p$ such elements $y$. Note that $q^{N-2} \geq 3^{N-2} > N/p$ as $N \geq p \geq 3$, whence $q^{N-1} - q^{N-2} > N(q-1)/p$, and the claim follows.

(iii) Now we consider the case $m > n$, so that $N = m$, and set $l := m - n$. Then we choose $s := \alpha/b$ with $\alpha$ satisfying (12.3.8.1), and take $t := -(\alpha + \alpha^{q^l})/2$. Note that $s, t \in \mathbb{F}_{q^m}^\times$ because of (12.3.8.1). Then modulo $x^N - 1$ we have

$$x^l\Delta(x) \equiv x^l\big(\alpha x^n + \alpha^{q^l}x^l + 2t\big) \equiv \alpha^{q^l}x^{2l} + \alpha - (\alpha^{q^l} + \alpha)x^l = \alpha^{q^l}(x^l - 1)(x^l - \alpha^{1-q^l}).$$

Suppose that $x \in \overline{\mathbb{F}_q}$ is a common root of $x^l - \alpha^{1-q^l}$ and $x^N - 1$. Then $1 = x^{Nl} = \alpha^{N(1-q^l)}$, which contradicts (12.3.8.1). It follows that $\gcd(\Delta(x), x^N - 1)$ must divide $\gcd(x^l - 1, x^m - 1) = x - 1$, as $\gcd(m, l) = \gcd(m, n) = 1$

Thus $W_R = \{x \in \mathbb{F}_{q^N} \mid x^q = x\} = \mathbb{F}_q$. For any $x \in W_R$, $\mathrm{Trace}_{\mathbb{F}_{q^N}/\mathbb{F}_p}(xR(x))$ is half the inner product of $x$ with itself, and by definition $x$ has inner product zero with everyone in $\mathbb{F}_{q^m}$, so it is zero. Also, for any $x \in W_R$ and with $s = \alpha/b$, $a, b \in \mathbb{F}_q^\times$, we have

$$\mathrm{Trace}_{\mathbb{F}_{q^N}/\mathbb{F}_q}(sax) = ab^{-1}x\big(\mathrm{Trace}_{\mathbb{F}_{q^N}/\mathbb{F}_q}(\alpha)\big) = 0.$$

It follows that $\mathrm{Trace}_{\mathbb{F}_{q^N}/\mathbb{F}_p}(xR(x)+sax) = 0$ for all $x \in W_R$, and hence $|\mathrm{Trace}(g)|^2 = \#W_R = q$.

(iv) Finally, we consider the case $n > m$, so that $N = n$, and set $l := n - m$. Then we choose $t := \alpha$ with $\alpha$ satisfying (12.3.8.1), and take $s := -(\alpha + \alpha^{q^l})/2b$. Note that $s, t \in \mathbb{F}_{q^n}^\times$ because of (12.3.8.1). Then modulo $x^N - 1$ we have

$$x^l\Delta(x) \equiv x^l\big(\alpha x^m + \alpha^{q^l}x^l + 2sb\big) \equiv \alpha^{q^l}x^{2l} + \alpha - (\alpha^{q^l} + \alpha)x^l = \alpha^{q^l}(x^l - 1)(x^l - \alpha^{1-q^l}).$$

As in (iii), the choice (12.3.8.1) of $\alpha$ implies that $\gcd(\Delta(x), x^N - 1) = x - 1$, and hence $W_R = \mathbb{F}_q$. Again, $\mathrm{Trace}_{\mathbb{F}_{q^N}/\mathbb{F}_p}(xR(x)) = 0$ for any $x \in W_R$. Next, for any $x \in W_R$, and with $a, b \in \mathbb{F}_q^\times$ we have

$$\mathrm{Trace}_{\mathbb{F}_{q^N}/\mathbb{F}_q}(sax) = (-ax/2b)\big(\mathrm{Trace}_{\mathbb{F}_{q^N}/\mathbb{F}_q}(\alpha)\big) = 0.$$

Thus $\mathrm{Trace}_{\mathbb{F}_{q^N}/\mathbb{F}_p}(xR(x) + sax) = 0$ for all $x \in W_R$, yielding $|\mathrm{Trace}(g)|^2 = \#W_R = q$. □

Lemma 12.3.9. *Let $p$ be prime, $q > 1$ a power of $p$, $k/\mathbb{F}_{q^2}$ a finite extension, and $a \in k$.*

(i) *Consider the local system on $\mathbb{G}_m/L$ whose trace function is given as follows: for $L/k$ a finite extension, and $s \in L^\times$,*

$$s \mapsto -\sum_{x \in L} \psi_L(ax + sx^{q+1}).$$

*Then its $G_{\mathrm{geom}}$ contains the cyclic group $\mu_{q+1}(k)$ of order $q + 1$.*

(ii) *For any $b, c \in k^\times$, the conclusion of* (i) *holds for the local system on $\mathbb{G}_m/L$ whose trace function is given as follows: for $L/k$ a finite extension, and $s \in L^\times$,*

$$s \mapsto -\sum_{x \in L} \psi_L\big(s(bx + cx^{q+1})\big).$$

Proof. (i) We first treat the case $a = 0$. Then our trace at time $s \in L^\times$ is

$$\begin{aligned} -\sum_{u \in L} \psi_L(su)\#\{x \in L | x^{q+1} = u\} &= -\sum_{u \in L} \psi_L(su)\big(1 + \sum_{\chi \in \mathsf{Char}(q+1), \chi \neq \mathbb{1}} \chi(u)\big) \\ &= -\sum_{\chi \in \mathsf{Char}(q+1), \chi \neq \mathbb{1}} \sum_{u \in L} \psi_L(u)\chi(u/s) \\ &= \sum_{\chi \in \mathsf{Char}(q+1), \chi \neq \mathbb{1}} \chi(s)(-\mathsf{Gauss}_L(\psi_L, \overline{\chi})). \end{aligned}$$

So in this $a = 0$ case, our local system is geometrically the direct sum of the Kummer sheaves $\mathcal{L}_\chi$ as $\chi$ runs over the nontrivial characters of order dividing $q + 1$. In terms of a chosen character $\chi_1$ of full order $q + 1$, our local system is, geometrically, the direct sum of the nontrivial powerss of $\mathcal{L}_{\chi_1}$. So in this $a = 0$ case, the entire $G_{\mathrm{geom}}$ is the cyclic group $\mu_{q+1}(k)$ of order $q + 1$.

Suppose now that $a \neq 0$. Then our sum at $s \in L^\times$ is

$$-\sum_{u \in L} \psi_L(s(ax + x^{q+1}) =$$

(making the change of variable $x \mapsto x/s$)

$$-\sum_{u \in L} \psi_L(ax + x^{q+1}/s^q).$$

As pullback by any power of Frobenius does not alter $G_{\rm geom}$, it suffices treat the local system on $\mathbb{G}_m/k$ whose trace function at $s \in L^\times$ is given by

$$s \mapsto -\sum_{x \in L} \psi_L(ax + x^{q+1}/s). \tag{12.3.9.1}$$

This local system is, up to multiplicative translation and change of $\psi_k$, isomorphic to the Kloosterman sheaf

$$\mathcal{K}l(\psi_k; \{\chi \in \mathsf{Char}(q+1) | \chi \neq \mathbb{1}\}),$$

cf. [**KRLT2**, 1.2]. For this Kloosterman sheaf, the image of $I(0)$ is the cyclic group $\mu_{q+1}(k)$ of order $q+1$.

(ii) After the change of variable $x \mapsto x/(sb)$, our trace function is

$$s \mapsto -\sum_{x \in L} \psi_L(x + cb^{-q-1}x^{q+1}/s^q).$$

This local system, after a change of $\psi_k$, is isomorphic to the local system with trace function (12.3.9.1) (for a suitable chosen $a \in k^\times$. Hence the statement follows. □

Corollary 12.3.10. *For $\mathcal{F}$ any of the sheaves considered in Theorem 12.3.4, both the cyclic groups $C_{q^n+1}$ and $C_{q^m+1}$ are subquotients of $G_{{\rm geom},\mathcal{F}}$.*

Proof. The general situation we are looking at is a local system $\mathcal{F}$ on $\mathbb{A}^1 \times \mathbb{G}_m$ obtained as follows. We have a finite extension $k/\mathbb{F}_p$, two polynomials $f(x)$, $g(x) \in k[x]$, each of degree prime to $p$ and with $\deg(g) > \deg(f)$. For $L/k$ a finite extension, and $(s,t) \in L \times L^\times$, the trace function of $\mathcal{F}$ is

$$(s,t) \mapsto -\sum_{x \in L} \psi_L\big(sf(x) + tg(x)\big).$$

The $s = 0$ pullback to $\mathbb{G}_m$, call it $\mathcal{F}_{s=0}$ has $G_{{\rm geom},\mathcal{F}_{s=0}}$ a subgroup of $G_{{\rm geom},\mathcal{F}}$. The $t = 0, s \neq 0$ pullback to $\mathbb{G}_m$, call it $\mathcal{F}_{t=0}$, has $G_{{\rm geom},\mathcal{F}_{t=0}}$ a subquotient of $G_{{\rm geom},\mathcal{F}}$. This is a special case of [**Ka-Scont**, Theorem 1], applied as follows. We start on $\mathbb{A}^3$, coordinates $x, s, t$, with the lisse sheaf $\mathcal{G} := \mathcal{L}_{\psi_k(s(fx)+tg(x))}$. Then $\mathcal{G}[3]$ is perverse on $\mathbb{A}^3$. So denoting by

$$\pi : \mathbb{A}^3 \to \mathbb{A}^2, (x,s,t) \mapsto (s,t),$$

the sheaf

$$\mathcal{H}^{-2}(R\pi_!(\mathcal{G}[3])) = R^1\pi_!\mathcal{G}$$

on $\mathbb{A}^2$ is a "sheaf of perverse origin", see [**Ka-Scont**, Lemma 6]. It is lisse outside the locus $t = 0$, and its pullback to the open set of $t = 0$ where $s$ is invertible is the local system $s \mapsto -\sum_x \psi(sf(x))$. The subquotient assertion is then just [**Ka-Scont**, Theorem 1].

In the cases of any of the sheaves $\mathcal{F}$ of Theorem 12.3.4, we have only to apply Lemma 12.3.9 to the $s = 0$ and to the $t = 0$ pullbacks to get the subquotient assertions. □

Here is a more general result of the same type.

Lemma 12.3.11. *Let $k/\mathbb{F}_p$ be a finite extension, $f(x), g(x) \in k[x]$ be polynomials of prime to $p$ degrees $(m, n)$ with $1 \le m < n$. Consider the lisse sheaf $\mathcal{F}$ on $(\mathbb{A}^1 \times \mathbb{G}_m)/k$ whose trace function is given as follows. For $L/k$ a finite extension, and $(s, t) \in L \times L^\times$,*

$$\mathrm{Trace}(\mathsf{Frob}_{(s,t),L}|\mathcal{F}) = -\sum_{x \in L} \psi_L(sf(x) + tg(x)).$$

*Then both of the cyclic groups $C_n$ and $C_m$ are subquotients of $G_{\mathrm{geom},\mathcal{F}}$.*

Proof. Exactly as in the proof of Corollary 12.3.10 above, it suffices to show

(a) The restriction to $\mathbb{G}_m$ of the $s = 0$ pullback of $\mathcal{F}$, call it $\mathcal{F}_{s=0}$, has $C_n$ as a subquotient of its $G_{\mathrm{geom}}$.

(b) If $m \ge 2$, the restriction to $\mathbb{G}_m$ of the $t = 0$ pullback of $\mathcal{F}$, call it $\mathcal{F}_{t=0}$, has $C_m$ as a subquotient of its $G_{\mathrm{geom}}$.

[In (b), we omit the case $m = 1$, simply because $C_1$ is a quotient of any group.] These statements follow from the following lemma. □

Lemma 12.3.12. *Let $f(x)$ have prime to $p$ degree $n \ge 2$. Then the $I(0)$-representation of the lisse sheaf $\mathcal{H}$ on $\mathbb{G}_m/k$ whose trace function is $s \mapsto -\sum_x \psi(sf(x))$ is the group $\bigoplus_{\mathbb{1} \neq \chi \in \mathsf{Char}(n)} \mathcal{L}_\chi$ (which is cyclic of order $n$).*

Proof. The sheaf $\mathcal{K} := f_\star\overline{\mathbb{Q}_\ell}/\overline{\mathbb{Q}_\ell}$ is a middle extension sheaf (view it as a direct factor of $f_\star\overline{\mathbb{Q}_\ell}$ and apply [**Ka-ESDE**, 7.3.2]). Because $f$ has degree $n$ prime to $p$, $f$ as a map of $\mathbb{P}^1$ to $\mathbb{P}^1$ is totally ramified over $\infty$, the $I(\infty)$-representation of $\mathcal{K}$ is $\bigoplus_{\mathbb{1} \neq \chi \in \mathsf{Char}(n)} \mathcal{L}_\chi$. For any nonzero $a \in k$, $\mathcal{K} \otimes \mathcal{L}_{\psi(ax)}$ is totally wild at $\infty$. Therefore $\mathcal{K}$ is an "elementary" sheaf in the sense of [**Ka-ESDE**, 7.3.4]. By [**Ka-ESDE**, 7.3.8], its Fourier transform is also elementary.

Just as in the proof of Lemma 12.4.10, but with no circularity, one sees that $\mathcal{H}$ is the restriction to $\mathbb{G}_m$ of the Fourier transform of $\mathcal{K} := f_\star\overline{\mathbb{Q}_\ell}/\overline{\mathbb{Q}_\ell}$. By Laumon's theory of local Fourier transform, we have [**Ka-ESDE**, 7.4.3.1]

$$\mathcal{H}_{I(0)}/\mathcal{H}^{I(0)} \cong \mathrm{FTloc}(\infty, 0)(\mathcal{K}_{I(\infty)}).$$

Laumon also gives [**Ka-ESDE**, 7.4.4 (2)]

$$\mathrm{FTloc}(\infty, 0)\mathcal{L}_\chi \cong \mathcal{L}_{\overline{\chi}}.$$

Thus $\bigoplus_{\mathbb{1} \neq \chi \in \mathsf{Char}(n)} \mathcal{L}_\chi$ is a quotient of the $I(0)$-representation of $\mathcal{H}$. But $\mathcal{H}$ has rank $n - 1$, so $\mathcal{H}^{I(0)} = 0$ for dimension reasons. □

When $\gcd(n, m) = 1$, we have the following extra information.

Lemma 12.3.13. *Let $k/\mathbb{F}_p$ be a finite extension, $f(x), g(x) \in k[x]$ be polynomials of prime to $p$ degrees $(m, n)$ with $1 \le m < n$. Consider the lisse sheaf $\mathcal{F}$ on $(\mathbb{A}^1 \times \mathbb{G}_m)/k$ whose trace function is given as follows. For $L/k$ a finite extension, and $(s, t) \in L \times L^\times$,*

$$\mathrm{Trace}(\mathsf{Frob}_{(s,t),L}|\mathcal{F}) = -\sum_{x \in L} \psi_L(sf(x) + tg(x)).$$

*Suppose that* $\gcd(n, m) = 1$. *Then $G_{\mathrm{geom},\mathcal{F}}$ admits a subquotient of order divisible by $n - m$.*

Proof. Exactly as in the proof of Corollary 12.3.10 above, it suffices to show that the $t = 1$ pullback $\mathcal{F}|_{t=1}$ on $\mathbb{A}^1$, whose trace function is given by

$$t \mapsto -\sum_x \psi(g(x) + tf(x))$$

has its $G_{\mathrm{geom},\mathcal{F}|_{t=1}}$ containing a finite subgroup of order divisible by $n - m$. This pullback is geometrically isomorphic to the Fourier transform

$$\mathrm{FT}(f_\star \mathcal{L}_{\psi(g)}).$$

The input $f_\star \mathcal{L}_{\psi(g)}$ has all its $\infty$-slopes $\deg(g)/\deg(f) = n/m > 1$. By Laumon's theory of local Fourier transform [**Ka-ESDE**, 7.4.1,(1)], the $I(\infty)$-representation of $\mathrm{FT}(f_\star \mathcal{L}_{\psi(g)})$ is of the form $\mathcal{A} \oplus \mathcal{B}$, with $\mathcal{A}$ having all slopes $n/(n-m)$ and rank $n - m$, and with $\mathcal{B}$ having all slopes $\le 1$. Because $\gcd(n,m) = 1$, we also have $\gcd(n, n-m) = 1$, and hence $\mathcal{A}$ is $I(\infty)$-irreducible (integrality of Swan conductors). Because we began over the finite field $k$, each of $\mathcal{A}, \mathcal{B}$ is stable by the decomposition group $D(\infty)$. By the local monodromy theorem, the action of $\Gamma$ is, on a normal open subgroup $\Gamma_1$, unipotent [**Ka-GKM**, 7.0.5]. Because $\Gamma$ acts irreducibly, the action of $\Gamma_1$ is completely reducible, and hence (being also unipotent) is trivial. Thus $\Gamma$ is finite. But the degree (here $n - m$) of an irreducible representation of a finite group (here $\Gamma$) always divides the order of the group. □

Lemma 12.3.14. *Let $p > 2$, $k/\mathbb{F}_p$ a finite extension, $a, b \in k$ with $(a, b) \neq (0, 0)$, and let $c_i \in k^\times$ for $0 \le i \le t$ and $(b, c_0) \neq (0, 0)$. Let*

$$0 \le m = n_0 < n_1 < n_2 < \ldots < n_t$$

*be integers, and set $f(x) := \sum_{i=1}^t c_i x^{q^{n_i}+1}$. For any $d \in \mathbb{Z}_{\ge 1}$, let $\Sigma_d(x, y, z, w) = x^d + y^d - z^d - w^d$; also let $\Sigma_f(x, y, z, w) := f(x) + f(y) - f(z) - f(w)$. Then the large $L$ limit of*

$$\frac{1}{(\#L)^2} \# \left\{(x, y, z, w) \in L^4 \mid \Sigma_1 = \Sigma_{q^m+1} = \Sigma_f = 0\right\}$$

*is $2 + \#\mu_{total}(\tilde{f}/x)$, where $\tilde{f} := f + x^{q^m+1}$ and*

$$\mu_{total}(\tilde{f}/x) = \bigcap_{i=0}^t \{x \in \overline{\mathbb{F}_p} \mid x^{q^{n_i}-1} = -1\},$$

*cf.* (12.1.0.2).

Proof. We will show that the number of $L$-points of the intersection of $\Sigma := \{\Sigma_1 = \Sigma_{q^m+1} = 0\}$ with the surface $\Sigma_f = 0$ is $(\#\mu_{total}(\tilde{f}) + 2)(\#L)^2 + O(\#L)$. Certainly, the union of the two planes $(x = z,\ y = w)$ and $(x = w,\ y = z)$ contributes $2(\#L)^2 - \#L$ points.

