MOMENTS, EXPONENTIAL SUMS, AND MONODROMY GROUPS

NICHOLAS M. KATZ AND PHAM HUU TIEP

Abstract. We determine the geometric monodromy groups attached to various families, both one-parameter and multi-parameter, of exponential sums over finite fields, or more precisely, the geometric monodromy groups of the ℓ-adic local systems on affine spaces in characteristic $p > 0$ whose trace functions are these exponential sums. The exponential sums here are much more general than we previously were able to consider. As a byproduct, we determine the number of irreducible components of maximal dimension in certain intersections of Fermat surfaces. We also show that in any family of such local systems, say parameterized by an affine space S, there is a dense open set of S over which the geometric monodromy group of the corresponding local system is a fixed known group.

Contents

1. Introduction

For V a finite dimensional $\mathbb{C}$ vector space, $G \leq \mathrm{GL}(V)$ a Zariski closed subgroup whose identity component G° is semisimple, and (a, b) a pair of non-negative integers, the (a, b)-*moment* of G acting on V, denoted

$$M_{a,b} = M_{a,b}(G, V),$$

is defined to be the dimension of the space $(V^{\otimes a} \otimes (V^*)^{\otimes b})^G$ of G-invariants.

1991 *Mathematics Subject Classification.* 11T23, 14J45, 20C15, 20D06, 20C33, 20G40, 22E46.

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

The second author gratefully acknowledges the support of the NSF (grants DMS-1840702 and DMS-2200850), the Simons Foundation, and the Joshua Barlaz Chair in Mathematics.

Part of this work was done when the second author visited the Department of Mathematics, Princeton University. It is a pleasure to thank Princeton University for its generous hospitality and its stimulating environment. We also thank János Kollár for helpful conversations about intersections of Fermat hypersurfaces.

By Larsen's Alternative [Ka3, 1.1.6], one knows that if $M_{2,2}(G,V)=2$, then either G is finite or $G^\circ = \mathrm{SL}(V)$. If V is endowed with an orthogonal autoduality and $G \le O(V)$, and if $M_{2,2}=3$, then either G is finite or $G^\circ = \mathrm{SO}(V)$[1]. If V is endowed with a symplectic autoduality, $\dim(V)\ge 4$, and $G \le \mathrm{Sp}(V)$, then $M_{2,2}=3$ implies that either G is finite or $G=\mathrm{Sp}(V)$.

The cases of Larsen's Alternative in which G is finite and $\dim(V)\ge 5$ are completely determined in [GT2, Theorem 1.5]. Two natural questions then occur. Which of these finite groups can be obtained as the geometric monodromy group of a hypergeometric sheaf on $\mathbb{G}_m$ in characteristic $p>0$? Which of these finite groups can be obtained as the geometric monodomy group of a family of one-variable exponential sums?

The kinds of families of one-variable exponential sums in a given characteristic $p>0$ we have in mind are these. We fix a prime $\ell \ne p$ and a nontrivial additive character $\psi : \mathbb{F}_p \to \mu_p(\overline{\mathbb{Q}_\ell})$. [In down to earth terms, we embed $\mathbb{Q}(\zeta_p)$ into $\overline{\mathbb{Q}_\ell}$, which amounts to choosing a place of $\mathbb{Q}(\zeta_p)$ over ℓ. The expressions we will write down will lie in $\mathbb{Q}(\zeta_p)$, but we need to view them as lying in $\overline{\mathbb{Q}_\ell}$ in order to apply ℓ-adic cohomology.]

We are given a finite extension $k/\mathbb{F}_p$, a polynomial $f(x)\in k[x]$, say

$$f(x)=\sum_i A_i x^i,$$

of degree $d\ge 1$ which is Artin-Schreier reduced (meaning that $A_i=0$ whenever $p|i$). Let $1\le a<b$ be prime-to-p integers. Suppose that either $\deg(f)>b$ or that $\deg(f)<b$. In the case when $\deg(f)<b$, we require that f is not a constant multiple of x^a. Another way of expressing this last condition is that the polynomial $sx^a+tx^b+f(x)$ contains monomials of least 3 different degrees, a condition which is automatic if $\deg(f)>b$.

Let χ be a multiplicative character of $k^\times$. When $\deg(f)>b$, consider the local system

$$\mathcal{F}(f,a,b,\chi)$$

on $\mathbb{A}^2/k$ whose trace function is given as follows: for L/k a finite extension, and $s,t\in L$,

$$\mathrm{Trace}(\mathrm{Frob}_{(s,t),L}|\mathcal{F}) = \frac{-1}{\sqrt{\#L}}\sum_{x\in L}\psi_L(sx^a+tx^b+f(x))\chi_L(x).$$

When $\deg(f)<b$, we consider the same local system, but on $\mathbb{A}^1\times\mathbb{G}_m$, since we need t to be invertible in this $\deg(f)<b$ case. These families are pure of weight zero, and lisse of rank $\max(\deg(f),b)-1$ when $\chi=\mathbb{1}$ and of rank $\max(\deg(f),b)$ when $\chi\ne\mathbb{1}$. They are geometrically irreducible precisely when

$$\gcd(a,b,\{i \ \text{ with } A_i\ne 0\})=1,$$

which we will assume in what follows.

As we will see in Theorems 2.3 and 2.6, the $M_{2,2}$ for the G_{geom} of this local system is given by the answer to what **should be** an easy question about intersections of Fermat surfaces in $\mathbb{P}^3$, with homogeneous coordinates x,y,z,w, or equivalently about intersections of their affine cones in $\mathbb{A}^4$.

For an integer $n\ge 1$, denote by $\Sigma_{n,\mathrm{proj}}\subset\mathbb{P}^3$ the locus

$$\Sigma_{n,\mathrm{proj}} := \{x^n+y^n-z^n-w^n=0\}\subset\mathbb{P}^3$$

and denote by $\Sigma_n\subset\mathbb{A}^4$ the locus

$$\Sigma_n := \{x^n+y^n-z^n-w^n=0\}\subset\mathbb{A}^4.$$

[1]If $\dim(V)=2$ in this orthogonal case, G must be finite, because SO_2 is not semisimple.

In what follows, when no confusion is possible, we also denote the polynomial $x^n + y^n - z^n - w^n$ by Σ_n. In $\mathbb{A}^4/\overline{\mathbb{F}_p}$, consider the intersection of the following Fermat threefolds:

$$\Sigma_a,\ \Sigma_{b,},\ \text{and every } \Sigma_i \text{ with } A_i \neq 0.$$

Already $\Sigma_a \cap \Sigma_b$ has dimension two. [Equivalently, $\Sigma_{a,\mathrm{proj}} \cap \Sigma_{b,\mathrm{proj}}$ has dimension one. Here is one argument. Because each of a, b is prime to p, each of $\Sigma_{a,\mathrm{proj}}$ and $\Sigma_{b,\mathrm{proj}}$ is a smooth, geometrically connected surface. The intersection, viewed as lying in $\Sigma_{b,\mathrm{proj}}$, is either one dimensional or it is all of $\Sigma_{b,\mathrm{proj}}$. The second case could only occur if the polynomial Σ_a is divisible by Σ_b, which cannot happen, because $a < b$. A second argument is this. If the intersection had dimension 2, it would be equal to both $\Sigma_{a,\mathrm{proj}}$ and to $\Sigma_{b,\mathrm{proj}}$, and we would get the conclusion that $\Sigma_{a,\mathrm{proj}} = \Sigma_{b,\mathrm{proj}}$, impossible because their $\mathbb{Q}_\ell$ Euler characteristics differ.]

Denote by $\Sigma(a, b, f)$ the intersection in $\mathbb{A}^4/\overline{\mathbb{F}_p}$ of the following affine Fermat threefolds,

$$\Sigma_a,\ \Sigma_b,\ \text{and every } \Sigma_i \text{ with } A_i \neq 0.$$

Then $M_{2,2}$ is the number of reduced irreducible components of dimension two of $\Sigma(f, a, b)$, cf. Theorems 2.3 and 2.6.

The loci $\Sigma(f, a, b)$ and $\Sigma_{\mathrm{aff}}(f, a, b)$ depend only on the set S of degrees of the Fermat surfaces being intersected. Given a set S of prime-to-p positive integers with $\#S \geq 2$, let us denote

$$\Sigma_{\mathrm{proj}}(S) := \bigcap_{i \in S} \Sigma_{i,\mathrm{proj}}, \quad \Sigma(S) := \bigcap_{i \in S} \Sigma_i \tag{1.0.1}$$

Recall that by assumption the set S of degrees occurring in $\Sigma_{\mathrm{proj}}(f, a, b)$ satisfies $\gcd(S) = 1$: this is equivalent to the geometric irreducibility of the family.

Every Fermat surface $\Sigma_{a,\mathrm{proj}}$ contains the two lines $(x = z, y = w)$ and $(x = w, y = z)$. If a is odd, $\Sigma_{a,\mathrm{proj}}$ contains the third line $(x = -y, z = -w)$. One knows that in any odd characteristic, the intersection $\Sigma_{1,\mathrm{proj}} \cap \Sigma_{2,\mathrm{proj}}$ consists precisely of the two lines $(x = z, y = w)$ and $(x = w, y = z)$, cf. [Ka3, p. 117]. And one knows that in any characteristic $p \neq 3$, the intersection $\Sigma_{1,\mathrm{proj}} \cap \Sigma_{3,\mathrm{proj}}$ consists precisely of the three lines $(x = z, y = w)$, $(x = w, y = z)$, and $(x = -y, z = -w)$, cf. [Ka4, 3.11.3].

Thus the question breaks into two natural parts: First, for which sets S with $\gcd(S) = 1$ consisting only of odd degrees will $\Sigma_{\mathrm{proj}}(S)$ have precisely three reduced irreducible components of dimension one (which would necessarily be the three known lines). There may also be zero-dimensional reduced irreducible components (i.e., finitely many closed points) outside these lines, these do not affect $M_{2,2}$. Second, for which sets S with $\gcd(S) = 1$ of degrees, at least one of which is even, will $\Sigma_{\mathrm{proj}}(S)$ have precisely two reduced irreducible components of dimension one (which would necessarily be the two known lines). Again having finitely many points outside the two known lines does not affect $M_{2,2}$.

Our original idea was to attack directly this algebro-geometric question. But in fact we turn this question on its head as follows. Given a set S of prime to p integers with $\#S = r + 1 \geq 3$ and $\gcd(S) = 1$, enumerate the elements of S, say

$$A > B_1 > \ldots > B_r \geq 1, \quad p \nmid A \prod_i B_i, \ \gcd(A, B_1, \ldots, B_r) = 1, \tag{1.0.2}$$

and consider the corresponding universal family of monic one-variable polynomials whose allowed degrees are precisely S:

$$x^A + \sum_{i=1}^{r} t_i x^{B_i}.$$

We obtain a local system $\mathcal{F}(S)$ on $\mathbb{A}^r/\mathbb{F}_p$ whose trace function is given as follows. For $k/\mathbb{F}_p$ a finite extension, and $(t_1, \ldots, t_r) \in \mathbb{A}^r(k)$

$$\mathrm{Trace}(\mathrm{Frob}_{(t_1,\ldots,t_r),k}]\mathcal{F}(S)) = \frac{-1}{\sqrt{\#L}} \sum_{x \in k} \psi_k(x^A + \sum_{i=1}^{r} t_i x^{B_i}).$$

Given a multiplicative character χ, we also have the local system (S, χ) on $\mathbb{A}^r/\mathbb{F}_p$ whose trace function is given as follows. For $k/\mathbb{F}_p$ a finite extension, and $(t_1, \ldots, t_r) \in \mathbb{A}^r(k)$

$$\mathrm{Trace}(\mathrm{Frob}_{(t_1,\ldots,t_r),k}]\mathcal{F}(S,\chi)) = \frac{-1}{\sqrt{\#L}} \sum_{x \in k} \psi_k(x^A + \sum_{i=1}^{r} t_i x^{B_i})\chi_L(x).$$

In this notation, the above $\mathcal{F}(S)$ is just $\mathcal{F}(S, \mathbb{1})$.

The local system $\mathcal{F}(S, \chi)$ is geometrically irreducible, lisse of rank

$$D := A - \delta_{\mathbb{1},\chi},$$

and pure of weight 0. Its geometric monodromy group $G_{\mathrm{geom},\mathcal{F}(S,\chi)}$ is a Zariski closed subgroup of $\mathrm{GL}_D/\overline{\mathbb{Q}_\ell}$ whose identity component is semisimple. On the one hand $M_{2,2}$ of the local system $\mathcal{F}(S, \chi)$ is the number of reduced irreducible 2-dimensional components of $\Sigma(S)$ over $\overline{\mathbb{F}_p}$, on which $\mathcal{L}_{\chi(xy)} \otimes \mathcal{L}_{\overline{\chi}(zw)}$ is geometrically trivial, cf. Theorem 2.4. On the other hand, $M_{2,2}$ is the $M_{2,2}$ for the given D dimensional representation $V := \mathcal{F}(S, \chi)_{\overline{\eta}}$ of $G := G_{\mathrm{geom},\mathcal{F}(S,\chi)}$.

The key point is that we can explicitly determine the group $G_{\mathrm{geom},\mathcal{F}(S,\chi)}$. This task, in the case the group is finite, was done in [KT6, Theorem 11.2.3]. One of the main results of this paper, Theorem 7.8, completes the task in the infinite case. In turn, this allows us to determine $M_{2,2}$ for $G_{\mathrm{geom},\mathcal{F}(s,\chi)}$, and thus solve the aforementioned algebro-geometric question about intersections of Fermat hypersurfaces, in Theorem 9.2.

Once we have these results in hand, a new question arises. Suppose given an S as in (1.0.2), $A > B_1 > \ldots > B_r$, with $r \geq 3$. Pick two indices in $\{B_1, \ldots, B_r\}$, say $a := B_i < b := B_j < A$, and denote by

$$\mathcal{C} := \{A, B_1, \ldots, B_r\} \smallsetminus \{B_i, B_j\}$$

with $\mathcal{C}$ enumerated as

$$A > C_1 > \ldots > C_{r-2}.$$

Suppose further given a finite extension $k/\mathbb{F}_p$ and elements $c_i \in k^\times$ for $i = 1, \ldots, r-2$. Consider the local system on $\mathbb{A}^2/k$ obtained from $\mathcal{F}(S, \chi)$ by the pullback $C_i \mapsto c_i$. Call it

$$\text{(1.0.3)} \quad \mathcal{F}(f, a, b, \chi) = \mathcal{F}(f, B_i, B_j, \chi), \text{ where } f(x) := x^A + \sum_{l=1}^{r-2} c_l x^{C_l}, \text{ with } c_i \neq 0,\ 1 \leq i \leq r-2.$$

This is the local system on $\mathbb{A}^2/k$ whose trace function is given as follows. For K/k a finite extension, and $(s, t) \in \mathbb{A}^2(K)$,

$$\text{(1.0.4)} \quad \mathrm{Trace}\big(\mathrm{Frob}_{(s,t),K}|\mathcal{F}(f, a, b, \chi)\big) = \frac{-1}{\sqrt{\#L}} \sum_{x \in k} \psi_K(f(x) + sx^a + tx^b)\chi_K(x), \text{ subject to (1.0.3)}.$$

By Theorem 2.3 and Corollary 2.5, each such system $\mathcal{F}(f, B_i, B_j, \chi)$ has the **same** $M_{2,2}$ as the system $\mathcal{F}(S, \chi)$. Because $\mathcal{F}(f, B_i, B_j, \chi)$ is a pullback of $\mathcal{F}(S, \chi)$, we have the a priori inclusion

$$G_{\mathrm{geom},\mathcal{F}(f,B_i,B_j,\chi)} \leq G_{\mathrm{geom},\mathcal{F}(S,\chi)}.$$

In the case when $G_{\mathrm{geom},\mathcal{F}(S,\chi)}$ is a (known!) finite group, we wish to classify those of its subgroups which in the given D-dimensional representation have the same $M_{2,2}$. We succeed entirely when the known finite group is (the image of) one of $\mathrm{Sp}_{2n}(q)$, $n \geq 1$, or $\mathrm{SU}_n(q)$, $n \geq 3$, in a Weil representation, by showing that, with very few exceptions, the only subgroups with the same $M_{2,2}$ are the whole group itself, see Theorems 8.2 and 8.4. This gives Theorem 11.9. A striking aspect of part (ii) of Theorem 11.9 is that it applies to the relevant $\mathcal{F}(f,a,b,\chi)$ for **any** f all of whose coefficients are nonzero and **any** (a,b).

We also consider one-parameter specializations of such $\mathcal{F}(S,\chi)$, i.e., systems $\mathcal{F}(f,a,\chi)$ with trace function as follows: for K/k a finite extension and $t \in K$,

$$\mathrm{Trace}\big(\mathrm{Frob}_{t,K}|\mathcal{F}(f,a,\chi)\big) = \frac{-1}{\sqrt{\#L}}\sum_{x\in k}\psi_K(f(x)+tx^a)\chi_K(x), \text{ subject to (1.0.3).} \tag{1.0.5}$$

In Theorem 11.9, we prove that for given a, the local system $\mathcal{F}(f,a,\chi)$ will have the same G_{geom} as $\mathcal{F}(S,\chi)$ for f in a dense open set of the affine space of allowed f's

In the cases when $\chi = \mathbb{1}$, and $G_{\mathrm{geom},\mathcal{F}(S,\mathbb{1})}$ is an extraspecial normalizer, we do not classify subgroups with the same $M_{2,2}$. Nonetheless, we prove that for given (a,b), the local system $\mathcal{F}(f,a,b,\mathbb{1})$ will have the same G_{geom} as $\mathcal{F}(S,\mathbb{1})$ for f in a dense open set of the affine space of allowed f's, see Theorems 11.7 and 11.8. Again in this case we have the same "dense open set" result for one-parameter specializations $\mathcal{F}(f,a,\mathbb{1})$, with the added wrinkle that the case $a=1$ behaves quite differently in the extraspecial normalizer case. In each of the Theorems 11.7, 11.8, and 11.9, there are unknown dense open sets. It would be of some interest to determine them explicitly.

The main results of this paper include Theorems 7.8, 9.2, 10.1, 11.7, 11.8, 11.9.

2. Moments and point counting

We begin this section with the basic fact about approximating moments by large L limits.

Theorem 2.1. *Let k be a finite field of characteristic p, ℓ a prime $\ell \neq p$, X/k a smooth, geometrically connected scheme of dimension $d \geq 1$, and $\mathcal{F}$ a lisse $\overline{\mathbb{Q}_\ell}$ sheaf on X which is ι-pure of weight zero for a chosen field embedding $\iota : \overline{\mathbb{Q}_\ell} \hookrightarrow \mathbb{C}$. For integers $a,b \geq 0$, the moment $M_{a,b}$ of $G_{\mathrm{geom},\mathcal{F}}$ is*

$$M_{a,b} = \limsup_{\text{finite extensions } L/k}\left|\frac{1}{\#X(L)}\sum_{x\in X(L)}(\mathrm{Trace}(\mathrm{Frob}_{x,L}|\mathcal{F}))^a(\mathrm{Trace}(\mathrm{Frob}_{x,L}|\mathcal{F}^\vee))^b\right|.$$

Proof. In terms of the auxiliary sheaf

$$\mathcal{G} := (\mathcal{F})^{\otimes a}\otimes(\mathcal{F}^\vee)^{\otimes b},$$

which is ι-pure of weight zero, and hence geometrically semisimple, cf. [De2, 3.4.1(iii)], we have

$$M_{a,b} = \dim H^{2d}_c(X_{\overline{k}},\mathcal{G}).$$

Our asserted formula for this dimension is

$$\limsup_{\text{finite extensions } L/k}\left|\frac{1}{\#X(L)}\sum_{x\in X(L)}\mathrm{Trace}(\mathrm{Frob}_{x,L}|\mathcal{G})\right|.$$

By the Lefschetz trace formula, this is

$$\limsup_{\text{finite extensions } L/k}\left|\frac{1}{\#X(L)}\sum_{i=0}^{2d}(-1)^i\mathrm{Trace}(\mathrm{Frob}_L|H^i_c(X_{\overline{k}},\mathcal{G}))\right|.$$

By Deligne's fundamental estimate [De2, 3.4], H^i_c is ι-mixed of weight $\leq i$, while H^{2d}_c is ι-pure of weight $2d$. But $\#X(L) = (\#L)^d + O((\#L)^{d-1/2}$, and hence the H^i_c summands with $i < 2d$ contribute 0 to the lim sup. So we must prove that $\dim H^{2d}_c(X_{\overline{k}},\mathcal{G})$ is

$$\limsup_{\text{finite extensions } L/k}\left|\frac{1}{\#X(L)}\mathrm{Trace}(\mathrm{Frob}_L|H^{2d}_c(X_{\overline{k}},\mathcal{G}))\right|.$$

If this H_c^{2d} vanishes, we are done.

If H_c^{2d} is nonzero, the eigenvalues of Frob_k on this H_c^{2d} are each of the form $(\#k)^d\alpha_i$, for $i = 1, \ldots, \dim H_c^{2d}$, and each of these α_i has complex absolute value $|\alpha_i| = 1$. Thus for L/k a finite extension, we have

$$\frac{1}{\#X(L)}\mathrm{Trace}(\mathrm{Frob}_L|H_c^{2d}(X_{\overline{k}}, \mathcal{G})) = \frac{(\#L)^d}{\#X(L)}\sum_{i=1}^{\dim H_c^{2d}}(\alpha_i)^{\deg(L/k)}.$$

For any L/k, this last expression visibly has absolute value $\leq (1/\#X(L))(\#L)^d)\dim H_c^{2d}$. As L/k grows, the tuple $(\alpha_1^{\deg(L/k)}, \ldots, \alpha_{\dim H_c^{2d}}^{\deg(L/k)})$ will, infinitely ofter, come arbitrarily close to $(1, \ldots, 1)$, while the ratio $\#X(L)/((\#L)^d)$ has limit 1 as L grows. ☐

We next give a lemma on counting geometrically irreducible components.

Lemma 2.2. *Let k be a finite field, and X/k a separated k-scheme of finite type, of dimension $d \geq 0$. Then*

$$\limsup_{\text{finite extensions } L/k} \#X(L)/(\#L)^d$$

is the number of geometrically irreducible components of $X_{\overline{k}}$ of dimension d.