So we have to count the points $P = (x, y, z, w) \in (\Sigma \cap \{\Sigma_f = 0\})$ outside of these two planes. For such a point, we have $w = x + y - z$. Setting $Q_0 = q^m$ and $Q_i = q^{n_i}$, $1 \le i \le t$, we may assume that $L \supseteq \mathbb{F}_{Q_i^2}$ for $0 \le i \le t$. Since $\Sigma_{Q_0+1}(P) = 0$ but $y \neq z$ and $x \neq z$, by Lemma 12.3.2 we can find some $A \in \mathbb{F}_{Q_0^2}^\times$ such that $x = (A+1)z - Ay$ and

$$A^{Q_0 - 1} = -1. \tag{12.3.14.1}$$

Now for any $p$-power $q$ we have

$$\begin{aligned}\Sigma_{q+1}(P) &= ((A+1)z-Ay)^{q+1}+y^{q+1}-z^{q+1}-(Az-(A-1)y)^{q+1}\\ &= ((A^q+1)z^q-A^qy^q)(A+1)z-Ay)+y^{q+1}-z^{q+1}-(A^qz^q-(A^q-1)y^q)(Az-(A-1)y)\\ &= (A^q+A)(z^{q+1}-y^qz-yz^q+y^{q+1}) = (A^q+A)(z-y)^{q+1}.\end{aligned}$$

We record this identity for later use:

$$((A+1)z-Ay)^{q+1}+y^{q+1}-z^{q+1} = (Az-(A-1)y)^{q+1}+(A^q+A)(z-y)^{q+1}. \tag{12.3.14.2}$$

Since $f(x)=\sum_{i=1}^t c_ix^{Q_i+1}$, it follows that

$$0 = f(x)+f(y)-f(z)-f(w) = \sum_{i=1}^t c_i(A^{Q_i}+A)(z-y)^{Q_i+1},$$

and so

$$\sum_{i=1}^t c_i(A^{Q_i-1}+1)(z-y)^{Q_i}=0.$$

Given (12.3.14.1), unless $A \in \mu_{total}(\tilde{f}/x)$, this condition gives us a non-identically-zero polynomial equation on $z-y$, yielding at most $Q_t$ values for $z$ once $y$ is given, and thus at most $Q_tL$ possibilities for $P$. On the other hand, when $A \in \mu_{total}(\tilde{f}/x)$, this condition is vacuously true, and so the desired zero locus contains the plane $w=x+y-z,\ x=(A+1)z-Ay$. The intersection of any two aforementioned planes is a line, so accounts for $\#L$ points. Hence the statement follows. □

THEOREM 12.3.15. *Let $q>1$ be a power of an odd prime $p$, $n \in \mathbb{Z}_{\geq 1}$, $q_i := q^{m_i}$, $1 \leq i \leq n$, with $1 \leq m_1 < m_2 < \ldots < m_n$. For a finite extension $k/\mathbb{F}_p$, let $c_i \in k^\times$ and set $f(x) = x + \sum_{i=1}^n c_ix^{q_i+1}$. Consider the local system $\mathcal{F}$ on $(\mathbb{A}^1 \times \mathbb{G}_m)/k$ of rank $q_n$, whose trace function, at a point $(s,t) \in L \times L^\times$ for $L/k$ a finite extension, given by*

$$\text{Trace}\big(\mathsf{Frob}_{(s,t),L}|\mathcal{F}\big) = \frac{-1}{\sqrt{\#L}}\sum_{x\in L}\psi_L(sx^2+tf(x)).$$

*Then $M_{2,2}(\mathcal{F})=2$.*

PROOF. The question is geometric, so we may assume that $k$ contains all roots of unity of order dividing $2\prod_i(q_i-1)$. Following the proof of Theorem 12.1.3, we see that $M_{2,2}+1$ is the large $L$ limit of $\#\Sigma(L)/\#L^2$, where

$$\Sigma := \left\{(x,y,z,w)\in\mathbb{A}^4 \mid \Sigma_2 := x^2+y^2-w^2-z^2=0,\ \Sigma_f := f(x)+f(y)-f(z)-f(w)=0\right\}.$$

Applying Lemma 12.3.14 with $m=0$, we see that the contribution of $\Sigma \cap (\Sigma_1=0)$ to this limit is 2; indeed it comes from the two planes $(x=z, y=w)$ and $(x=w, y=z)$.

It remains to count the number of $L$-points $P=(x,y,z,w)$ of $\Sigma \cap (\Sigma_1 \neq 0)$. For such a point $P$, assume that $y=z$. Then $0=\Sigma_2(P)=x^2-w^2$, whence $x^2=w^2$ and so $x^{q_i+1}=w^{q_i+1}$ for all $i$. It follows that $0=\Sigma_f(P)=x-w$, and so $x=w$ and $P\in(\Sigma_1=0)$, contrary to the assumption. Similarly, if $x=z$, then we get $y=w$ and $\Sigma_1(P)=0$. So we may assume that

$$u := z-y \neq 0,\ x \neq z.$$

Setting $A := (x-z)/(z-y)$, we have

$$x = (A+1)z - Ay,$$

where $A \neq 0$ as $x \neq z$. Setting

$$v := x + y - z = Az - (A-1)y$$

and applying (12.3.14.2), we get

$$w^2 = x^2 + y^2 - z^2 = v^2 + 2Au^2.$$

Now, for any $1 \leq i \leq n$, again applying (12.3.14.2) we obtain

$$\Sigma_{q_i+1}(P) = x^{q_i+1} + y^{q_i+1} - z^{q_i+1} - w^{q_i+1} = v^{q_i+1} + (A^{q_i} + A)u^{q_i+1} - (v^2 + 2Au^2)^{(q_i+1)/2}.$$

The condition $0 = \Sigma_f(P) = x + y - z - w + \sum_{i=1}^n c_i \Sigma_{q_i+1}(P)$ then yields

$$w = v + \sum_{i=1}^{n} c_i\big(v^{q_i+1} + (A^{q_i} + A)u^{q_i+1} - (v^2 + 2Au^2)^{(q_i+1)/2}\big); \tag{12.3.15.1}$$

in particular, $w$ is completely determined by $A, u, v$. Hence $P$ is completely determined by $(A, u, v)$, since $x = u + v$, $y = v - Au$, and $z = v - (A-1)u$. The condition $\Sigma_2(P) = 0$ now becomes

$$\Big(v + \sum_{i=1}^{n} c_i\big(v^{q_i+1} + (A^{q_i} + A)u^{q_i+1} - (v^2 + 2Au^2)^{(q_i+1)/2}\big)\Big)^2 - (v^2 + 2Au^2) = 0.$$

Modulo $Au^2$, the left-hand-side of this equation is $v^2 - v^2 = 0$. Recalling $A \neq 0$ (as $x \neq z$) and $u \neq 0$ (as $y \neq z$), the intersection in question satisfies the equation $F(A, u, v) = 0$, where

$$F := \frac{1}{Au^2}\Big(\big(v + \sum_{i=1}^{n} c_i(v^{q_i+1} + (A^{q_i} + A)u^{q_i+1} - (v^2 + 2Au^2)^{(q_i+1)/2})\big)^2 - (v^2 + 2Au^2)\Big).$$

We will view $F(A, u, v)$ as a polynomial in the variable $u$ over $k[A, v]$. Modulo the ideal $(A - v)$, this polynomial is

$$G(u) := \frac{1}{Au^2}\Big(\big(A + \sum_{i=1}^{n} c_i(A^{q_i+1} + (A^{q_i} + A)u^{q_i+1} - (A^2 + 2Au^2)^{(q_i+1)/2})\big)^2 - (A^2 + 2Au^2)\Big),$$

a polynomial in the variable $v$ over $k[A]$. Since $q_i \geq 3$, modulo $A^2$ the latter polynomial is

$$\begin{aligned} &\frac{1}{Au^2}\Big(\big(A + \sum_{i=1}^{n} c_i(Au^{q_i+1} - (2Au^2)^{(q_i+1)/2})\big)^2 - (A^2 + 2Au^2)\Big) \\ \equiv &\frac{1}{Au^2}\Big(A^2\big(1 + \sum_{i=1}^{n} c_i u^{q_i+1}\big)^2 - (A^2 + 2Au^2)\Big) \qquad\qquad , \\ \equiv &-2 + 2A\sum_{i=1}^{n} c_i u^{q_i-1} + Au^{-2}\big(\sum_{i=1}^{n} c_i u^{q_i+1}\big)^2 \end{aligned}$$

with the leading term congruent to $Ac_n^2 u^{2q_n}$. Thus $G(u)$ is a palindrome Eisenstein polynomial over $k[A]$, and so it is irreducible over $k(A)$.

Note that $F$ is of degree $2q_n$ in $u$, with leading coefficient

$$X(A) := c_n^2\big(A^{q_n} + A - (2A)^{(q_n+1)/2}\big)^2/A,$$

a polynomial of degree $2q_n - 1$ in $A$, and constant term

$$Y(v) := -2\sum_{i=1}^{n} c_i v^{q_i},$$

a polynomial of degree $q_n$ in $v$. Thus the content of $F$, as a polynomial in $u$ over $\bar{k}[A, v]$ is 1, and so $F$ is irreducible in $\bar{k}[A, u, v]$. [Indeed, if $F$ factors as $F_1F_2$ in $\bar{k}[A, u, v]$ with $\deg_u F_1 \geq \deg_u F_2$, then the irreducibility of $G(u)$ implies that $F_2$ is constant in $u$. Now if $F_{11}$ is the leading coefficient in $u$ of $F_1$, then $F_{11}F_2 = X(A)$, and so $F_2$ divides $X(A)$. Similarly, $F_2$ divides $Y(v)$ by equating the constant term in $F = F_1F_2$. Thus $F_2$ is a constant.]

The irreducibility of $F$ implies that the locus $\Sigma \cap (\Sigma_1 \neq 0)$, which is contained in $F(A, u, v) = 0$, has at most $\#L^2 + O(\#L)$ points in $L^3$, completing the proof. □

## 12.4. Another approach to $M_{2,2}$

In this section, we indicate another approach to determine $M_{2,2}$ for a general class of local systems with non-monomial coefficients. This approach is based on resultants, whose basic properties we now recall. For a commutative ring $R$ and polynomials $f(x), g(x) \in R[x]$ of degrees $n, m \geq 1$, both of whose leading coefficients lie in $R^\times$, the *resultant* $\mathsf{Res}_x(f, g)$ is an element of $R$ defined as follows. Denote by $R[x]_{<d} \subset R[x]$ the $R$-span of the monomials $x^n$ with $n \leq d - 1$. The *Sylvester map* is

$$\mathsf{Syl}_{f,g} : R[x]_{<m} \oplus R[x]_{<n} \to R[x]_{<n+m}, (a, b) \mapsto fa + gb.$$

Both source and target are free $R$-modules of rank $n + m$.[ Its matrix is called the *Sylvester matrix.*] One defines

$$\mathsf{Res}_x(f, g) := \det(\mathsf{Syl}_{f,g}).$$

For any ring homomorphism $\phi : R \to S$, assuming the polynomials $\phi(f), \phi(g) \in S[x]$, obtained by applying $\phi$ to the coefficients of $f, g$, have the same degrees $(n, m)$, we have

$$\mathsf{Res}_x(\phi(f), \phi(g)) = \phi(\mathsf{Res}_x(f, g)).$$

[Simply view the resultant as the determinant of the Sylvester matrix, whose formation commutes with arbitrary extension of scalars. Also see [**KT8**, Lemma 3.1] for a more general statement.] When $R$ is a field $k$, $\mathsf{Res}_x(f, g) = 0$ if and only if $\gcd(f, g) \neq 1$, i.e., if and only if $f$ and $g$ have a common zero in an algebraic closure of $k$.

We begin with the notion of “almost injectivity” of a map from $\mathbb{A}^1$ to $\mathbb{A}^2$. Let $k$ be an algebraically closed field, and

$$f(x) = \sum_{i=0}^{m} a_i x^i,\ g(x) = \sum_{j=0}^{n} b_j x^j \in k[x],$$

be polynomials of strictly positive degrees $m, n$. We say that the map $x \mapsto (f(x), g(x))$ of $\mathbb{A}^1$ to $\mathbb{A}^2$ is *almost injective* if its restriction to a dense open set $U := \mathbb{A}^1 \smallsetminus$(a finite set $Z$ of closed points) is injective as a map from $U(k)$ to $\mathbb{A}^2(k)$. With no loss of generality, we may assume both $f, g$ are monic (simply because for $a, b \in k^\times$, the map $(x, y) \mapsto (ax, by)$ is bijective on $\mathbb{A}^2(k)$).

If $k$ has characteristic $p > 0$, then the map $x \mapsto (f(x), g(x))$ is almost injective if and only $x \mapsto (f(x)^p, g(x)^p)$ is almost injective (simply because $(x, y) \mapsto (x^p, y^p)$ is bijective on $\mathbb{A}^2(k)$). So we may always reduce to the case when at least one of $f(x), g(x)$ is not a $p^{\text{th}}$ power, if we are in characteristic $p > 0$. Equivalently, we may always reduce to the case when at least one of the derivatives $f'(x), g'(x)$ is nonzero.

In $k[x, y]$, define

$$\Delta_f := \frac{f(x) - f(y)}{x - y}, \quad \Delta_g := \frac{g(x) - g(y)}{x - y},$$

viewed as polynomials in $x$ with coefficients in $k[y]$. Because $f, g$ were monic of degrees $m, n$, $\Delta_f$ and $\Delta_g$ are monic of degrees $m - 1$ and $n - 1$ respectively.

Lemma 12.4.1. *Suppose that $f, g$ are both monic of strictly positive degrees $m, n$, and that $(f'(x), g'(x)) \neq (0, 0)$ in $k[x]^2$. Viewing $\Delta_f$ and $\Delta_g$ as monic polynomials in the ring $A[x]$, $A := k[y]$, form their resultant as polynomials in $x$. This is an element*

$$R(y) := \mathsf{Res}_x(\Delta_f, \Delta_g) \in k[y]. \tag{12.4.1.1}$$

*Then the map $x \mapsto (f(x), g(x))$ is almost injective if and only if the polynomial $R(y)$ is nonzero.*

Proof. (i) Suppose first that $R(y)$ vanishes identically. For every $y_0 \in k$, the specialization $y \mapsto y_0$ preserves the degree in $x$ of $\Delta_f$. By [**KT8**, Lemma 3.1], $R(y_0) = 0$ now means that the two polynomials

$$\frac{f(x) - f(y_0)}{x - y_0}, \quad \frac{g(x) - g(y_0)}{x - y_0}$$

have a common zero $x_0$. If $x_0 = y_0$ in addition, then this vanishing means precisely that $f'(y_0) = g'(y_0) = 0$. Because at least one of $f', g'$ is a nonzero polynomial, there are only finitely many such $y_0$; let $Z$ denote the finite set of such $y_0$.

Now consider any point $y_1 \in \mathbb{A}^1 \smallsetminus Z$, so that at least one of $f'(y_1), g'(y_1)$ is nonzero. The above argument shows that the common zero $x_1$ of

$$\frac{f(x) - f(y_1)}{x - y_1}, \quad \frac{g(x) - g(y_1)}{x - y_1}$$

must satisfy $x_1 \neq y_1$. Then the denominator $x_1 - y_1$ is nonzero, and hence both $f(x_1) = f(y_1)$ and $g(x_1) = g(y_1)$, i.e. we have $(f(x_1), g(x_1)) = (f(y_1), g(y_1))$ but $x_1 \neq y_1$. This holds for all $y_1 \in \mathbb{A}^1 \smallsetminus Z$, whence the failure of almost injectivity.

(ii) Conversely, suppose that $R(y)$ is nonzero in $k[y]$. For a point $y_0$ with $R(y_0) \neq 0$, an application of [**KT8**, Lemma 3.1] as in (i) shows that there are no $x_0$ which are common zeroes of

$$\frac{f(x) - f(y_0)}{x - y_0}, \quad \frac{g(x) - g(y_0)}{x - y_0}.$$

In particular, there are no $x_0 \neq y_0$ which are common zeroes, which is to say that there are no $x_0 \neq y_0$ with both $f(x_0) = f(y_0)$ and $g(x_0) = g(y_0)$. Thus, if $R(y_0) \neq 0$, then $(f(x), g(x)) = (f(y_0), g(y_0))$ implies $x = y_0$. Since $R(y)$ has only finitely many zeroes, almost injectivity follows. □

Corollary 12.4.2. *Let $k/\mathbb{F}_p$ be a finite extension, $f, g \in k[x]$ of degrees $1 \le n < m$, $p \nmid nm$. Consider the local system $\mathcal{F}(k, f, g)$ on $(\mathbb{A}^1 \times \mathbb{G}_m)/k$ whose trace function is given as follows: for $L/k$ a finite extension, and $(s, t) \in L \times L^\times$,*

$$\mathrm{Trace}(\mathsf{Frob}_{(s,t),L}|\mathcal{F}(k, f, g)) = -\sum_{x \in L} \psi_L(sf(x) + tg(x)).$$

*Then $\mathcal{F}(k, f, g)$ is geometrically irreducible if and only if the resultant $\mathsf{Res}_x(\Delta_f, \Delta_g) \in k[y]$ is nonzero, i.e., if and only if the map $x \mapsto (f(x), g(x))$ from $\mathbb{A}^1$ to $\mathbb{A}^2$ is almost injective.*

Proof. The empirical $M_{1,1}$ over a finite extension $\mathbb{F}_q/k$ is

$$\frac{1}{q(q-1)} \sum_{s \in L, t \in L^\times} \frac{1}{q} \sum_{x,y \in L} \psi_L(s(f(x) - f(y)) + t(g(x) - g(y)).$$

This “missing” sum over $s \in L, t = 0$ is

$$\frac{1}{q(q-1)} \sum_{s \in L} \frac{1}{q} \sum_{x,y \in L} \psi_L(s(f(x) - f(y)) = \frac{\#\{(x, y) \in \mathbb{F}_q^2 \mid f(x) = f(y)\}}{q(q-1)}$$

is $O(1/q)$, simply because $f(x) = f(y)$ is a curve, so has $O(q)$ points over $\mathbb{F}_q$. This missing term does not alter the large $L$ limit. So $M_{1,1}$ is the large $L$ limit of

$$\frac{1}{q(q-1)} \sum_{s,t \in L} \frac{1}{q} \sum_{x,y \in L} \psi_L(s(f(x)-f(y))+t(g(x)-g(y)) = \frac{\#\{(x, y) \in \mathbb{F}_q^2 \mid f(x) = f(y),\ g(x) = g(y)\}}{(q-1)}.$$

The solutions with $x = y$ are $q$ in number. The others are among the common zeroes of $\Delta_f$ and $\Delta_g$, This set of common zeroes over $\overline{k}$ is finite if and only if the resultant does not vanish identically. □

In view of the previous Lemma 12.4.1, we now investigate some situations in which we can show the resultant $R(y)$ in (12.4.1.1) is nonzero.

Lemma 12.4.3. *Suppose that $f, g$ are both monic of strictly positive degrees $m, n$, and that $(f'(x), g'(x)) \ne (0, 0)$ in $k[x]^2$. If $k$ has characteristic $p > 0$, suppose $p \nmid mn$. Suppose $\Delta_f$ is absolutely irreducible in $k[x, y]$, and* $\deg(f) \nmid \deg(g)$*. Then $R(y)$ as defined in* (12.4.1.1) *is nonzero in $k[y]$.*

Proof. It suffices to treat the case when $k$ is algebraically closed. If $R(y)$ vanishes identically, then for every $y_0$, there exists an $x_0$ such that $(x_0, y_0)$ is a zero of both $\Delta_f$ and $\Delta_g$. In other words, the vanishing of $R(y)$ implies that the two loci $\Delta_f = 0$ and $\Delta_g = 0$ have infinite intersection.