Proof. Each geometrically irreducible component of $X_{\overline{k}}$ is defined over some finite extension of k, so at the expense of replacing k by a finite extension of itself, we reduce to the case where each geometrically irreducible component Z is defined over k, i.e. is a geometrically irreducible k-scheme of dimension $e_Z \leq d$. The result then follows from the Lang-Weil estimate, that for each such component Z, $\#Z(L) = (\#L)^{e_Z} + O((\#L)^{e_Z - 1/2})$. ☐

Theorem 2.3. *Let k be a finite field of characteristic $p > 0$, and $f(x) \in k[x]$, say $f(x) = \sum_i A_i x^i$, of degree $d \geq 3$ which is Artin-Schreier reduced (meaning that $A_i = 0$ if $p|i$). Let $1 \leq a < b < \deg(f)$ be prime to p integers, χ a multiplicative character of $k^\times$, and consider the local system $\mathcal{F}_\chi$ on $\mathbb{A}^2/k$ whose trace function is given as follows: for L/k a finite extension, and $s, t \in L$,*

$$\mathrm{Trace}(\mathrm{Frob}_{(s,t),L}|\mathcal{F}_\chi) = \frac{-1}{\sqrt{\#L}}\sum_{x\in L}\psi_L(sx^a + tx^b + f(x))\chi_L(x),$$

with the convention that $\mathbb{1}_L(0) = 1$, but $\chi_L(0) = 0$ for χ nontrivial. Consider the set $\mathcal{E}$ of exponents which occur in f:

$$\mathcal{E} := \{i \in \mathbb{Z},\ A_i \neq 0\}$$

and the affine locus $\Sigma(S)$ as defined in (1.0.1) with $S := \{a, b\} \cup \mathcal{E}$. Then

$$M_{2,2}(\mathcal{F}_\chi) \leq M_{2,2}(\mathcal{F}_{\mathbb{1}}) = \limsup_{\#L\to\infty}\frac{\#\Sigma(S)(L)}{(\#L)^2}.$$

Moreover, if $\chi^2 \neq \mathbb{1}$ and all integers in S are odd, then

$$M_{2,2}(\mathcal{F}_\chi) < M_{2,2}(\mathcal{F}_{\mathbb{1}}).$$

More precisely, $M_{2,2}(\mathcal{F}_{\mathbb{1}})$ is the number of geometrically irreducible components of dimension one in $\Sigma_{\mathrm{proj}}(S)$, while $M_{2,2}(\mathcal{F}_\chi)$ is the number of those components on which $\chi(xy)\bar{\chi}(zw)$ is geometrically trivial.

Proof. Recall that Σ_d denotes the Fermat form $x^d + y^d - z^d - w^d$ for any $d \in \mathbb{Z}_{\geq 1}$. By Theorem 2.1, $M_{2,2}(\mathcal{F}_\chi)$ is the large L limit of the sums

$$\frac{1}{(\#L)^2} \sum_{(x,y,z,w)\in\mathbb{A}^4(L),\ \Sigma_a=\Sigma_b=0} \psi_L(f(x)+f(y)-f(z)-f(w))\chi_L(xy)\bar{\chi}_L(zw)$$
$$=\frac{1}{(\#L)^2} \sum_{(x,y,z,w)\in\mathbb{A}^4(L),\ \Sigma_a=\Sigma_b=0} \psi_L(\sum_{i\in\mathcal{E}} A_i\Sigma_i(x,y,z,w))\chi_L(xy)\bar{\chi}_L(zw).$$

The key observation is that the affine variety

$$\Sigma_{a,b} := \{\Sigma_a = \Sigma_b = 0\}$$

in $\mathbb{A}^4$ is homogeneous, the affine cone over the projective variety $\Sigma_{a,b,\mathrm{proj}} \subset \mathbb{P}^3$ defined by these same equations. We may omit the origin $(0,0,0,0) \in \mathbb{A}^4$ without changing the large L limit. Then we choose, for each point in $\Sigma_{a,b,\mathrm{proj}}(L)$ a representative $(x_0,y_0,z_0,w_0) \in \Sigma_{a,b}(L)$. Then every point (x,y,z,w) in $\Sigma_{a,b}(L) \smallsetminus \{0\}$ is uniquely of the form (rx_0,ry_0,rz_0,rw_0) with $r \in L^\times$ and $(x_0,y_0,z_0,w_0) \in \Sigma_{a,b}(L)$ a chosen representative. Moreover,

$$\chi_L(xy)\bar{\chi}_L(zw) = \chi_L(x_0y_0)\bar{\chi}_L(z_0w_0).$$

Thus we are looking at the large L limit of the sums

$$\frac{1}{(\#L)^2} \sum_{(x_0,y_0,z_0,w_0)\text{ chosen rep. over }L} \chi_L(x_0y_0)\bar{\chi}_L(z_0w_0) \sum_{r\in L^\times} \psi_L(\sum_{i\in\mathcal{E}} A_i\Sigma_i(x_0,y_0,z_0,w_0)r^i).$$

The innermost sum is $O(\#L)^{1/2}$ so long as the polynomial

$$\sum_{i\in\mathcal{E}} A_i\Sigma_i(x_0,y_0,z_0,w_0)r^i$$

in r is not Artin-Schreier trivial. The number of L-valued points on $\Sigma_{a,b,\mathrm{proj}}$ is $O(\#L)$, so the Artin-Schreier nontrivial cases contribute $O((\#L)^{3/2})/(\#L)^2$ to the sum, and hence contribute 0 to the large L limit.

Because $f(x)$ is Artin-Schreier reduced, the only way the polynomial $\sum_{i\in\mathcal{E}} A_i\Sigma_i(x_0,y_0,z_0,w_0)r^i$ in r can be Artin-Schreier trivial is for every $\Sigma_i(x_0,y_0,z_0,w_0)$ with $i \in \mathcal{E}$ to vanish, in which case the inner sum is $\#L - 1$. Thus our large L limiting sum is

$$\frac{1}{(\#L)^2} \sum_{(x,y,z,w)\in\mathbb{P}^3(L),\ \Sigma_a=\Sigma_b=0,\ \Sigma_i=0,\ \forall i\in\mathcal{E}} (\#L-1)\chi_L(xy)\bar{\chi}_L(zw).$$

We break the domain of summation into finitely many closed points and the one-dimensional geometrically irreducible components Z of the projective variety $\Sigma_{\mathrm{proj}}(S)$ defined by

$$\Sigma_a = \Sigma_b = 0,\ \Sigma_i = 0,\ \forall i \in \mathcal{E},$$

each of which is defined over some finite extension of k. At the expense of enlarging k, we may assume each Z is defined over k. Then $\#Z(L) = \#L + O(\sqrt{\#L})$. So our lim sup is the lim sup of the sum

$$\sum_{\text{1-dim irred. compt's } Z} \frac{1}{(\#L)^2} \sum_{(x,y,z,w)\in Z(L)} (\#L-1)\chi_L(xy)\bar{\chi}_L(zw).$$

When $\chi(xy)\bar{\chi}(zw)$ is geometrically trivial on (the dense open set where $xyzw \neq 0$ of) Z, this sum over Z contributes 1 to the lim sup, while if $\chi(xy)\bar{\chi}(zw)$ is geometrically nontrivial on (the dense open set where $xyzw \neq 0$ of) Z, it contributes 0 to the limsup. Thus we have

$$M_{2,2}(\mathcal{F}_\chi) \leq M_{2,2}(\mathcal{F}_{\mathbb{1}}) = \limsup_{\#L\to\infty} \frac{\#\Sigma(S)(L)}{(\#L)^2}.$$

So $M_{2,2}(\mathcal{F}_{\mathbb{1}})$ is the number of geometrically irreducible components of dimension one in $\Sigma_{\mathrm{proj}}(S)$, while $M_{2,2}(\mathcal{F}_\chi)$ is the number of those components on which $\chi(xy)\bar{\chi}(zw)$ is geometrically trivial.

Now assume that all integers in S are odd. Then $\Sigma_{\mathrm{proj}}(S)$ contains the line $x + y = 0 = z + w$. For any character χ of $k^\times$, the sum of $\chi_L(xy)\bar{\chi}_L(zw)$ over this line is $\#L - 1$ if $\chi^2 = \mathbb{1}$ and 0 otherwise. Thus if $\chi^2 \neq \mathbb{1}$, this line is an irreducible component on which $\chi(xy)\bar{\chi}(zw)$ is geometrically nontrivial, hence the asserted inequality

$$M_{2,2}(\mathcal{F}_\chi) < M_{2,2}(\mathcal{F}_{\mathbb{1}})$$

if $\chi^2 \neq \mathbb{1}$. ☐

For ease of later reference, we given a slight generalization of this last result.

Theorem 2.4. *Let k be a finite field of characteristic $p > 0$, and $f(x) \in k[x]$, say $f(x) = \sum_i A_i x^i$, of degree $d \geq 3$ which is Artin-Schreier reduced (meaning that $A_i = 0$ if $p|i$). Let $n \geq 2$, and let*

$$1 \leq b_1 < b_2 < \ldots < b_n < \deg(f)$$

be prime to p integers, χ a multiplicative character of $k^\times$, and consider the local system $\mathcal{F}_\chi$ on $\mathbb{A}^n/k$ whose trace function is given as follows: for L/k a finite extension, and $(t_1, \ldots, t_n) \in L^n$,

$$\mathrm{Trace}(\mathrm{Frob}_{(t_1,\ldots,t_n),L}|\mathcal{F}_\chi) = \frac{-1}{\sqrt{\#L}} \sum_{x\in L} \psi_L(\Sigma_i t_i x^{b_i} + f(x))\chi_L(x),$$

with the convention that $\mathbb{1}_L(0) = 1$, but $\chi_L(0) = 0$ for χ nontrivial. Consider the set $\mathcal{E}$ of exponents which occur in f:

$$\mathcal{E} := \{i \in \mathbb{Z},\ A_i \neq 0\}$$

and the affine locus $\Sigma(S)$ as defined in (1.0.1) with $S := \{b_1, \ldots, b_n\} \cup \mathcal{E}$. Then

$$M_{2,2}(\mathcal{F}_\chi) \leq M_{2,2}(\mathcal{F}_{\mathbb{1}}) = \limsup_{\#L\to\infty} \frac{\#\Sigma(S)(L)}{(\#L)^2}.$$

Moreover, if $\chi^2 \neq \mathbb{1}$ and all integers in S are odd, then

$$M_{2,2}(\mathcal{F}_\chi) < M_{2,2}(\mathcal{F}_{\mathbb{1}}).$$

More precisely, $M_{2,2}(\mathcal{F}_{\mathbb{1}})$ is the number of geometrically irreducible components of dimension one in $\Sigma_{\mathrm{proj}}(S)$, while $M_{2,2}(\mathcal{F}_\chi)$ is the number of those components on which $\chi(xy)\bar{\chi}(zw)$ is geometrically trivial.

Proof. The proof is essentially identical to that of the previous Theorem 2.3, which is the case $n = 2$. Let us denote

$$B := \{b_1, \ldots, b_n\}.$$

The role of $\Sigma_{a,b}$ there is played by $\Sigma_B := \cap_i \Sigma_{b_i}$ here. The affine variety Σ_B is homogeneous, the affine cone over the projective variety $\Sigma_{B,\mathrm{proj}}$ defined by the same equations. Because $n \geq 2$, the projective variety $\Sigma_{B,\mathrm{proj}}$ has dimension one, i.e., all its geometriically irreducible components have dimension ≤ 1, so over any finite extension L/k has $O(\#L)$ L-valued points. From here on, the proof is identical. ☐

Corollary 2.5. *In the setting of Theorem 2.3, with* $S := \mathcal{E} \cup \{a, b\}$*, write* S *as*

$$A > B_1 > \ldots > B_r \geq 1$$

with $r \geq 2$*. Consider the local system* $\mathcal{F}(S, \chi)$ *on* $\mathbb{A}^r$*, whose trace function is given as follows: For* $k/\mathbb{F}_p$ *a finite extension, and* $(t_1, \ldots, t_r) \in \mathbb{A}^r(k)$

$$\mathrm{Trace}(\mathrm{Frob}_{(t_1,\ldots,t_r),k}]\mathcal{F}(S,\chi)) = \frac{-1}{\sqrt{\#L}} \sum_{x \in k} \psi_k(x^A + \sum_{i=1}^{r} t_i x^{B_i})\chi_L(x).$$

It is lisse of rank $D := A - \delta_{\mathbb{1},\chi}$ *and pure of weight zero.* [It is geometrically irreducible if and only if $\gcd(S) = 1$, but that is irrelevant here.] *Then* $\mathcal{F}(f, a, b, \chi)$ *has the same* $M_{2,2}$ *as* $\mathcal{F}(S, \chi)$*.*

Proof. That $\mathcal{F}(S, \chi)$ has its $M_{2,2}$ given by the same recipe, purely in terms of the data (S, χ), as did $\mathcal{F}(f, a, b, \chi)$, is the special case $f(x) = x^A$, $n = r$, and $b_i = B_{r+1-i}$, of Theorem 2.4. □

Theorem 2.6. *Let* k *be a finite field of characteristic* $p > 0$*, and* $f(x) \in k[x]$*, say* $f(x) = \sum_i A_i x^i$*, of degree* $d \geq 1$ *which is Artin-Schreier reduced (meaning that* $A_i = 0$ *if* $p|i$*). Let* $1 \leq a < b$ *be prime to* p *integers, and suppose* $\deg(f) < b$*. For* χ *a character of* $k^\times$*, consider the local system* $\mathcal{F}_\chi$ *on* $(\mathbb{A}^1 \times \mathbb{G}_m)/k$ *whose trace function is given as follows: for* L/k *a finite extension, and* $s \in L$*,* $t \in L^\times$*,*

$$\mathrm{Trace}(\mathrm{Frob}_{(s,t),L}|\mathcal{F}_\chi) = \frac{-1}{\sqrt{\#L}} \sum_{x \in L} \psi_L(sx^a + tx^b + f(x))\chi_L(x),$$

with the convention that $\mathbb{1}_L(0) = 1$*, but* $\chi_L(0) = 0$ *for* χ *nontrivial. Consider the set* $\mathcal{E}$ *of exponents which occur in* f*:*

$$\mathcal{E} := \{i \in \mathbb{Z},\ A_i \neq 0\}$$

and the affine locus $\Sigma(S)$ *as defined in* (1.0.1) *with* $S := \{a, b\} \cup \mathcal{E}$*.*

(i) *Suppose that* $f(x)$ *is not of the form* (nonzero constant)x^a*. Then*

$$M_{2,2}(\mathcal{F}_\chi) \leq M_{2,2}(\mathcal{F}_{\mathbb{1}}) = \limsup_{\#L \to \infty} \frac{\#\Sigma(S)(L)}{(\#L)^2}.$$

Moreover, if $\chi^2 \neq \mathbb{1}$ *and all integers in* S *are odd, then*

$$M_{2,2}(\mathcal{F}_\chi) < M_{2,2}(\mathcal{F}_{\mathbb{1}}).$$

More precisely, $M_{2,2}(\mathcal{F}_{\mathbb{1}})$ *is the number of geometrically irreducible components of dimension one in* $\Sigma_{\mathrm{proj}}(S)$*, while* $M_{2,2}(\mathcal{F}_\chi)$ *is the number of those components on which* $\chi(xy)\bar{\chi}(zw)$ *is geometrically trivial.*

(ii) *Suppose that* $f(x) =$ (nonzero constant)x^a*. If* $\chi = \mathbb{1}$*, then*

$$M_{2,2}(\mathcal{F}_{\mathbb{1}}) = -1 + \limsup_{\#L \to \infty} \frac{\#\Sigma(S)(L)}{(\#L)^2},$$

while for $\chi \neq \mathbb{1}$ *we have*

$$M_{2,2}(\mathcal{F}_\chi) = \limsup_{\#L \to \infty} \frac{\#\Sigma(S)(L)}{(\#L)^2}.$$

Moreover, if a, b *are both odd, and* $\chi^2 \neq \mathbb{1}$*, we have*

$$M_{2,2}(\mathcal{F}_\chi) < \limsup_{\#L \to \infty} \frac{\#\Sigma(S)(L)}{(\#L)^2}.$$

Proof. By Theorem 2.1 and the argument of Theorem 2.3, $M_{2,2}$ for $\mathcal{F}_\chi$ is the lim sup over L of

$$\frac{1}{(\#L)(\#L-1)}\sum_{s\in L, t\in L^\times}\frac{1}{(\#L)^2}\sum_{x,y,z,w\in L}\psi_L(s\Sigma_a+t\Sigma_b+f(x)+f(y)-f(z)-f(w))\chi_L(xy)\bar{\chi}_L(zw).$$

If the summation were over all $(s,t)\in L^2$, this would be

$$\frac{1}{(\#L)(\#L-1)}\sum_{x,y,z,w\in L,\ \Sigma_a=\Sigma_b=0}\psi_L(f(x)+f(y)-f(z)-f(w))\chi_L(xy)\bar{\chi}_L(zw),$$

and just as in the proof of Theorem 2.3 we would get

$$M_{2,2}(\mathcal{F}_\chi)\le M_{2,2}(\mathcal{F}_{\mathbb{1}})=\limsup_{\#L\to\infty}\frac{\#\Sigma(S)(L)}{(\#L)^2}.$$

However, the summation is only over $(s,t)\in L\times L^\times$. So we must **subtract**, for each L/k, the expression

$$\frac{1}{(\#L)(\#L-1)}\sum_{s\in L}\frac{1}{(\#L)^2}\sum_{x,y,z,w\in L}\psi_L(s\Sigma_a+f(x)+f(y)-f(z)-f(w))\chi_L(xy)\bar{\chi}_L(zw)$$
$$=\frac{1}{(\#L)^2(\#L-1)}\sum_{x,y,z,w\in L,\ \Sigma_a=0}\psi_L(f(x)+f(y)-f(z)-f(w))\chi_L(xy)\bar{\chi}_L(zw).$$

So long as $f(x)$ contains monomials of degree $e_i\neq a$, the ray calculation used in the proof of Theorem 2.3 shows that this limit (not just lim sup) vanishes. The assertion about $\chi^2\neq\mathbb{1}$ is proven exactly as in Theorem 2.3.

Suppose now that $f(x)$ is a constant multiple of x^a and $\chi=\mathbb{1}$. Then the term we are subtracting is equal to

$$\frac{1}{(\#L)^2(\#L-1)}\sum_{x,y,z,w\in L,\ \Sigma_a=0}\psi_L(0)=\#\Sigma_a(L)/((\#L)^2(\#L-1)),$$

which tends to 1 as L grows, simply because Σ_a is the affine cone over the smooth surface $\Sigma_{a,\mathrm{proj}}$.

Suppose finally that $f(x)$ is a constant multiple of x^a and $\chi\neq\mathbb{1}$. Then the sum we are subtracing is

$$\frac{1}{(\#L)^2(\#L-1)}\sum_{x,y,z,w\in L,\ xyzw\neq0,\ \Sigma_a=0}\chi_L(xy/zw).$$

This sum will be $O(1/\sqrt{\#L})$, and thus have large L limit zero, if the Kummer sheaf $\mathcal{L}_{\chi(xy/zw)}$ is geometrically nontrivial on the dense open set U of $\Sigma_{a,\mathrm{proj}}$ where $xyzw$ is invertible. Thus U is the open set in the affine surface $x^a+y^a=z^a+1$ where yz is invertible, and our sheaf is $\mathcal{L}_{\chi(xy/z)}$ on U. We will show that this sheaf has a geometrically nontrivial pullback.

Choose an element $\alpha\in\mathbb{F}_{p^2}\smallsetminus\mathbb{F}_p$, and β with $\beta^a=\alpha$. It suffices to show the pullback of $\mathcal{L}_{\chi(xy/z)}$ to the closed subscheme $y=\beta$ of U is geometrically nontrivial. This pullback is $\mathcal{L}_{\chi(\beta x/z)}$, on the open set of the curve

$$\mathcal{C}: x^a+\alpha=z^a+1$$

where xz is invertible. But the function $\beta x/z$ on $\mathcal{C}$ has a simple zero at each point $(0,\gamma)$ with γ one of the a distinct roots of the polynomial $T^a=\alpha-1$. Hence $\mathcal{L}_{\chi(\beta x/z)}$ is geometrically nontrvial on $\mathcal{C}$.

So in this case when $f(x)$ is a constant multiple of x^a and $\chi\neq\mathbb{1}$, we have

$$M_{2,2}(\mathcal{F}_\chi)\le\limsup_{\#L\to\infty}\frac{\#\Sigma(S)(L)}{(\#L)^2}.$$

[Of course in this case the set $S = \{a, b\}$.] The argument in the proof of Theorem 2.3 shows that if a, b are both odd, but $\chi^2 \neq \mathbb{1}$, then

$$M_{2,2}(\mathcal{F}_\chi) < \limsup_{\#L \to \infty} \frac{\#\Sigma(S)(L)}{(\#L)^2}.$$

□

The following result explains the moment drop for some local systems.

Theorem 2.7. *Let k be a finite field of* **odd** *characteristic $p > 0$, and $f(x) \in k[x]$, say $f(x) = \sum_i A_i x^i$, of degree $d \geq 1$ which is Artin-Schreier reduced (meaning that $A_i = 0$ if $p|i$). Let $1 \leq a < b$ be prime to p integers, and suppose $\deg(f) \neq b$. Consider the local system $\mathcal{F}$ on $(\mathbb{A}^1 \times \mathbb{G}_m)/k$ whose trace function is given as follows: for L/k a finite extension, and $s \in L$, $t \in L^\times$,*

$$\mathrm{Trace}(\mathrm{Frob}_{(s,t),L}|\mathcal{F}) = \frac{-1}{\sqrt{\#L}} \sum_{x \in L} \psi_L(sx^a + tx^b + f(x)).$$

Suppose further that f is odd, i.e., that $f(-x) = -f(x)$, that f is not a constant multiple of x^a, and that both a, b are odd. Let $g(x) \in k[x]$, say $g(x) = \sum_i B_i x^i$, of degree $e \geq 1$ which is Artin-Schreier reduced (meaning that $B_i = 0$ if $p|i$). Consider the local system $\mathcal{G}$ on $(\mathbb{A}^1 \times \mathbb{G}_m)/k$ whose trace function is given as follows: for L/k a finite extension, and $s \in L$, $t \in L^\times$,

$$\mathrm{Trace}(\mathrm{Frob}_{(s,t),L}|\mathcal{G}) = \frac{-1}{\sqrt{\#L}} \sum_{x \in L} \psi_L(sx^a + tx^b + f(x) + g(x^2)).$$

Then $M_{2,2}(\mathcal{G}) \leq M_{2,2}(\mathcal{F}) - 1$.

Proof. Consider the set $\mathcal{E}_f$ of exponents which occur in f:

$$\mathcal{E}_f := \{i \in \mathbb{Z},\ A_i \neq 0\}$$

and $S_f := \{a, b\} \cup \mathcal{E}_f$.

Consider also the set $\mathcal{E}_{f,+}$ of exponents with occur in $f(x) + g(x^2)$:

$$\mathcal{E}_{f,} := \{i \in \mathbb{Z},\ A_i \neq 0\} \cup \{2j,\ B - J \neq 0\}$$

and $S_{f,+} := \{a, b\} \cup \mathcal{E}_{f,+}$. Then from Theorems 2.3 and 2.6, we know that

$$M_{2,2}(\mathcal{F}) = \limsup_{\#L \to \infty} \frac{\#\Sigma(S_f)(L)}{(\#L)^2}.$$

$$M_{2,2}(\mathcal{G}) = \limsup_{\#L \to \infty} \frac{\#\Sigma(S_{f,+})(L)}{(\#L)^2}.$$

As $S_f \subset S_{f,+}$, we trivially have $M_{2,2}(\mathcal{G}) \leq M_{2,2}(\mathcal{F})$. Because S_f consists entirely of odd integers, among the two-dimensional geometrically irreducible components of $\Sigma(S_f)$ is the locus $x + y = 0 = z + w$.

It suffices to show that this locus $x + y = 0 = z + w$ does not lie in $\Sigma(S_{f,+})$. Indeed, $S_{f,+}$ contains some nonzero even integer $2j$, and hence $\Sigma(S_{f,+})$ lies inside the hypersurface of equation $x^{2j} + y^2 = z^{2j} + w^{2j}$. So it suffices to show that the locus $x + y = 0 = z + w$ does not lie in this hypersurface. The intersection of this hypersurface with the locus $x + y = 0 = z + w$ is the locus in (x, z) space defined by $x^{2j} + (-x)^{2j} = z^{2j} + (-z)^{2j}$. As we are in odd characteristic, this intersection is the locus $x^{2j} = z^{2j}$, which is the union of $2j$ lines. □

3. $M_{2,2}$ AND RESULTANTS

We will need the following property of resultants, which is well-known:

Lemma 3.1. *Let R, S be commutative rings, $f, g \in R[x]$, and let $\varphi : R \to S$ be a ring homomorphism.*

(i) *If $\varphi(\mathsf{Res}(f,g)) \neq 0$, then $\mathsf{Res}(\varphi(f), \varphi(g))$ (computed as of two polynomials in $S[x]$) is also nonzero.*
(ii) *If φ preserves the degree of each of f and g, then $\mathsf{Res}(\varphi(f), \varphi(g)) \neq 0$ implies $\varphi(\mathsf{Res}(f,g)) \neq 0$.*
(iii) *If S is an integral domain and φ preserves the degree of at least one of f and g, then $\mathsf{Res}(\varphi(f), \varphi(g)) \neq 0$ if and only if $\varphi(\mathsf{Res}(f,g)) \neq 0$.*

Proof. (i) Assume that $\varphi(\mathsf{Res}(f,g)) \neq 0$. Let $f(x)$ be of degree d and with leading term ax^d, and let $g(x)$ be of degree e and with leading term bx^e. Suppose that $\varphi(a) = \varphi(b) = 0$, so that $\varphi(f) \in S[x]$ has degree $< d$ and $\varphi(g) \in S[x]$ has degree $< e$. In this case, $\varphi(\mathsf{Res}(f,g)) = 0$, a contradiction. So we may assume that $\varphi(a) \neq 0$, so that $\varphi(f) \in S[x]$ has degree d. Now, if $\varphi(g)$ has degree $e' \leq e$, then

$$\varphi(\mathsf{Res}(f,g)) = \pm\varphi(a)^{e-e'}\mathsf{Res}(\varphi(f), \varphi(g)), \tag{3.1.1}$$

and hence $\mathsf{Res}(\varphi(f), \varphi(g)) \neq 0$.

(ii) follows from (3.1.1) (with $e' = e$).

(iii) follows from (i), (3.1.1), and the assumption that S is an integral domain. ☐

Fix a prime p. First we look at any set $\mathcal{Q} := \{q_1 < \ldots < q_n\}$ of $n \geq 1$ positive powers of p, and consider

$$\mu_{total}(\mathcal{Q}) := \bigcap_{1 \leq i \leq n} \{\zeta \in \overline{\mathbb{F}_p} | \zeta^{q_i - 1} = (-1)^p\}. \tag{3.1.2}$$

In the special case of characteristic $p = 2$, we have $(-1)^p = 1$, and so

$$\mu_{total}(\mathcal{Q}) = \mu_{\gcd_{i=1}^n (q_i - 1)}. \tag{3.1.3}$$

The following observation is helpful in computing $\mu_{total}(\mathcal{Q})$.

Lemma 3.2. *Let $n \geq 2$, p any prime, $q = p^f$, $q_i = q^{m_i}$ for $1 \leq i \leq n$, and $m_1 < \ldots < m_n$. Also let $e := \gcd(m_1, \ldots, m_n)$. Then*

$$\#\mu_{total}(\mathcal{Q}) = \begin{cases} q^e - 1, & p = 2, \\ q^e - 1, & p > 2 \text{ and } 2 \nmid (m_i/e) \text{ for all } i, \\ 0, & p > 2 \text{ and } 2 | (m_i/e) \text{ for some } i. \end{cases}$$

Proof. The statement is obvious when $p = 2$, so we will assume $p > 2$. 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 $\zeta \in \mu_{total}(\mathcal{Q})$. Since $\zeta^{q^{m_j} - 1} = -1$ and m_j is odd, we see that the 2-part 2^f of the order of ζ 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 $(2q-2)^{\text{th}}$ root of unity $\theta \in \overline{\mathbb{F}_p}$. Then $-1 = \theta^{q-1} = \theta^{q^{m_i} - 1}$, and hence $\zeta \in \mu_{total}(\mathcal{Q})$ 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 $\zeta\theta$. ☐

For any $a \in \mathbb{Z}_{\geq 2}$, let

$$\mathcal{M}_p(a) := \left\{ A \in \overline{\mathbb{F}_p}^\times \mid \forall j,\ 2 \leq j \leq a,\ \binom{a}{j}\big((A+1)^j - A^j - 1\big) = 0 \right\}. \tag{3.2.1}$$

Note that $\mathcal{M}_p(a)$ is finite (by looking at the condition at $j = a$, if $p \nmid a$. In fact, $\mathcal{M}_p(2) = \varnothing$ if $p > 2$, $\mathcal{M}_p(3) = \varnothing$ if $p > 3$; more generally, $\mathcal{M}_p(a) = \varnothing$ if $2 \leq a < p$ or if $p \nmid a(a-1)$. As we will see in the proof of Proposition 3.3, see (3.3.6), for $q = p^f$ we have

$$\mathcal{M}_p(q+1) = \mu_{total}(\{q\}) = \{A \in \overline{\mathbb{F}_p}^\times \mid A^{q-1} = -1\}.$$

We also set

$$F_a(A,v) := \frac{\big((A+1)v+1\big)^a - (Av+1)^a - (v+1)^a + 1}{Av^2} \in \mathbb{F}_p[A,v].$$

Keep the notation

$$\Sigma_a := x^a + y^a - z^a - w^a \in \mathbb{F}_p[x,y,z,w].$$

Proposition 3.3. *Let $2 \leq b < c$ be integers coprime to p. For finite extensions $L/\mathbb{F}_p$, the following statements hold for the set $\Sigma(L)$ of L-points of the surface*

$$\Sigma:\ \Sigma_1 = \Sigma_b = \Sigma_c = 0$$

of $\mathbb{A}^4(x,y,z,w)$.

(i) $\lim_{\#L\to\infty} \#\Sigma(L)/L^2 \geq 2 + \#\big(\mathcal{M}_p(b) \cap \mathcal{M}_p(c)\big)$.

(ii) *If the resultant $R(A) := \mathsf{Res}_v(F_b(A,v), F_c(A,v))$ of the polynomials $F_b(A,v)$ and $F_c(A,v)$ in the variable v is not identically zero as a function of A, then*

$$\lim_{\#L\to\infty} \#\Sigma(L)/L^2 = 2 + \#\big(\mathcal{M}_p(b) \cap \mathcal{M}_p(c)\big).$$

(iii) *If $b = 2 < p$ then $\lim_{\#L\to\infty} \#\Sigma(L)/L^2 = 2$.*

(iv) *If $b = 3 < p$ then $\lim_{\#L\to\infty} \#\Sigma(L)/L^2$ equals 2 when $2|c$ and 3 when $2 \nmid c$.*

(v) *The equality in* (ii) *holds if $b = p^f + 1$.*

(vi) *Suppose $\gcd\big((b-1)_{p'}, (c-1)_{p'}\big) = 1$, where $n_{p'}$ denotes the p'-part of $n \in \mathbb{Z}_{\geq 1}$. Then $R(A) \not\equiv 0$ and hence the equality in* (ii) *holds.*

(vii) *If $\gcd(b-1, c-1) = 1$, then $\lim_{\#L\to\infty} \#\Sigma(L)/L^2 = 2$.*

(viii) *If $\gcd\big((b-1)_{p'}, (c-1)_{p'}\big) = 1$, $p > 2$, and $(b-1)_p = p^{fm}$, $(c-1)_p = p^{fn}$ with $f, m, n \in \mathbb{Z}_{\geq 1}$, $\gcd(m,n) = 1$, and $2|mn$, then we also have $\lim_{\#L\to\infty} \#\Sigma(L)/L^2 = 2$.*

Proof. For (i), consider any point $P = (x,y,z,w) \in \Sigma(L)$. Then $x + y = z + w$. Certainly, Σ contains the two planes

$$(x = z,\ y = w) \text{ and } (x = w,\ y = z)$$

which contribute $2(\#L)^2 - \#L$ points to $\Sigma(L)$. So we have to count the points $P \in \Sigma(L)$ for which $z \neq x, y$. For these points, we can use the parametrization

$$x = (A+1)z - Ay = (A+1)u + y,\ z = y + u,\ w = Az - (A-1)y = Au + y, \tag{3.3.1}$$

for P in terms of A, u, y, where $u := z - y \neq 0$ and $A := (x-z)/(z-y) \neq 0$. The condition $\Sigma_b(P) = 0$ now reads

$$\big((A+1)u + y\big)^b + y^b - (y+u)^b - (Au+y)^b = 0. \tag{3.3.2}$$

First we look at such points P with $y = 0$. Since $u \neq 0$, (3.3.2) implies $(A+1)^b - A^b - 1 = 0$. The leading term of this polynomial equation in A is bA^{b-1}. Since $p \nmid b$, there are at most $b-1$ such A's, which contributes at most $(b-1)\#L$ points to $\Sigma(L)$. This dies in the large L-limit.

So we may now assume $y \neq 0$, and replace (A, y, u) by (A, y, v), where $v := u/y \neq 0$. Since $y \neq 0$, now (3.3.2) becomes

$$((A+1)v+1)^b - (Av+1)^b - (v+1)^b + 1 = 0. \tag{3.3.3}$$

Note that the coefficient for v^j in the left-hand-side of (3.3.3) is $\binom{b}{j}\big((A+1)^j - A^j - 1\big)$ when $2 \leq j \leq b$, and 0 if $j = 0, 1$. So the condition $P \in \Sigma(L)$ now reads

$$F_b(A, v) = F_c(A, v) = 0. \tag{3.3.4}$$

Furthermore, if $A \in \mathcal{M}_p(b)$, then (3.3.3) is vacuously true. Hence, if $A \in \mathcal{M}_p(b) \cap \mathcal{M}_p(c)$, then (3.3.4) is vacuously true, and each A contributes $(\#L-1)^2$ points to $\Sigma(L)$ with $y, v \neq 0$, which do not belong to the two planes $(x = z,\ y = w)$ and $(x = w,\ y = z)$. This yields the lower bound in (i).

Now we look at $A \notin \mathcal{M}_p(b) \cap \mathcal{M}_p(c)$, and assume that $R(A) \not\equiv 0$ as a function of A. Applying Lemma 3.1 to the specialization homomorphism $A \mapsto \gamma$ at any point γ where $R(\gamma) \neq 0$, we see that (3.3.4) has no solution v when $A = \gamma$. Thus (3.3.4) can have solutions in v only at $A = \gamma$ with $R(\gamma) = 0$. This implies that the number of A for which (3.3.4) has a common solution in v is bounded independently of L (in fact by $2bc$, an upper bound for the degree of $R(A)$). If $A \notin \mathcal{M}_p(b)$ for instance, then $F_b(A, v)$ is a nonzero polynomial in v, and hence has at most b zeros once A is fixed. Thus each such A contributes at most $\max(b, c)(\#L-1)$ points to $\Sigma(L)$ (with y running), and again this dies in the large L-limit. This proves the equality in (ii).

Suppose $b = 2 < p$. Then $F_2(A, v) = 2$, and hence (3.3.4) has no solutions. Furthermore, $\mathcal{M}_p(2) = \varnothing$, proving (iii).

Suppose $b = 3 < p$. Then $F_3(A, v) = 3((A+1)v+2)$. Hence (3.3.4) is equivalent to $(A+1)v = -2$ and $(-1)^c - (-v-1)^c - (v+1)^c + 1 = 0$. If $2|c$, this shows that $(v+1)^c = 1$. Thus there are at most c pairs (A, v) that satisfy (3.3.4), contributing at most $c(\#L-1)$ points to $\Sigma(L)$, and this dies in the large L-limit. Suppose $2 \nmid c$. This argument then shows that there are exactly $\#L-2$ pairs (A, v) that satisfy (3.3.4) and $A, v \neq 0$, namely one for each $v \neq 0, -2$. This gives $(\#L-1)(\#L-2)$ more points to $\Sigma(L)$, proving (iv).

Next, suppose that $b = q+1$ with $q := p^f \geq p$. Then (3.3.3) becomes

$$(A^q + A)v^{q+1} = 0, \tag{3.3.5}$$

which shows that

$$A \in \mathcal{M}_p(q+1) \text{ if and only if } A^{q-1} = -1, \tag{3.3.6}$$

i.e. $A \in \mu_{total}(\{q\})$. Now, if $A \notin \mathcal{M}_p(b)$, then (3.3.5) has no solution since $v \neq 0$, and hence (3.3.3), respectively (3.3.4), has no solution. If $A \in \mathcal{M}_p(b) \smallsetminus \mathcal{M}_p(c)$, then we have at most $b-2 = q-1$ possibilities for A, for each of which $F_c(A, v) = 0$ yields at most c possibilities for v. This contributes at most $(b-2)c(\#L-1)$ points to $\Sigma(L)$, and this dies in the large L-limit. Hence we have to count only the A's in $\mathcal{M}_p(b) \cap \mathcal{M}_p(c)$, and hence (v) holds.

For (vi), note that the coefficient for v^{j-2} in $F_b(A, v)$ is

$$\frac{1}{A}\binom{b}{j}\big((A+1)^j - A^j - 1\big) \equiv j\binom{b}{j} = b\binom{b-1}{j-1} \pmod{A}$$

when $2 \leq j \leq b$. Hence,

$$F_b(0, v) = b\sum_{j=2}^{b}\binom{b-1}{j-1}v^{j-2} = b\frac{(v+1)^{b-1}-1}{v}.$$

Thus the only roots of $F_b(0,v)$ are the elements of $\mu_{(b-1)_{p'}} \smallsetminus \{1\}$ (subtracted by 1). Similarly, the set of roots of $F_c(0,v)$ is $\mu_{(c-1)_{p'}} \smallsetminus \{1\}$ (translated by -1). So the assumption $\gcd\big((b-1)_{p'}, (c-1)_{p'}\big) = 1$ implies that $F_b(0,v)$ and $F_c(0,v)$ have no common root. Furthermore, the specialization $A \mapsto 0$ preserves the degree $b-2$ of $F_b(A,v)$ (as $p \nmid b$). It follows from Lemma 3.1 that $R(0) \neq 0$, and so $R(A) \not\equiv 0$.

Note that (vi) implies (iii) and (v), since $(b-1)_{p'} = 1$ when $b = p^f + 1$ with $f \geq 0$.

Assume now that $\gcd(b-1, c-1) = 1$. Then we may assume that $p \nmid b(b-1)$. In this case,

$$\binom{b}{2}\big((A+1)^2 - A^2 - 1\big) = b(b-1)A,$$

and hence $\mathcal{M}_p(b) = \varnothing$, implying $\lim_{\#L\to\infty} \#\Sigma(L)/L^2 = 2$ by (vi).

For (viii), note that $(b-1)_p = p^{fm}$ implies that $p \nmid \binom{b}{j}$ for $j = p^{fm}+1$. Now

$$\binom{b}{j}\big((A+1)^j - A^j - 1\big) = \binom{b}{j}\big(A^{q^m} + A\big),$$

where $q := p^f$. Thus $\mathcal{M}_p(b)$ is contained in $\{A \mid A^{q^m-1} = -1\}$. Similarly, $\mathcal{M}_p(c)$ is contained in $\{A \mid A^{q^n-1} = -1\}$. By Lemma 3.2, the set $\{A \mid A^{q^m-1} = A^{q^n-1} = -1\}$ is empty, and so we are done by (vi). □

We will need the following well-known observation:

Lemma 3.4. *Let p be a prime and $n = \sum_{i\geq 0} n_i p^i$ and $m = \sum_{i\geq 0} m_i p^i$ be the base p expansions of integers $n, m \geq 1$. Suppose that $m_i \leq n_i$ for all i. Then $p \nmid \binom{n}{m}$.*

Proof. The hypothesis implies that $n - m = \sum_{i\geq 0}(n_i - m_i)p^i$ is the base p expansion of $n-m$. Now for any $j \geq 0$ we have

$$\lfloor \frac{m}{p^j} \rfloor + \lfloor \frac{n-m}{p^j} \rfloor = \sum_{i\geq j} m_i p^{i-j} + \sum_{i\geq j}(n_i - m_i)p^{i-j} = \sum_{i\geq j} n_i p^{i-j} = \lfloor \frac{n}{p^j} \rfloor.$$

Since $\sum_{j\geq 0}\lfloor \frac{n}{p^j} \rfloor$ is the exponent of the highest power of p that divides $n!$, and similarly for $m!$ and $(n-m)!$, the above equalities imply the claim. □

Proposition 3.5. *Fix a prime p, integers $n, r \geq 1$, and consider prime to p integers*

$$a = p^n + 1 > b_1 > b_2 > \ldots > b_r \geq 2.$$

For finite extensions $L/\mathbb{F}_p$, consider the set $\Sigma(L)$ of L-points of the surface

$$\Sigma: \ \Sigma_1 = \Sigma_a = \Sigma_{b_1} = \ldots = \Sigma_{b_r} = 0$$

of $\mathbb{A}^4(x,y,z,w)$. Then exactly one of the following statements holds for

$$M := \limsup_{\#L\to\infty} \#\Sigma(L)/L^2.$$

(a) *$p > 2$ and $M = 2$.*
(b) *$p = 2$ and $M = 3$.*
(c) *$p > 2$ and $M = p^e + 1 \geq 4$, where $b_i = p^{m_i} + 1$ for $1 \leq i \leq r$, and the integers $n/e, m_1/e, \ldots, m_r/e$ are all odd for $e := \gcd(n, m_1, \ldots, m_r)$.*
(d) *$p = 2$ and $M = 2^e + 1 \geq 5$, where $b_i = 2^{m_i} + 1$ for $1 \leq i \leq r$, and $e := \gcd(n, m_1, \ldots, m_r) \geq 2$.*

Proof. We will follow the proof of Proposition 3.3 and count the points $P = (x, y, z, w) \in \Sigma(L)$ that lie outside of the two planes $(x = z, y = w)$ and $(x = w, y = z)$, for which we can use the parametrization (3.3.1). For these points, the condition $P \in \Sigma$ reads

$$F_a(A, v) = F_{b_1}(A, v) = \ldots = F_{b_r}(A, v) = 0,$$

cf. (3.3.4). Since $\Sigma_a(P) = 0$ and $a = p^n + 1$, we have $A^{p^n-1} = 0$, see (3.3.5). Now the proof of Proposition 3.3(v) can be repeated verbatim to show that

$$M = 2 + \#\big(\mathcal{M}_a \cap \bigcap_{i=1}^{r} \mathcal{M}_{b_i}\big),$$

where $\mathcal{M}_a$ and $\mathcal{M}_{b_i}$ are defined in (3.2.1).

We will assume that $M > 2$ if $p > 2$, $M > 3$ if $p = 2$, and aim to show that we are in (c) with $M = p^e + 1 \geq 4$ or in (d) with $M = 2^e + 1 \geq 5$. Note that when $p = 2$, $1 \in \mathcal{M}_b$ for any integer $b \geq 3$. Hence our assumption implies that

(3.5.1) $$\text{For all } i,\ \mathcal{M}_{b_i} \neq \varnothing \text{ if } p > 2, \text{ and } \mathcal{M}_{b_i} \supset \{1\} \text{ if } p = 2.$$

Consider the base p expansion

$$c = \sum_{i \geq 0} c_i p^i$$

of $c := b_1$. We already noted that $\mathcal{M}_c = \varnothing$ if $2 < p \nmid c(c-1)$, contrary to (3.5.1). On the other hand, if $p = 2$ then $2 \nmid c$ and so $p|(c-1)$. Henceforth we may assume that $p|(c-1)$, whence $c_0 = 1$.

Consider any digit $c_i \geq 1$ of c, with $i \geq 1$. By Lemma 3.4, $p \nmid \binom{c}{p^i+1}$. Taking $j := p^i + 1$ in the definition (3.2.1) of $\mathcal{M}_c$, we get

$$0 = (A+1)^{p^i+1} - A^{p^i+1} - 1 = (A^{p^i} + 1)(A+1) - A^{p^i+1} - 1 = A^{p^i} + A$$

for $A \in \mathcal{M}_c$. As $A \neq 0$, we get

(3.5.2) $$A^{p^i-1} = -1,$$

in particular,

(3.5.3) $$A^{p^i} = -A,\ A^{2p^i+1} = A^3.$$

Assume in addition that $c_i \geq 2$ (and so $p > 2$ as $c_i \leq p-1$.) Then by Lemma 3.4 we have $p \nmid \binom{c}{2p^i+1}$. Taking $j := p^i + 1$ in the definition (3.2.1) of $\mathcal{M}_c$, we get

$$\begin{aligned} 0 &= (A+1)^{2p^i+1} - A^{2p^i+1} - 1 \\ &= (A^{p^i} + 1)^2(A+1) - A^{2p^i+1} - 1 \\ &= (-A+1)^2(A+1) - A^3 - 1 \\ &= -A(A+1), \end{aligned}$$

and so $A = -1$. But this is impossible by (3.5.2) (since $p^i \geq 3$ is odd in the case under consideration), and so $\mathcal{M}_c = \varnothing$, again contradicting (3.5.1).

We have shown that any positive digit c_i of c must be equal to 1. Suppose now that $c_i = 1 = c_j$ for some $i > j \geq 1$. Then (3.5.2) holds for both A^{p^i} and A^{p^j}, and so

$$A^{p^i} = A^{p^j} = -A,\ A^{p^i+p^j+1} = A^3.$$

Furthermore, by Lemma 3.4 we have $p \nmid \binom{c}{p^i+p^j+1}$. Taking $j := p^i + p^j + 1$ in the definition (3.2.1) of $\mathcal{M}_c$, we now get

$$\begin{aligned} 0 &= (A+1)^{p^i+p^j1} - A^{p^i+p^j+1} - 1 \\ &= (A^{p^i}+1)(A^{p^j}+1)(A+1) - A^{p^i+p^j+1} - 1 \\ &= (-A+1)^2(A+1) - A^3 - 1 \\ &= -A(A+1), \end{aligned}$$

and so $A = -1$. If $p > 2$, then this is again impossible by (3.5.2), and so $\mathcal{M}_c = \varnothing$, contrary to (3.5.1). If $p = 2$, then $\mathcal{M}_c \subseteq \{1\}$, contradicting (3.5.1).

We have shown that $b_1 = c$ has only two positive digits, c_0 and c_{m_1}, and both are equal to 1. Thus $b_1 = p^{m_1} + 1$. Applying the same argument to any b_i, we see that $b_i = p^{m_i} + 1$. Hence

$$\mathcal{M}_{b_i} = \{A \in \overline{\mathbb{F}_p} \mid A^{p^{m_i}-1} = -1\}.$$

Let $e := \gcd(n, m_1, \dots, m_r)$. If $p > 2$, then it follows from Lemma 3.2 that

$$\#(\mathcal{M}_a \cap \bigcap_{i=1}^{r} \mathcal{M}_{b_i})$$

equals $p^e + 1$ if all n/e and m_i/e are odd, and 0 otherwise, and thus we arrive at (c). Similarly, if $p = 2$ then using Lemma 3.2 we arrive at (d). □

Corollary 3.6. *Fix a prime p, a power $q = p^f$, an integer $r \geq 1$, and consider $q_i := q^{m_i}$ with $1 \leq m_1 < \dots < m_r$ and $\gcd(m_1, \dots, m_r) = 1$. If $p > 2$, assume in addition that $2 \nmid m_1 m_2 \dots m_r$. For finite extensions $L/\mathbb{F}_p$, consider the set $\Sigma(L)$ of L-points of the surface*

$$\Sigma : \ \Sigma_1 = \Sigma_{q_1+1} = \dots = \Sigma_{q_r+1} = 0$$

of $\mathbb{A}^4(x, y, z, w)$. Then

$$\limsup_{\#L\to\infty} \#\Sigma(L)/L^2 = q + 1.$$

Proof. Arguing as in the proof of Proposition 3.5, we have

$$\limsup_{\#L\to\infty} \#\Sigma(L)/L^2 = 2 + \# \cap_{i=1}^{r} \mathcal{M}_p(q_i + 1).$$

According to (3.3.6), $\cap_{i=1}^{r} \mathcal{M}_p(q_i + 1)$ is precisely $\mu_{total}(\mathcal{Q})$ for $\mathcal{Q} := \{q_1, \dots, q_r\}$. The statement now follows from Lemma 3.2. □

In hindsight, Corollary 3.6 is a reflection of [KT6, Theorem 16.7(i-bis), (ii)] and the fact that $\mathrm{SU}_N(q)$ acting on the natural module $\mathbb{F}_{q^2}^N$, respectively $\Omega^-_{2N}(q)$ acting on the natural module $\mathbb{F}_q^{2N}$ when $p = 2$, has at least $q + 1$ orbits. (Also see Theorem 1.5 and Lemma 5.1 of [GT2].)