Since $\Delta_f$ is absolutely irreducible, $\Delta_f = 0$ is a geometrically irreducible curve. So it suffices to show that the restriction of $\Delta_g$ to this curve is a nonzero function, which is to say that $\Delta_g$ is not divisible by $\Delta_f$. If $m > n$, this is obvious, because $\Delta_f$ has larger degree than $\Delta_g$.

If $m < n$, it suffices to observe that the highest degree term of $\Delta_f$ does not divide the highest degree term of $\Delta_g$. Indeed, the highest degree term of $\Delta_f$ is the product

$$\prod_{1 \ne \zeta \in \mu_m(k)} (x - \zeta y),$$

while the highest degree term of $\Delta_g$ is the product

$$\prod_{1\neq\zeta\in\mu_n(k)} (x-\zeta y).$$

Since $m = \deg(f) \nmid \deg(g) = n$, $m > 1$ and no primitive $m^{\text{th}}$ root of unity lies in $\mu_n(k)$. □

We now give some cases where $\Delta_f$ is absolutely irreducible.

Lemma 12.4.4. *For $a, b \in k^\times$ and an integer $n \geq 2$ invertible in $k$, the polynomial $f(x) := ax + bx^n$ has $\Delta_f$ absolutely irreducible.*

Proof. We reduce to the case when $k$ is algebraically closed and $b = 1$. For $f(x) := ax + x^n$, we have

$$\Delta_f = a + \prod_{1\neq\zeta\in\mu_n(k)} (x-\zeta y).$$

So it suffices to show that the curve in $\mathbb{P}^2$ defined by the vanishing of the homogenous form in $x, y, z$ given by

$$z^{n-1} + (1/a) \prod_{1\neq\zeta\in\mu_n(k)} (x-\zeta y)$$

is absolutely irreducible (for then the dense open set where $z$ is invertible is the locus $\Delta_f = 0$). This is a monic polynomial in $z$, with coefficients in the unique factorization domain $k[x, y]$, so any factor of it is itself monic in $z$ with coefficients in $k[x, y]$. Hence, it suffices to show that after the specialization $(x, y) \mapsto (x, 1)$, the polynomial

$$z^{n-1} + (1/a) \prod_{1\neq\zeta\in\mu_n(k)} (x-\zeta)$$

is absolutely irreducible in $k[x, z]$. But this is clear, because as a polynomial in $z$ with coefficients in $k[x]$, it is Eisenstein for any one of the linear factors $x - \zeta$. □

Here is a variant of Lemma 12.4.4.

Lemma 12.4.5. *Let $q$ be a power of a prime $p$, $k = \overline{k}$ a field of characteristic $p$, $a \in k^\times$, $0 \leq n_1 < n_2 < \ldots < n_r$ a sequence of integers, $A_1, \ldots, A_r$ a sequence of elements of $k^\times$, and*

$$f(x) = ax + \sum_{i=1}^{r} A_i x^{1+q^{n_i}}.$$

*Suppose that either $q$ is odd, or that $q$ is even and each $n_i$ is odd. Then $\Delta_f$ is absolutely irreducible.*

Proof. Here $\Delta_f$ is the polynomial

$$a + \sum_{i=1}^{r} A_i \prod_{1\neq\zeta\in k,\ \zeta^{1+q^{n_i}}=1} (x-\zeta y).$$

Just as in the proof of the preceding lemma 12.4.4, it suffices to show that the homogenous form in $x, y, z$ given by

$$az^{q^{n_r}} + \sum_{i=1}^{r} z^{q^{n_r}-q^{n_i}} A_i \prod_{1\neq\zeta\in k,\ \zeta^{1+q^{n_i}}=1} (x-\zeta y)$$

is absolutely irreducible in $k[x, y, z]$. This polynomial is monic in $z$, so any factor of it will be monic in $z$, with coefficients in $k[x, y]$. Hence, it suffices to show that after specializing $y \mapsto 1$, the resulting polynomial

$$az^{q^{n_r}} + \sum_{i=1}^{r} z^{q^{n_r}-q^{n_i}} A_i \prod_{1\neq\zeta\in k,\ \zeta^{1+q^{n_i}}=1} (x-\zeta)$$

in $k[x][z]$ is irreducible.

When $q$ is odd, each each $1 + q^{n_i}$ is even, so we have an Eisenstein polynomial for the linear factor $x + 1$.

When $q$ is even, and each power $n_i$ is odd, each $1 + q^{n_i}$ is divisible by $1 + q$. So for any nontrivial $\zeta \in \mu_{1+q}(k)$, we have an Eisenstein polynomial for the linear factor $x - \zeta$. □

Example 12.4.6. (i) Trivially, if $f(x) = f_1(v(x))$ and $g(x) = g_1(v(x))$ for some $f_1, g_1, v \in k[x]$ and $\deg(v) \geq 2$, then the map $x \mapsto (f(x), g(x))$ is not almost injective.

(ii) Assume $f(x) = ax^m \in k[x]$ is a monomial of degree $m \geq 1$, and $g(x) = \sum_{i=0}^{n} b_i x^i \in k[x]$ is such that $b_{i_0} \neq 0$ for some $i_0$ coprime to $m$. Then the map $F : x \mapsto (f(x), g(x))$ is almost injective. Indeed, suppose $F(x) = F(y)$ for some $x \neq y$. Then $x \neq 0$ and $y = \epsilon x$ for some $m^{\text{th}}$ root of unity $\epsilon \in \overline{k}$. Now

$$0 = g(y) - g(x) = \sum_{i=0}^{n} b_i(\epsilon^i - 1)x^i.$$

Since $b_{i_0}(\epsilon^{i_0} - 1) \neq 0$, this equation in $x$ can have only finitely many solutions. Thus $F$ can fail to be injective only at finitely many points $x$.

(iii) Assume that $f(x) = ax + bx^m$ with $a, b \in k^\times$, $m \geq 2$ coprime to $p = \operatorname{char}(k)$, $g(x) \in k[x]$ of positive degree $n$ coprime to $p$, and $m \nmid n$. Then the map $F : x \mapsto (f(x), g(x))$ is almost injective. Indeed, $\Delta_f$ is absolutely irreducible by Lemma 12.4.4, and the claim then follows from Lemma 12.4.3.

Below is a somewhat different way to test almost-injectivity using resultants.

Lemma 12.4.7. *Let $k$ be an algebraically closed field of characteristic $p \geq 0$, and let*

$$f(x) = \sum_{i=0}^{m} a_i x^i,\ \ g(x) = \sum_{j=0}^{n} b_j x^j \in k[x].$$

*Then the question of whether the map $F(x) = (f(x), g(x)) : \mathbb{A}^1 \to \mathbb{A}^2$ is almost injective can be decided as follows.*

(i) *$F$ is almost injective if and only if so is $x \mapsto (f(x) - a_0, g(x) - b_0)$. Hence we may assume that $f(x) = \sum_{i=r}^{m} a_i x^i$ with $1 \leq r \leq m$, $a_r a_m \neq 0$, and $g(x) = \sum_{i=s}^{n} b_j x^j$ with $1 \leq s \leq n$, $b_s b_n \neq 0$.*

(ii) *Suppose $p > 0$ and $a_i = 0$ whenever $p \nmid i$, so that $f(x) = f_1(x)^p$ where $f_1(x) = \sum_{0 \le i \le m/p} a_{pi}^{1/p} x^i$. Then $F$ is almost injective if and only if so is $x \mapsto (f_1(x), g(x))$. Hence, regardless of $p = 0$ or $p > 0$, we may assume that there is some $i_0$ with $a_{i_0} i_0 \neq 0$ and there is some $j_0$ with $b_{j_0} j_0 \neq 0$.*

(iii) *Assume $f$ and $g$ are as in the conclusions of* (i) *and* (ii)*, and set*

$$\tilde{f}(x,u) := \frac{f(ux) - f(x)}{x^r(u-1)}, \ \tilde{g}(x,u) = \frac{g(ux) - g(x)}{x^s(u-1)}.$$

*Then $\tilde{f}(x,u), \tilde{g}(x,u) \in k[x,u]$; let $\tilde{R}(x)$ denotes the resultant $\mathsf{Res}(\tilde{f}, \tilde{g})$ of two polynomials in the variable $u$ with coefficients in $k[x]$. Then $F$ is almost injective if and only if $\tilde{R}(x)$ is not identically zero.*

Proof. (i) is obvious as the translation $z \mapsto z - a$ on $\mathbb{A}^1$ is bijective.

(ii) follows since the Frobenius map $z \mapsto z^p$ on $\mathbb{A}^1$ is bijective.

(iii) Note that

$$\tilde{f}(x,u) = \sum_{i=r}^{m} a_i \frac{u^i - 1}{u-1} x^{i-r} \in k[x,u],$$

and similarly

$$\tilde{g}(x,u) = \sum_{j=s}^{n} b_j \frac{u^j - 1}{u-1} x^{j-s} \in k[x,u].$$

By (ii), $a_{i_0} i_0 \neq 0$ for some $r \le i_0 \le n$. Hence $\tilde{f}(x,1) = \sum_{i=r}^m a_i i x^{i-r}$ is a nonzero polynomial in $x$ and so its zero locus is a finite set $Z$.

Suppose $x \in k \smallsetminus (Z \cup \{0\})$ is such that $\tilde{R}(x) \neq 0$. We claim that $F(x) = F(y)$ implies $x = y$. If not, then since $x \neq 0$, we can write $y = ux$ for some $1 \neq u \in k$. Then $F(x) = F(ux)$ implies that $\tilde{f}(x,u) = 0 = \tilde{g}(x,u)$. Thus $\tilde{f}$ and $\tilde{g}$ have a common zero at $u$, and so $\tilde{R}(x) = 0$, a contradiction. This argument shows that if $\tilde{R}(x) \not\equiv 0$, then aside from $Z \cup \{0\} \cup \{x : \tilde{R}(x) = 0\}$, $F$ is injective, and hence it is almost injective on $\mathbb{A}^1$.

Suppose $x \in k \smallsetminus (Z \cup \{0\})$ is such that $\tilde{R}(x) = 0$. We claim that $F(x) = F(y)$ for some $y \neq x$. Indeed, $\tilde{R}(x) = 0$ implies that $\tilde{f}$ and $\tilde{g}$ have a common zero at $u$. Now we have $\tilde{f}(x,u) = 0 = \tilde{g}(x,u)$, and so $F(x) = F(ux)$. Note that $\tilde{f}(x,1) \neq 0$ since $x \notin Z$, so $u \neq 1$. Since $x \neq 0$ and $u \neq 1$, $ux \neq x$, as desired. This argument shows that if $\tilde{R}(x) \equiv 0$, then aside from $Z \cup \{0\}$, $F$ is at least two-to-one, and hence it is not almost injective on $\mathbb{A}^1$. □

We now recall the notion of a *weakly superMorse* polynomial $f(x) \in k[x]$, cf. [**Ka-ACT**, 5.5]. We require the following three conditions.

(WSM1) $n := \deg(f)$ is invertible in $k$, and $n \ge 2$.

(WSM2) The derivative $f'(x)$ has $n-1$ distinct zeroes in $\overline{k}$.

(WSM3) $f$ separates the zeroes of $f'$, i.e., if $f'(\alpha) = f'(\beta) = 0$ and $f(\alpha) = f(\beta)$, then $\alpha = \beta$.

Remark 12.4.8. The condition (WSM2) forces the characteristic $p \neq 2$, since (WSM2) means precisely that (WSM1) holds and that $\gcd(f', f'') = 1$, while $f''$ vanishes in characteristic 2. When $p \nmid n(n-1)$ and $n \ge 2$, the polynomial $x^n + ax$, for any $a \neq 0$, is weakly superMorse. When $n \ge 3$ is odd and $p \nmid n(n-2)$, the polynomial $x^n + ax^2$, for any $a \neq 0$, is weakly superMorse. And for any $f$ whose degree is prime to $p$, and for which $f''$ is not identically zero, then $f(x)+ax$ is weakly superMorse for all but at most finitely many $a \in \overline{k}$, cf. [**Ka-ACT**, 5.15].

We have the following result, which already appears in [**BSD**, Lemma 3].

LEMMA 12.4.9. *Suppose $f(x)$ is weakly superMorse of degree $n$. Then the sheaf $\mathcal{F} := f_\star(\overline{\mathbb{Q}_\ell})/\overline{\mathbb{Q}_\ell}$ on $\mathbb{A}^1$, lisse outside the critical values of $f$, is geometrically irreducible with geometric monodromy group $\mathsf{S}_n$ in its deleted permutation representation.*

PROOF. Because $\deg(f)$ is prime to $p$, $\mathcal{F}$ is tame at $\infty$, cf. [**Ka-ACT**, 5.5.4], from which the result follows just as in the proof of [**Ka-ESDE**, 7.10.2.3]. □

LEMMA 12.4.10. *Suppose $f$ is weakly superMorse, in $k[x]$ for a finite field $k$. Then $\Delta_f$ is absolutely irreducible in $k[x,y]$.*

PROOF. By Lemma 12.4.9, the sheaf $\mathcal{F} := f_\star(\overline{\mathbb{Q}_\ell})/\overline{\mathbb{Q}_\ell}$ is geometrically irreducible. The restriction to $\mathbb{G}_m$ of its Fourier transform $\mathcal{H}$ is geometrically isomorphic to the lisse sheaf on $\mathbb{G}_m/k$ whose trace function is given as follows: for $L/k$ a finite extension, and $t \in L^\times$,

$$\mathrm{Trace}(\mathsf{Frob}_{t,L}|\mathcal{H}) = \frac{1}{\mathsf{Gauss}(\psi_L, \chi_{2,L})} \sum_{x \in L} \psi_L(tf(x)).$$

To see this, write the raw sum as

$$\sum_{u \in L} \psi_L(tu)\#\{x \in L : f(x) = u\},$$

which is equal to the sum

$$\sum_{u \in L} \psi_L(tu)(\#\{x \in L : f(x) = u\} - 1),$$

simply because the term being subtracted is, for each $t \neq 0$, the sum $\sum_{u \in L} \psi_L(tu) = 0$. This sheaf $\mathcal{H}$ is geometrically irreducible, hence its $M_{1,1} = 1$. Its empirical $M_{1,1}$ is then the sum

$$\frac{1}{(\#L)(\#L-1)} \sum_{t \in L^\times} \sum_{x,y \in L} \psi_L(t(f(x) - f(y))$$

The “missing term” for $t = 0$ is

$$\frac{(\#L)^2}{(\#L)(\#L-1)} = 1 + O(1/\#L).$$

Thus $2 = 1 + M_{1,1}$ is the large $L$ limit of

$$\frac{1}{(\#L)(\#L-1)} \sum_{t \in L} \sum_{x,y \in L} \psi_L(t(f(x) - f(y)) = \frac{1}{(\#L-1)}\#\{(x,y) \in L^2 \mid f(x) = f(y)\}.$$

Thus the polynomial $f(x) - f(y)$ is, geometrically, the product of powers of two distinct geometrically irreducible factors, one of which is visibly $x - y$. In the factorization

$$f(x) - f(y) = (x - y)\Delta_f,$$

we must first show that $\Delta_f$ is not divisible by $x-y$, and second that $\Delta_f$ is not a proper power. But the highest degree term of $\Delta_f$ is a product of linear factors, none of which is $x-y$, so $x-y$ does not divide $\Delta_f$. As the highest degree term of $\Delta_f$ is a product of pairwise distinct linear factors, the highest degeree term is not a proper power, and hence $\Delta_f$ is not a proper power. □

We next recall some basic facts about Deligne polynomials. They arise naturally here, as follows. Given a polynomial $f(x) \in k[x]$ whose degree $d$ is invertible in $k$, the polynomial $f(x) + f(y) - f(z) - f(w)$ is a Deligne polynomial in four variables, and the polynomial $f(x) + f(y) - f(z)$ is a Deligne polynomial in three variables,

Let $k$ be a field, $n \geq 2$ an integer, and $F(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$ a polynomial of degree $d \geq 1$, say $F = F_d + F_{d-1} + \ldots + F_0$ with $F_i$ homogeneous of degree $i$. Following [**De1**, 8.4], we say that $F$ is a *Deligne polynomial* if its degree $d$ is invertible in $k$ and if the locus $F_d = 0$ in $\mathbb{P}^{n-1}$ is a non-singular hypersurface.

Lemma 12.4.11. *Suppose $F$ is a Deligne polynomial in $n \geq 3$ variables. Then we have the following results.*

(i) *The polynomial $F \in k[x_1, \ldots, x_n]$ is geometrically irreducible (i.e., for $L$ any algebraically closed extension of $k$, $F$ is irreducible in $L[x_1, \ldots, x_n]$).*

(ii) *The affine hypersurface $H$ defined by $F = 0$ in $\mathbb{A}^n$, and its projective closure $H_0$ in $\mathbb{P}^n$, defined by the vanishing of*

$$F_T := F_d + TF_{d-1} + \ldots + T^d F_0$$

*each have at worst isolated singularities.*

(iii) *If $k$ is finite, then the for $\mathbb{F}_q/k$ a finite extension we have*

$$\#H(\mathbb{F}_q) = q^{n-1} + O(q^{n/2}).$$

Proof. We first prove (i). For this, we may extend scalars, and reduce to the case when $k$ is algebraically closed. If $F$ were reducible, say $F = AB$, with $\deg(A) = a, \deg(B) = b$, then their higest degree terms give a factorization $A_a B_b = F_d$. But $F_d$ is irreducible, because it defines a smooth hypersurface in $\mathbb{P}^{n-1}$. Recall why this is so. Any hypersurface $Z$ in $\mathbb{P}^r$ with $r \geq 2$ is connected ("weak Lefschetz": because $\mathbb{P}^r \smallsetminus Z$ is smooth and affine, we have $H^i_c(\mathbb{P}^r \smallsetminus Z, \overline{\mathbb{Q}_\ell}) = 0$ for $i < r$, hence from the long exact excision sequence with $\overline{\mathbb{Q}_\ell}$-coefficients

$$\ldots \to H^i_c(\mathbb{P}^r \smallsetminus Z) \to H^i(\mathbb{P}^r) \to H^i(Z) \to H^{i+1}_c(\mathbb{P}^r \smallsetminus Z) \to \ldots$$

In particular, as $H^i_c(\mathbb{P}^r \smallsetminus Z) = 0$ for $i = 0, 1$ we get $H^0(\mathbb{P}^r) \cong H^0(Z)$ so long as $r \geq 2$, hence $H^0(Z)$ has dimension one, i.e., $Z$ is connected.) If $Z$ is smooth in addition, then it is irreducible (because smooth and connected).