Theorem 3.7. *Let k be a finite field of characteristic $p > 0$, and $f(x) \in k[x]$, say $f(x) = \sum_i A_i x^i$, of degree $d \geq 1$ which is Artin-Schreier reduced. Let $1 \leq a < b$ be prime to p integers. Suppose that we are in one of the following two situations.*

(a) *We have $1 \leq a < b < \deg(f)$. We consider the local system $\mathcal{F}$ on $\mathbb{A}^2/k$ whose trace function is given as follows: for L/k a finite extension, and $s, t \in L$,*

$$\mathrm{Trace}(\mathrm{Frob}_{(s,t),L}|\mathcal{F}) = \frac{-1}{\sqrt{\#L}} \sum_{x\in L} \psi_L(sx^a + tx^b + f(x)).$$

(b) *We have* $1 \le a < b$, $\deg(f) < b$, $f(x)$ *is not of the form* (nonzero constant)x^a. *We consider the local system* $\mathcal{F}$ *on* $(\mathbb{A}^1 \times \mathbb{G}_m)/k$ *whose trace function is given as follows: for* L/k *a finite extension, and* $s, t \in L \times L^\times$,

$$\mathrm{Trace}(\mathrm{Frob}_{(s,t),L}|\mathcal{F}) = \frac{-1}{\sqrt{\#L}} \sum_{x \in L} \psi_L(f(x) + sx^a + tx^b)).$$

Consider the set $\mathcal{E}$ *of exponents which occur in* f*:*

$$\mathcal{E} := \{i \in \mathbb{Z} \mid A_i \neq 0\},$$

and denote by S *the set*

$$S := \{a, b\} \cup \mathcal{E}.$$

Enumerate (in some order) the set S*:*

$$S = \{A, B, C_1, \ldots, C_r\}.$$

Suppose that

$$\gcd(A, B, C_1, \ldots, C_r) = 1.$$

Then we have the following results.

(i) *Suppose* $B = 2A$. *Then* $M_{2,2}(\mathcal{F}) = 2$.
(ii) *Suppose* $B = 3A$. *Then* $M_{2,2}(\mathcal{F}) = 3$ *if every* $s \in S$ *is odd, and* $M_{2,2}(\mathcal{F}) = 2$ *if some* $s \in S$ *is even.*

Proof. The idea is to make use of the limsup formulas of Theorems 2.3 and 2.6 to compute $M_{2,2}$.

Consider first the case when $B = 2A$. Then the two equations $\Sigma_A = 0, \Sigma_{2A} = 0$, which we view as the equations $\Sigma_1 = \Sigma_2 = 0$ applied to the variables x^A, y^A, z^A, w^A, show that we have an equality of sets

$$\{x^A, y^A\} = \{z^A, w^A\}.$$

If any of x, y, z, w vanishes, this equality of sets has $O(\#L)$ solutions, so we may assume that each of x, y, z, w is nonzero. Then we are in one of $2A^2$ cases, as follows. For each ordered pair ζ, η of A^{th} roots of unity in $\mu_A(\overline{k})$, either

$$[z, w] = [\zeta x, \eta y] \quad \text{or} \quad [w, z] = [\zeta x, \eta y].$$

In this first case of $[z, w] = [\zeta x, \eta y]$, we use the various Σ_{C_i} equations, that $x^{C_i} + y^{C_i} = z^{C_i} + w^{C_i}$, to get

$$x^{C_i} + y^{C_i} = \zeta^{C_i} x^{C_i} + \eta^{C_i} y^{C_i}, \quad \text{i.e., we have } (\zeta^{C_i} - 1)x_i^{C_i} + (\eta^{C_i} - 1)y^{C_i} = 0.$$

This equation has $\#L$ solutions unless both $\zeta^{C_i} = \eta^{C_i} = 1$. But gcd(the $C_i, A, 2A) = 1$, hence gcd((the $C_i, A) = 1$. So in order to have more than $O(\#L)$ solutions, we must have

$$\zeta^{C_i} = \eta^{C_i} = 1 \text{ for each } C_i.$$

As both ζ, η are A^{th} roots of unity, and gcd(the $C_i, A) = 1$, these equalities force $\zeta = 1 = \eta$, Thus in this first case, we have the solution $[z, w] = [x, y]$, with its $(\#L)^2$ points, and $A^2 - 1$ other solutions, each with $\#L$ points.The treatment of the second case, $[w, z] = [\zeta x, \eta y]$, is identical.

Consider now the case when $B = 3A$. Then the two equations $\Sigma_A = 0, \Sigma_{3A} = 0$, which we view as the equations $\Sigma_1 = \Sigma_3 = 0$ applied to the variables x^A, y^A, z^A, w^A, show that either we have an equality of sets

$$\{x^A, y^A\} = \{z^A, w^A\}.$$

or we have the relations

$$x^A + y^A = 0 = z^A + w^A.$$

Exactly as in the $B = 2A$ discussion above, we use the fact that gcd((the $C_i, A) = 1$ to show that from the equality of sets $\{x^A, y^A\} = \{z^A, w^A\}$ we get that, up to $O(\#L)$, the $(\#L)^2$ solutions $\{x, y\} = \{z, w\}$.

It remains to deal with with the equation $x^A + y^A = 0 = z^A + w^A$. Fix an A^{th} root τ of -1. Then this breaks into the A^2 cases $y = \tau\zeta x, z = \tau\eta w$, for each pair ζ, η of A^{th} roots of unity. We then use the Σ_{C_i} equations to obtain the relations

$$x^{C_i}(1 + (\tau\zeta)^{C_i}) = 0, \quad z^{C_i}(1 + (\tau\eta)^{C_i}) = 0.$$

In order to get more than $O(\#L)$ solutions, we must have

$$1 + (\tau\zeta)^{C_i} = 0, \quad 1 + (\tau\eta)^{C_i} = 0 \text{ for each } C_i.$$

Suppose first that A is odd. Then we take $\tau := -1$, and our equations become

$$\zeta^{C_i} = -(-1)^{C_i} = \eta^{C_i} \text{ for each } C_i.$$

If all C_i are odd, these are the equations

$$\zeta^{C_i} = 1 = \eta^{C_i} \text{ for each } C_i.$$

In order to get more than $O(\#L)$ solutions, we must have $\zeta = 1 = \eta$.

Suppose next that A is odd but some C_i is even, say C_1 is even. (This can only happen if we are in odd characteristic, as f is Artin-Schreier reduced, and $p \nmid ab$.)Then we have the equation

$$\zeta^{C_1} = -1 = \eta^{C_1}.$$

But ζ and η are roots of unity of odd order, so no powers of either can be -1. So in this case we have only $x = y = z = w = 0$.

Finally, consider the case when A is even. Then gcd(the $C_i, A) = 1$, so there is some odd C_i, say C_1 is odd. Then the two equations

$$1 + (\tau\zeta)^{C_1} = 0, \quad 1 + (\tau\eta)^{C_1} = 0,$$

rewritten as

$$(\tau\zeta)^{C_1} = -1, (\tau\eta)^{C_1}$$

and raised to the A power give

$$(\tau\zeta)^{AC_1} = (-1)^A = 1, (\tau\eta)^{AC_1} = (-1)^A = 1.$$

But $\zeta^A = \eta^A = 1$, so we get $\tau^{AC_1} = 1 = \eta^{AC_1}$. But $\tau^A = -1$ and C_1 is odd, so we get $-1 = 1$, which is nonsense. Thus in this case as well the only solution is $x = y = z = w = 0$. ☐

Theorem 3.8. *Let k be a finite field of characteristic $p > 0$, and $f(x) \in k[x]$, say $f(x) = \sum_i A_i x^i$, of degree $d \geq 3$ which is Artin-Schreier reduced (meaning that $A_i = 0$ if $p|i$). Let $1 \leq a < b < \deg(f)$ be prime to p integers, and consider the local system $\mathcal{F}$ on $\mathbb{A}^2/k$ whose trace function is given as follows: for L/k a finite extension, and $s, t \in L$,*

$$\text{Trace}(\text{Frob}_{(s,t),L}|\mathcal{F}) = \frac{-1}{\sqrt{\#L}} \sum_{x \in L} \psi_L(sx^a + tx^b + f(x)).$$

Consider the set $\mathcal{E}$ of exponents which occur in f:

$$\mathcal{E} := \{i \in \mathbb{Z}, \ A_i \neq 0\}.$$

Suppose that the set $\{a, b\} \cup \mathcal{E}$ contains 1, c, and d, where $1 < c < d$ and either of the following conditions is satisfied.

(i) $\gcd(c - 1, d - 1) = 1$.

(ii) $p > 2$, $\gcd\big((c-1)_{p'}, (d-1)_{p'}\big) = 1$, *and* $(c-1)_p = p^{fm}$, $(d-1)_p = p^{fn}$ *with* $f, m, n \in \mathbb{Z}_{\geq 1}$, $\gcd(m,n) = 1$, *and* $2|mn$.

Then $M_{2,2}(\mathcal{F}) = 2$.

Proof. The local system $\mathcal{F}$ is pure of weight zero, so geometrically semisimple, and of rank

$$\deg(f) - 1 \geq 2,$$

so has $M_{2,2}(\mathcal{F}) \geq 2$. Thus it suffices to show that $M_{2,2}(\mathcal{F}) \leq 2$ under the stated hypotheses. Now apply Theorem 2.3 and Proposition 3.3(vii), (viii). □

4. p-finite and strongly p-finite data

In this and the next section, we consider local systems $\mathcal{F}$ on $\mathbb{A}^r/\mathbb{F}_p$ defined as follows. We are given a list of integers

$$A > B_1 > \ldots > B_r \geq 1, \ \ p \nmid A \prod_i B_i, \ \gcd(A, B_1, \ldots, B_r) = 1. \tag{4.0.1}$$

For $L/\mathbb{F}_p$ a finite extension, and $(t_1, \ldots, t_r) \in L^r$,

$$\mathrm{Trace}(\mathrm{Frob}_{(t_1,\ldots,t_r),L}|\mathcal{F}) = (-1/\sqrt{\#L}) \sum_{x \in L} \psi_L(x^A + \sum_{i=1}^{r} t_i x^{B_i}).$$

Here we make a choice of $\sqrt{p} \in \overline{\mathbb{Q}_\ell}$, and define $\sqrt{\#L} := \sqrt{p}^{\deg(L/\mathbb{F}_p)}$. We will name this $\mathcal{F}$ as

$$\mathcal{F}(A, B_1, \ldots, B_r, \mathbb{1})$$

when confusion about "which $\mathcal{F}$?" is possible. Recall from [KT4, 2.5, 2.6] that such an $\mathcal{F}$ is geometrically irreducible.

When $r = 1$, these local systems were the main subject of study in Chapter 10 of [KT6]. In general, the local systems $\mathcal{F}(A, B_1, \ldots, B_r, \mathbb{1})$ with finite G_{geom} (and their G_{geom}) have been classified in Chapter 11 of [KT6], some of whose results can be stated using the following notion.

Definition 4.1. Data $(A, B_1, \ldots, B_r)$ with $r \geq 1$ subject to (4.0.1) is said to be *p-finite* if one of the following conditions holds.

(i) $p > 2$, $q = p^f$, $A = (q^n+1)/2$, and $B_i = (q^{m_i}+1)/2$ for $1 \leq i \leq r$ and $n > m_1 > \ldots > m_r \geq 0$ are integers such that $2|nm_1 \ldots m_r$ and $\gcd(n, m_1, \ldots, m_r) = 1$.

(ii) $q = p^f$ and $A = q^n + 1$. Furthermore, either $(r, B_1, n) = (1, 1, 1)$, or $r \geq 2$ and $B_i = q^{m_i} + 1$, $1 \leq i \leq r-1$, where $n > m_1 > \ldots > m_{r-1} \geq 0$ are integers with $\gcd(n, m_1, \ldots, m_{r-1}) = 1$, and $B_r = 1$.

(iii) $p = 2$, $q = 2^f$, $A = q^n + 1$, $B_i = q^{m_i} + 1$, $1 \leq i \leq r$, where $n > m_1 > \ldots > m_r \geq 1$ are integers such that $2|nm_1 \ldots m_r$ and $\gcd(n, m_1, \ldots, m_r) = 1$.

(iv) $q = p^f$, $A = (q^n+1)/(q+1)$, $B_i = (q^{m_i}+1)/(q+1)$, $1 \leq i \leq r$, where $n > m_1 > \ldots > m_r \geq 1$ are odd integers with $\gcd(n, m_1, \ldots, m_r) = 1$.

(v) $p = 2$, $(A, B_1, \ldots, B_r) = (13, 3)$ or $(13, 3, 1)$.

(vi) $p = 3$, $1 \leq r \leq 3$, $A = 7$, $\{B_1, \ldots, B_r\} \subseteq \{4, 2, 1\}$.

(vii) $p = 3$, $1 \leq r \leq 3$, $A = 5$, $\{B_1, \ldots, B_r\} \subseteq \{4, 2, 1\}$.

(viii) $p = 5$, $1 \leq r \leq 2$, $A = 3$, $\{B_1, \ldots, B_r\} \subseteq \{2, 1\}$.

(ix) $p = 5$, $r = 1$, $A = 7$, $B_1 = 1$.

(x) $p = 7$, $r = 1$, $A = 5$, $B_1 = 2$.

Definition 4.2. Data $(A, B_1, \ldots, B_r)$ with $k \geq 1$ subject to (4.0.1) is said to be *strongly p-finite*, if it satisfies 4.1(i) with $q \in \{3, 5\}$, 4.1(ii) with $r \geq 2$ and either $q = 2$, or $2 \nmid q$ but $2|nm_1 \ldots m_{r-1}$, 4.1(iii) with $q = 2$, 4.1(iv) with $q = 2$, or one of (v)–(x) of 4.1.

Theorem 4.3. *A local system $\mathcal{F} = \mathcal{F}(A, B_1, \ldots, B_r, \mathbb{1})$ in characteristic p subject to (4.0.1) has finite $G_{\rm geom}$ if and only if $(A, B_1, \ldots, B_r)$ is p-finite. If the data is strongly p-finite, then $M_{2,2}(\mathcal{F})$ equals 2 if $2|AB_1 \ldots B_r$, and 3 otherwise.*

Proof. The first statement summarizes Theorems 10.2.6, 10.3.13 and 11.2.3 of [KT6]. The second statement follows from the explicit determination of $G_{\rm geom}$ and [GT2, Theorem 1.5], if we assume in addition that $A > 9$ in the cases of 4.1(ii), (iii) with $q = 2$. Assume we are in the cases of 4.1(ii), (iii) with $q = 2$ and $A = 2^n + 1 \leq 9$. Now if $B_r = 1$ (so we are in 4.1(ii) with $r \geq 2$), then $M_{2,2} = 3$ by Corollary 3.6. Thus we are left with the cases where $p = 2$, $(A, B_1, \ldots, B_r) = (5, 3)$, $(9, 5)$, $(9, 5, 3)$. The third case has $M_{2,2} = 3$ by Theorem 3.7. The two remaining local systems of rank 8 and 4, with $r = 1$ and $(A, B_1) = (9, 5)$, $(5, 3)$, are dealt with in the next result, which also resolves some open cases left in [KT6, Chapter 8]. □

Theorem 4.4. *Suppose $p = 2$. Then the following statements hold.*

(i) *Each of the following local systems $\mathcal{F}_{531} := \mathcal{F}(5, 3, 1, \mathbb{1})$, $\mathcal{F}_{53} := \mathcal{F}(5, 3, \mathbb{1})$, and $\mathcal{H}_{53} := \mathcal{H}yp(\mathsf{Char}_5^\times, \mathsf{Char}_3^\times)$ has geometric monodromy group $2^{1+4}_- \cdot \mathsf{A}_5$, which is also the arithmetic monodromy group over any finite extensions of $\mathbb{F}_4$. For each of them, the arithmetic monodromy group over $\mathbb{F}_2$ is $2^{1+4}_- \cdot \mathsf{S}_5$.*

(ii) *Each of the local systems $\mathcal{F}_{9531} := \mathcal{F}(9, 5, 3, 1, \mathbb{1})$, $\mathcal{F}_{953} := \mathcal{F}(9, 5, 3, \mathbb{1})$, $\mathcal{F}_{951} := \mathcal{F}(9, 5, 1, \mathbb{1})$, $\mathcal{F}_{95} := \mathcal{F}(9, 5, \mathbb{1})$, and $\mathcal{H}_{95} := \mathcal{H}yp(\mathsf{Char}_9^\times, \mathsf{Char}_5^\times)$ has geometric monodromy group $2^{1+6}_- \cdot \Omega^-_6(2)$, which is also the arithmetic monodromy group over any finite extensions of $\mathbb{F}_4$. For each of them, the arithmetic monodromy group over $\mathbb{F}_2$ is $2^{1+6}_- \cdot \mathrm{O}^-_6(2)$.*

(iii) *The local system $\mathcal{F}_{931} := \mathcal{F}(9, 3, 1, \mathbb{1})$ has geometric monodromy group $2^{1+6}_- \cdot \mathrm{SU}_3(2)$, which is also the arithmetic monodromy group over any finite extensions of $\mathbb{F}_4$. Over $\mathbb{F}_2$, the arithmetic monodromy group is $2^{1+6}_- \cdot \mathrm{SU}_3(2) \cdot 2$.*

Furthermore, all the local systems considered in this theorem have $M_{2,2} = 3$.

Proof. (a) First we note that both $\mathcal{H}_{95}$ and $\mathcal{H}_{53}$ satisfy (**S**+) by [KT3, Theorem 3.13]. Furthermore, each of $\mathcal{F}_{531}$, $\mathcal{F}_{9531}$, $\mathcal{F}_{951}$, $\mathcal{F}_{931}$ has $M_{2,2} = 3$ by Corollary 3.6. We also use the facts that if φ denotes the character of the underlying representation for the arithmetic monodromy group $G_{{\rm arith},\mathbb{F}_2}$ of any of the listed sheaves over $\mathbb{F}_2$, then φ is irreducible of symplectic type; in particular, $\mathbf{Z}(G_{{\rm arith},\mathbb{F}_2}) \leq C_2$. (Indeed, φ is visibly real-valued, and its restriction to $G_{\rm geom}$ of $\mathcal{H}_{95}$, respectively $\mathcal{H}_{53}$, is symplectically self-dual by [Ka2, 8.8.1-2].) Furthermore, the restriction of φ to the arithmetic monodromy group $G_{{\rm arith},\mathbb{F}_4}$ of any of the listed sheaves over $\mathbb{F}_4$ is rational-valued by [KT6, Theorem 7.1.2].

(b) Let $\tilde{\mathcal{F}}$ denote any of the systems $\mathcal{F}_{9531}$, $\mathcal{F}_{951}$, $\mathcal{F}_{953}$, and let $\tilde{G}$ denote its geometric monodromy group. By the above, $\tilde{G}$ is a finite irreducible subgroup of $\mathrm{Sp}_8(\mathbb{C})$ with $M_{2,2} = 3$. Now we can apply [GT2, Theorem 1.5] to $\tilde{G}$, and note that case (B) cannot occur because the dimension $D = 8$, whereas case (D) cannot occur because φ is of symplectic type. It follows that we are in case (C) of [GT2, Theorem 1.5]:

$$2^{1+6}_- \cong E \lhd \tilde{G} \leq \mathbf{N}_{\mathrm{Sp}_8(\mathbb{C})}(E) = E \cdot \mathrm{O}^-_6(2), \qquad (4.4.1)$$

and $\tilde{G}/E \leq \mathrm{O}^-_6(2)$ acts transitively on 27 (nonzero) singular vectors and on 36 nonsingular vectors of the natural module $\mathbb{F}_2^6$ for $\mathrm{O}^-_6(2)$. In particular, 27 divides $|\tilde{G}/E|$. In fact, the observations in (a) imply that (4.4.1) also holds for $G_{{\rm arith},\mathbb{F}_2,\tilde{\mathcal{F}}}$, the arithmetic monodromy group of $\tilde{\mathcal{F}}$ over $\mathbb{F}_2$.

Next, observe that a pullback of $\tilde{\mathcal{F}}$ yields $\mathcal{F}_{95}$, which is a Kummer pullback of $\mathcal{H}_{95}$. In particular, if G denotes the geometric monodromy group of $\mathcal{F}_{95}$ and H denotes that of $\mathcal{H}_{95}$, then $G \lhd H$, $H/G \hookrightarrow C_9$, and $G \hookrightarrow \tilde{G}$. Clearly 5 divides $|H|$, so it also divides $|\tilde{G}|$ and $|\tilde{G}/E|$. Thus $27 \cdot 5$ divides

$|\tilde{G}/E|$. Using the list of maximal subgroups of $\mathrm{O}_6^-(2)$ [Atlas] we deduce that $\tilde{G}/E$ is either $\Omega_6^-(2)$ or $\mathrm{O}_6^-(2)$. In the latter case, [KT6, Proposition 8.2.4] implies, however, that $|\varphi(g)| = \sqrt{2}$ for some $g \in \tilde{G}$, which is impossible by (a). Hence we conclude that $\tilde{G} = E \cdot \Omega_6^-(2)$, and the same holds for $G_{\mathrm{arith},\mathbb{F}_4,\tilde{\mathcal{F}}}$. On the other hand, the Frobenius at $(1, 0, \dots, 0)$ over $\mathbb{F}_2$ (where 1 is the coefficient for x^5) has trace $-2/\sqrt{2}$ and hence does not belong to $G_{\mathrm{arith},\mathbb{F}_4,\tilde{\mathcal{F}}}$. Together with (4.4.1), this implies that $G_{\mathrm{arith},\mathbb{F}_2,\tilde{\mathcal{F}}} = E \cdot \mathrm{O}_6^-(2)$.

(c) To identify H, the G_{geom} for $\mathcal{H}_{95}$, we recall that H satisfies ($\mathbf{S}$+) by (a). First suppose that H is an extraspecial normalizer. Together with (a), this implies that

$$2_-^{1+6} \cong E_1 \lhd H \leq \mathbf{N}_{\mathrm{Sp}_8(\mathbb{C})}(E_1) = E_1 \cdot \mathrm{O}_6^-(2). \tag{4.4.2}$$

We already mentioned that each of C_9 and C_5 injects in H, hence also in $H/E_1 \leq \mathrm{O}_6^-(2)$. Again using the list of maximal subgroups of $\Omega_6^-(2)$ [Atlas] we deduce that H/E_1 is either $\Omega_6^-(2)$ or $\mathrm{O}_6^-(2)$. In the latter case, [KT6, Proposition 8.2.4] implies, however, that $|\varphi(g)| = \sqrt{2}$ for some $g \in H$, which is impossible by (a). Hence we conclude that $H = E_1 \cdot \Omega_6^-(2)$ (in fact, the same holds for $G_{\mathrm{arith},\mathbb{F}_4,\mathcal{H}_{95}}$ because it normalizes $\mathbf{O}_2(H) = E_1$ and hence also satisfies (4.4.2)). In particular, H is perfect. Since $H/G \hookrightarrow C_9$, we also have $G = H$. Knowing now that

$$G \leq G_{\mathrm{arith},\mathbb{F}_4,\mathcal{F}_{95}} \leq G_{\mathrm{arith},\mathbb{F}_4,\mathcal{F}_{951}} = G,$$

we conclude that $G_{\mathrm{arith},\mathbb{F}_4,\mathcal{F}_{95}} = G$. Next, again using the Frobenius at $s = 1$ of $\mathcal{F}_{95}$ with trace $-\sqrt{2}$, we see that this Frobenius is in $G_{\mathrm{arith},\mathbb{F}_2,\mathcal{F}_{951}}$ but not in its subgroup G of index 2. This shows that $G_{\mathrm{arith},\mathbb{F}_2,\mathcal{F}_{95}} = G_{\mathrm{arith},\mathbb{F}_2,\mathcal{F}_{951}} = E \cdot \mathrm{O}_6^-(2)$. As $G_{\mathrm{arith},\mathbb{F}_2,\mathcal{F}_{95}}$ is a subgroup of $G_{\mathrm{arith},\mathbb{F}_2,\mathcal{H}_{95}}$, which normalizes $\mathbf{O}_2(H) = E_1$ and hence satisfies (4.4.2), we deduce that $G_{\mathrm{arith},\mathbb{F}_2,\mathcal{H}_{95}} = 2_-^{1+6} \cdot \mathrm{O}_6^-(2)$.

Assume now that H is almost quasisimple, with R the unique non-abelian composition factor. Then $G^{(\infty)} = H^{(\infty)}$ is a cover of R with center $\mathbf{Z}(H^{(\infty)}) \leq \mathbf{Z}(H) \leq C_2 = \mathbf{Z}(E_1) = \mathbf{Z}(E)$, cf. (4.4.1), (4.4.2). On the other hand, $E \cap G^{(\infty)}$ is a normal 2-subgroup of $G^{(\infty)}$, so

$$E \cap G^{(\infty)} \leq \mathbf{Z}(E) \cap G^{(\infty)} = \mathbf{Z}(G^{(\infty)}).$$

We also know from $G \leq \tilde{G} = E \cdot S$ that

$$G^{(\infty)}/(E \cap G^{(\infty)}) \cong G^{(\infty)}E/E \leq \tilde{G}/E = S \cong \mathrm{SU}_4(2).$$

It follows that R is a simple subquotient of $\mathrm{SU}_4(2)$. Using [Atlas], we readily see that $R = \mathsf{A}_5$, A_6, or $\mathrm{SU}_4(2)$; in particular, $\mathrm{Out}(R)$ is a 2-group. Recalling that

$$R \lhd H/\mathbf{Z}(H) \leq \mathrm{Aut}(R),\ \mathbf{Z}(H) \leq C_2,\ C_9 \hookrightarrow H,$$

we have that $C_9 \hookrightarrow R$. This rules out the possibilities A_5 and A_6, and so $R = \mathrm{SU}_4(2)$. But H acts irreducibly on $\mathcal{H}_{95}$ of dimension 8, so we must have that $H \cong \mathrm{Sp}_4(3) \cdot 2$. This is however impossible, because $H = \mathbf{O}^2(H)$.

(d) In dimension 8, it remains to determine G_1, the G_{geom} for $\mathcal{F}_{931}$, which also has $M_{2,2} = 3$. As in the case of $\tilde{G}$, this equality implies by [GT2, Theorem 1.5] that

$$2_-^{1+6} \cong E_2 \lhd G_1 \leq \mathbf{N}_{\mathrm{Sp}_8(\mathbb{C})}(E_2) = E_2 \cdot \mathrm{O}_6^-(2), \tag{4.4.3}$$

moreover, $G_1/E_2 \leq \mathrm{O}_6^-(2)$ still acts acts transitively on 27 (nonzero) singular vectors and on 36 non-singular vectors of the natural module $W = \mathbb{F}_2^6$ for $\mathrm{O}_6^-(2)$; in particular, 27 divides $|G_1/E_2|$. Using the list of maximal subgroups of $\mathrm{O}_6^-(2)$ [Atlas] we deduce that G_1/E_2 is either $\mathrm{O}_6^-(2)$, $\Omega_6^-(2)$, a subgroup of $M := \mathrm{O}_2^-(2) \wr \mathsf{S}_3$, or a subgroup of $N := \mathrm{GU}_3(2) \cdot 2 \cong 3_+^{1+2} \rtimes 2\mathsf{S}_4$. The first case is impossible since $|G_1| \leq |\tilde{G}| = |E_2| \cdot |\Omega_6^-(2)|$. To rule out the second possibility, we make use of [KT6, Corollary 7.1.5], which shows that

$$\varphi(x) \equiv -1 \pmod 3 \tag{4.4.4}$$

for any odd-order element $x \in G_1$. Indeed, in this case we have $G_1 = \tilde{G}$ since $|G_1| = |\tilde{G}|$ and $G_1 \leq \tilde{G}$; in particular, G_1 contains an element g_1 of order 5 which has rational trace. The latter condition implies that $\varphi(g_1) \in \{-2, 3\}$, violating (4.4.4). In the third possibility, we can realize M as the stabilizer of the decomposition

$$W = \langle e_1, e_2 \rangle_{\mathbb{F}_2} \oplus \langle e_3, e_4 \rangle_{\mathbb{F}_2} \oplus \langle e_5, e_6 \rangle_{\mathbb{F}_2},$$

where the quadratic form Q on W takes value

$$x_1^2 + x_1x_2 + x_2^2 + x_3^2 + x_3x_4 + x_4^2 + x_5^2 + x_5x_6 + x_6^2$$

at the vector $\sum_{i=1}^6 x_ie_i$. But then the vectors $u := e_1 + e_2$ and $v := \sum_{i=1}^6 e_i$ have $Q(u) = Q(v) = 1$ and belong to different M-orbits, showing that M is not transitive on the non-singular vectors of W. This leaves only the fourth possibility: $G_1/E_2 \leq N$. In particular, G_1 is solvable.

Now we use the embedding $G_1 \hookrightarrow \tilde{G} = G_{\mathrm{geom}, \mathcal{F}_{9531}} = E \cdot \Omega_6^-(2)$. Then

$$3 = M_{2,2}(G_1) \geq M_{2,2}(EG_1) \geq M_{2,2}(\mathrm{Sp}_8(\mathbb{C})) = 3,$$

showing that $M_{2,2}(EG_1) = 3$. Thus EG_1/E is a solvable subgroup of $\Omega_6^-(2)$ which acts transitively on 27 singular vectors and on 36 non-singular vectors of $\mathbb{F}_2^6$. Using the list of maximal subgroups of $\Omega_6^-(2)$ as in the preceding paragraph, we see that EG_1/E is contained in $N_1 \cong \mathrm{GU}_3(2)$. Recalling E is a 2-group and $G_1 = \mathbf{O}^{2'}(G_1)$ (as the G_{geom} for a local system on $\mathbb{A}^2/\overline{\mathbb{F}_2}$), we then have

$$EG_1/E \leq \mathbf{O}^{2'}(N_1) \cong \mathrm{SU}_3(2) \cong 3_+^{1+2} \rtimes Q_8.$$

Moreover, 27 and 36 both divide $|G_1/E_2| = |G_1|/|E|$, so in fact we have

$$3_+^{1+2} \rtimes C_4 \leq EG_1/E \leq 3_+^{1+2} \rtimes Q_8. \tag{4.4.5}$$

Suppose that $EG_1/E = 3_+^{1+2} \rtimes C_4$ in (4.4.5). Note that we can turn the quadratic space $W = \mathbb{F}_2^6$ into the Hermitian space $W_1 := \mathbb{F}_4^3$ for $\mathrm{SU}_3(2)$ in such a way that the set $N(W)$ of 36 non-singular vectors of W is exactly the set $N(W_1)$ of 36 non-singular vectors of W_1. Since EG_1/E acts transitively on $N(W) = N(W_1)$, the stabilizer of any $w \in N(W_1)$ has order 3, which implies that a fixed involution j in EG_1/E does not fix any $w \in N(W_1)$. The Sylow 2-subgroups of $\mathrm{SU}_3(2)$ are isomorphic to Q_8, so any involution in $\mathrm{SU}_3(2)$ is conjugate to j and hence does not fix any $w \in N(W_1)$. But this is a contradiction, since the stabilizer of any $w \in N(W_1)$ in $\mathrm{SU}_3(2)$ is $\mathrm{SU}_2(2) \cong \mathsf{S}_3$, which clearly contains an involution. We have therefore shown that

$$EG_1/E \cong \mathrm{SU}_3(2). \tag{4.4.6}$$

Recall that a pullback of $\mathcal{F}_{931}$ contains the Pink-Sawin system $\mathcal{F}(9, 1, \mathbb{1})$ which has 2_-^{1+6} as its G_{geom} by [KT6, Theorem 7.3.8]. This implies that G_1 contains $\mathbf{Z}(E) \cong C_2$. As $[E, E] = \mathbf{Z}(E)$, in the conjugation action on $E/\mathbf{Z}(E) \cong \mathbb{F}_2^6$ the subgroup E acts trivially, whereas $\mathrm{SU}_3(2)$ acts irreducibly (indeed, no proper parabolic subgroup of $\mathrm{GL}_6(2)$ can contain $3_+^{1+2} = \mathbf{O}_3(\mathrm{SU}_3(2))$ as a subgroup). So (4.4.6) shows that G_1 acts irreducibly on $E/\mathbf{Z}(E)$. It follows that $E \cap G_1 = \mathbf{Z}(E)$ or E. In the former case, (4.4.6) implies that $|G_1| = 2|\mathrm{SU}_3(2)| = 2^4 \cdot 3^3$, which is impossible since G_1 contains E_2 of order 2^7. We conclude that $G_1 \lhd E$, and

$$G_1 \cong E \cdot \mathrm{SU}_3(2)$$

by (4.4.6).

To identify $G_{\mathrm{arith},\mathbb{F}_2,\mathcal{F}_{931}}$, we note that $G_{\mathrm{arith},\mathbb{F}_2,\mathcal{F}_{931}} = \langle G_1, g_1\rangle$, where $g_1 = \mathrm{Frob}_{(0,1),\mathbb{F}_2}$. The pullback $s = 0$ of $\mathcal{F}_{931}$ is the Pink-Sawin system $\mathcal{F}(9,1,\mathbb{1})$, so by [KT6, Theorem 7.3.8], g_1^2 is contained in its G_{geom}, which is contained in G_1. Moreover, g_1 has trace $-\sqrt{2}$, showing $g_1 \notin G_1$. Thus G_1 has 2 in $G_{\mathrm{arith},\mathbb{F}_2,\mathcal{F}_{931}}$, whence we also have $G_{\mathrm{arith},\mathbb{F}_4,\mathcal{F}_{931}} = G_1$.

(e) Now we work in dimension 4. Let $\tilde{G}$ denote the geometric monodromy group of $\mathcal{F}_{531}$. Since it has $M_{2,2} = 3$ and is of symplectic type, the restriction of $\mathrm{Sym}^2(\varphi)$ to $\tilde{G}$ is irreducible, whence $\tilde{G}$ satisfies (**S**+) by [GT3, Lemma 2.1].

First we consider the case where $\tilde{G}$ is almost quasisimple. Then $\tilde{G}^{(\infty)}$ is a quasisimple irreducible subgroup of $\mathrm{Sp}_4(\mathbb{C})$. Using [HM] we then deduce that $\tilde{G}^{(\infty)}$ is $2\cdot\mathsf{A}_5$ or $2\cdot\mathsf{A}_6$. Potentially $\tilde{G}$ could still have index 2 over $\tilde{G}^{(\infty)}$. But using the rationality of the restriction of φ to $\tilde{G}$, we get $\tilde{G} = \tilde{G}^{(\infty)} \leq 2\cdot\mathsf{A}_6$. On the other hand, a pullback of $\mathcal{F}_{531}$ is the Pink-Sawin system $\mathcal{F}(5,1,\mathbb{1})$ which has 2_-^{1+4} as its G_{geom} by [KT6, Theorem 7.3.8]. This yields a contradiction, since 2_-^{1+4} cannot embed in $2\cdot\mathsf{A}_6$.

We have therefore shown that $\tilde{G}$ is an extraspecial normalizer, and so

$$2_-^{1+4} \cong E \lhd \tilde{G} \leq \mathbf{N}_{\mathrm{Sp}_4(\mathbb{C})}(E) = E\cdot\mathrm{O}_4^-(2); \tag{4.4.7}$$

note that $\mathrm{O}_4^-(2) \cong \mathsf{S}_5$. Now let H denote the G_{geom} for $\mathcal{H}_{53}$ and let G denote the G_{geom} for $\mathcal{F}_{53}$, so that $H/G \hookrightarrow C_5$. Recall from (a) that H satisfies (**S**+). Assume in addition that H is almost quasisimple. Then $G^{(\infty)} = H^{(\infty)}$ is a cover of a non-abelian simple group R. But $G \hookrightarrow \tilde{G}$, so (4.4.7) implies that R is a simple subquotient of S_5. It follows that $R = \mathsf{A}_5$. We also know that $H \leq \mathrm{Sp}_4(\mathbb{C})$ is almost quasisimple with rational traces. Hence $H = \mathrm{SL}_2(5)$ in a faithful irreducible representation of degree 4; in particular, any element of order 3 in H has trace 1 [Atlas]. Thus any element t of order 3 in $I(\infty)$ has trace 1 in φ, and trace -1 on the tame part of $\mathcal{H}_{53}$. So t has trace 2 on the wild part Wild of $\mathcal{H}_{53}$, which means that t acts trivially on Wild, a contradiction.

We have now shown that H is also an extraspecial normalizer, and so (4.4.7) also holds for H. Note that both C_5 and C_3 inject in H, so 15 divides the order of $H/E \leq \mathsf{S}_5$. Inspecting the list of maximal subgroups of Sym_5 [Atlas], we see that $H/E = \mathsf{S}_5$ or A_5. But $H = \mathbf{O}^2(H)$, so $H = E\cdot\mathsf{A}_5$; in particular, H is perfect. Since $H/G \hookrightarrow C_5$, we also have that $G = H$. Now $G_{\mathrm{arith},\mathbb{F}_4,\mathcal{F}_{53}}$ normalizes G and $\mathbf{O}_2(G) = E$, so (4.4.7) holds for $G_{\mathrm{arith},\mathbb{F}_4,\mathcal{F}_{53}}$, which already contains the subgroup $G = E\cdot\mathsf{A}_5$ of index 2 in $E\cdot\mathsf{S}_5$. By [KT6, Proposition 8.2.4], $E\cdot\mathsf{S}_5$ contains an element x with $|\varphi(x)| = \sqrt{2}$. Since φ is rational on $G_{\mathrm{arith},\mathbb{F}_4,\mathcal{F}_{53}}$, we conclude that $G_{\mathrm{arith},\mathbb{F}_4,\mathcal{F}_{53}} = G$. Noting that (4.4.7) holds for $G_{\mathrm{arith},\mathbb{F}_4,\mathcal{H}_{53}}$ which has only rational traces and contains $G_{\mathrm{arith},\mathbb{F}_4,\mathcal{F}_{53}}$, we deduce that $G_{\mathrm{arith},\mathbb{F}_4,\mathcal{H}_{53}} = G$.

Next, $G_{\mathrm{arith},\mathbb{F}_2,\mathcal{F}_{53}}$ normalizes G and $\mathbf{O}_2(G) = E$, so (4.4.7) holds for $G_{\mathrm{arith},\mathbb{F}_2,\mathcal{F}_{53}}$. But now $G_{\mathrm{arith},\mathbb{F}_2,\mathcal{F}_{53}}$ contains the Frobenius at $s = 1$ with trace $-\sqrt{2}$ that does not belong to G. Using (4.4.7), we conclude that $G_{\mathrm{arith},\mathbb{F}_2,\mathcal{F}_{53}} = E\cdot\mathsf{S}_5$. As $G_{\mathrm{arith},\mathbb{F}_2,\mathcal{F}_{53}}$ embeds in $G_{\mathrm{arith},\mathbb{F}_2,\mathcal{H}_{53}}$ which also satisfies (4.4.7) (as it normalizes $\mathbf{O}_2(H) = E$), we must have that $G_{\mathrm{arith},\mathbb{F}_2,\mathcal{H}_{53}} = E\cdot\mathsf{S}_5$.

Now, $E\cdot\mathsf{A}_5 = G = G_{\mathrm{geom},\mathcal{F}_{53}} \leq G_{\mathrm{geom},\mathcal{F}_{531}} = \tilde{G} \leq E\cdot\mathsf{S}_5$ and $\varphi|_{\tilde{G}}$ is rational-valued, so $\tilde{G} = G$. Repeating the same inclusions for $G_{\mathrm{arith},\mathbb{F}_4}$, we get $G_{\mathrm{arith},\mathbb{F}_4,\mathcal{F}_{531}} = G$. Finally, as $G_{\mathrm{arith},\mathbb{F}_2,\mathcal{F}_{531}}$ normalizes $\mathbf{O}_2(\tilde{G}) = E$, we have

$$E\cdot\mathsf{S}_5 = G_{\mathrm{arith},\mathbb{F}_2,\mathcal{F}_{53}} \leq G_{\mathrm{arith},\mathbb{F}_2,\mathcal{F}_{531}} \leq E\cdot\mathsf{S}_5,$$

whence $G_{\mathrm{arith},\mathbb{F}_2,\mathcal{F}_{531}} = E\cdot\mathsf{S}_5$.

(f) As mentioned in the proof of Theorem 4.3, we already know $M_{2,2} = 3$ unless $\mathcal{F} = \mathcal{F}_{53}$ or $\mathcal{F}_{95}$. But $G_{\mathrm{geom},\mathcal{F}_{53}} = G_{\mathrm{geom},\mathcal{F}_{531}}$ according to (i) and $G_{\mathrm{geom},\mathcal{F}_{95}} = G_{\mathrm{geom},\mathcal{F}_{9531}}$, so $\mathcal{F}_{53}$ and $\mathcal{F}_{95}$ both have $M_{2,2} = 3$ as well. ∎

5. Multiparameter local systems: Balanced pairs and $\mathbf{Infmono}(A, B)$

We will now develop some framework to study the case in which $r \geq 2$ and $\mathcal{F}(A, B_1, \dots, B_r, \mathbb{1})$ has infinite $G_{\rm geom}$. First we attach to the data $(A, B_1, \dots, B_r)$ a *balanced pair* $(A, B = \text{some } B_i)$ as follows. We must distinguish three cases.

(i) If A and all B_i are odd, we choose any of the B_i.
(ii) If A is even, then some B_i is odd, and we choose any odd B_i.
(iii) If A is odd and some B_i is even, then we choose some even B_i.

Notice that, in all cases, at least one of A, B is odd, and hence C is odd. We now formulate the following hypothesis $\mathbf{infmono}(A, B)$ for a pair (A, B) of integers $A > B \geq 1$ with $p \nmid AB$. For $C := \gcd(A, B)$, $A = CA_0$, $B = CB_0$, we have the direct sum decomposition

$$\mathcal{F}(A, B, \mathbb{1}) = \bigoplus_{\chi \in \mathsf{Char}(C)} \mathcal{F}(A_0, B_0, \chi),$$

where, in general, $\mathcal{F}(A, B, \chi)$ is the local system on $\mathbb{A}^1/\mathbb{F}_p(\chi)$ whose trace function is given as follows: for $L/\mathbb{F}_p(\chi)$ a finite extension and $t \in L$,

$$\text{Trace}(\text{Frob}_{t,L}|\mathcal{F}(A, B, \chi)) = (-1/\sqrt{\#L}) \sum_{x \in L} \psi_L(x^A + tx^B)\chi_L(x).$$

The hypothesis $\mathbf{infmono}(A, B)$ is the following:

$$\text{(5.0.1)} \qquad \mathbf{infmono}(A, B): \quad \begin{array}{l} \text{for each } \chi \in \mathsf{Char}(C), G_{\text{geom}, \mathcal{F}(A_0, B_0, \chi)} \text{ is infinite,} \\ \text{with the exception of } G_{\text{geom}, \mathcal{F}(A_0, B_0, \mathbb{1})} \text{ when } (A_0, B_0) = (2, 1). \end{array}$$

Lemma 5.1. *For $C := \gcd(A, B), A = CA_0,\ B = CB_0$, suppose C is odd and $C \geq 3$. Then the following statements hold.*

(i) *If $\mathcal{F}(A_0, B_0, \mathbb{1})$ has infinite $G_{\rm geom}$, then* $\mathbf{infmono}(A, B)$ *holds.*
(ii) *Suppose $\mathcal{F}(A_0, B_0, \mathbb{1})$ has finite $G_{\rm geom}$ but some summand $\mathcal{F}(A_0, B_0, \chi)$ of $\mathcal{F}(A, B, \mathbb{1})$ has infinite $G_{\rm geom}$. Then there is a divisor C_0 of C with $C_0 < C$ such that any summand $\mathcal{F}(A_0, B_0, \varphi)$ of $\mathcal{F}(A, B, \mathbb{1})$ has infinite $G_{\rm geom}$ precisely when $\varphi^C = \mathbb{1} \neq \varphi^{C_0}$, i.e. $\varphi \in \mathsf{Char}(C) \smallsetminus \mathsf{Char}(C_0)$.*

Proof. (i) is immediate from [KT6, Corollary 11.2.8(ii)].

For (ii), let S denote the set of $\chi \in \mathsf{Char}(C)$ for which $\mathcal{F}(A_0, B_0, \chi)$ has infinite $G_{\rm geom}$; in particular, $\chi \in S$ but $\mathbb{1} \notin S$. For any $\chi \in \mathsf{Char}(C) \smallsetminus S$, $\mathcal{F}(A_0, B_0, \chi)$ has finite $G_{\rm geom}$, so by [KT6, Corollary 11.2.8(i)] we have $(A_0, B_0) = ((q^n+1)/(q+1), (q^m+1)/(q+1)$ and $\mathsf{o}(\chi) | \gcd(q+1, C)$ for some power q of p and some odd integers $n > m$; furthermore, $\mathcal{F}(A_0, B_0, \chi')$ has finite $G_{\rm geom}$ for all $\chi' \in \mathsf{Char}(q+1)$. In particular, $\mathsf{Char}(C_0) \subseteq \mathsf{Char}(C) \smallsetminus S$ for $C_0 := \gcd(q+1, C)$. It follows that $S = \mathsf{Char}(C) \smallsetminus \mathsf{Char}(C_0)$. Since $\chi \in S$, $C_0 < C$. ☐

The following statement is a consequence of Lemma 5.1(ii), but we will offer an independent proof.