To prove (ii), we argue as follows. We tack on a new variable $T$, and consider the homogenous form

$$F_T := F_d + TF_{d-1} + \ldots + T^d F_0$$

in $n+1$ variables. We denote by $H_0$ the projective hypersurface $F_T = 0$ in $\mathbb{P}^n$ (with $X_1, \ldots, X_n, T$ as homogeneous coordinates). Then the affine hypersurface $H$ is the open set $H_0[1/T]$ of $H_0$, so it suffices to show that $H_0$ has at worst isolated singularities. The key observation is that $H_0 \cap (T = 0)$ is the smooth hypersurface $F_d = 0$ in $\mathbb{P}^{n-1}$. On the one hand, we have

$$\mathrm{Sing}(H_0) \cap (T = 0) \subset \mathrm{Sing}(H_0 \cap (T = 0)).$$

[This is the affine statement that if a polynomial $f(y_1, \dots, y_n)$ only starts in degree $\geq 2$ (meaning that the origin is a singular point of $f = 0$), then after putting $y_n$ to 0, the resulting polynomial $f(y_1, \dots, y_{n-1}, 0)$ in $n-1$ variables only starts in degree $\geq 2$.] On the other hand, for any closed subscheme $Z$ of $\mathbb{P}^n$, we have [**Hart**, Prop. 7.2]

$$\dim(Z \cap (T = 0)) \geq \dim(Z) - 1.$$

Applied to $Z := \mathrm{Sing}(H_0)$, we see that if $\mathrm{Sing}(H_0)$ had dimension $\geq 1$, then $\mathrm{Sing}(H_0 \cap (T = 0))$ would be non-empty, a contradiction.

To prove (iiii), we argue as follows. Because $H_0$ has at worst isolated singularities, one knows [**Hoo**, Thm. 1] that

$$\#H_0(\mathbb{F}_q) = \#\mathbb{P}^{n-1}(\mathbb{F}_q) + O(q^{n/2}),$$

while by Deligne one knows that the nonsingular hypersurface $H_0 \cap (T = 0)$ has

$$\#(H_0 \cap (T = 0))(\mathbb{F}_q) = \#\mathbb{P}^{n-2}(\mathbb{F}_q) + O(q^{n/2-1}).$$

Subtracting, we get the the assertion (iii). □

LEMMA 12.4.12. *Suppose $F$ and $G$ are Deligne polynomials in $n \geq 3$ variables over $k$ which are not multiple of each other. For the affine hypersurfaces $H$ and $J$ in $\mathbb{A}^n$ defined by $F = 0$ and $G = 0$, we have* $\dim(H \cap J) \leq n - 2$.

PROOF. If $H \cap J$ is empty, there is nothing to prove. If not, then $\dim(H \cap J) \geq n - 2$, cf. [**Hart**, Prop. 7.1]. On the other hand, it is obvious that $\dim(H \cap J) \leq \dim(H) = n - 1$. If $H \cap J$ had an irreducible component of dimension $n - 1$, that component must be $H$, and it must also be $J$, nonsense. □

COROLLARY 12.4.13. *Suppose $F$ and $G$ are Deligne polynomials of different degrees in $n \geq 3$ variables over a finite field $k$. For $\alpha, \beta \in k$, define the hypersurfaces $H_\alpha$ of equation $F = \alpha$ and $J_\beta$ of equation $G = \beta$. Then for $\mathbb{F}_q/k$ a finite extension, we have $\#(H_\alpha(\mathbb{F}_q) \cap J_\beta(\mathbb{F}_q)) = O(q^{n-2})$.*

PROOF. Each of $F - \alpha$ and $G - \beta$ is a Deligne polynomial. Because their degrees are different, they are not $k^\times$ proportional, so the result is immediate from Lemma 12.4.12 and Lang–Weil. □

With these preliminaries established, we now give the main result of this section.

THEOREM 12.4.14. *Let $p$ be a a prime, $k/\mathbb{F}_p$ a finite extension, and let*

$$f(x) = \sum_{i=0}^{m} a_i x^i, \ g(x) = \sum_{j=0}^{n} b_j x^j \in k[x]$$

*be polynomials of degree $m$, respectively $n > m$, with $p \nmid mn$. Consider the local system $\mathcal{F}$ on $\mathbb{A}^1 \times \mathbb{G}_m$ with the following trace function. For $L/k$ a finite extension, and $(s, t) \in L \times L^\times$,* *the trace function of $\mathcal{F}$ is*

$$(s,t) \mapsto -\sum_{x\in L} \psi_L\big(sf(x)+tg(x)\big).$$

*Assume that the map $x \mapsto (f(x), g(x))$ is almost injective. Then $M_{2,2}(\mathcal{F})+1$ is equal to the number $M$ of distinct geometrically irreducible factors of the polynomial*

$$R(x,y,z) := \mathsf{Res}_w\big(f(w)-(f(x)+f(y)-f(z)), g(w)-(g(x)+g(y)-g(z))\big).$$

Proof. Let $\Sigma_f(x,y,z,w) := f(x)+f(y)-f(z)-f(w)$ and similarly for $\Sigma_g$. As in the proof of Theorem 12.1.3, we may assume that $k$ contains all roots of unity of order dividing a sufficiently divisible integer, and then $M_{2,2}$ is the large $L$ limit of the sums

$$\begin{aligned}&\frac{1}{(\#L)^3(\#L-1)}\sum_{s\in L,\ t\in L^\times}\ \sum_{x,y,z,w\in L}\psi_L\big(s\Sigma_f+t\Sigma_g\big)\\ =&\frac{1}{(\#L)^3(\#L-1)}\sum_{x,y,z,w\in L}\Big(\sum_{s\in L}\psi_L(s\Sigma_f)\Big)\Big(\sum_{t\in L^\times}\psi_L(t\Sigma_g)\Big)\\ =&\frac{1}{(\#L)^2(\#L-1)}\sum_{x,y,z,w\in L,\ \Sigma_f=0}\Big(\sum_{t\in L}\psi_L(t\Sigma_g)-1\Big)\end{aligned}$$

The "correction term"

$$\frac{1}{(\#L)^2(\#L-1)}\#\{(x,y,z,w)\in L^4 \mid \Sigma_f=0\},$$

is $1+o(1)$, by part (3) of Lemma 12.4.11. Hence $M_{2,2}+1$ is the large $L$ limit of

$$\frac{1}{(\#L)(\#L-1)}\#\{(x,y,z,w)\in L^4 \mid \Sigma_f=0=\Sigma_g\}.$$

Now we count the points $P=(x_0,y_0,z_0,w_0)\in L^4$ that belong to $\Sigma_f=0=\Sigma_g$, i.e., solutions of

$$(12.4.14.1)\qquad f(w)-(f(x)+f(y)-f(z))=0,\ \ g(w)-(g(x)+g(y)-g(z))=0.$$

First, being a solution means that $(x_0,y_0,z_0)$ is in the zero locus of $R(x,y,z)$. Once $(x_0,y_0,z_0)$ is a zero of $R(x,y,z)$, this means the two polynomials in $w$

$$f(w)-(f(x_0)+f(y_0)-f(z_0)),\quad g(w)-(g(x_0)+g(y_0)-g(z_0))$$

have a common zero. Because the map $w\mapsto(f(w),g(w))$ is injective on $\mathbb{A}^1$ except possibly at $w_1,\ldots,w_N$, these two equations determine $w$, so long as $w$ is not among $w_1,\ldots,w_N$. For each of these exceptional $w_i$, the number of solutions in $L^3$ of

$$f(w_i)=f(x)+f(y)-f(z),\quad g(w_i)=g(x)+f(y-g(z)$$

is $O(\#L)$, by Corollary 12.4.13. Thus up to an $O(\#L)$ error, then number of $L$ points in $\Sigma_f=0=\Sigma_g$ is the number of zeroes in $L^3$ of the polynomial $R(x,y,z)$.

Notice that the polynomial $R(x,y,z)$ is nonzero. For if $R(x,y,z)=0$ identically, then the locus $\Sigma_f=\Sigma_g=0$ maps onto the $\mathbb{A}^3$ of $(x,y,z)$, so has dimension $\geq 3$, contradicting Lemma 12.4.12, according to which the locus $\Sigma_f=\Sigma_g=0$ has dimension $\leq 2$.

At the expense of passing to a finite extension, we may assume that all irreducible factors of $R(x,y,z)$ are geometrically irreducible. Then for $M$ the number of distinct geometrically irreducible factors of $R(x,y,z)$, Lang–Weil gives the number of $L$-points as

$$M(\#L)^2 + O((\#L)^{3/2}),$$

completing the proof. □

## 12.5. Some applications of almost injectivity

Recall [**Zs**] that if $a \geq 2$ and $n \geq 2$ are any integers with $(a,n) \neq (2,6)$, $(2^k-1,2)$, then $a^n-1$ has a *primitive prime divisor*, that is, a prime divisor $\ell$ that does not divide $\prod_{i=1}^{n-1}(a^i-1)$; write $\ell = \mathrm{ppd}(a,n)$ in this case. Furthermore, if in addition $a,n \geq 3$ and $(a,n) \neq (3,4)$, $(3,6)$, $(5,6)$, then $a^n-1$ admits a *large primitive prime divisor*, i.e. a primitive prime divisor $\ell$ where either $\ell > n+1$ (whence $\ell \geq 2n+1$), or $\ell^2 | (a^n-1)$, see [**F2**]. We will need the following recognition theorem.

Theorem 12.5.1. [**KT2**, Theorem 4.6] *Let $q = p^f$ be a power of an odd prime $p$ and let $d \geq 2$. If $d = 2$, suppose that $p^{df}-1$ admits a primitive prime divisor $\ell \geq 5$ with $(p^{df}-1)_\ell \geq 7$. If $d \geq 3$, suppose in addition that $(p,df) \neq (3,4)$, $(3,6)$, $(5,6)$, so that $p^{df}-1$ admits a large primitive prime divisor $\ell$. In either case, we choose such an $\ell$ to maximize the $\ell$-part of $p^{df}-1$. Let $W = \mathbb{F}_q^d$ and let $G$ be a subgroup of $\mathrm{GL}(W) \cong \mathrm{GL}_d(q)$ of order divisible by the $\ell$-part $Q := (q^d-1)_\ell$ of $q^d-1$. Then either $L := \mathbf{O}^{\ell'}(G)$ is a cyclic $\ell$-group of order $Q$, or there is a divisor $j < d$ of $d$ such that one of the following statements holds.*

(i) *$L = \mathrm{SL}(W_j) \cong \mathrm{SL}_{d/j}(q^j)$, $d/j \geq 3$, and $W_j$ is $W$ viewed as a $d/j$-dimensional vector space over $\mathbb{F}_{q^j}$.*

(ii) *$2j|d$, $W_j$ is $W$ viewed as a $d/j$-dimensional vector space over $\mathbb{F}_{q^j}$ endowed with a non-degenerate symplectic form, and $L = \mathrm{Sp}(W_j) \cong \mathrm{Sp}_{d/j}(q^j)$.*

(iii) *$2|jf$, $2 \nmid d/j$, $W_j$ is $W$ viewed as a $d/j$-dimensional vector space over $\mathbb{F}_{q^j}$ endowed with a non-degenerate Hermitian form, and $L = \mathrm{SU}(W_j) \cong \mathrm{SU}_{d/j}(q^{j/2})$.*

(iv) *$2j|d$, $d/j \geq 4$, $W_j$ is $W$ viewed as a $d/j$-dimensional vector space over $\mathbb{F}_{q^j}$ endowed with a non-degenerate quadratic form of type $-$, and $L = \Omega(W_j) \cong \Omega^-_{d/j}(q^j)$.*

(v) *$(p, df, L/\mathbf{Z}(L)) = (3, 18, \mathrm{PSL}_2(37))$, $(17, 6, \mathrm{PSL}_2(13))$.*

Theorem 12.5.2. *Let $q = p^f$ be a power of an odd prime $p$, and let $n > m \geq 1$ be integers with $m > n/2$ and $\gcd(m,n) = 1$, so that there exist primitive prime divisors $\ell = \mathrm{ppd}(p,2nf)$ and $\ell' = \mathrm{ppd}(p,2mf)$. If $(p,2nf) \neq (3,6)$, $(5,6)$, assume $\ell$ is chosen to be a large primitive prime divisor of $p^{2nf}-1$. Let $W = \mathbb{F}_q^{2n}$ and let $G$ be a subgroup of $\Gamma := \mathrm{Sp}(W) \cong \mathrm{Sp}_{2n}(q)$ of order divisible by $Q\ell'$, where $Q := (q^{2n}-1)_\ell$ is the $\ell$-part of $q^{2n}-1$. Then one of the following statements holds.*

(i) *$G = \mathrm{Sp}(W)$.*

(ii) *$2 \nmid mn$ and $\mathrm{SU}(W) \lhd G \leq \mathrm{GU}(W) \rtimes C_2$, where $W$ viewed as an $n$-dimensional vector space over $\mathbb{F}_{q^2}$ endowed with a non-degenerate Hermitian form.*

Proof. (a) The conditions on $m,n$ imply that $m \geq 2$ and $n \geq 3$. Assume furthermore that $(p,2nf) = (3,6)$ or $(5,6)$. Then $(n.m) = (3,2)$ and $q = p$ is 3, respectively 5. Our subgroup $G$ now has order divisible by 35, respectively by 91. Inspecting the list of maximal subgroups of $\mathrm{PSp}_6(p)$ [**BHR**, Tables 8.28, 8.29], we conclude that $G\mathbf{Z}(\Gamma) = \Gamma$, and hence $G = \Gamma$. Hence, in what follows, we may assume that

$$(p, 2nf) \neq (3, 6),\ (5, 6)$$

and thus $\ell$ is a large primitive prime divisor of $p^{2nf} - 1$. Assume now that $(p, 2nf) = (17, 6)$. Then $(n, m) = (3, 2)$, $\ell = 13$, and $\ell' = 5$ or $29$. Again using the list of maximal subgroups of $\mathrm{PSp}_6(p)$ [**BHR**, Tables 8.28, 8.29], we see that the condition $|G|$ is divisible by $\ell\ell'$ forces $G = \Gamma$ in this case. So we may assume

$$(p, 2nf) \neq (17, 6)$$

and apply Theorem 12.5.1 (with $d = 2n$) to $L = \mathbf{O}^{\ell'}(G)$.

Suppose $L = \langle g \rangle$ is cyclic of order $Q$. Then $L$ is a Sylow $\ell$-subgroup $R$ of $\Gamma$, and acts irreducibly on $W$ (by the choice of $\ell$). Thus, by Lemma 8.3.2(i), $W$ becomes an 1-dimensional $R$-representation over $\mathrm{End}_R(W)$, which implies that $\mathrm{End}_R(W) \cong \mathbb{F}_{q^{2n}}$ and so $\mathbf{C}_{\mathrm{GL}(W)}(R)$ has order dividing $q^{2n} - 1$. In fact, $\mathbf{C}_\Gamma(R)$ already contains a maximal torus of order $q^n + 1$, so we must have that

$$|\mathbf{C}_\Gamma(R)| = q^n + 1. \tag{12.5.2.1}$$

By looking at the spectrum of $g$ on $W$, we see that the action of $\mathbf{N}_\Gamma(L)$ can induce only a subgroup of order dividing $2n$ of $\mathrm{Aut}(L)$. Hence $|G|$ divides $2n(q^n + 1)$, and this contradicts the assumption that $\ell'$ divides $|G|$, since

$$\ell' = \mathrm{ppd}(p, 2mf) \geq 2mf + 1 > nf > 2. \tag{12.5.2.2}$$

Suppose now that $(p, 2nf, L/\mathbf{Z}(L)) = (3, 18, \mathrm{PSL}_2(37))$. Since the smallest dimension of nontrivial projective representations of $\mathrm{PSL}_2(37)$ in characteristic 3 is 18, we must have that $n = 9$ and $q = 3$. It follows that $m \in \{5, 7, 8\}$, and so $\ell' \in \{17, 61, 73, 193, 547\}$. In particular, $\ell'$ does not divide $|\mathrm{Aut}(L)|$, so any element $h \in G$ of order $\ell'$ must centralize $L$. But $L$ acts absolutely irreducibly on $W = \mathbb{F}_3^{18}$, so $h \in \mathrm{Sp}(W)$ must be scalar and hence of order $\leq 2$, a contradiction. We have therefore shown that $L$ satisfies one of the conclusions (i)–(iv) of Theorem 12.5.1.

(b) Recall that $G \rhd L$ contains an element $h$ of order $\ell'$. We now show that

$$\ell' \text{ divides } |L|. \tag{12.5.2.3}$$

First, in (12.5.2.1) we have shown that the centralizer of any Sylow $\ell$-subgroup $R$ of $\Gamma$ has order $q^n + 1$, which is coprime to $\ell'$. The same is true for $\mathbf{C}_\Gamma(L)$, so $h$ must act nontrivially on $L$. If $\ell'$ does not divide $|L|$, then $h$ induces a coprime automorphism of $L$, a quasisimple group of Lie type over $\mathbb{F}_{p^{jf}}$. Using [**GLS**, Theorem 2.5.12] we then have $\ell'$ divides $jf$, and so $\ell' | 2nf$, which is impossible because of (12.5.2.2).

Next suppose that we are in case (i) of Theorem 12.5.1. Then $2n/j \geq 3$, and $L \cong \mathrm{SL}_{2n/j}(q^j)$ contains a maximal torus of order

$$\frac{q^{2n} - 1}{q^j - 1} \geq \frac{q^{2n} - 1}{q^{2n/3} - 1} > q^n + 1$$

which centralizes a Sylow $\ell$-subgroup $R$ of $L$. But this contradicts (12.5.2.1).

Suppose now that we are in case (ii) of Theorem 12.5.1. Then $j|n$ and $L \cong \mathrm{Sp}_{2n/j}(q^j)$. Hence (12.5.2.3) implies that there is some integer $1 \leq i \leq n/j$ such that $\ell'$ divides $q^{2ij} - 1$. The primitivity of $\ell'$ then implies that $2mf|2ijf$, and so $m|ij \leq n < 2m$. It follows that $ij = m$, and thus $j$ divides both $m$ and $n$. But $\gcd(m, n) = 1$, so $j = 1$. We have shown that $\Gamma = \mathrm{Sp}_{2n}(q) \geq G \rhd L \cong \mathrm{Sp}_{2n}(q)$, whence $G = \Gamma$, as stated in conclusion (i).

Suppose next that we are in case (iv) of Theorem 12.5.1. Then $j|n$, $j \leq n/2$, and $L \cong \Omega^-_{2n/j}(q^j)$. Using (12.5.2.3) and arguing as in the preceding case, we obtain that $j = 1$. It follows that

$$\Omega^-_{2n}(q) \cong L \leq \Gamma = \mathrm{Sp}_{2n}(q).$$

Moreover, as stated in Theorem 12.5.1(iv), $W = \mathbb{F}_q^{2n}$ is a natural, hence absolutely irreducible, $L$-module endowed with a non-degenerate quadratic form of type $-$. At the same time, $L$, as a subgroup of $\Gamma = \mathrm{Sp}(W)$, fixes a non-degenerate symplectic form on $W$. This is impossible since $p > 2$.