Lemma 5.2. *Suppose that χ and ρ are nontrivial characters of odd order C which are Galois conjugate under* $\text{Gal}(\mathbb{Q}(\zeta_C)/\mathbb{Q})$. *Then $\mathcal{F}(A_0, B_0, \chi)$ has finite $G_{\rm geom}$ if and only if $\mathcal{F}(A_0, B_0, \rho)$ has finite $G_{\rm geom}$.*

Proof. The question is geometric, so we may work over extensions of $\mathbb{F}_{p^2}(\chi, \rho)$. Over a finite extension $k/\mathbb{F}_{p^2}(\chi, \rho)$, all traces of $\mathcal{F}(A_0, B_0, \chi)$ and of $\mathcal{F}(A_0, B_0, \rho)$ lie in $\mathbb{Q}(\zeta_p, \zeta_C)$, and point by point their traces are conjugate under $\text{Gal}(\mathbb{Q}(\zeta_C, \zeta_p)/\mathbb{Q}(\zeta_p))$. In both cases, finiteness of $G_{\rm geom}$ is equivalent to all traces being algebraic integers, a condition which is invariant under Galois conjugation. ☐

Because $\mathcal{F}$ is geometrically irreducible and starts life over $\mathbb{F}_p$, if $G_{\mathrm{geom},\mathcal{F}}$ is infinite, then its identity component G° is semisimple, by Grothendieck's local monodromy theorem [De2, 1.3.9]. Next we determine $G_{\mathrm{geom},\mathcal{F}}$ in some "easy" cases.

Theorem 5.3. *Consider the local system $\mathcal{F} := \mathcal{F}(A, B_1, \ldots, B_r, \mathbb{1})$ subject to* (4.0.1). *Suppose that $\mathcal{F}(A, B, \mathbb{1})$ has infinite geometric monodromy group H for some balanced pair $(A, B = B_i)$ with* $\gcd(A, B) = 1$. *Then we have the following results.*

(i) *If $2 \nmid AB_i$ then $G_{\mathrm{geom},\mathcal{F}} = \mathrm{Sp}_{A-1}$.*
(ii) *Otherwise,* $\mathrm{SL}_{A-1} \leq G_{\mathrm{geom},\mathcal{F}} \leq \{g \in \mathrm{GL}_{A-1} \,|\, \det(g)^p = 1\}$.

Proof. Suppose first that $2 \nmid AB_i$. Then by [KT6, Theorems 10.2.4(iii) and 10.3.21(iii)], $H = \mathrm{Sp}_{A-1}$. As $\mathcal{F}(A, B, \mathbb{1})$ is a pullback of $\mathcal{F}$, we have $H \leq G_{\mathrm{geom},\mathcal{F}}$. But we have an a priori inclusion $G_{\mathrm{geom},\mathcal{F}} \leq \mathrm{Sp}_{A-1}$. Hence $G_{\mathrm{geom},\mathcal{F}} = \mathrm{Sp}_{A-1}$ in this case.

Suppose next that $2|AB_i$. Then by [KT6, Theorems 10.2.4(i) and 10.3.21(i)], we have

$$\mathrm{SL}_{A-1} \leq H \leq \{g \in \mathrm{GL}_{A-1} \,|\, \det(g)^p = 1\}, \text{ in fact, } H = \mathrm{SL}_{A-1} \text{ if } B \neq A-1. \tag{5.3.1}$$

As $\mathcal{F}(A, B, \mathbb{1})$ is a pullback of $\mathcal{F}$, we again have $H \leq G_{\mathrm{geom},\mathcal{F}}$, and so $\mathrm{SL}_{A-1} \lhd G_{\mathrm{geom},\mathcal{F}} \leq \mathrm{GL}_{A_1}$ is irreducible. By [KT6, 2.3.1], we have $G_{\mathrm{geom},\mathcal{F}} \leq \{g \in \mathrm{GL}_{A-1} \,|\, \det(g)^p = 1\}$. [To apply the cited result, use the fact that the question is geometric, and after pullback to $\mathbb{A}^r/\mathbb{F}_{p^2}$, all Frobenius traces of $\mathcal{F}$ lie in $\mathbb{Q}(\zeta_p)$.] ☐

Theorem 5.4. *Consider the local system $\mathcal{F} := \mathcal{F}(A, B_1, \ldots, B_r, \mathbb{1})$ with $r \geq 2$ subject to* (4.0.1). *Suppose $G_{\mathrm{geom},\mathcal{F}}$ is infinite. Then we have the following results.*

(i) *Suppose that $A = 2B_i$ for some i. Then $G^\circ_{\mathrm{geom},\mathcal{F}} = \mathrm{SL}_{A-1}$.*
(ii) *Suppose that $A = 3B_i$ for some i. Then $G_{\mathrm{geom},\mathcal{F}} = \mathrm{Sp}_{A-1}$ if $2 \nmid AB_1 \ldots B_r$, and $G^\circ_{\mathrm{geom},\mathcal{F}} = \mathrm{SL}_{A-1}$ if and $2|AB_1 \ldots B_r$.*

Proof. Both assertions result from Theorem 3.7. In (i), by Theorem 3.7, we have $M_{2,2}(\mathcal{F}) = 2$. This in turn implies by [GT2, Theorem 1.5] that $G^\circ_{\mathrm{geom},\mathcal{F}} = \mathrm{SL}_{A-1}$.

In (ii), by Theorem 3.7, we have $M_{2,2}(\mathcal{F}) = 3$ if $2 \nmid AB_1 \ldots B_r$, and $M_{2,2}(\mathcal{F}) = 2$ if $2|AB_1 \ldots B_r$. In the former case we also have an a priori inclusion $G_{\mathrm{geom},\mathcal{F}} \leq \mathrm{Sp}_{A-1}$. This in turn implies by [GT2, Theorem 1.5] that $G_{\mathrm{geom},\mathcal{F}} = \mathrm{Sp}_{A-1}$. In the latter case, we have $G^\circ_{\mathrm{geom},\mathcal{F}} = \mathrm{SL}_{A-1}$ as in (i). ☐

To work with pairs (A, B) with $C = \gcd(A, B) > 1$, we first observe:

Lemma 5.5. *Let $A_0 > B_0$ be prime to p integers with* $\gcd(A_0, B_0) = 1$, *and $\chi \neq \varphi$ two multiplicative characters. We have the following results.*

(i) *In all cases, $\mathcal{F}(A_0, B_0, \chi)$ is not geometrically isomorphic to $\mathcal{F}(A_0, B_0, \varphi)$.*
(ii) *If A_0B_0 is even, then $\mathcal{F}(A_0, B_0, \chi)$ is not geometrically isomorphic to $\mathcal{F}(A_0, B_0, \varphi)^\vee$.*
(ii-bis) *If A_0B_0 is even, then $\mathcal{F}(A_0, B_0, \chi)$ is not geometrically isomorphic to $\mathcal{F}(A_0, B_0, \chi)^\vee$.*
(iii) *If A_0B_0 is odd, the dual of $\mathcal{F}(A_0, B_0, \chi)$ is $\mathcal{F}(A_0, B_0, \overline{\chi})$.*
(iv) *If A_0B_0 is odd, $\mathcal{F}(A_0, B_0, \chi)$ is not geometrically isomorphic to $\mathcal{F}(A_0, B_0, \varphi)$. It is isomorphic to the dual of $\mathcal{F}(A_0, B_0, \varphi)$ only for $\varphi = \overline{\chi}$.*

Proof. We first prove that $\mathcal{F}(A_0, B_0, \chi)$ is not geometrically isomorphic to $\mathcal{F}(A_0, B_0, \varphi)$, i.e., that $H^2_c(\mathbb{G}_m/\overline{\mathbb{F}_p}, \mathcal{F}(A_0, B_0, \chi) \otimes \mathcal{F}(A_0, B_0, \varphi)^\vee) = 0$. The dimension of this H^2_c ia the limsup, over finite extensions L of $\mathbb{F}_p(\chi,\varphi)$, of the sums

$$\begin{aligned}&\frac{1}{(\#L)^2}\sum_{t\in L}\sum_{x,y\in L^\times}\psi_L(x^{A_0}-y^{A_0}+t(x^{B_0}-y^{B_0}))\chi(x)\varphi(1/y)\\ =&\frac{1}{\#L}\sum_{\zeta\in\mu_{B_0}}\sum_{x\in L^\times}\psi_L(x^{A_0}(1-\zeta^{A_0}))\chi(x)\varphi(1/(\zeta x)).\end{aligned}$$

The inner sum for $\zeta\neq 1$ has $\zeta^{A_0}\neq 1$ (because $\gcd(A_0,B_0)=1$), so this inner sum is bounded in absolute value by $A_0\sqrt{\#L}$ (Weil bound). For $\zeta=1$, the inner sum is $\sum_{x\in L^\times}\chi(x)\varphi(1/x)$, which vanishes unless $\chi\overline{\varphi}=\mathbb{1}$, in which case the inner sum is $\#L-1$,

We next prove that if A_0B_0 is even, then $\mathcal{F}(A_0,B_0,\chi)$ is not geometrically isomorphic to the dual $\mathcal{F}(A_0,B_0,\varphi)^\vee$. This amounts to the vanishing of $H^2_c(\mathbb{G}_m/\overline{\mathbb{F}_p},\mathcal{F}(A_0,B_0,\chi)\otimes\mathcal{F}(A_0,B_0,\varphi))$. The dimension of this H^2_c ia the limsup, over finite extensions L of $\mathbb{F}_p(\chi,\varphi)$, of the sums

$$(1/\#L)^2\sum_{t\in L}\sum_{x,y\in L^\times}\psi_L(x^{A_0}+y^{A_0}+t(x^{B_0}+y^{B_0}))\chi(x)\varphi(y).$$

Choose a root of unity τ with $\tau^{B_0}=-1$. Then this sum is

$$(1/\#L)\sum_{\zeta\in\mu_{B_0}}\sum_{x\in L^\times}\psi_L(x^{A_0}(1+(\tau\zeta)^{A_0})\chi(x)\varphi(\tau\zeta x).$$

For every $\zeta\in\mu_{B_0}$, we claim that $(\tau\zeta)^{A_0}\neq -1$. Indeed, if $(\tau\zeta)^{A_0}=-1$, then $(\tau\zeta)^{A_0B_0}=(-1)^{B_0}$, but$(\tau\zeta)^{A_0B_0}=(-1)^{A_0}(\zeta)^{A_0B_0}=(-1)^{A_0}$, and hence $(-1)^{A_0}=(-1)^{B_0}$, impossible as A_0 and B_0 have opposite parities in the A_0B_0 even case. Therefore each inner sum is bounded in absolute value by $A_0\sqrt{\#L}$ (Weil bound), and we are done in this A_0B_0 even case.

The proof of (ii-bis) is identical: the particular χ,φ play no role in the proof of (ii).

Assertion (iii) is obvious: the trace functions of $\mathcal{F}(A_0,B_0,\chi)$ and $\mathcal{F}(A_0,B_0,\overline{\chi})$ are complex conjugates of each other if A_0B_0 is odd. Assertion (iv) then follows from (i) and (iii). ☐

In view of assertion (iii) of Lemma 5.5, in the case when AB is odd, for $C=\gcd(A,B)$, we choose a set $\mathrm{Rep}(C)\subset\mathsf{Char}(C)$ of $(C-1)/2$ nontrivial characters such that for each nontrivial $\chi\in\mathsf{Char}(C)$, precisely one of $\chi,\overline{\chi}$ lies in $\mathrm{Rep}(C)$.

Theorem 5.6. *Let $A>B\geq 1$ be prime to p integers with $2\nmid\gcd(A,B)=C>1$. Suppose that* **infmono**(A,B) *holds, and write $(A,B)=(CA_0,CB_0)$. Then we have the following results.*

(i) *Suppose that AB is even and $A_0>2$. Then $G^\circ_{\mathrm{geom},\mathcal{F}(A,B,\mathbb{1})}=\mathrm{SL}_{A_0-1}\times\prod_{\mathbb{1}\neq\chi\in\mathsf{Char}(C)}\mathrm{SL}_{A_0}$.*

(ii) *Suppose that AB is odd and $A_0>3$. Then precisely one of $\chi,\overline{\chi}$ lies in $\mathrm{Rep}(C)$, and $G_{\mathrm{geom},\mathcal{F}(A,B,\mathbb{1})}=\mathrm{Sp}_{A_0-1}\times\prod_{\chi\in\mathrm{Rep}(C)}\mathrm{SL}_{A_0}$.*

Proof. We begin with the direct sum decomposition

$$\mathcal{F}(A,B,\mathbb{1})=\bigoplus_{\chi\in\mathsf{Char}(C)}\mathcal{F}(A_0,B_0,\chi),$$

Recall from [KT4, 3.10] that, up to multiplicative translation, the local systems $\mathcal{F}(A_0,B_0,\chi)$ are each geometrically isomorphic to Kummer $[A_0]^\star$ pullbacks of hypergeometric sheaves. We have

$$\mathcal{F}(A_0,B_0,\mathbb{1})=[A_0]^\star\mathcal{H}_{small,A_0,B_0},$$

and for $\chi\neq\mathbb{1}$. and any choice of ρ_χ with $\rho_\chi^{A_0}=\chi$, we have

$$\mathcal{F}(A_0,B_0,\chi)=[A_0]^\star\mathcal{H}_{big,A_0,B_0,\rho_\chi}.$$

(i) Suppose first that AB is even, and $A_0 \geq 3$. By **infmono**(A,B), each $G_{\mathrm{geom},\mathcal{F}(A_0,B_0,\chi)}$ is infinite. Then by [KT6, 10.2.4 and 10.3.21], we have

$$G^{\circ}_{\mathrm{geom},\mathcal{F}(A_0,B_0,\mathbb{1})} = \mathrm{SL}_{A_0-1},$$

and for each $\chi \neq \mathbb{1}$ we have

$$G^{\circ}_{\mathrm{geom},\mathcal{F}(A_0,B_0,\chi)} = \mathrm{SL}_{A_0}.$$

Now consider the direct sum of hypergeometric sheaves $\mathcal{H}(A,B,\mathbb{1})$ defined as

$$\mathcal{H}(A,B,\mathbb{1}) := \mathcal{H}_{small,A_0,B_0} \oplus \bigoplus_{\mathbb{1}\neq\chi\in\mathsf{Char}(C)} \mathcal{H}_{big,A_0,B_0,\rho_\chi}.$$

Up to multiplicative translation, we have a geometric isomorphism

$$\mathcal{F}(A,B,\mathbb{1}) = [A_0]^{\star}\mathcal{H}(A,B,\mathbb{1}).$$

As finite pullback doesn't change $G^{\circ}_{\mathrm{geom}}$, we have

$$G^{\circ}_{\mathrm{geom},\mathcal{H}_{small,A_0,B_0}} = \mathrm{SL}_{A_0-1},$$

and for each $\chi \neq \mathbb{1}$ we have

$$G^{\circ}_{\mathrm{geom},\mathcal{H}_{big,A_0,B_0,\rho_\chi}} = \mathrm{SL}_{A_0}.$$

In this AB even case, it suffices to show that $G^{\circ}_{\mathrm{geom},\mathcal{H}(A,B,\mathbb{1})}$ is the asserted product

$$G^{\circ}_{\mathrm{geom},\mathcal{H}(A,B,\mathbb{1})} = \mathrm{SL}_{A_0-1} \times \prod_{\chi\in\mathsf{Char}(C),\chi\neq\mathbb{1}} \mathrm{SL}_{A_0}.$$

For this, we apply Goursat-Kolchin-Ribet [Ka2, 1.8.2]. We must show that for any character $\mathcal{L}$ of $G_{\mathrm{geom},\mathcal{H}(A,B,\mathbb{1})}$,

(a) there is no isomorphism between $\mathcal{L}\otimes\mathcal{H}_{small,A_0,B_0}$ and any $\mathcal{H}_{big,A_0,B_0,\rho_\chi}$ or its dual $\mathcal{H}^{\vee}_{big,A_0,B_0,\rho_\chi}$

(b) For $\chi \neq \varphi$ both nontrivial, there is no isomorphism between $\mathcal{L} \otimes \mathcal{H}_{big,A_0,B_0,\rho_\chi}$ and either $\mathcal{H}_{big,A_0,B_0,\rho_\varphi}$ or its dual $\mathcal{H}^{\vee}_{big,A_0,B_0,\rho_\varphi}$.

The first condition holds trivially, as the ranks are different, $A_0 - 1$ versus A_0. It suffices to show the second condition with the stronger statement for $\mathcal{L}$ any character of $\pi_1^{\mathrm{geom,tame\ at\ 0}}(\mathbb{G}_m/\mathbb{F}_p)$. Such a character is a Kummer sheaf $\mathcal{L}_\sigma$. Indeed, as $A_0 \geq 3$, either $A_0 - B_0 > 1$, in which case all ∞-slopes are < 1, and so $\mathcal{L}$ is tame at ∞, or $A_0 - B_0 = 1$, in which case there is a single slope 1 at ∞, but $A_0 - 1 \geq 2$ slopes 0 at ∞, so again $\mathcal{L}$ must be tame at ∞.

As the "upstairs" characters of $\mathcal{H}_{big,A_0,B_0,\rho_\chi}$ and of both $\mathcal{H}_{big,A_0,B_0,\rho_\varphi}$ and its dual $\mathcal{H}^{\vee}_{big,A_0,B_0,\rho_\varphi}$ are $\mathsf{Char}(A_0)$, the set of all characters, the only possible $\mathcal{L}$ is a Kummer $\mathcal{L}_\chi$ for some $\chi \in \mathsf{Char}(A_0)$.

It there were such an isomorphism, it would persist after $[A_0]^{\star}$ Kummer pullback, which makes the $\mathcal{L}$ disappear. So in this AB even case, we are reduced to showing that for $\chi \neq \varphi$ both nontrivial, $\mathcal{F}(A_0,B_0,\chi)$ is not geometrically isomorphic to either $\mathcal{F}(A_0,B_0,\varphi)$ or its dual $\mathcal{F}(A_0,B_0,\varphi)^{\vee}$. Applying Lemma 5.5, we complete the proof in the AB even case.

(ii) We now treat the case when AB is odd. Then A_0B_0 is odd, and for each nontrivial $\chi \in \mathsf{Char}(C)$, the two local systems $\mathcal{F}(A_0,B_0,\chi)$ and $\mathcal{F}(A_0,B_0,\overline{\chi})$ are dual. Therefore $\mathcal{F}(A,B,\mathbb{1})$ has the same G_{geom} as the "reduced" direct sum

$$\mathcal{F}_{reduced}(A,B,\mathbb{1}) := \mathcal{F}(A_0,B_0,\mathbb{1}) \oplus \bigoplus_{\chi\in\mathrm{Rep}(C)} \mathcal{F}(A_0,B_0,\chi).$$

Let us explain this last point. Our situation is that we have two local systems $\mathcal{A}$ and $\mathcal{B}$ of ranks M and N respectively. We consider both the direct sum $\mathcal{A}\oplus\mathcal{B}$ and the direct sum $\mathcal{A}\oplus\mathcal{B}\oplus\mathcal{B}^{\vee}$. For the latter, an element $\gamma \in \pi_1(\mathbb{A}_1/\overline{\mathbb{F}_p})$ maps to a "diagonal" element $\mathrm{diag}(Z,X,Y)$ in $\mathrm{GL}(\mathcal{A}\oplus\mathcal{B}\oplus\mathcal{B}^{\vee})$, This element satisfies the matrix equation ${}^tXY = \mathrm{Id}_{2N}$. Hence every element (Z, X, Y) in the Zariski closure also satisfies the matrix equation ${}^tXY = \mathrm{Id}_{2N}$. Thus the map

$$G_{\mathrm{geom},\mathcal{A}\oplus\mathcal{B}\oplus\mathcal{B}^\vee} \to G_{\mathrm{geom},\mathcal{A}\oplus\mathcal{B}},\ (Z, X, Y) \mapsto (Z, X)$$

is injective: we recover Y as ${}^tX^{-1}$. But this projection is surjective, so we get the asserted isomorphism

$$G_{\mathrm{geom},\mathcal{A}\oplus\mathcal{B}\oplus\mathcal{B}^\vee} \cong G_{\mathrm{geom},\mathcal{A}\oplus\mathcal{B}}.$$

Analogously to the AB even case, we introduce the "reduced" direct sum of hypergeometric sheaves

$$\mathcal{H}_{reduced}(A, B, \mathbb{1}) := \mathcal{H}_{small,A_0,B_0} \oplus \bigoplus_{\chi\in\mathrm{Rep}(C),\chi\neq\mathbb{1}} \mathcal{H}_{big,A_0,B_0,\rho_\chi},$$

whose $[A_0]^\star$ Kummer pullback is $\mathcal{F}_{reduced}(A, B, \mathbb{1})$. Then it suffices to prove that $G^\circ_{\mathrm{geom},\mathcal{H}_{reduced}(A,B,\mathbb{1})}$ is the asserted product

$$G^\circ_{\mathrm{geom},\mathcal{H}_{reduced}(A,B,\mathbb{1})} = \mathrm{Sp}_{A_0-1} \times \prod_{\chi\in\mathrm{Rep}(C)} \mathrm{SL}_{A_0}.$$

In view of Lemma 5.5, this is immediate from Goursat-Kolchin-Ribet [Ka2, 1.8.2]. Indeed, with the hypothesis $A_0 > 3$, we can instead directly apply [Ka2, 8.11.7.2], because the exclusion (1) of that result, concerning factors of rank 2, is vacuous, as there are no such factors. ☐

6. Multiparameter local systems with infinite monodromy. I

We continue to work with local systems defined in (4.0.1), for which **infmono**(A, B) does not necessarily hold. First we give a slight variant of Theorem 5.6.

Theorem 6.1. *Given prime to p integers $A > B \geq 1$, suppose that $C := \gcd(A, B)$ is both odd and ≥ 3. Write $(A, B) = (CA_0, CB_0)$. Let S_{inf}, respectively S_{fin} be the set of those characters $\chi \in \mathsf{Char}(C)$ for which $\mathcal{F}(A_0, B_0, \chi)$ has infinite, respectively finite, G_{geom}. Suppose that $\varnothing \neq S_{\mathrm{inf}} \neq \mathsf{Char}(C)$. Then, by Lemma 5.1(ii),*

$$S_{\mathrm{fin}} = \mathsf{Char}(C_0) \text{ and } S_{\mathrm{inf}} = \mathsf{Char}(C) \smallsetminus \mathsf{Char}(C_0)$$

for some divisor $C_0 < C$ of C. Denote

$$\mathcal{F}_{\mathrm{inf}}(A, B) := \oplus_{\chi\in S_{\mathrm{inf}}}\mathcal{F}(A_0, B_0, \chi),\ \mathcal{F}_{\mathrm{fin}}(A, B) := \oplus_{\chi\in S_{\mathrm{fin}}}\mathcal{F}(A_0, B_0, \chi) = \mathcal{F}(A_0C_0, B_0C_0, \mathbb{1}).$$

Then the following statements hold for $G := G_{\mathrm{geom},\mathcal{F}(A,B,\mathbb{1})}$ and $H_{\mathrm{fin}} := G_{\mathrm{geom},\mathcal{F}_{\mathrm{fin}}(A,B)}$.

(i) *Suppose A_0B_0 is even. Then*

$$G^\circ_{\mathrm{geom},\mathcal{F}(A,B,\mathbb{1})} = G^\circ_{\mathrm{geom},\mathcal{F}_{\mathrm{inf}}(A,B)} \cong \prod_{\chi\in S_{\mathrm{inf}}} \mathrm{SL}_{A_0}.$$

If $A_0 - 1 \neq B_0$, then $G_{\mathrm{geom},\mathcal{F}_{\mathrm{inf}}(A,B)} = G^\circ_{\mathrm{geom},\mathcal{F}_{\mathrm{inf}}(A,B)}$ and

$$G = H_{\mathrm{fin}} \times G_{\mathrm{geom},\mathcal{F}_{\mathrm{inf}}(A,B)}.$$

If $A_0 - 1 = B_0$ but $A_0 > 2$, then

$$[G, G] = [H_{\mathrm{fin}}, H_{\mathrm{fin}}] \times G^\circ_{\mathrm{geom},\mathcal{F}_{\mathrm{inf}}(A,B)},$$

and the quotient $G/[G, G]$ is a nontrivial finite elementary abelian p-group.

(ii) *Suppose A_0B_0 is odd. Choose a subset $\mathrm{Rep}(S_{\mathrm{inf}}) \subset S_{\mathrm{inf}}$ of $\#S_{\mathrm{inf}}/2$ nontrivial characters such that for each nontrivial $\chi \in S_{\mathrm{inf}}$, precisely one of $\chi, \overline{\chi}$ lies in $\mathrm{Rep}(S_{\mathrm{inf}})$. Then*

$$G_{\mathrm{geom},\mathcal{F}_{\mathrm{inf}}(A,B)} \cong \prod_{\chi\in\mathrm{Rep}(S_{\mathrm{inf}})} \mathrm{SL}_{A_0},\ G = H_{\mathrm{fin}} \times G_{\mathrm{geom},\mathcal{F}_{\mathrm{inf}}(A,B)}.$$

Proof. The proof of the identification of $G^\circ_{\mathrm{geom},\mathcal{F}(A,B,\mathbb{1})} = G^\circ_{\mathrm{geom},\mathcal{F}_{\mathrm{inf}}(A,B)}$, via Goursat-Kolchin-Ribet, is a subset of the proof of Theorem 5.6, and is left to the reader.

Next, observe that $G^\circ_{\mathrm{geom},\mathcal{F}_{\mathrm{inf}}(A,B)}$ is perfect and has no nontrivial finite quotient; furthermore,

$$\mathcal{F}(A,B,\mathbb{1}) = \mathcal{F}_{\mathrm{fin}}(A,B,\mathbb{1}) \oplus \mathcal{F}_{\mathrm{inf}}(A,B). \tag{6.1.1}$$

Assume in addition that $A_0 - 1 \neq B_0$. Then (5.3.1) and the arguments in the proof of Theorem 5.6 show that $G_{\mathrm{geom},\mathcal{F}_{\mathrm{inf}}(A,B)} = G^\circ_{\mathrm{geom},\mathcal{F}_{\mathrm{inf}}(A,B)}$. Now, the action of G on the two summands in (6.1.1) projects G onto the finite group H_{fin} and onto $G_{\mathrm{geom},\mathcal{F}_{\mathrm{inf}}(A,B)}$. Since $G_{\mathrm{geom},\mathcal{F}_{\mathrm{inf}}(A,B)}$ has no finite quotient, an application of the classical Goursat lemma, cf. [L, Exercise 5, p. 75], shows that

$$G = H_{\mathrm{fin}} \times G_{\mathrm{geom},\mathcal{F}_{\mathrm{inf}}(A,B)}.$$

Assume now that $A_0 - 1 = B_0$ but $A_0 > 2$. By [KT6, Theorem 10.3.13], we have $C_0 = 1$, and

$$(p, A_0, H_{\mathrm{fin}}) = (3, 5, \mathrm{Sp}_4(3) \times 3),\ (5, 3, \mathrm{SL}_2(5) \times 5). \tag{6.1.2}$$

The action of G on any summand $\mathcal{F}(A_0,B_0,\chi)$ of $\mathcal{F}(A,B,\chi)$ projects G onto H_{fin} when $\chi = 1$ and onto an intermediate group between SL_{A_0} and $\mathrm{SL}_{A_0} \cdot p$ when $\chi \in S_{\mathrm{inf}}$. Hence it projects $[G,G]$ onto the quasisimple group $[H_{\mathrm{fin}}, H_{\mathrm{fin}}]$ when $\chi = 1$, and onto SL_{A_0}. Again using the classical Goursat lemma, we conclude that

$$[G,G] = [H_{\mathrm{fin}}, H_{\mathrm{fin}}] \times G^\circ_{\mathrm{geom},\mathcal{F}_{\mathrm{inf}}(A,B)}.$$

Now, the above action projects $G/[G,G]$ onto C_p on every summand, hence $G/[G,G]$ is a nontrivial finite elementary abelian p-group. ☐

This last result allows a partial strengthening of Lemma 5.5(i).

Corollary 6.2. *Hypotheses and notations as in Theorem 6.1, the local systems $\mathcal{F}(A_0,B_0,\chi)$ with $\chi \in S_{\mathrm{inf}}$ are pairwise non-isomorphic as representations of $G^\circ_{\mathrm{geom},\mathcal{F}_{\mathrm{inf}}(A,B)}$.*

Proof. In the case when A_0B_0 is even, the group $G^\circ_{\mathrm{geom},\mathcal{F}_{\mathrm{inf}}(A,B)}$ is a product of nontrivial groups, and the constituents $\mathcal{F}(A_0,B_0,\chi)$ indexed by $\chi \in S_{\mathrm{inf}}$ are nontrivial irreducible representations of the various nontrivial factor groups. In the case when A_0B_0 is odd, the group $G_{\mathrm{geom},\mathcal{F}_{\mathrm{inf}}(A,B)}$ is a product of copies of SL_{A_0}, $A_0 \geq 3$, and the constituents are either the natural module for one of the SL_{A_0} factors or the dual of the natural module for that factor. In this case it remains to observe that, because $A_0 > 2$, the natural module for a given SL_{A_0} factor is not self-dual. ☐

Theorem 6.3. *Consider the local system $\mathcal{F} := \mathcal{F}(A, B_1, \ldots, B_r, \mathbb{1})$ with $r \geq 2$, subject to* (4.0.1). *Suppose that $\mathcal{F}(A,B,\mathbb{1})$ has infinite geometric monodromy group for some (not necessarily) balanced pair $(A, B = B_i)$ with $2 \nmid C = \gcd(A,B)$. Then $\mathcal{F}$ is Lie-irreducible, i.e., $G^\circ_{\mathrm{geom},\mathcal{F}}$ acts irreducibly.*

Proof. Write $(A,B) = (CA_0, CB_0)$. When $C = 1$, or when $A_0 = 2$, or when $A_0 = 3$ and B is odd, we have already established the statement in Theorem 5.3 (and its proof), and in Theorem 5.4.

It remains to treat the case when $C \geq 3$ and either $A_0 > 2$ or both A_0B_0 is odd and $A_0 > 3$. In these cases, we have the direct sum decomposition

$$\mathcal{F}(A,B,\mathbb{1}) = \bigoplus_{\chi \in \mathsf{Char}(C)} \mathcal{F}(A_0,B_0,\chi),$$

into pairwise non-isomorphic geometrically irreducible constituents. Precisely one of these constituents has rank $A_0 - 1$, namely $\mathcal{F}(A_0,B_0,\mathbb{1})$, the other $C-1$ constituents each have rank A_0.

(a) Let S_{inf}, respectively S_{fin} be the set of those characters $\chi \in \mathsf{Char}(C)$ for which $\mathcal{F}(A_0,B_0,\chi)$ has infinite, respectively finite, G_{geom}, and write

$$C_0 := \#S_{\mathrm{fin}}.$$

Recall from Lemma 5.1 that either $C_0 = 0$, or C_0 is a proper divisor of $C \geq 3$, hence

$$\#S_{\text{inf}} = C - C_0 \geq 2.$$

Because $\mathcal{F}(A, B, \mathbb{1})$ is a pullback of $\mathcal{F}$, we have $H \leq G$ for

$$G := G_{\text{geom},\mathcal{F}},\ H := G_{\text{geom},\mathcal{F}(A,B,\mathbb{1})},$$

and hence $H^\circ \leq G^\circ$. Now we can apply Theorem 5.6 and Theorem 6.1 to see that

$$H^\circ = H^\circ_{\text{inf}} = G^\circ_{\text{geom},\mathcal{F}_{\text{inf}}(A,B)}. \tag{6.3.1}$$

By Lemma 5.5(i) and Corollary 6.2, each of $C - C_0 \geq 2$ constituents $\mathcal{F}(A_0, B_0, \chi)$, $\chi \in S_{\text{inf}}$, is irreducible under H°, and that they are pairwise non-isomorphic as representations of H°.

(b) We argue by contradiction. We know [KT5, 2.6] that $\mathcal{F}$ is geometrically irreducible, i.e. that G is an irreducible subgroup of $\mathrm{GL}_{A-1} = \mathrm{GL}(V)$ with $V := \mathcal{F}_{\overline{\eta}}$. Suppose that G° is reducible on V. Because $G^\circ \lhd G$, the action of G° on V is completely reducible. Let

$$V = \bigoplus_{i=1}^{m} n_i W_i$$

be the decomposition of V into isotypical components under the action of G°. Then G transitively permutes these m isotypical components, and it must also transitively permute the isomorphism classes of the W_i. Therefore the multiplicities n_i have a common value n, and $V = n(\oplus_{i=1}^m W_i)$ under G°. Now if $n > 1$, then some simple summand of $V|_{H^\circ}$ has multiplicity $\geq n$, contradicting the conclusion of (a). Hence

$$n = 1 \text{ and } m \geq 2, \tag{6.3.2}$$

the latter because we assume $V|_{G^\circ}$ is reducible.

Now the summands W_i are transitively permuted by G, so all have the same dimension as each other, say common dimension M. Under the subgroup H°, each W_i is a partial direct sum of the H°-components of V. In the case $C_0 = 0$, exactly one of these $G^\circ_{\text{geom},\mathcal{F}(A,B,\mathbb{1})}$-components has dimension $A_0 - 1 \geq 2$, all the others have dimension A_0. So exactly one of the W_i has dimension which is $-1 \pmod{A_0}$, any other W_i has dimension divisible by A_0. This contradicts the fact that $\dim(W_i) = M$ for all i.

Assume now that $C_0 \geq 1$. By Theorem 6.1, H contains the subgroup

$$H'_{\text{fin}} \times H^\circ \tag{6.3.3}$$

where $H'_{\text{fin}} = H_{\text{fin}}$, unless $A_0 - 1 = B_0$, in which case we take $H'_{\text{fin}} = [H_{\text{fin}}, H_{\text{fin}}]$. Observe that in either case, $\mathcal{F}(A_0C_0, B_0C_0, \mathbb{1})$ splits into a direct sum of C_0 simple modules under H'_{fin}, one of dimension $A_0 - 1$, and the other $C_0 - 1$ of dimension A_0. On all of these summands H° acts trivially, see (6.3.1).

On the other hand, the remaining $C - C_0$ subsheaves $\mathcal{F}(A_0, B_0, \chi)$, $\chi \in S_{\text{inf}}$, give simple, pairwise non-isomorphic H°-submodules, as mentioned in (a). Thus each of these simple modules of multiplicity 1 must occur in some, and exactly one, W_i upon restriction to H°. Call W_i *big* if $W_i|_{H^\circ}$ is nontrivial, equivalently, contains some $\mathcal{F}(A_0, B_0, \chi)$ with $\chi \in S_{\text{inf}}$, and *small* otherwise. As before, we have

$$mM = D := \dim(V) = A_0C - 1 \equiv -1 \pmod{A_0},$$

and so

$$A_0 \nmid M = \dim(W_j). \tag{6.3.4}$$

Suppose W_i is big, so its restriction to H° contains some $\mathcal{F}(A_0, B_0, \chi_i)$ with $\chi_i \in S_{\text{inf}}$, and consider any $h \in H'_{\text{fin}}$. Recall that h, as any other element in G, sends W_i to some $W_{i'}$. Since h centralizes

H°, see (6.3.3), the H°-modules $h(W_i)$ and W_i are isomorphic and hence have the same H° simple summands. But $\mathcal{F}(A_0, B_0, \chi_i)$ occurs with multiplicity 1 in $V|_{H^\circ}$, hence $h(W_i) = W_{i'} = W_i$. Thus W_i is stabilized by H'_{fin} and hence it is an $H'_{\mathrm{fin}} \times H^\circ$-submodule. Recall that all but one simple summand of the $H'_{\mathrm{fin}} \times H^\circ$-module V has dimension A_0, and the remaining one, $\mathcal{F}(A_0, B_0, \mathbb{1})$, has dimension $A_0 - 1$. As $A_0 \geq 3$, condition (6.3.4) now implies that W_i must contain $\mathcal{F}(A_0, B_0, \mathbb{1})$, which uniquely determines W_i. We have shown that among the W_j's, there is exactly one big summand, and all other are small.

Relabeling the W_j's we may assume W_1 is big, and $W_2, \ldots, W_m$ are all small. As $m \geq 2$ by (6.3.2), we have

$$\dim(\oplus_{i=2}^m W_i) \geq D/2 = (A_0 C - 1)/2. \tag{6.3.5}$$

On the other hand, each small W_j is trivial on H° (by definition), and so must be contained in $\mathcal{F}(A_0 C_0, B_0 C_0, \mathbb{1})$, and does not contain $\mathcal{F}(A_0, B_0, \mathbb{1})$ (which already occurs in the big W_1). It follows that

$$\dim(\oplus_{i=2}^m W_i) \leq A_0(C_0 - 1).$$

As $C_0 < C/2$, this contradicts (6.3.5). ☐

In tandem with Theorem 6.3, we prove:

Proposition 6.4. *Consider the local system $\mathcal{F} := \mathcal{F}(A, B_1, \ldots, B_r, \mathbb{1})$ with $r \geq 2$ subject to* (4.0.1). *Suppose that $A \geq 5$, that for some j, A and B_j have different parity, and that $G^\circ := G^\circ_{\mathrm{geom}, \mathcal{F}}$ acts irreducibly on $\mathcal{F}$. Then $\mathcal{F}$ cannot be self-dual for the action of G°.*

Proof. We argue by contradiction. Assume that the underlying $(A-1)$-dimensional representation space

$$V := \mathcal{F}_{\overline{\eta}}$$

for $G := G_{\mathrm{geom}, \mathcal{F}}$ is self-dual over G°. Then $\mathrm{Hom}_{G^\circ}(V^\vee, V)$ is a one-dimensional representation of G/G°, call it $\mathcal{L}$. This means precisely that $V \cong \mathcal{L} \otimes V^\vee$ as a representation of G. By pullback, we get a geometric isomorphism

$$\mathcal{F}(A, B_j, \mathbb{1}) \cong \mathcal{L}_0 \otimes \mathcal{F}(A, B_j, \mathbb{1})^\vee$$

for $\mathcal{L}_0$ the restriction of $\mathcal{L}$ to the subgroup $G_{\mathrm{geom}, \mathcal{F}(A, B_j, \mathbb{1})} \leq G$.

Now define $C := \gcd(A, B_j)$, and write $(A, B_j) = (CA_0, CB_0)$. Then C is odd, and precisely one of A_0, B_0 is even. In the decomposition

$$\mathcal{F}(A, B_j, \mathbb{1}) = \mathcal{F}(A_0, B_0, \mathbb{1}) \oplus \bigoplus_{\chi \in \mathsf{Char}(C), \chi \neq \mathbb{1}} \mathcal{F}(A_0, B_0, \chi)$$

into a direct sum of local systems which are pairwise not geometrically isomorphic, the summand $\mathcal{F}(A_0, B_0, \mathbb{1})$ is the unique one of lowest rank $A_0 - 1$. Therefore the isomorphism above,

$$\mathcal{F}(A, B_j, \mathbb{1}) \cong \mathcal{L}_0 \otimes \mathcal{F}(A, B_j, \mathbb{1})^\vee,$$

gives a geometric isomorphism

$$\mathcal{F}(A_0, B_j, \mathbb{1}) \cong \mathcal{L}_{0,0} \otimes \mathcal{F}(A_0, B_0, \mathbb{1})^\vee,$$

for $\mathcal{L}_{0,0}$ the restriction of $\mathcal{L}_0$ to the image in $G_{\mathrm{geom}, \mathcal{F}(A_0, B_0, \mathbb{1})}$ of $G_{\mathrm{geom}, \mathcal{F}(A, B_j, \mathbb{1})}$.

We now consider the local system $\mathcal{F}(A_0, B_0, \mathbb{1})$. Up to a multiplicative translation, it is the $[A_0]^\star$ pullback

$$[A_0]^\star \mathcal{H}_{small, A_0, B_0}.$$

Thus $\mathcal{F}(A_0, B_0, \mathbb{1})$ is lisse at 0, and (as $\mathcal{H}_{small, A_0, B_0}$ is hypergeometric of type $(A_0 - 1, B_0 - 1)$) its $I(\infty)$-representation is the direct sum $\mathsf{Tame} \oplus \mathsf{Wild}$ with Tame of rank $B_0 - 1$ and Wild of rank

$A_0 - B_0$, with all slopes $A_0/(A_0 - B_0)$. The same statements about local monodromy hold for its dual $\mathcal{F}(A_0, B_0, \mathbb{1})^\vee$.

Our $\mathcal{L}_{0,0}$ is a constituent of $\mathcal{F}(A_0, B_0, \mathbb{1}) \otimes \mathcal{F}(A_0, B_0, \mathbb{1})$, so is lisse on $\mathbb{A}^1$.

We first treat the case when A_0 is odd and B_0 is even. Suppose first that $A_0 - B_0 \neq 1$. Because $\gcd(A_0, A_0 - B_0) = 1$, the slope $A_0/(A_0 - B_0) > 1$ is not an integer. But the ∞-slope of $\mathcal{L}_{0,0}$, namely $\mathrm{Swan}_\infty(\mathcal{L}_{0,0})$ is an integer. So if $\mathrm{Swan}_\infty(\mathcal{L}_{0,0}) > 0$, then $\mathcal{L}_{0,0} \otimes \mathcal{F}(A_0, B_0, \mathbb{1})^\vee$ will be totally wild at ∞, so cannot be geometrically isomorphic to $\mathcal{F}(A_0, B_0, \mathbb{1})$, which at ∞ has a tame part of dimension $B_0 - 1 \geq 1$ (≥ 1 because B_0 is odd). Therefore $\mathcal{L}_{0,0}$ must be tame at ∞, hence is geometrically trivial. But then we have a geometric isomorphism of $\mathcal{F}(A_0, B_0, \mathbb{1})$ with its dual, contradicting (ii-bis) of Lemma 5.5.

Suppose next that $A_0 - B_0 = 1$ but that $A_0 - B_0 \neq B_0 - 1 > 1$. Then $\mathcal{F}(A_0, B_0, \mathbb{1})$ at ∞ has a wild part of dimension 1 with slope A_0 and a tame part of dimension $B_0 - 1 > 1$. So if $\mathrm{Swan}_\infty(\mathcal{L}_{0,0}) > 0$, then $\mathcal{L}_{0,0} \otimes \mathcal{F}(A_0, B_0, \mathbb{1})^\vee$ will have a wild part of dimension ≥ 2, so cannot be geometrically isomorphic to $\mathcal{F}(A_0, B_0, \mathbb{1})$. Again $\mathcal{L}_{0,0}$ must be tame at ∞, hence geometrically trivial, and again a contradiction of (ii-bis) of Lemma 5.5.

Finally, we have the case when $A_0 - B_0 = 1$ and $B_0 - 1 = 1$, i.e., the case $(A_0, B_0) = (3, 2)$. Here $(A, B) = (3C, 2C)$. As $A \geq 5$, we have $C > 1$. So in the decomposition

$$\mathcal{F}(A, B_j, \mathbb{1}) = \mathcal{F}(A_0, B_0, \mathbb{1}) \oplus \bigoplus_{\chi \in \mathsf{Char}(C), \chi \neq \mathbb{1}} \mathcal{F}(A_0, B_0, \chi)$$

there are $C - 1 > 1$ distinct irreducible components $\mathcal{F}(A_0, B_0, \chi)$ of rank A_0. The geometric isomorphism

$$\mathcal{F}(A, B_j, \mathbb{1}) \cong \mathcal{L}_0 \otimes \mathcal{F}(A, B_j, \mathbb{1})^\vee$$

then gives a geometric isomorphism

$$\bigoplus_{\chi \in \mathsf{Char}(C), \chi \neq \mathbb{1}} \mathcal{F}(A_0, B_0, \chi) \cong \bigoplus_{\chi \in \mathsf{Char}(C), \chi \neq \mathbb{1}} \mathcal{L}_0 \otimes \mathcal{F}(A_0, B_0, \chi)^\vee.$$

Matching irreducible constituents, we see that for some pair χ, φ of (not necessarily distint) non-trivial characters in $\mathsf{Char}(C)$, we have a geometric isomorphism

$$\mathcal{F}(A_0, B_0, \chi) \cong \mathcal{L}_{0,0} \otimes \mathcal{F}(A_0, B_0, \varphi)^\vee.$$

Again in this situation, both $\mathcal{F}(A_0, B_0, \chi)$ and $\mathcal{F}(A_0, B_0, \varphi)$ are lisse on $\mathbb{A}^1$. Each is the $[A_0]^\star$ pullback of a hypergeometric $\mathcal{H}_{big, A_0, B_0, \rho_\chi}$, respectively $\mathcal{H}_{big, A_0, B_0, \rho_\varphi}$. Thus both of $\mathcal{F}(A_0, B_0, \chi)$ and $\mathcal{F}(A_0, B_0, \varphi)$ at ∞ have a wild part of dimension $A_0 - B_0 = 3 - 2 = 1$ and a tame part of dimension $B_0 = 2$. So if $\mathcal{L}_{0,0}$ were not tame at ∞, $\mathcal{L}_{0,0} \otimes \mathcal{F}(A_0, B_0, \varphi)^\vee$ would have a wild part of dimension $\geq B_0 = 2$, impossible as $\mathcal{F}(A_0, B_0, \chi)$ has a wild part of dimension 1. Thus $\mathcal{L}_{0,0}$ is geometrically trivial, and hence we get

$$\mathcal{F}(A_0, B_0, \chi) \cong \mathcal{F}(A_0, B_0, \varphi)^\vee,$$

contradicting either (ii) or (ii-bis) of Lemma 5.5. This concludes the proof in the case that A_0 is odd and B_0 is even.

We now treat the case when A_0 is even and B_0 is odd. If $A_0 = 2$, then $B_0 = 1$ and hence $(A, B) = (2C, C)$; in this case we have $M_{2,2}(\mathcal{F}) = 2$ by Theorem 3.7. As $G_{\mathrm{geom},\mathcal{F}}$ is infinite, we have $G^0_{\mathrm{geom},\mathcal{F}} = \mathrm{SL}_{A-1}$ and we are done in this $A_0 = 2$ case.

It remains to treat the case when $A_0 \geq 4$ is even and B_0 is odd. If $\gcd(A, B) = 1$, then $G_{\mathrm{geom},\mathcal{F}(A,B)}$ is infinite, hence has $G^0_{\mathrm{geom},\mathcal{F}} = \mathrm{SL}_{A-1}$, and we are done in this case.

Suppose now that $C > 1$. The just as in the case $(A_0, B_0) = (3, 2)$ discussed above, we match irreducible constituents to see that for some pair χ, φ of (not necessarily distint) nontrivial characters in $\mathsf{Char}(C)$, we have a geometric isomorphism

$$\mathcal{F}(A_0, B_0, \chi) \cong \mathcal{L}_{0,0} \otimes \mathcal{F}(A_0, B_0, \varphi)^\vee.$$

Both $\mathcal{F}(A_0, B_0, \chi)$ and $\mathcal{F}(A_0, B_0, \varphi)^\vee$ are lisse at 0. As $I(\infty)$-representations each is $\mathsf{Tame} \oplus \mathsf{Wild}$, with Tame of rank B_0 and Wild of rank $A_0 - B_0$ with all slopes $A_0/(A_0 - B_0)$.