Finally, assume that we are in case (iii) of Theorem 12.5.1. Then $j|2n$, but $2n/j$ is odd and at least 3. So $j = 2j_0$ with $j_0|n$, and $n/j_0$ is still odd and at least 3. Furthermore, $L \cong \mathrm{SU}_{n/j_0}(q^{j_0})$. Now (12.5.2.3) implies that there is some integer $1 \leq i \leq n/j_0$ such that $\ell'$ divides $q^{ij_0} - (-1)^i$. The primitivity of $\ell'$ then implies that $2mf|2ij_0f$, and so $m|ij_0 \leq n < 2m$. It follows that $ij_0 = m$, and thus $j$ divides both $m$ and $n$. But $\gcd(m, n) = 1$, so $j_0 = 1$, $n$ is odd, and $m = i$. If $2|i$ in addition, then $\ell'$ divides $q^i - 1 = q^m - 1$, contrary to $\ell' = \mathrm{ppd}(p, 2mf)$. So $m$ is odd. We have shown that $2 \nmid mn$, and $\Gamma = \mathrm{Sp}_{2n}(q) \geq G \rhd L \cong \mathrm{SU}_n(q)$. Moreover, as stated in Theorem 12.5.1(iii), $W$ viewed as an $n$-dimensional space over $\mathbb{F}_{q^2}$ is a natural module for $L$. Since $\mathbf{N}_\Gamma(L) \cong \mathrm{GU}(W) \rtimes C_2$, we arrive at conclusion (ii). □

REMARK 12.5.3. Note that Theorem 12.5.2 does not hold without the assumption that $m > n/2$. For instance, the subgroup $\mathrm{Sp}_8(q^2)$ of $\mathrm{Sp}_{16}(q)$ has order divisible by $q^{12} - 1$, giving a counterexample for $(n, m) = (8, 3)$ or $(8, 1)$. Furthermore, if $m = n/2$, then $(n, m) = (2, 1)$ (as $\gcd(m, n) = 1$), in which case $\mathrm{Sp}_2(q^2)$ is a counterexample. More generally, if $\gcd(m, n) = j > 1$ then $\mathrm{Sp}_{2n/j}(q^j)$ would be a counterexample.

Now we are in position to determine, for the first time, the geometric monodromy groups of a large family of two-parameters local systems with non-monomial coefficients for both parameters:

THEOREM 12.5.4. *Let $q = p^\nu$ be a power of an odd prime $p$, $k/\mathbb{F}_p$ a finite extension, $a, b \in k$, $0 \leq n_1 < n_2 < \ldots < n_r$, $0 \leq m_1 < \ldots < m_u$ two sequences of integers, $A_1, \ldots, A_r$ and $B_1, \ldots, B_u$ two sequences of elements of $k^\times$, and*

$$f(x) = ax + \sum_{i=1}^{r} A_i x^{1+q^{n_i}},\ g(x) = bx + \sum_{j=1}^{u} B_j x^{1+q^{m_j}}.$$

*Assume that $n := n_r \geq 1$ and $m := m_u \geq 1$ are coprime, $2|mn$, and $n > m > n/2$. Consider the local system $\mathcal{F} = \mathcal{F}(k, f, g)$ of rank $q^n$ on $(\mathbb{G}_m \times \mathbb{A}^1)/k$, whose trace function is given as follows: for $L/k$ a finite extension, and $(s, t) \in L^\times \times L$,*

$$\mathrm{Trace}(\mathsf{Frob}_{(s,t),L}|\mathcal{F}(k, f, g)) = -\sum_{x \in L} \psi_L(sf(x) + tg(x)).$$

*Then the following statements hold for the geometric monodromy group $G = G_{\mathrm{geom}}$ of $\mathcal{F}$.*

(i) *If* $(a,b) \neq (0,0)$, *then* $G = p_+^{1+2n\nu} \rtimes \mathrm{Sp}_{2n}(q)$; *in particular,* $\mathcal{F}$ *has* $M_{2,2} = 2$.
(ii) *If* $(a,b) = (0,0)$, *then* $G = \mathrm{Sp}_{2n}(q)$ *in its total Weil representation.*

Proof. (a) Consider the local system $\mathcal{H}^\sharp$ whose trace function is given as follows: for any finite extension $L/k$, the trace at $(s_0, s_1, \dots, s_r, t_0, t_1, \dots, t_u) \in L^\times \times L^{t+u+1}$ is given by

$$-\sum_{x \in L} \psi_L\big(s_0 x + \sum_{i=1}^{r} s_i x^{1+q^{n_i}} + t_0 x + \sum_{j=1}^{u} t_j x^{1+q^{m_j}}\big).$$

By Corollary 11.2.5(i), $\mathcal{H}^\sharp$ has geometric monodromy group

$$H = p_+^{1+2n\nu} \rtimes \mathrm{Sp}_{2n}(q) = E \rtimes \Gamma,$$

where $E = p_+^{1+2n\nu}$ and $\Gamma = \mathrm{Sp}_{2n}(q)$. Since $\mathcal{F}$ is obtained from $\mathcal{H}^\sharp$ by a suitable specialization, we have $G \leq H$. Moreover, $H$ has $M_{2,2} = 2$. Hence, in the case $(a,b) \neq (0,0)$, it suffices to prove that $G = H$.

(b) Assume that $(a,b) \neq (0,0)$. If $a \neq 0$ then $\Delta_f$ is absolutely irreducible by Lemma 12.4.5. Similarly, if $b \neq 0$ then $\Delta_g$ is absolutely irreducible. Hence, in this case at least one of $\Delta_f$, $\Delta_g$ is absolutely irreducible. Note that $\deg(f) = q^n + 1$ and $\deg(g) = q^m + 1$, with $\gcd(m,n) = 1$ and $2|mn$. It follows that

$$\gcd(\deg(f), \deg(g)) = 2$$

and so none of $\deg(f)$, $\deg(g)$ divides the other one. Hence $f$ and $g$ satisfy the hypothesis of Lemma 12.4.3, and so $R(y)$ as defined in (12.4.1.1) is nonzero in $k[y]$. In turn, this implies by Lemma 12.4.1 that the map $x \mapsto (f(x), g(x)$ is almost injective, and hence $\mathcal{F}$ is irreducible by Corollary 12.4.2. We have shown that $G$ is an irreducible subgroup of $H$ if $(a,b) \neq (0,0)$.

(c) Next, applying Lemma 12.3.11, we see that $|G|$ is divisible by both $q^n+1$ and $q^m+1$.

Assume in addition that $(a,b) = (0,0)$. Applying Corollary 11.2.5(ii) to the specialization $s_0 = t_0 = 0$ of $\mathcal{H}^\sharp$, we see that $G$ is contained in the image of $\mathrm{Sp}_{2n}(q)$ in its total Weil representation. Applying Theorem 12.5.2 to $G$, we conclude that $G = \mathrm{Sp}_{2n}(q)$, and the proof of (ii) is completed.

In the rest of the proof we will assume that $(a,b) \neq (0,0)$. Then both $q^n+1$ and $q^m+1$ divide the order of $EG/E$, a subgroup of $\Gamma = \mathrm{Sp}_{2n}(q)$. Applying Theorem 12.5.2 to $EG/E$, we conclude that $EG/E = \Gamma = H/E$, and hence $EG = H$.

Now we note $\mathbf{Z}(E) \leq \mathbf{Z}(H)$, and work in $EG/\mathbf{Z}(E) = (E/\mathbf{Z}(E)) \rtimes \Gamma$. Since $\mathbf{Z}(E)G/\mathbf{Z}(E)$ has order divisible by $q^n+1$, it acts irreducibly on $E/\mathbf{Z}(E)$. It follows that

$$\mathbf{Z}(E)G \cap E \text{ is either } \mathbf{Z}(E) \text{ or } E.$$

In the former case, $\mathbf{Z}(E)G/\mathbf{Z}(E)$ intersects $E/\mathbf{Z}(E)$ trivially but $EG = H$. In such a case, $\mathbf{Z}(E)G/\mathbf{Z}(E)$ is a complement to $E/\mathbf{Z}(E)$ in $H/\mathbf{Z}(E)$, whence $\mathbf{Z}(E)G/\mathbf{Z}(E) \cong H/E = \Gamma$. Thus $\mathbf{Z}(E)G/\mathbf{Z}(E)$ is an extension of $\mathbf{Z}(E) \cong C_p$ by $\Gamma = \mathrm{Sp}_{2n}(q)$. As $\Gamma$ is quasisimple and it is the universal cover of $\mathrm{PSp}_{2N}(q)$, we get $(\mathbf{Z}(E)G)^{(\infty)} \cong \Gamma$ and thus $\mathbf{Z}(E)G \cong \mathbf{Z}(E) \times \Gamma$. In particular, $\mathbf{Z}(E)G$ cannot have an irreducible representation of degree $q^n$ by [**TZ1**, Theorem 5.2]. Thus $G$ cannot be irreducible on $\mathcal{F}$, contrary to the conclusion of (b).

We have shown that $\mathbf{Z}(E)G \geq E$, and so $\mathbf{Z}(E)G = EG = H$. Taking derived subgroups, we have

$$[G,G] = [\mathbf{Z}(E)G, \mathbf{Z}(E)G] = [H,H] \geq [E,E] = \mathbf{Z}(E).$$

Consequently, $G = \mathbf{Z}(E)G = H$. $\square$

The next result gives a $p = 2$ analogue of Theorem 12.5.4.

Theorem 12.5.5. *Let $q = 2^\nu \geq 2$, $k/\mathbb{F}_2$ a finite extension, $a, b \in k$, $1 \leq n_1 < n_2 < \ldots < n_r$, $1 \leq m_1 < \ldots < m_u$ two sequences of integers, $A_1, \ldots, A_r$ and $B_1, \ldots, B_u$ two sequences of elements of $k^\times$, and*

$$f(x) = ax + \sum_{i=1}^{r} A_i x^{1+q^{n_i}},\ \ g(x) = bx + \sum_{j=1}^{u} B_j x^{1+q^{m_j}}.$$

*Assume that $n := n_r \geq 1$ and $m := m_u \geq 1$ are coprime, $2|mn$, $n > m$, and $n\nu \geq 4$. Consider the local system $\mathcal{F} = \mathcal{F}(k, f, g)$ of rank $q^n$ on $(\mathbb{G}_m \times \mathbb{A}^1)/k$, whose trace function is given as follows: for $L/k$ a finite extension and $(s, t) \in L^\times \times L$,*

$$\mathrm{Trace}(\mathsf{Frob}_{(s,t),L}|\mathcal{F}(k, f, g)) = -\sum_{x \in L} \psi_L(sf(x) + tg(x)).$$

*Then $\mathcal{F}$ has geometric monodromy group $G = G_{\mathrm{geom}} = H_\nu^\circ = 2_-^{1+2n\nu} \cdot \Omega_{2n}^-(q)$, cf. (8.2.2.1).*

Proof. Consider the local system $\mathcal{H}^\sharp$ whose trace function is given as follows: for any finite extension $L/k$, the trace at $(s_0, s_1, \ldots, s_r, t_0, t_1, \ldots, t_u) \in L^\times \times L^{t+u+1}$ is given by

$$-\sum_{x \in L} \psi_L\big(s_0 x + \sum_{i=1}^{r} s_i x^{1+q^{n_i}} + t_0 x + \sum_{j=1}^{u} t_j x^{1+q^{m_j}}\big).$$

By Corollary 11.2.7, $\mathcal{H}^\sharp$ has geometric monodromy group

$$H = H_\nu^\circ = E \cdot S = 2_-^{1+2n\nu} \cdot \Omega_{2n}^-(q),$$

where $E = 2_-^{1+2n\nu}$ and $S = \Omega_{2n}^-(q)$. Since $\mathcal{F}$ is obtained from $\mathcal{H}^\sharp$ by a suitable specialization, we have $G \leq H$.

The hypothesis on $n$ and $m$ implies that $\gcd(q^n + 1, q^m + 1) = 1$. Now, applying Lemmas 12.3.11 and 12.3.13, we see that $|G|$ is divisible by all three integers $q^n + 1$, $q^m + 1$, and $q^n - q^m$. Hence, $EG/E$ is a subgroup of $S = \Omega_{2n}^-(q)$, of order divisible by

$$\mathrm{lcm}(q^n + 1, q^m + 1, (q^{n-m} - 1).$$

Applying Theorem 8.3.4 to $EG/E$, we obtain that $EG/E = S$, unless $(n, m, q) = (5, 2, 2)$ and $L \in \{\mathsf{A}_{11}, \mathsf{A}_{12}\}$ for $L := \mathbf{O}^{11'}(\bar{G})$ and $\bar{G} := EG/E \cong G/(G \cap E)$. In these exceptional cases, by Lemma 12.3.11, $G$, and so $\bar{G}$, admit an element $g$ of order $2^5 + 1 = 33$. Certainly, the element $g^3$ of order 11 is contained in $L = \mathbf{O}^{11'}(\bar{G})$. But $L$ does not have any element of order 33, so $g \notin L$. As $L \lhd \bar{G}$ and $|\mathrm{Out}(L)| = 2$, we conclude that $\langle L, g \rangle \cong L \times C_3$ is a subgroup of $S = \Omega_{10}^-(2)$. The latter is however impossible, by an inspection of maximal subgroups of $\Omega_{10}^-(2)$ [**CCNPW**].

We have shown that $EG/E = S$, and hence

$$EG = H.$$

Next we note $\mathbf{Z}(E) \leq \mathbf{Z}(H)$, and work in $EG/\mathbf{Z}(E) = (E/\mathbf{Z}(E)) \cdot S$. Since $\mathbf{Z}(E)G/\mathbf{Z}(E)$ has order divisible by $q^n + 1$ (and $n\nu \geq 4$), it acts irreducibly on $E/\mathbf{Z}(E)$. It follows that

$$\mathbf{Z}(E)G \cap E \text{ is either } \mathbf{Z}(E) \text{ or } E.$$

In the former case, $\mathbf{Z}(E)G/\mathbf{Z}(E)$ intersects $E/\mathbf{Z}(E)$ trivially but $EG = H$. In such a case, $\mathbf{Z}(E)G/\mathbf{Z}(E)$ is a complement to $E/\mathbf{Z}(E)$ in $H/\mathbf{Z}(E)$, whence $\mathbf{Z}(E)G/\mathbf{Z}(E) \cong H/E = S$. Thus $\mathbf{Z}(E)G/\mathbf{Z}(E)$ is an extension of $\mathbf{Z}(E) \cong C_2$ by $\Gamma = \Omega^-_{2n}(q)$. The hypothesis on $m, n, q$ implies that either $n \geq 4$, or $n = 3$ but $q \geq 4$. Hence $\Gamma$ is simple and has trivial Schur multiplier, see [**KlL**, Theorem 5.1.4]. It follows that $(\mathbf{Z}(E)G)^{(\infty)} \cong S$ and thus $\mathbf{Z}(E)G \cong \mathbf{Z}(E) \times S$. In particular, $S$ embeds in $H$, and so admits a faithful complex representation $\Phi$ of degree $q^n$. If $n \geq 4$, this however contradicts [**TZ1**, Theorem 1.1]. Hence $n = 3$, $q \geq 4$, and $S \cong \mathrm{SU}_4(q)$. Applying [**TZ1**, Theorem 4.1], we see that every nontrivial irreducible constituents $\Phi_i$ of $\Phi$ is a Weil representation of degree $d$ or $d+1$, where

$$d := (q^4 - 1)/(q + 1).$$

Since $2d > q^3$ when $q \geq 4$, we conclude that $\Phi$ has a unique nontrivial irreducible constituent, say $\Phi_1$, and all others are trivial. As mentioned in the proof of Corollary 11.2.7, $\Phi$ is of symplectic type. However, by [**TZ1**, Theorem 4.1], $\Phi_1$ is non-self-dual if it is of degree $d$, whereas it is of quadratic type if it has degree $d + 1$ by Lemma 5.2 and Theorem 16.11 of [**KT7**]. This is a contradiction in either case.

We have shown that $\mathbf{Z}(E)G \geq E$, and so

$$\mathbf{Z}(E)G = EG = H.$$

Taking derived subgroups, we have

$$[G, G] = [\mathbf{Z}(E)G, \mathbf{Z}(E)G] = [H, H] \geq [E, E] = \mathbf{Z}(E).$$

Consequently, $G = \mathbf{Z}(E)G = H$. □

Our next application of almost injectivity is concerned with the following local system

$$\mathcal{F}(p, n, m) \tag{12.5.5.1}$$

on $(\mathbb{A}^1 \times \mathbb{G}_m)/\mathbb{F}_p$, with $1 < n < m$ and $p \nmid nm$, whose trace function is given as follows: for $L/\mathbb{F}_p$ a finite extension, and $(s, t) \in L \times L^\times$,

$$\mathrm{Trace}\big(\mathsf{Frob}_{(s,t),L} | \mathcal{F}(p, n, m)\big) = -\sum_{x \in L} \psi_L\big(s(x^n - x) + t(x^m - x)\big).$$

First we give an irreducibility criterion that is sometimes amenable to machine calculation.

Lemma 12.5.6. *Let $q$ be a power of a prime $p$, $n \geq 2$ an integer, and $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ a polynomial of total degree $d \geq 1$. Then $f$ is geometrically irreducible, i.e., irreducible in $\overline{\mathbb{F}_q}[x_1, \ldots, x_n]$, if and only if it is irreducible in $\mathbb{F}_{q^d}[x_1, \ldots, x_n]$.*

Proof. If $f$ is reducible over $\mathbb{F}_q$, it is not geometrically irreducible.

Suppose that $f$ is irreducible over $\mathbb{F}_q$, but that $f$ is not geometrically irreducible. Choose an irreducible factor $g \in \overline{\mathbb{F}_q}[x_1, \ldots, x_n]$ of $f$, scaled to have some coefficient 1. Denote by $K$ the field $\mathbb{F}_q$(the coefficients of $g$). Then in $K[x_1, \ldots, x_n]$, we have $g|f$. Applying $\mathrm{Gal}(K/\mathbb{F}_q)$ to this divisibility, we see that $g^\sigma | f$ for every $\sigma \in \mathrm{Gal}(K/\mathbb{F}_q)$. By the definition of $K$, we see that the various $g^\sigma$ are pairwise distinct irreducible divisors of $f$; none is a scalar multiple of another, as all have a fixed coefficient 1. Then $\prod_{\sigma \in \mathrm{Gal}(K/\mathbb{F}_q)} g^\sigma$ divides $f$. But this product lies in $\mathbb{F}_q[x_1, \ldots, x_n]$. As $f$ is irreducible over $\mathbb{F}_q$, we have, up to an $\mathbb{F}_q^\times$ factor, an equality of $f$ with this product. Thus $d := \deg(f) = \deg(K/\mathbb{F}_q)\deg(g)$, hence $K \subset \mathbb{F}_{q^d}$, and $f$, being reducible over $K$, is reducible over $\mathbb{F}_{q^d}$. □

We first give a result which eliminates calculation when $p$ is large compared to $m$.

THEOREM 12.5.7. *The following statements hold for the geometric monodromy group* $G_{\rm geom}$ *of the local system* $\mathcal{F}(p,n,m)$ *defined in* (12.5.5.1).

(i) *If* $p > 2m$, *and* $nm$ *is odd, then* $G_{\rm geom} = \mathrm{Sp}_{m-1}$ *(and hence* $M_{2,2} = 3$*).*
(ii) *If* $p > 2m$, *and* $m$ *is even then* $G_{\rm geom} \geq \mathrm{SL}_{m-1}$ *(and hence* $M_{2,2} = 2$*).*
(iii) *If* $p > 2m$, $m$ *is odd,* $n$ *is even, and* $\gcd(n,m) = 1$, *then* $G_{\rm geom} \geq \mathrm{SL}_{m-1}$ *(and hence* $M_{2,2} = 2$*).*

PROOF. We first prove (i) and (ii). The specialization $s \mapsto 0$ is the local system $\mathcal{A}$ whose trace function is

$$t \mapsto -\sum_x \psi(t(x^m - x)).$$

So $G_{{\rm geom},\mathcal{A}} \leq G_{{\rm geom},\mathcal{F}}$ is a subgroup. The further Kummer pullback $[m]^\star\mathcal{A}$ is the local system $\mathcal{B}$ whose trace function is

$$t \mapsto -\sum_x \psi(t^m(x^m - x)),$$

which, after the change of variable $x \mapsto x/t$ for $t \neq 0$ becomes

$$t \mapsto -\sum_x \psi(x^m - tx).$$

Thus $G_{{\rm geom},\mathcal{B}}$ is a subgroup of $G_{{\rm geom},\mathcal{F}}$. One knows [**Ka-MG**, Theorem 19] that $G_{{\rm geom},\mathcal{B}} = \mathrm{Sp}_{m-1}$ if $m$ is odd, is $\mu_p$ if $m = 2$, and is $\mathrm{SL}_{m-1}$ if $m \geq 4$ is even. This proves (ii). If $nm$ is odd, then the original $\mathcal{F}(k,n,m)$ is symplectically self-dual, so its $G_{\rm geom} \leq \mathrm{Sp}_{m-1}$, but its $G_{\rm geom}$ contains that of $\mathcal{B}$, which is $\mathrm{Sp}_{m-1}$. This proves (i).

To prove (iii), we argue as follows. The specialization $(s,t) \mapsto (-t,t)$ is the local system $\mathcal{C}$ whose trace function is

$$t \mapsto -\sum_x \psi(t(x^m - x^n)).$$

The Kummer pullback $[m]^\star\mathcal{C}$ is the local system $\mathcal{D}$ whose trace function is

$$t \mapsto -\sum_x \psi(t^m(x^m - x^n)),$$

which after the change of variable $x \mapsto x/t$ for $t$ nonzero becomes

$$t \mapsto -\sum_x \psi(x^m - t^{m-n}x^n).$$

So far, we have $G_{{\rm geom},\mathcal{D}} \leq G_{{\rm geom},\mathcal{F}}$. Now $\mathcal{D}$ is the Kummer $[n-m]^\star$ pullback of the local system $\mathcal{E}$ whose trace function is

$$t \mapsto -\sum_x \psi(x^m - tx^n).$$

We now have $G_{{\rm geom},\mathcal{D}} \lhd G_{{\rm geom},\mathcal{E}}$ as a normal subgroup of finite index dividing the prime to $p$ part of $m-n$. Because $\gcd(n,m) = 1$, one knows [**KT6**, Corollary 3.10(i)] that the local system $\mathcal{E}$ is the Kummer $[m]^\star$ pullback of the hypergeometric sheaf

$$\mathcal{H} := \mathcal{H}_{small,m,n} := \mathcal{H}yp(\mathsf{Char}(m) \smallsetminus \mathbb{1}; \mathsf{Char}(n) \smallsetminus \mathbb{1}).$$

We next observe that $\mathcal{H}$ is primitive for $p > 2m$. Indeed, it cannot be Kummer induced because $\gcd(n, m) = 1$, and it cannot be Belyi induced because $p - 1$ does not divide $m - n$ (being too large), cf. [**KT6**, Proposition 5.15]. This sheaf $\mathcal{H}$ has wild part $w = m - n$, and hence $p > 2w + 1$. By Theorem 2.4.4, we conclude that $G_{\mathrm{geom},\mathcal{H}}$ is infinite. Therefore its Kummer pullback $\mathcal{E}$ has $G_{\mathrm{geom},\mathcal{E}}$ infinite. Then $G_{\mathrm{geom},\mathcal{D}}$ is infinite, being a (normal) subgroup of finite index in $G_{\mathrm{geom},\mathcal{E}}$. Then by Theorem 10.3.21, we find that $G_{\mathrm{geom},\mathcal{D}} \geq \mathrm{SL}_{m-1}$. But $G_{\mathrm{geom},\mathcal{D}} \leq G_{\mathrm{geom},\mathcal{F}}$, so we are done. □

We now turn to the detailed examination of a few $\mathcal{F}(p, n, m)$.

LEMMA 12.5.8. *We have the following results.*

(i) $\mathcal{F}(p, 3, 13)$ *has* $M_{2,2} = 3$ *for all* $p \neq 3, 13$, $p \leq 26$.
(ii) $\mathcal{F}(p, 4, 7)$ *has* $M_{2,2} = 2$ *for all* $p \neq 2, 7$, $p \leq 14$.
(iii) $\mathcal{F}(p, 2, 7)$ *has* $M_{2,2} = 2$ *for all* $p \neq 2, 7$, $p \leq 14$.

PROOF. In each case, we compute the relevant resultant $R(y, z, w)$. In case (i), where the representation is symplectic, we divide out the visible factors, and define

$$R_{\mathrm{red}} := R/((z + w)(w - y)(z - y)).$$

Here the degree of $R_{\mathrm{red}}$ is $nm - 3 = 36$, and we use Magma to check the irreducibility of $R_{\mathrm{red}}$ over $\mathbb{F}_{p^{36}}$ for the indicated $p$. In cases (ii) and (iii), where the representation has no visible autoduality, we divide out the visible factors, and define

$$R_{\mathrm{red}} := R/((w - y)(z - y)).$$

In case (i), the degee of $R_{\mathrm{red}}$ is $nm - 2 = 26$, and we use Magma to check the irreducibility of $R_{\mathrm{red}}$ over $\mathbb{F}_{p^{26}}$ for the indicated $p$. In case (iii), the degree of $R_{\mathrm{red}}$ is $nm - 2 = 12$, we we use Magma to check the irreducibility of $R_{\mathrm{red}}$ over $\mathbb{F}_{p^{12}}$, for the indicated $p$. □

THEOREM 12.5.9. *We have the following results for the local system* $\mathcal{F}(p, 3, 13)$ *defined in* (12.5.5.1).

(i) *For all* $p \neq 2, 3, 5, 13$, $\mathcal{F}(p, 3, 13)$ *has* $G_{\mathrm{geom}} = \mathrm{Sp}_{12}$.
(ii) *For* $p = 5$, $\mathcal{F}(5, 3, 13)$ *has* $G_{\mathrm{geom}} = \mathrm{Sp}_4(5)$.
(iii) *For* $p = 2$, $\mathcal{F}(2, 3, 13)$ *has* $G_{\mathrm{geom}} = 2 \cdot G_2(4)$.

PROOF. The pullback of $\mathcal{F}(p, 3, 13)$ to $\mathbb{G}_m$ by $(s, t) \mapsto (-t, t)$ is the local system $\mathcal{A}$ on $\mathbb{G}_m/\mathbb{F}_p$ whose trace function is

$$t \mapsto -\sum_x \psi(t(x^{13} - x^3)).$$

The further pullback of this local system $\mathcal{A}$ by $t \mapsto t^{13}$ is the local system $\mathcal{B}$ whose trace function is, after the change of variable $x \mapsto x/t$,

$$t \mapsto -\sum_x \psi(x^{13} - t^{10}x^3).$$

which is the $t \mapsto t^{10}$ pullback of the local system $\mathcal{C}$ with trace function

$$t \mapsto -\sum_x \psi(x^{13} - tx^3).$$

This last local system $\mathcal{C}$ has $G_{\mathrm{geom},\mathcal{C}} = 2 \cdot G_2(4)$ for $p = 2$, and has $G_{\mathrm{geom},\mathcal{C}} = \mathrm{Sp}_4(5)$ for $p = 5$, by Theorem 10.3.13(iv), and (i) with $q = 5$ and $n = 1$, $m = 2$.

We first prove (i). For $p > 5$, $p \neq 13$, Theorem 10.3.13(ii) shows that $\mathcal{C}$ has infinite $G_{\mathrm{geom}}$, hence by Theorem 10.2.4 it has $G_{\mathrm{geom},\mathcal{C}} = \mathrm{Sp}_{12}$. In these cases, $\mathcal{B}$ is symplectic, so $G_{\mathrm{geom},\mathcal{B}} \leq \mathrm{Sp}_{12}$, while $G_{\mathrm{geom},\mathcal{B}} \lhd G_{\mathrm{geom},\mathcal{C}}$ is a normal subgroup of index dividing 10. Thus $G_{\mathrm{geom},\mathcal{B}} = \mathrm{Sp}_{12}$. As $\mathcal{B}$ is a pullback of the symplectic $\mathcal{F}(p, 3, 13)$, we have $\mathrm{Sp}_{12} = G_{\mathrm{geom},\mathcal{B}} \leq G_{\mathrm{geom},\mathcal{F}} \leq \mathrm{Sp}_{12}$.

We now prove (ii).

In the case $p = 5$, we have $G_{\mathrm{geom},\mathcal{B}} \lhd G_{\mathrm{geom},\mathcal{C}} = \mathrm{Sp}_4(5)$ of index dividing 2 (the prime to 5 part of 10). Since $\mathrm{Sp}_4(5)$ is perfect, we have $G_{\mathrm{geom},\mathcal{B}} = \mathrm{Sp}_4(5)$. But $\mathcal{B}$ was a pullback of $\mathcal{F}(5, 3, 13)$, so we have the inclusion $\mathrm{Sp}_4(5) \leq G_{\mathrm{geom},\mathcal{F}}$.

We continue with the case $p = 5$. The key fact here is that by Theorem 11.2.3(i) with $q = 5$, the two parameter local system $\mathcal{K}$ on $\mathbb{A}^2/\mathbb{F}_5$ whose trace function is

$$(u, v) \mapsto -\sum_x \psi(x^{13} + ux^3 + vx)$$

has $G_{\mathrm{geom},\mathcal{K}} = \mathrm{Sp}_4(5)$ in a Weil representation. We can view $\mathcal{K}$ as living on $\mathbb{G}_m \times \mathbb{A}^2$ with coordinates $(w, u, v)$ simply by pulling back by the projection $(w, u, v) \mapsto (u, v)$. This sort of "independent of $w$" pullback does not change $G_{\mathrm{geom}}$. Let us call this local system $\mathcal{K}_1$. By the change of variable $x \mapsto xw$, this becomes the local system $\mathcal{K}_3$ whose trace function is

$$(w, u, v) \mapsto -\sum_x \psi(w^{13}x^{13} + uw^3x^3 + vwx).$$

By the automorphism $(w, u, v) \mapsto (w, u/w^3, v/w)$ of $\mathbb{G}_m \times \mathbb{A}^2$, this becomes the local system $\mathcal{K}_4$ whose trace function is

$$(w, u, v) \mapsto -\sum_x \psi(w^{13}x^{13} + ux^3 + vx),$$

whose $G_{\mathrm{geom},\mathcal{K}_4}$ is still $\mathrm{Sp}_4(5)$. Now $\mathcal{K}_4$ is the Kummer pullback by $w \mapsto w^{13}$ of the local system $\mathcal{K}_5$ whose trace function is

$$(w, u, v) \mapsto -\sum_x \psi(wx^{13} + ux^3 + vx).$$

Thus $\mathrm{Sp}_4(5) = G_{\mathrm{geom},\mathcal{K}_4} \lhd G_{\mathrm{geom},\mathcal{K}_5}$ is a normal subgroup of index dividing 13. In fact, $G_{\mathrm{geom},\mathcal{K}_4} = G_{\mathrm{geom},\mathcal{K}_5}$. To see this, we argue as follows. As $\mathcal{K}_5$ is itself symplectic, $G_{\mathrm{geom},\mathcal{K}_5}$ lies in the normalizer of (the faithful image in $\mathrm{Sp}_{12}$ of) $\mathrm{Sp}_4(5)$ in the ambient $\mathrm{Sp}_{12}$. The outer automorphism of $\mathrm{Sp}_4(5)$ fuses the two Weil representations of degree 12 of $\mathrm{Sp}_4(5)$. Therefore $G_{\mathrm{geom},\mathcal{K}_5}$ must act by inner automorphisms on $\mathrm{Sp}_4(5)$, and hence (as the only scalars in $\mathrm{Sp}_{12}$ are $\pm 1$, which already lie in $\mathrm{Sp}_4(5)$) we have $G_{\mathrm{geom},\mathcal{K}_4} = G_{\mathrm{geom},\mathcal{K}_5}$, and hence $G_{\mathrm{geom},\mathcal{K}_5} = \mathrm{Sp}_4(5)$.

The local system $\mathcal{F}(5, 3, 13)$ is a pullback of $\mathcal{K}_5$, so $G_{\mathrm{geom},\mathcal{F}} \leq \mathrm{Sp}_4(5)$. But as we saw above with the $\mathcal{B}, \mathcal{C}$ analysis, $\mathrm{Sp}_4(5) \leq G_{\mathrm{geom},\mathcal{F}}$.

We now prove (iii). Thus $p = 2$. In the $\mathcal{A}, \mathcal{B}, \mathcal{C}$ story, we have $G_{\mathrm{geom},\mathcal{B}} \lhd G_{\mathrm{geom},\mathcal{C}} = 2 \cdot G_2(4)$ is a normal subgroup of index dividing 5 (the prime to 2 part of 10). But the perfect group $2 \cdot G_2(4)$ has no $C_5$-quotient, hence $G_{\mathrm{geom},\mathcal{B}} = 2 \cdot G_2(4)$. As $G_{\mathrm{geom},\mathcal{B}} \leq G_{\mathrm{geom},\mathcal{F}}$ (because $\mathcal{B}$ is a pullback of $\mathcal{F}$, we have $2 \cdot G_2(4) \leq G_{\mathrm{geom},\mathcal{F}}$.

Now repeat the arguments with $\mathcal{K}_1, \ldots, \mathcal{K}_5$ in this situation. We now have $G_{\text{geom},\mathcal{K}_4} = 2 \cdot G_2(4)$, and $2 \cdot G_2(4) = G_{\text{geom},\mathcal{K}_4} \lhd G_{\text{geom},\mathcal{K}_5}$ is a normal subgroup of index dividing 13. Therefore $G_{\text{geom},\mathcal{K}_5}$, which itself lies in $\mathrm{Sp}_{12}$, normalizes (the faithful image in $\mathrm{Sp}_{12}$ of) $2{\cdot}G_2(4)$. Since $\mathrm{Out}(2{\cdot}G_2(4))$ has order two, $G_{\text{geom},\mathcal{K}_5}$ must act by inner automorphisms on $2{\cdot}G_2(4)$, and hence (as the only scalars in $\mathrm{Sp}_{12}$ are $\pm 1$, which already lie in $2 \cdot G_2(4)$) we have $G_{\text{geom},\mathcal{K}_4} = G_{\text{geom},\mathcal{K}_5}$, and hence $G_{\text{geom},\mathcal{K}_5} = 2 \cdot G_2(4)$. The local system $\mathcal{F}(2,3,13)$ is a pullback of $\mathcal{K}_5$, so $G_{\text{geom},\mathcal{F}} \le 2 \cdot G_2(4)$. But as we saw above with the $\mathcal{B}, \mathcal{C}$ analysis, $2 \cdot G_2(4) \le G_{\text{geom},\mathcal{F}}$. □

Theorem 12.5.10. *The following statements hold for the local systems $\mathcal{F}(p,4,7)$ and $\mathcal{F}(p,2,7)$ defined in* (12.5.5.1)*.*

(i) *For all $p \neq 2,3,7$, both $\mathcal{F}(p,2,7)$ and $\mathcal{F}(p,4,7)$ have $G_{\text{geom}} \ge \mathrm{SL}_6$.*
(ii) *For $p = 3$, both $\mathcal{F}(p,2,7)$ and $\mathcal{F}(p,4,7)$ have $G_{\text{geom}} = 6_1 \cdot \mathrm{PSU}_4(3)$.*

Proof. We first prove (i). The auxiliary sheaves $\mathcal{C}$ in the two cases are the local systems $t \mapsto -\sum_x \psi(x^7 + tx^d)$ for $d = 4$ and $d = 2$. For $p \neq 2,3,7$, Theorem 10.3.13(ii) shows that $\mathcal{C}$ has infinite $G_{\text{geom}}$, hence by Theorem 10.2.4 it has $G_{\text{geom},\mathcal{C}} \ge \mathrm{SL}_6$. As $G_{\text{geom},\mathcal{B}} \lhd G_{\text{geom},\mathcal{C}} \ge \mathrm{SL}_{16}$ is a normal subgroup of finite index dividing 7. Thus $G_{\text{geom},\mathcal{B}} \ge \mathrm{SL}_6$, As $G_{\text{geom},\mathcal{B}} \le G_{\text{geom},\mathcal{F}}$, we have $G_{\text{geom},\mathcal{F}} \ge \mathrm{SL}_6$.

We now treat the case $p = 3$. Here $\mathcal{C}$ has $G_{\text{geom},\mathcal{C}} = 6_1 \cdot \mathrm{PSU}_4(3)$, and $G_{\text{geom},\mathcal{B}} \lhd G_{\text{geom},\mathcal{C}}$ is a normal subgroup of finite index dividing 7. But $6_1 \cdot \mathrm{PSU}_4(3)$ is perfect, hence $G_{\text{geom},\mathcal{B}} = 6_1 \cdot \mathrm{PSU}_4(3)$, and hence $6_1 \cdot \mathrm{PSU}_4(3) \le G_{\text{geom},\mathcal{F}}$. We next run the $\mathcal{K}_1, \ldots, \mathcal{K}_5$ argument. At the penultimate step, we have $G_{\text{geom},\mathcal{K}_4} = 6_1 \cdot \mathrm{PSU}_4(3)$, and $G_{\text{geom},\mathcal{K}_4} \lhd G_{\text{geom},\mathcal{K}_5}$ is a normal subgroup of index dividing the prime to 3 part of $7-4$ and of $7-2$ respectively.

In the case of $\mathcal{F}(3,4,7)$, this prime to 3 part is 1, hence $G_{\text{geom},\mathcal{K}_5} = 6_1 \cdot \mathrm{PSU}_4(3)$. The local system $\mathcal{F}(3,4,7)$ is a pullback of $\mathcal{K}_5$, so $G_{\text{geom},\mathcal{F}} \le 6_1 \cdot \mathrm{PSU}_4(3)$.

In the case of $\mathcal{F}(3,4,7)$, this prime to 3 part is 5, but $\mathrm{Out}(6_1 \cdot \mathrm{PSU}_4(3))$ is a 2-group. Hence $G_{\text{geom},\mathcal{K}_5}$ acts by inner automorphisms, hence lies in $\mu_5 \times 6_1 \cdot \mathrm{PSU}_4(3)$ in the ambient $\mathrm{GL}_6$. In fact, there can be no $\mu_5$ factor in $G_{\text{geom},\mathcal{K}_5}$. To see this, use the fact that $\mathcal{K}_4$ has geometric determinant of finite order with values in $\mathbb{Z}]\zeta_3]$, so has determinant of order dividing 6. One the other hand, $6_1 \cdot \mathrm{PSU}_4(3)$ lies in $\mathrm{SL}_6$, so any scalar $\alpha \in \mu_5$ reappears as $\alpha^6 = \alpha$ in the determinant, which has order dividing 6. Therefore $G_{\text{geom},\mathcal{K}_5} = 6_1 \cdot \mathrm{PSU}_4(3)$. The local system $\mathcal{F}(3,4,7)$ is a pullback of $\mathcal{K}_5$, so $G_{\text{geom},\mathcal{F}} \le 6_1 \cdot \mathrm{PSU}_4(3)$. □

We now give some cases for which we have a strengthening of Theorem 12.5.7.

Theorem 12.5.11. *Consider the local system $\mathcal{F}(p,A,B)$ as defined in* (12.5.5.1)*, where $A, B$ are given as follows. We take*

$$q := 2^f, f \ge 1,$$

*integers $1 \le a < b$ with $\gcd(a,b) = 1, 2|ab$, and*

$$A := q^a + 1, B := q^b + 1.$$

*Then for $p \nmid 2AB$, $\mathcal{F}(p,A,B)$ has $G_{\text{geom}} = \mathrm{Sp}_{q^b}$.* [Recall that by Theorem 12.5.5, $\mathcal{F}(2,A,B)$ has $G_{\text{geom}} = 2_-^{1+2bf} \cdot \Omega_{2b}^-(q)$ provided that $bf \ge 4$, and by van der Geer–van der Vlugt, this group is finite whatever the value of $bf$.]

PROOF. Because only odd powers of $x$ occur inside $\psi$, we have an a priori inclusion, for any $p \nmid AB$, $G_{\mathrm{geom}} < \mathrm{Sp}_{q^b}$. The $s = -t$ pullback, call it $\mathcal{A}$, is the local system on $\mathbb{G}_m$ whose trace function is given as follows: for $L/\mathbb{F}_p$ a finite extension, and $t \in L^\times$,

$$\mathrm{Trace}(\mathsf{Frob}_{t,L}|\mathcal{F}(p,A,B)_{s=-t}) = -\sum_{x \in L} \psi_L(t(x^{q^b+1} - x^{q^a+1})).$$

The Kummer pullback $\mathcal{B}$ of $\mathcal{A}$ by $[q^b+1]^\star$, rewritten after the change of variable $x \mapsto x/t$ has trace function

$$-\sum_{x \in L} \psi_L(x^{q^b+1} - t^{q^b-q^a} x^{q^a+1})).$$

This local system is in turn the Kummer pullback $[q^b - q^a]^\star$ of the local system $\mathcal{D}$ whose trace function is

$$-\sum_{x \in L} \psi_L(x^{q^b+1} - t x^{q^a+1})).$$

So the $G_{\mathrm{geom}}$ groups are related as follows:

$$\mathrm{Sp}_{q^b} > G_{\mathrm{geom},\mathcal{F}(p,A,B)} > G_{\mathrm{geom},\mathcal{A}} > G_{\mathrm{geom},\mathcal{B}} = G_{\mathrm{geom},\mathcal{C}} \lhd G_{\mathrm{geom},\mathcal{D}},$$

with $G_{\mathrm{geom},\mathcal{C}} \lhd G_{\mathrm{geom},\mathcal{D}}$ a normal subgroup of finite index with quotient cyclic of order dividing the prime to $p$ part of $q^b - q^a$ (the prime to $p$ part because Frobenius pullback does not change $G_{\mathrm{geom}}$). So it suffices to prove that $G_{\mathrm{geom},\mathcal{D}} = \mathrm{Sp}_{q^b}$; suffices simply because $\mathrm{Sp}_{q^b}$ has no proper normal subgroups of finite cyclic index (this last fact because $\mathrm{Sp}_{q^b}$ is its own commutator subgroup).

For this, we first invoke Theorem 10.3.13 (where the roles of $A$ and $B$ are reversed!). We use it to show that in any odd characteristic $p \nmid AB$, $G_{\mathrm{geom},\mathcal{D}}$ is not finite. For if $G_{\mathrm{geom},\mathcal{D}}$ were finite for such a $p$, then we would be in one of two cases. The first is that for some power $Q$ of $p$, and some integer $d \geq 2$, we have

$$q^b + 1 = (Q^d + 1)/2,$$

and moreover that for some integer $1 \leq e < d$ with $\gcd(e,d) = 1$, $2|ed$, we also have

$$q^a + 1 = (Q^e + 1)/2,$$

in this case, we cross multiply and get

$$2q^b + 1 = Q^d, \text{ i.e., } 2^{1+bf} = Q^d,$$

q an equation of the form

$$2^N + 1 = \text{ a prime power, but not a prime.}$$

It is known that this special case of Catalan's equation can hold only with $2^3 + 1 = 3^2$. [Indeed, suppose $2^N + 1 = p^c$ with $N \geq 3$ and $c \geq 2$. If $c$ is odd, then $2^N = p^c - 1$ has an odd divisor $(p^c - 1)/p - 1)$, a contradiction. If $c = 2s$ is even, then $2^N = (p^s - 1)(p^s + 1)$, so $p^s + 1$ and $p^s - 1$ are 2-powers differing by 2, and so $p^s = 3$ and $N = 3$.] In our situation, the exponent $N = 1 + bf$ is $\geq 5$ with the single exception $q = 2, b = 2$, in which case $a = 1$. So the exceptional case is $\mathcal{F}(p,3,5)$ with $p = 3$, but $p = 3$ is excluded by the $p \nmid 2AB$ hypothesis.

The second case has

$$q^b + 1 = (Q^d + 1)/(Q + 1), \ d \geq 3 \text{ odd.}$$

But here we write

$$(Q^d+1)/(Q+1) = 1 + Q(-1+Q-\ldots+Q^{d-2}).$$

So in this second case we would have $q^b = Q(-1+Q-\ldots+Q^{d-2})$ being divisible by $Q$, a contradiction.

Once we know that $G_{\rm geom}$ for $\mathcal{D}$ is not finite, Theorem 10.3.21(iii) yields $G_{{\rm geom},\mathcal{D}} = \mathrm{Sp}_{q^b}$. □

Theorem 12.5.12. *Consider the local system* $\mathcal{F}(p,A,B)$ *as defined in* (12.5.5.1)*, where* $A, B$ *are given as follows. We take*

$$q := p_0^f,\ f \geq 1,\ p_0 \text{ an odd prime},$$

*integers* $1 \leq a < b$ *with* $\gcd(a,b) = 1, 2|ab$, *and*

$$A := q^a+1,\ B := q^b+1.$$

*Then for* $p \nmid p_0AB$, $\mathcal{F}(p,A,B)$ *has infinite* $G = G_{\rm geom}$ *with* $[G,G] = \mathrm{SL}_{q^b}$. [Recall that by Theorem 12.5.4, $\mathcal{F}(p_0,A,B)$ has $G_{\rm geom} = {p_0}_+^{1+2bf} \rtimes \mathrm{Sp}_{2b}(q)$ provided that in addition $a > b/2$, and by van der Geer–van der Vlugt, this group is finite whatever the value of $(a,b)$.]

Proof. (i) We first use Theorem 10.2.6 to show that with the possible exception of a single prime $p_1 \nmid p_0AB$, already the $s=0$ pullback, call it $\mathcal{A}$, has $G_{{\rm geom},\mathcal{A}} = \mathrm{SL}_{q^b}$. This pullback has trace function

$$t \in L^\times \mapsto -\sum_{x\in L}\psi_L(t(x^{q^b+1}-x)).$$

Its further Kummer pullback by $[q^b-1]$, call it $\mathcal{B}$, has trace function (after the change of variable $x \mapsto x/t$, given by

$$t \in L^\times \mapsto -\sum_{x\in L}\psi_L(x^{q^b+1}-t^{q^b}x).$$

Then $\mathcal{B}$ is the Kummer pullback by $[q^b]$ of the local system $\mathcal{C}$ whose trace function is

$$t \in L^\times \mapsto -\sum_{x\in L}\psi_L(x^{q^b+1}-tx).$$

We now examine Theorem 10.2.6 to see if $\mathcal{C}$ could have finite $G_{\rm geom}$. By our assumption, none of the cases (iii)–(vi) is possible (recall $p \neq p_0$). We cannot be in case (ii), which requires $q^b+1$ to be of the form $(Q^n+1)/(Q+1)$ with $Q$ a power of an odd prime $p$ and $n \geq 3$ odd. Just as in the proof of Theorem 12.5.11 above, this gives the contradiction that $q^b$ is divisible by $Q$. Case (i) is potentially problematic. It arises if

$$q^b+1 = (Q+1)/2$$

for some prime power $Q$, or equivalently if

$$2q^b+1 = Q,$$

an equation of Sophie Germain type, which, if it holds, determines the prime $p_1$ of which $Q$ is a power. In this case, by Theorem 10.2.7(i), $\mathcal{C}$ has geometric monodromy group the image of $\mathrm{SL}_2(Q)$ in a Weil representation of degree $(Q-1)/2$. Since $Q = 2q^b+1 \geq 19$, $\mathrm{SL}_2(Q)$ is perfect, and hence this image is also contained in $G_{\rm geom}$.

(ii) Suppose, for the time being, that we look at $\mathcal{F}(p, A, B)$ for a prime $p \nmid p_0 p_1 AB$. Then $\mathcal{C}$ has infinite $G_{\mathrm{geom}}$, and then by Theorem 10.2.4(i), we have $G_{\mathrm{geom},\mathcal{C}} = \mathrm{SL}_{q^b}$. Then we must also have $G_{\mathrm{geom},\mathcal{B}} = \mathrm{SL}_{q^b}$, as $\mathrm{SL}_{q^b}$ has no nontrivial cyclic quotients, and hence for $G = G_{\mathrm{geom},\mathcal{F}(p,A,B)}$ we have $G \geq \mathrm{SL}_{q^b}$. As $G \leq \mathrm{GL}_{q^b}$, this implies that $[G, G] = \mathrm{SL}_{q^b}$.

If $2q^b + 1$ is a prime power, some power of the prime $p_1$, we need a separate argument to determine $G_{\mathrm{geom}}$ for $\mathcal{F}(p_1, A, B)$. We now show that if we have such a $p_1$, then $\mathcal{F}(p_1, A, B)$ has infinite $G_{\mathrm{geom}}$. Consider the $t = 0$ pullback, call it $\mathcal{G}$, of $\mathcal{F}(p_1, A, B)$. By [**Ka-Scont**, Theorem 1], $G_{\mathrm{geom},\mathcal{G}}$ is a subquotient of $G_{\mathrm{geom},\mathcal{F}(p_1,A,B)}$. So it suffices to show that $\mathcal{G}$ has infinite $G_{\mathrm{geom}}$. Exactly as in the proof of Theorem 12.5.11, up to normal subgroups of finite cyclic index, its $G_{\mathrm{geom}}$ agrees with that of the local system $\mathcal{H}$ whose trace function is

$$t \in L^\times \mapsto -\sum_{x \in L} \psi_L(x^{q^a+1} - tx).$$

So it suffices to show that $\mathcal{H}$ has infinite $G_{\mathrm{geom}}$, which is $\mathrm{SL}_{q^a}$ by Theorem 10.3.21(i) as above.

We now examine Theorem 10.2.6 to see if $\mathcal{H}$ could have finite $G_{\mathrm{geom}}$. As in (i), the only problematic case is where $q^a + 1$ is of the form $(Q_1 + 1)/2$ for some power $Q_1$ of $p_1$. In this case we have

$$(p_1^\beta - 1)/2 = q^b,\ (p_1^\alpha - 1)/2 = q^a$$

for some integers $\beta > \alpha \geq 1$.

Suppose $\beta \geq 3$. Then, as $p_1 > 2$, $p_1^\beta - 1$ has a primitive prime divisor $\ell$ [**Zs**] which divides $q^b$, so $\ell = p_0$. But then $\ell$ divides $q^a = (p_1^\alpha - 1)/2$, and this contradicts primitivity of $\ell$.

So $\beta = 2$ and $\alpha = 1$. In this case, $q^{\beta-\alpha} = (p_1^2 - 1)/(p_1 - 1) = p_1 + 1$, so $p_0 > 2$ divides both $p_1 + 1$ and $p_1 - 1$, again a contradiction.

We have shown that $G = G_{\mathrm{geom}}$ contains $\mathrm{SL}_{q^a}$ as a subquotient. As $q^a \geq 3$, this implies that $G/\mathbf{Z}(G)$ is infinite. As mentioned at the end of (i), $G$ contains the image of $\mathrm{SL}_2(Q)$ in a Weil representation of degree $D = (Q - 1)/2 \geq 9$. Applying Proposition 11.1.3, (with its $p$ our $p_1$, with its $D$ our $D$, with its $q^n$ our $Q$, and with $D = (Q - 1)/2$) we conclude that $[G, G] = \mathrm{SL}_D = \mathrm{SL}_{q^b}$. □

# Appendices

## Appendix A1: the Magma program used in Lemma 6.2.6

```
Ncheck:=procedure(p);
R:=GF(p);
a:=1;
for b in R do
for c in R do
for d in R do
for e in R do
f:=((p-1) div 2)*(a+b+c+d+e);
F:={* f,f+a+b,f+a+c,f+a+d,f+a+e,f+b+c,f+b+d,f+b+e,f+c+d,f+c+e,
f+d+e,-f-a,-f-b,-f-c,-f-d, -f-e *};
if Multiplicity(F,0) ge 6 then
if Max(Multiplicity(F,i):i in [1..p-1]) le 10 then
print F;
end if;
end if;
end for;
end for;
end for;
end for;
end procedure;
```

## Appendix A2: the Magma program used in Lemma 10.3.17

```
E6check:=procedure(N);
for a in [0..26] do
for b in [a+1..26] do
for c in [b+1..26] do
for d in [c+1..26] do
for e in [d+1..26] do
ee:=-(a+b+c+d+e);
for g in [1..26] do
F:=[a+g,b+g,c+g,d+g,e+g,ee+g,a-g,b-g,c-g,d-g,e-g,ee-g, -a-b,-a-c,-a-d,
-a-e,-a-ee,-b-c,-b-d, -b-e,-b-ee,-c-d,-c-e,-c-ee,-d-e,-d-ee,-e-ee];
FF:=F[i] mod 27:  i in [1..27];
if #FF eq 27 then print FF;
end if;
end for;
end for;
end for;
end for;
end for;
end for;
end procedure;
```

## Acknowledgements

The second author gratefully acknowledges the support of the NSF (grants DMS-1840702 and DMS-2200850), the Simons Foundation, the Charles Simonyi Endowment at the Institute for Advanced Study (Princeton, NJ), and the Joshua Barlaz Chair in Mathematics at Rutgers University.

Part of this work was done when the second author visited the Institute for Advanced Study, MIT, and Princeton University. It is a pleasure to thank the Institute for Advanced Study, MIT, and Princeton University for generous hospitality and stimulating environment.

Another part of this work was done while the second author participated in the programme "*Groups, Representations, and Applications: New Perspectives*" at the Isaac Newton Institute for Mathematical Sciences in 2022. This work was supported by EPSRC grant number EP/R014604/1.

The authors are grateful to Frank Lübeck for helping them with some computer calculation (cf. the proof of Theorem 6.2.12), and to the referees for their careful reading and helpful comments.

# Bibliography

[Abh] Abhyankar, S., Coverings of algebraic curves, *Amer. J. Math.* **79** (1957), 825–856.

[AKNOT] Alpöge, L., Katz, N., Navarro, G., O'Brien, E. A., and Tiep, P. H., Local systems and Suzuki groups, *Contemp. Math.* **800** (2024), 15–79.

[Asch] Aschbacher, M., Maximal subgroups of classical groups, On the maximal subgroups of the finite classical groups, *Invent. Math.* **76** (1984), 469–514.

[Bal] Ballantine, C. S., Cosquares: complex and otherwise, *Linear Multilinear Alg.* **6** (1978), 201–217.

[BBOO] Balog, A., Bessenrodt, C., Olsson, J. B., and Ono, K., Prime power degree representations of the symmetric and alternating groups, *J. Lond. Math. Soc.* **64** (2001) 344–356.

[BNRT] Bannai, E., Navarro, G., Rizo, N., and Tiep, P. H., Unitary $t$-groups, *J. Math. Soc. Japan* **72** (2020), 909–921.

[Ben] Benson, D. J., Spin modules for symmetric groups, *J. Lond. Math. Soc.* **38** (1988), 250–262.

[BEW] Berndt, B.C., Evans, R.J., and Williams, K.S., Gauss and Jacobi Sums, Can. Math. Soc. Series of Monographs and Advanced Texts, Wiley, New York, 1998, xii+583 pp.

[BH] Beukers, F., Heckman, G., Monodromy for the hypergeometric function ${}_nF_{n-1}$, *Invent. Math.* **95** (1989), 325–354.

[BSD] Birch, B. J., Swinnerton-Dyer, H. P. F., Note on a problem of Chowla. *Acta Arith.* **5** (1959), 417–423.

[Bl] Blichfeldt, H., Finite collineation groups, Univ. of Chicago Press, 1917.

[Bor] Borel, A., Carter, R., Curtis, C. W., Iwahori, N., Springer, T. A., Steinberg, R., Seminar on algebraic groups and related finite groups, Lectures Note Math. **131**, Springer-Verlag, 1970.

[Bour] Bourbaki, N., Groupes et algèbres de Lie, Chapitres 7 et 8, Diffusion C.C.L.S., Paris, 1975.

[BHR] Bray, J. N., Holt, D. F., and Roney-Dougal, C. M., The maximal subgroups of the low-dimensional finite classical groups. With a foreword by Martin Liebeck. London Mathematical Society Lecture Note Series, **407**, 2013.

[Bur] Burkhardt, R., Über die Zerlegungszahlen der Suzukigruppen $Sz(q)$, *J. Algebra* **59** (1979), 421–433.

[CCNPW] Conway, J. H., Curtis, R. T., Norton, S. P., Parker, R. A. and Wilson, R. A., Atlas of finite groups. Maximal subgroups and ordinary characters for simple groups. Oxford University Press, Eynsham, 1985.

[Cam] Cameron, P. J., Finite permutation groups and finite simple groups, *Bull. Lond. Math. Soc.* **13** (1981), 1–22.

[Cav] Cavallin, M., An algorithm for computing weight multiplicities in irreducible modules for complex semisimple Lie algebras, *J. Algebra* **471** (2017), 492–510.

[CPS] Cline, E., Parshall, B., and Scott, L., Cohomology of finite groups of Lie type, II, *J. Algebra* **45** (1977), 182–198.

[CG] Cohen, A. M., and Griess, R. L, On finite simple subgroups of the complex Lie group of type $E_8$, *Proc. Symp. Pure Math.* **47** (1987), 367–405.

[CS] Cohen, A. M. and Seitz, G. M., The $r$-rank of groups of exceptional Lie type, *Indag. Math.* **90** (1987), 251–259.

[CW] Cohen, A. M., and Wales, D. B, Finite subgroups of $F_4(\mathbb{C})$ and $E_6(\mathbb{C})$, *Proc. Lond. Math. Soc.* **74** (1997), 105–150.

[De1] Deligne, P., La conjecture de Weil I, *Pub. Math. IHES* **43** (1974), 273-307.

[De2] Deligne, P., La conjecture de Weil II. *Publ. Math. IHES* **52** (1981), 313–428.

[De3] Deligne, P., Finitude de l'extension de $\mathbb{Q}$ engendrée par des traces de Frobenius, en caractéristique finie. *Mosc. Math. J.* **12** (2012), 497–514, 668.

[DZ] Dixon, J. D., and Zalesskii, A. E., Finite primitive linear groups of prime degree, *J. Lond. Math. Soc.* **57** (1998), 126–134.

[Erd] Erdös, P., On a Diophantine equation, *J. Lond. Math. Soc.* **26** (1951), 176–178.

[F1] Feit, W., The representation theory of finite groups, North-Holland, Amsterdam, 1982.

[F2] Feit, W., On large Zsigmondy primes, *Proc. Amer. Math. Soc.* **102** (1988), 28–36.

[FT] Feit, W., and Thompson, J. G., Groups which have a faithful representation of degree less than $(p-1)/2$, *Pacific J. Math.* **11** (1961), 1257–1262.

[Fr] Fried, M., On a conjecture of Schur, *Michigan Math. J.* **17** (1970), 41–55.

[FH] W. Fulton and J. Harris, Representation theory, Springer-Verlag, New York, 1991.

[GAP] The GAP group, GAP - groups, algorithms, and programming, Version 4.4, 2004, `http://www.gap-system.org`.

[Ge] Gérardin, P., Weil representations associated to finite fields, *J. Algebra* **46** (1977), 54 –101.

[GI] Gluck, D., and Isaacs, I. M., Tensor induction of generalized characters and permutation characters, *Illinois J. Math.* **27** (1983), 514–518.

[Gor] Gorenstein, D., On a theorem of Philip Hall, *Pacific J. Math.* **19** (1966), 77–80.

[GLS] Gorenstein, D., Lyons, R., and Solomon, R.M., The classification of the finite simple groups, Number 3. Part I. Chapter A, **40**, Mathematical Surveys and Monographs, Amer. Math. Soc., Providence, RI, 1998.

[Gri] Griess, R. L., Automorphisms of extra special groups and nonvanishing degree 2 cohomology, *Pacific J. Math.* **48** (1973), 403–422.

[GrR] Griess, R. L. and Ryba, A. J. E., Finite simple groups which projectively embed in an exceptional Lie group are classified, *Bull. Amer. Math. Soc.* **36** (1999), 75–93.

[Gr] Gross, B. H., Group representations and lattices, *J. Amer. Math. Soc.* **3** (1990), 929–960.

[GMPS] Guest, S., Morris J., Praeger, C. E., and Spiga, P., On the maximum orders of elements of finite almost simple groups and primitive permutation groups, *Trans. Amer. Math. Soc.* **367** (2015), 7665–7694.

[GKT] Guralnick, R. M., Katz, N., and Tiep, P. H., Rigid local systems and alternating groups, *Tunisian J. Math.* **1** (2019), 295–320.

[GLT] Guralnick, R. M., Larsen, M., and Tiep, P.H., Representation growth in positive characteristic and conjugacy classes of maximal subgroups, *Duke Math. J.* **161** (2012), 107–137.

[GMST] Guralnick, R. M., Magaard, K., Saxl, J., and Tiep, P. H., Cross characteristic representations of symplectic groups and unitary groups, *J. Algebra* **257** (2002), 291–347.

[GPPS] Guralnick, R. M., Penttila, T., Praeger, C., Saxl, J., Linear groups with orders having certain large prime divisors, *Proc. London Math. Soc.* **78** (1999), 167–214.

[GT1] Guralnick, R. M. and Tiep, P. H., Cross characteristic representations of even characteristic symplectic groups, *Trans. Amer. Math. Soc.* **356** (2004), 4969–5023.

[GT2] Guralnick, R. M. and Tiep, P. H., Decompositions of small tensor powers and Larsen's conjecture, *Represent. Theory* **9** (2005), 138–208.

[GT3] Guralnick, R. M. and Tiep, P. H., Symmetric powers and a conjecture of Kollár and Larsen, *Invent. Math.* **174** (2008), 505–554.

[Gy] Györy, K., On the Diophantine equation $\binom{n}{k} = x^l$, *Acta Arith.* **80** (1997), 289–295.

[HD] Hasse, H. and Davenport, H., Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fallen, *J. Reine Angew. Math.* **172** (1934), 151–182.

[Har] Harbater, D., Abhyankar's conjecture on Galois groups over curves, *Invent. Math.* **117** (1994), 1–25.

[Hart] Hartshorne, R., Algebraic geometry. Graduate Texts in Mathematics, **52**, Springer-Verlag, New York-Heidelberg, 1977. xvi+496 pp.

[HM] Hiss, G. and Malle, G., Low-dimensional representations of quasi-simple groups, *LMS J. Comput. Math.* **4** (2001), 22–63; Corrigenda: Low-dimensional representations of quasi-simple groups, *LMS J. Comput. Math.* **5** (2002), 95–126.

[Ho] Hochschild, G., The structure of Lie groups, Holden-Day, Inc., San Francisco-London-Amsterdam,1965, ix+230 pp.

[Hoo] Hooley, C., On the number of points on a complete intersection over a finite field. With an appendix by Nicholas M. Katz, *J. Number Theory* **38** (1991), 338–358.

[HS] Howe, R. and Sarnak, P., The Schur lectures (1992), Israel Math. Conf. Proc., **8**, Bar-Ilan University, 1995.

[Hum] Humphreys, J., Introduction to Lie algebras and representation theory, Graduate Texts in Mathematics, **9**, Springer-Verlag, New York-Heidelberg, 1978, 2nd printing.

[Hup] Huppert, B., Singer-Zyklen in klassischen Gruppen, *Math. Z.* **117** (1970), 141–150.

[JW] Janwa, H. and Wilson, R. M., Hyperplane sections of Fermat varieties in $\mathbb{P}^3$ in char. 2 and some applications to cyclic codes. Applied algebra, algebraic algorithms and error-correcting codes (San Juan, PR, 1993), 180–194, Lecture Notes in Comput. Sci., **673**, Springer, Berlin, 1993.

[Kan1] Kantor, W. M., Automorphism groups of designs, *Math. Z.* **109** (1969), 246–252.

[Kan2] Kantor, W. M., $k$-Homogeneous groups, *Math. Z.* **124** (1972), 261–265.

[Is] Isaacs, I. M., Character theory of finite groups, AMS-Chelsea, Providence, 2006.

[Ka-ACT] Katz, N., Affine cohomological transforms, perversity, and monodromy, *J. Amer. Math. Soc.* **6** (1993), 149–222.

[Ka-CC] Katz, N.. From Clausen to Carlitz: low-dimensional spin groups and identities among character sums, *Mosc. Math. J.* **9** (2009), 57–89.

[Ka-ESDE] Katz, N., Exponential sums and differential equations. Annals of Mathematics Studies, **124**. Princeton Univ. Press, Princeton, NJ, 1990. xii+430 pp.

[Ka-GKM] Katz, N., Gauss sums, Kloosterman sums, and monodromy groups, Annals of Mathematics Studies, **116**. Princeton Univ. Press, Princeton, NJ, 1988. ix+246 pp.

[Ka-G2] Katz, N., $G_2$ and hypergeometric sheaves, *Finite Fields Appl.* **13** (2007), no. 2, 175–223.

[Ka-LAMM] Katz, N., Larsen's alternative, moments, and the monodromy of Lefschetz pencils. Contributions to automorphic forms, geometry, and number theory, 521–560, Johns Hopkins Univ. Press, Baltimore, MD, 2004.

[Ka-LGE] Katz, N., Local-to-global extensions of representations of fundamental groups, *Annales de L'Institut Fourier* **36** (1986), $n^o$ 4, 59–106.

[Ka-MG] Katz, N., On the monodromy groups attached to certain families of exponential sums, *Duke Math. J.* **54** (1987), no. 1, 41–56.

[Ka-MMP] Katz, N., Moments, monodromy, and perversity. Annals of Mathematics Studies, **159**. Princeton University Press, Princeton, NJ, 2005. viii+475 pp.

[Ka-Scont] Katz, N., A semicontinuity result for monodromy under degeneration, *Forum Math.* **15** (2003), no. 2, 191–200.

[Ka-TLFM] Katz, N., Twisted L-functions and monodromy. Annals of Mathematics Studies, **150**. Princeton University Press, Princeton, NJ, 2002.

[Kl] Kloosterman, H. D., On the representation of numbers in the form $ax^2 + by^2 + cz^2 + dt^2$, *Acta Math.* **49** (1926), 407–464.

[KRL] Katz, N., and Rojas-León, A., A rigid local system with monodromy group $2.J_2$, *Finite Fields Appl.* **57** (2019), 276–286.

[KRLT1] Katz, N., Rojas-León, A., and Tiep, P.H., Rigid local systems with monodromy group the Conway group $\mathsf{Co}_3$, *J. Number Theory* **206** (2020), 1–23.

[KRLT2] Katz, N., Rojas-León, A., and Tiep, P.H., Rigid local systems with monodromy group the Conway group $\mathsf{Co}_2$, *Int. J. Number Theory* **16** (2020), 341–360.

[KRLT3] Katz, N., Rojas-León, A., and Tiep, P.H., A rigid local system with monodromy group the big Conway group $2.\mathsf{Co}_1$ and two others with monodromy group the Suzuki group $6.\mathsf{Suz}$, *Trans. Amer. Math. Soc.* **373** (2020), 2007–2044.

[KRLT4] Katz, N., Rojas-León, A., and Tiep, P.H., Rigid local systems and sporadic simple groups, *Mem. Amer. Math. Soc.* (to appear).

[Ka-Sar] Katz, N., and Sarnak, P., Random matrices, Frobenius eigenvalues, and monodromy. American Mathematical Society Colloquium Publications, **45**. American Mathematical Society, Providence, RI, 1999. xii+419 pp.

[KT1] Katz, N., with an Appendix by Tiep, P.H., Rigid local systems on $\mathbb{A}^1$ with finite monodromy, *Mathematika* **64** (2018), 785–846.

[KT2] Katz, N., and Tiep, P.H., Rigid local systems and finite symplectic groups, *Finite Fields Appl.* **59** (2019), 134–174.

[KT3] Katz, N., and Tiep, P.H., Local systems and finite unitary and symplectic groups, *Advances in Math.* **358** (2019), 106859, 37 pp.

[KT4] Katz, N., and Tiep, P.H., Rigid local systems and finite general linear groups, *Math. Z.* **298** (2021), 1293–1321.

[KT5] Katz, N., and Tiep, P.H., Monodromy groups of Kloosterman and hypergeometric sheaves, *Geom. Funct. Analysis* **31** (2021), 562–662.

[KT6] Katz, N., and Tiep, P.H., Exponential sums and total Weil representations of finite symplectic and unitary groups, *Proc. Lond. Math. Soc.* **122** (2021), 745–807.

[KT7] Katz, N., and Tiep, P.H., Hypergeometric sheaves and finite symplectic and unitary groups, *Cambridge J. Math.* **9** (2021), 577–691.

[KT8] Katz, N., and Tiep, P.H., Moments, exponential sums, and monodromy groups, available at https://web.math.princeton.edu/~nmk/kt24_70.pdf.

[KlL] Kleidman, P. B., and Liebeck, M. W., The subgroup structure of the finite classical groups, London Math. Soc. Lecture Note Ser. no. **129**, Cambridge University Press, 1990.

[KlT] Kleshchev, A. S., and Tiep, P. H., On restrictions of modular spin representations of symmetric and alternating groups, *Trans. Amer. Math. Soc.* **356** (2004), 1971–1999.

[KS] Kurzweil, H., and Stellmacher, B., The theory of finite groups, An introduction, Universitext, Springer-Verlag, 2004.

[L] Lafforgue, L., Chtoucas de Drinfeld et correspondance de Langlands, *Invent. Math.* **147** (2002), 1–241.

[LW] Lang, S, and Weil, A., Number of points of varieties in finite fields, *Amer. J. Math.* **76** (1954), 819–827.

[Lau] Laumon, G., Semi-continuité du conducteur de Swan (d'après P. Deligne). The Euler-Poincaré characteristic (French), pp. 173–219, Astérisque, **83**, Soc. Math. France, Paris, 1981.

[Lie] van Leeuwen, M. A. A., Cohen, A. M., and Lisser, B., LiE, A package for Lie group computation, Computer Algebra Nederland, Amsterdam, 1992, http://www-math.univ-poitiers.fr/~maavl/LiE/form.html

[Li] Liebeck, M. W., The affine primitive permutation groups of rank three, *Proc. Lond. Math. Soc.* **54** (1987), 477–516.

[Lu] Lübeck, F., Small degree representations of finite Chevalley groups in defining characteristic, *LMS J. Comput. Math.* **4** (2001), 135–169.

[MZ] Malle, G., and Zalesskii, A. E., Prime power degree representations of quasi-simple groups, *Arch. Math.* **77** (2001), 461-468.

[Mit] Mitchell, H., Determination of all primitive collineation groups in more than four variables which contain homologies, *Amer. J. Math.* **36** (1914), 1–12.

[Mos] Mostow, G.D., Self-adjoint groups, *Ann. of Math.* **62** (1955), 44–55.

[NRS] Nebe, G., Rains, E., and Sloane, N.J.A., The invariants of the Clifford groups, *Des. Codes Crypt.* **24** (2001), 99–122.

[OV] Onishchik, A. L., and Vinberg, E. B., Lie groups and algebraic groups, Springer-Verlag, 1990.

[Pink] Pink, R., Lectures at Princeton University, May 1986.

[Pop] Pop, F., Étale Galois covers of affine smooth curves. The geometric case of a conjecture of Shafarevich. On Abhyankar's conjecture, *Invent. Math.* **120** (1995), 555–578.

[Ray] Raynaud, M. Revêtements de la droite affine en caractéristique $p > 0$ et conjecture d'Abhyankar, *Invent. Math.* **116** (1994), 425–462.

[Rob] Robinson, G. R., On elements with restricted eigenvalues in linear groups, *J. Algebra* **178** (1995), 635–642.

[R-L] Rojas-León, A., Finite monodromy of some families of exponential sums, *J. Number. Theory* **197** (2019), 37–48.

[Se] Serre, J.-P., Corps Locaux, Hermann, 1968.

[Seitz] Seitz, G. M., The maximal subgroups of classical algebraic groups, *Mem. Amer. Math. Soc.* no. **365**, Amer. Math. Soc., Providence, 1987.

[SGA4] A. Grothendieck et al, Séminaire de Géometrie Algébrique du Bois-Marie, SGA 4, Part III, Springer Lecture Notes in Math. 305, Springer, 1973.

[ST] Shephard, G. C., and Todd, J. A., Finite unitary reflection groups, *Can. J. Math.* **6** (1954), 274–304.

[Sm] Smith, S., Irreducible modules and parabolic subgroups, *J. Algebra* **75** (1982), 286–289.

[Such] Šuch, O., Monodromy of Airy and Kloosterman sheaves, *Duke Math. J.* **103** (2000), 397–444.

[Syl1] Sylvester, J., Sur les quantités formant un groupe de nonions analogues aux quaternions de Hamilton, *C. R. Acad. Sci. Paris* **98**, I (1884), pp. 273–276 and 471–475, available on `https://rcin.org.pl/dlibra/doccontent?id=119678`.

[Syl2] Sylvester, J., On arithmetical series, *Messenger of Math.* **21** (1892), 1–19, 87–120; and Collected Mathematical Papers, **4** (1912), 687–731.

[T] Tiep, P. H., Subgroup structure and representations of finite and algebraic groups, *Vietnam J. Math.* **43** (2015), 501–513.

[TZ1] Tiep, P. H. and Zalesskii, A. E., Minimal characters of the finite classical groups, *Comm. Algebra* **24** (1996), 2093–2167.

[TZ2] Tiep, P. H. and Zalesskii, A. E., Some characterizations of the Weil representations of the symplectic and unitary groups, *J. Algebra* **192** (1997), 130–165.

[TZ3] Tiep, P. H. and Zalesskii, A. E., Real conjugacy classes in algebraic groups and finite groups of Lie type, *J. Group Theory* **8** (2005), 291–315.

[Tr] Trefethen, S., Non-abelian Composition Factors of $m$-rational Groups, Ph. D. Thesis, University of Arizona, 2016.

[vdG-vdV] van der Geer, G., van der Vlugt, M., Reed-Muller codes and supersingular curves. I, *Compos. Math.* **84** (1992), 333–367.

[Wa] Wales, D., Quasiprimitive linear groups with quadratic elements, *J. Algebra* **245** (2001), 584–606.

[Weil1] Weil, A., Sur les courbes algébriques et les variétés qui s'en déduisent, Publ. Inst. Math. Univ. Strasbourg, **7** (1945). Actualités Scientifiques et Industrielles No. 1041 Hermann & Cie, Paris, 1948. iv+85 pp.

[Weil2] Weil, A., On some exponential sums, *Proc. Nat. Acad. Sci. U.S.A.* **34** (1948), 204–207.

[Weil3] Weil, A., Numbers of solutions of equations in finite fields, *Bull. Amer. Math. Soc.* **55** (1949), 497–508.

[Wi] Winter, D., The automorphism group of an extraspecial $p$-group, *Rocky Mount. J. Math.* **2** (1972), 159–168.

[Y] Young, L. T., Hypergeometric sheaves and extraspecial groups in even characteristic, (in preparation).

[Za1] Zalesskii, A. E., Linear groups, *Russian Math. Surveys* **36** (1981), 63–128.

[Za2] Zalesski, A. E., Matrices of simple spectrum in irreducible representations of cyclic extensions of simple algebraic groups, `https://arxiv.org/abs/2104.10882`

[ZS] Zalesskii, A. E. and Suprunenko, I. D., Representations of dimensions $(p^n \pm 1)/2$ of the symplectic group of degree $2n$ over a field of characteristic $p$, *Vesti AN BSSR, ser. fiz.-mat. navuk* 1987, no. 6, 9–15.

[Zan] Zannier, U., Integral points on curves $\dfrac{f(x)-f(y)}{x-y}$, *Math. Z.* **301** (2022), 3609–3616.

[Zar1] Zarhin, Y., Endomorphisms of Abelian varieties over fields of finite characteristic. (Russian) *Izv. Akad. Nauk SSSR* Ser. Mat. **39** (1975), 272–277, 471.

[Zar2] Zarhin, Y., Abelian varieties over fields of finite characteristic, *Cent. Eur. J. Math.* **12** (2014), 659–674.

[Zs] Zsigmondy, K., Zur Theorie der Potenzreste, *Monatsh. Math. Phys.* **3** (1892), 265–284.