If $A_0 - B_0 \neq 1$, then the slope $A_0/(A_0 - B_0)$ is not an integer. If $\mathcal{L}_{0,0}$ had $\mathrm{Swan}_\infty > 0$, then $\mathcal{L}_{0,0} \otimes \mathcal{F}(A_0, B_0, \varphi)^\vee$ would be totally wild at ∞, impossible because $\mathcal{F}(A_0, B_0, \chi)$ has a tame part of dimension $B_0 \geq 1$. Thus $\mathcal{L}_{0,0}$ is geometrically trivial. Then

$$\mathcal{F}(A_0, B_0, \chi) \cong \mathcal{F}(A_0, B_0, \varphi)^\vee,$$

contradicting either (ii) or (ii-bis) of Lemma 5.5.

It remains to treat the case when $A_0 - B_0 = 1$. Here Tame has dimension $B_0 = A_0 - 1 \geq 3$, while Wild has dimension 1. If If $\mathcal{L}_{0,0}$ had $\mathrm{Swan}_\infty > 0$, then $\mathcal{L}_{0,0} \otimes \mathcal{F}(A_0, B_0, \varphi)^\vee$ would have a wild part of dimension at least $B_0 \geq 3$, impossible because $\mathcal{F}(A_0, B_0, \chi)$ has a wild part of dimension 1. So again here, we get

$$\mathcal{F}(A_0, B_0, \chi) \cong \mathcal{F}(A_0, B_0, \varphi)^\vee,$$

contradicting either (ii) or (ii-bis) of Lemma 5.5. $\square$

Remark 6.5. We exclude the case $A = 3$ in Proposition 6.4 because $\mathcal{F}(3, 2, \mathbb{1})$ has rank two, and in any characteristic $p > 5$ has infinite G_{geom}, and hence $G^\circ_{\mathrm{geom}} = \mathrm{SL}_2 = \mathrm{Sp}_2$ in any characteristic $p > 5$.

Now we can determine G_{geom} in the presence of **infmono**(A, B):

Theorem 6.6. *Consider the local system $\mathcal{F} := \mathcal{F}(A, B_1, \ldots, B_r, \mathbb{1})$ with $r \geq 2$ subject to (4.0.1). Suppose that condition* **infmono**(A, B) *holds for some, not necessarily balanced, pair $(A, B = B_i)$ with $2 \nmid C = \gcd(A, B)$. Then the following statements hold for $G_{\mathrm{geom},\mathcal{F}}$.*

(i) *Suppose that AB is even. Then $G^\circ_{\mathrm{geom},\mathcal{F}} = \mathrm{SL}_{A-1}$.*

(ii) *Suppose that AB is odd. If $2 \nmid AB_1 \ldots B_r$, then $G_{\mathrm{geom},\mathcal{F}} = \mathrm{Sp}_{A-1}$. If $2 | AB_1 \ldots B_r$, then $G^\circ_{\mathrm{geom},\mathcal{F}} = \mathrm{SL}_{A-1}$.*

Proof. (a) First we assume that the pair (A, B) is balanced, and write $A_0 = A/C$ and $B_0 = B/C$. In view of Theorems 5.3 and 5.4, it suffices to treat the cases with

$$C \geq 3,\ A_0 \geq 5 \text{ if } 2 \nmid AB, \text{ and } A_0 \geq 3 \text{ if } 2|AB. \tag{6.6.1}$$

Recall the condition **infmono**(A, B) for the balanced pair (A, B) implies that $G = G_{\mathrm{geom},\mathcal{F}}$ is infinite, so G° is semisimple, say of rank

$$r = \mathrm{rank}(G^\circ).$$

By Theorem 6.3, G° acts irreducibly on the underlying representation V of dimension $D = A - 1$.

We aim to show that G° is a simple algebraic group. Assume the contrary:

$$G = G_1 * G_2 * \ldots * G_n,$$

where $n > 1$, G_i is a simple algebraic group of rank a_i, and $a_1 \geq a_2 \geq \ldots \geq a_n \geq 1$. Thus

$$r = \sum_{i=1}^n a_i.$$

We will derive a contradiction when $n \geq 2$.

As G° acts irreducibly and faithfully on V, the underlying representation of G, we can write

$$V|_{G^\circ} = V_1 \otimes V_2 \otimes \ldots \otimes V_n,$$

where V_i is an irreducible G_i-module of dimension $d_i \geq 2$. In fact, by [KlL2, Proposition 5.4.11] we have

$$d_i \geq a_i + 1.$$

Since $(x+1)(y+1) \geq x + y + 1$ for all $x, y \in \mathbb{Z}_{\geq 0}$, we have

$$D = \prod_{i=1}^{n} d_i \geq \prod_{i=1}^{n} (a_i + 1) \geq (a+1)(b+1), \tag{6.6.2}$$

where

$$a := a_1 + a_2 + \ldots + a_{n-1},\ b := a_n,\ a + b = r.$$

(a1) First we consider the case $2|AB$. By Theorem 5.6(i), G° contains a semisimple subgroup of rank

$$A_0 - 2 + (A_0 - 1)(C - 1) = A - 1 - C,$$

and so $r \geq A - 1 - C$. As $C = A/A_0 \leq A/3$ by (6.6.1), we have

$$r \geq 2A/3 - 1 = (2D - 1)/3,$$

and so

$$D \leq \frac{3r+1}{2}. \tag{6.6.3}$$

As $A_0 \geq 3$ and $C \geq 3$ by (6.6.1), we also have

$$r \geq 5. \tag{6.6.4}$$

On the other hand, $a, b \geq 1$ implies that $(2a-1)(2b-1) \geq 1$, i.e. $2ab \geq a + b$. Hence, using (6.6.2) we now have

$$D - \frac{3r+1}{2} = D - \frac{3(a+b)+1}{2} \geq (a+1)(b+1) - \frac{3(a+b)+1}{2} = \frac{2ab - a - b + 1}{2} > 0,$$

contrary to (6.6.3).

(a2) Now suppose that $2 \nmid AB$. By Theorem 5.6(ii), G° contains a semisimple subgroup H of rank

$$\frac{A_0 - 1}{2} + (A_0 - 1)\frac{C-1}{2} = (A_0 - 1)C/2 = (A - C)/2,$$

and so $r \geq (A - C)/2$. As $C = A/A_0 \leq A/5$ by (6.6.1), we have

$$r \geq 2A/5 = (2D + 2)/5,$$

and so

$$D \leq \frac{5r-2}{2}. \tag{6.6.5}$$

As $A_0 \geq 5$ and $C \geq 3$ by (6.6.1), we also have

$$r \geq 6. \tag{6.6.6}$$

Assume in addition that $b \geq 2$. Then either $a, b \geq 3$, or $b = 2$ but $a \geq 4$, and so $(2a-3)(2b-3) \geq 5$, i.e. $2ab \geq 3a + 3b - 2$. Hence, using (6.6.2) we now have

$$D - \frac{5r-2}{2} = D - \frac{5(a+b)-2}{2} \geq (a+1)(b+1) - \frac{5(a+b)-2}{2} = \frac{2ab - 3a - 3b + 4}{2} > 0,$$

contrary to (6.6.5).

It remains to consider the case $a_n = b = 1$. Write $G^\circ = X * Y$, where $X := G_1 * \ldots * G_{n-1}$ and $Y := G_n$. Then

$$G^\circ/X = XY/X \cong Y/(X \cap Y)$$

is isomorphic to SL_2 or PSL_2. Recall that each of the simple factor of the subgroup H have rank $\geq (A_0 - 1)/2 \geq 2$, and hence any homomorphism from it into SL_2 or PSL_2 is trivial. It follows that $H \leq X$. Note that X acts on V via a sum of $d_n = b + 1 \geq 2$ copies of $V_1 \otimes \ldots \otimes V_{n-1}$, we see that each simple summand of $V|_H$ has multiplicity ≥ 2. However, the simple summand $\mathcal{F}(A_0, B_0, \mathbb{1})$ of $V|_H$ has multiplicity 1, again a contradiction.

(b) Continue with the assumption of (a). We have shown that G° is a simple algebraic group of rank $r \geq 5$, see (6.6.4), (6.6.6). Furthermore, (6.6.3), respectively (6.6.5), still holds, so

$$D \leq (5r - 2)/2.$$

In particular, $D \leq 14$ if $r = 6$, $D \leq 16$ if $r = 7$, and $D \leq 19$ if $r = 8$. Applying [KlL2, Proposition 5.4.12], we see that G° is not an exceptional algebraic group, and thus it is a classical group. Since $r \geq 5$, we have that

$$D \leq \frac{5r-2}{2} < \min(r(r+1)/2, r(2r-1) - 1, 2^{r-1}),$$

and

$$D \leq \frac{5r-2}{2} < \min(r(r+1)/2, r(2r-1) - 1, 2^{r-1}, 20),$$

when $r = 5$. Applying [KlL2, Proposition 5.4.11], we conclude that $V|_{G^\circ}$ (of dimension $D = A - 1$) must be the natural module or its dual for the classical group G°. In other words, $G^\circ = \mathrm{SL}_D$, Sp_D, or SO_D.

Suppose $2|AB$. Then (6.6.3) rules out the groups Sp_D and SO_D since they have $D \geq 2r$. Hence we must have $G^\circ = \mathrm{SL}_{A-1}$ in this case.

Suppose $2 \nmid AB$. The choice of the balanced pair (A, B) implies that A and B_i are all odd, so V is symplectic, ruling out SL_D and SO_D. Hence we must have $\mathrm{Sp}_D = G^\circ \leq G \leq \mathrm{Sp}_D$, and so $G = \mathrm{Sp}_{A-1}$.

(c) It remains to consider the case $2|AB_1 \ldots B_r$, $2 \nmid AB$, and **infmono**(A, B) holds for the (unbalanced) pair $(A, B = B_i)$. By Theorem 6.3 we still know that G° is irreducible on V.

Suppose first that $\gcd(A, B_i) = 1$. Then $H := G_{\mathrm{geom}, \mathcal{F}(A,B,\mathbb{1})}$ is Sp_{A-1} by [KT6, Theorems 10.2.4(iii) and 10.3.21(iii)]. As $\mathcal{F}(A, B)$ is a pullback of $\mathcal{F}$, our $G = G_{\mathrm{geom}, \mathcal{F}}$, and hence G°, contains $H = \mathrm{Sp}_{A-1}$. Thus

$$r \geq (A - 1)/2 = D/2. \tag{6.6.7}$$

Assume G° is not simple. Now we can continue the analysis in (a2) to show that $r = a + b$ with $a \geq b \geq 1$ and $D \geq (a + 1)(b + 1)$. If $b \geq 2$, then $(a - 1)(b - 1) \geq 1$, $ab \geq a + b$, and so $D \geq 2(a + b) + 1 = 2r + 1$, contradicting (6.6.7). If $b = 1$, then as in (a2) we arrive at the contradiction that $V|_H$ has simple summands with multiplicity ≥ 2.

We have shown that G° is simple of rank r. Recall that $A > B_i$ are odd, so $A \geq 3$ and $D \geq 2$. If $r = 1$ or $A = 3$, then necessarily $D = 2$, $G^\circ = \mathrm{SL}_2$, and we are done. We may therefore assume

$$A \geq 5, \ r \geq 2.$$

Hence (6.6.7) implies $D \leq (5r - 2)/2$. Assume in addition that $r \geq 5$. Then the same arguments as in (b) show that $G^\circ \cong \mathrm{SL}_D$, Sp_D, or SO_D. Applying Proposition 6.4, we conclude that $G^\circ = \mathrm{SL}_D$.

Suppose $r = 4$. Then $G^\circ = \mathrm{SL}_5$, SO_9, Sp_8, SO_8, or F_4, and $D \leq 8$ by (6.6.7). Since V is irreducible and faithful over G°, using [Lu] we see that $(G^\circ, D) = (\mathrm{SL}_5, 5)$, $(\mathrm{Sp}_8, 8)$, or $(\mathrm{SO}_8, 8)$. The latter two cases are impossible by Proposition 6.4, so $G^\circ = \mathrm{SL}_D$.

Suppose $r = 3$. Then $G^\circ = \mathrm{SL}_4$, SO_7, or Sp_6, and $D \le 6$ by (6.6.7). Since V is irreducible and faithful over G°, using [Lu] we see that $(G^\circ, D) = (\mathrm{SL}_4, 4)$, $(\mathrm{SO}_6, 6)$, or $(\mathrm{Sp}_6, 6)$. The latter two cases are impossible by Proposition 6.4, so $G^\circ = \mathrm{SL}_D$.

Suppose $r = 2$. Then $G^\circ = \mathrm{SL}_3$, Sp_4, or G_2, and $D \le 4$ by (6.6.7). Since V is irreducible and faithful over G°, using [Lu] we see that $(G^\circ, D) = (\mathrm{SL}_3, 3)$, or $(\mathrm{Sp}_4, 6)$. The latter case is ruled out by Proposition 6.4, and so $G^\circ = \mathrm{SL}_D$.

Now suppose that $\gcd(A, B_i) = C > 1$ for the unbalanced pair $(A, B = B_i)$ with **infmono**(A, B). Again write $(A, B) = (CA_0, CB_0)$. If $A_0 = 3$, then $B_0 = 1$, and we are done by Theorem 5.3(ii).

It now remains to treat the case $A_0 \ge 5$. Exactly as in the discussion of the case when $2 \nmid AB$ in the balanced case, we prove that $G^0_{\mathrm{geom},\mathcal{F}}$ is a simple algebraic group, then that G° is one of the classical groups SL_{A-1}, Sp_{A-1} if A is odd, or SO_{A-1}, acting on its natural module or its dual. Proposition 6.4 then shows that $G^\circ_{\mathrm{geom},\mathcal{F}} = \mathrm{SL}_{A-1}$. □

Our next result visibly improves Theorem 6.6:

Theorem 6.7. *Consider the local system $\mathcal{F} := \mathcal{F}(A, B_1, \dots, B_r, \mathbb{1})$ with $r \ge 2$ subject to* (4.0.1). *Suppose that $\mathcal{F}(A, B, \mathbb{1})$ has infinite geometric monodromy group H for some (not necessarily balanced) pair $(A, B = B_i)$ with $2 \nmid C = \gcd(A, B)$. Then the following statements hold.*

(i) *Suppose that AB is even. Then $G^\circ_{\mathrm{geom},\mathcal{F}} = \mathrm{SL}_{A-1}$.*
(ii) *Suppose that AB is odd. If $2 \nmid AB_1 \dots B_r$, then $G_{\mathrm{geom},\mathcal{F}} = \mathrm{Sp}_{A-1}$. If $2|AB_1 \dots B_r$, then $G^\circ_{\mathrm{geom},\mathcal{F}} = \mathrm{SL}_{A-1}$.*

Proof. (a) Since $\mathcal{F}(A, B, \mathbb{1})$ is a pullback of $\mathcal{F}$, $H \le G := G_{\mathrm{geom},\mathcal{F}}$, and G is infinite. Hence G° is semisimple, say of rank

$$r = \mathrm{rank}(G^\circ).$$

We aim to show that G° is a simple algebraic group. Assume the contrary:

$$G^\circ = G_1 * G_2 * \ldots * G_n,$$

where $n > 1$, G_i is a simple algebraic group of rank a_i, and $a_1 \ge a_2 \ge \ldots \ge a_n \ge 1$. Thus

$$r = \sum_{i=1}^n a_i.$$

We will derive a contradiction when $n \ge 2$.

By Theorem 6.3, G° acts irreducibly and faithfully on V, the underlying representation of G. So we can write

$$V|_{G^\circ} = V_1 \otimes V_2 \otimes \ldots \otimes V_n,$$

where V_i is an irreducible G_i-module of dimension $d_i \ge 2$. In fact, by [KlL2, Proposition 5.4.11] we have

$$d_i \ge a_i + 1.$$

Since $(x+1)(y+1) \ge x + y + 1$ for all $x, y \in \mathbb{Z}_{\ge 0}$, we have

$$A - 1 = D = \prod_{i=1}^n d_i \ge \prod_{i=1}^n (a_i + 1) \ge (a+1)(b+1), \tag{6.7.1}$$

where

$$a := a_1 + a_2 + \ldots + a_{n-1},\ b := a_n,\ a + b = r.$$

Write $A_0 = A/C$ and $B_0 = B/C$, and let V denote the underlying representation for G. Also, let $S_{\rm inf}$ denote the set of characters $\chi \in \mathsf{Char}(C)$ such that $\mathcal{F}(A_0, B_0, \chi)$ has infinite $G_{\rm geom}$. By Theorem 6.6, we may assume

$$C > 1, \ S_{\rm inf} \neq \mathsf{Char}(C), \tag{6.7.2}$$

so that $S_{\rm inf} = \mathsf{Char}(C) \smallsetminus \mathsf{Char}(C_0)$ for some proper divisor C_0 of C by Lemma 5.1(ii). As C is odd, we have

$$C_0 \leq C/3.$$

Also, in view of Theorem 5.4, it suffices to treat the cases with

$$A_0 \geq 5 \text{ if } 2 \nmid AB, \text{ and } A_0 \geq 3 \text{ if } 2|AB. \tag{6.7.3}$$

(a1) First we consider the case $2|AB$. By Theorem 6.1, G° contains a semisimple subgroup H° of rank $(A_0-1)(C-C_0) \geq 2C(A_0-1)/3$. Namely, H° is the product of the SL_{A_0} factors, one for each $\mathcal{F}(A_0, B_0, \chi)$ with $\chi \in S_{\rm inf}$. By Corollary 6.2, the subsheaves $\mathcal{F}(A_0, B_0, \chi)$ with $\chi \in S_{\rm inf}$ are simple summands with multiplicity 1 for the module $V|_{H^\circ}$. Thus we have

$$r \geq 2C(A_0-1)/3 \geq 4. \tag{6.7.4}$$

In this case, $C = (D+1)/A_0 \leq (D+1)/3$, so $3r \geq 2A_0C - 2C \geq 4(D+1)/3$, and thus

$$D + 1 \leq 9r/4. \tag{6.7.5}$$

Suppose that $b < A_0 - 1$. Then every homomorphism from H° to G_n of rank b is trivial. It follows that $H^\circ \leq G_1 * \ldots * G_{n-1}$, and hence the restriction of V to H° is a sum of $d_n = \dim(V_n) \geq 2$ copies of the same module. But this contradicts the above multiplicity-one assertion.

We have therefore shown that

$$r/2 \geq b \geq A_0 - 1. \tag{6.7.6}$$

Together with (6.7.3) and (6.7.4), this implies that

$$ab = b(r-b) \geq (A_0-1)(r-(A_0-1)) \geq (A_0-1)^2(2C/3-1) \geq (A_0-1)(4C/3-2).$$

Hence

$$\begin{aligned}(a+1)(b+1) - D &= (ab + r + 1) - (A_0C - 1) \\ &= (A_0-1)(4C/3 - 2 + 2C/3) + 1 - (A_0C-1) \\ &\geq (A_0-1)(2C-2) + 1 - (A_0C-1) \\ &= (A_0-2)(C_0-2) \geq 1.\end{aligned}$$

This however contradicts (6.7.1).

(a2) Next we consider the case $2 \nmid AB$. By Theorem 6.1, G° contains a semisimple subgroup H° of rank $(A_0-1)(C-C_0)/2 \geq C(A_0-1)/3$. Namely, H° is the product of the SL_{A_0} factors, one for each $\mathcal{F}(A_0, B_0, \chi)$ with $\chi \in \mathrm{Rep}(S_{\rm inf})$. By Corollary 6.2, the subsheaves $\mathcal{F}(A_0, B_0, \chi)$ with $\chi \in S_{\rm inf}$ are simple summands with multiplicity 1 for the module $V|_{H^\circ}$. Thus we have

$$r \geq C(A_0-1)/3 \geq 4. \tag{6.7.7}$$

In this case, $C = (D+1)/A_0 \leq (D+1)/5$, so $3r \geq A_0C - C \geq 4(D+1)/5$, and thus

$$D + 1 \leq 15r/4. \tag{6.7.8}$$

Arguing as in (a1), we see that (6.7.6) still holds. Together with (6.7.3) and (6.7.7), this implies that

$$ab = b(r-b) \geq (A_0-1)(r-(A_0-1)) \geq (A_0-1)^2(C/3-1) \geq (A_0-1)(4C/3-4).$$

Suppose $C \geq 9$. Then

$$\begin{aligned}(a+1)(b+1) - D &= (ab + r + 1) - (A_0C - 1) \\ &= (A_0 - 1)(4C/3 - 4 + C/3) + 1 - (A_0C - 1) \\ &\geq (A_0 - 1)(5C/3 - 4) + 1 - (A_0C - 1) \\ &= (2/3)(A_0C - 5C/2 - 6A_0) + 6 \\ &= (2/3)(A_0 - 5/2)(C_0 - 6) - 4 \geq 1\end{aligned}$$

since $A_0 \geq 5$. This however contradicts (6.7.1).

It remains to consider the case $C \in \{3, 5, 7\}$, in which we have $C_0 = 1$ and $r \geq (A_0 - 1)(C - 1)/2$. Now we have

$$ab = b(r - b) \geq (A_0 - 1)(r - (A_0 - 1)) \geq (A_0 - 1)^2(C - 3)/2 \geq (A_0 - 1)(2C - 6).$$

If $C = 7$, then $ab \geq 8(A_0 - 1)$, $a + b = r \geq 3(A_0 - 1)$, and so

$$(a+1)(b+1) \geq 11(A_0 - 1) + 1 - (7A_0 - 1) = 4A_0 - 9 > 0.$$

If $C = 5$, then $ab \geq 4(A_0 - 1)$, $a + b \geq 2(A_0 - 1)$, and so

$$(a+1)(b+1) \geq 6(A_0 - 1) + 1 - (5A_0 - 1) = A_0 - 4 > 0.$$

If $C = 3$, then $ab \geq (A_0 - 1)^2 \geq 4(A_0 - 1)$, $a + b = r \geq (A_0 - 1)$, and so

$$(a+1)(b+1) \geq 5(A_0 - 1) + 1 - (3A_0 - 1) = 2A_0 - 3 > 0.$$

In all cases, we arrive at a contradiction with (6.7.1).

(b) We have shown that G° is a simple algebraic group of rank $r \geq 4$, see (6.7.4), (6.7.7). Furthermore, (6.7.5), respectively (6.7.8), still holds, so

$$D \leq (15r - 4)/4.$$

In particular, $D \leq 14$ if $r = 4$, $D \leq 21$ if $r = 6$, $D \leq 25$ if $r = 7$, and $D \leq 29$ if $r = 8$. Applying [KlL2, Proposition 5.4.12], we see that G° is not an exceptional algebraic group, and thus it is a classical group.

Assume in addition that $r \geq 7$. Then

$$D \leq \frac{15r - 4}{4} < \min(r(r+1)/2, r(2r-1) - 1, 2^{r-1}).$$

Applying [KlL2, Proposition 5.4.11], we conclude that $V|_{G^\circ}$ (of dimension $D = A - 1$) must be the natural module or its dual for the classical group G°. In other words, $G^\circ = \mathrm{SL}_D$, Sp_D, or SO_D.

Suppose $2|AB_1 \ldots B_r$. As $A = A_0C \geq 9$, Proposition 6.4 rules out the groups Sp_D and SO_D. Hence we must have $G^\circ = \mathrm{SL}_{A-1}$ in this case.

Suppose $2 \nmid AB_1 \ldots B_r$. Then V is symplectic, ruling out SL_D and SO_D. Hence we must have $\mathrm{Sp}_D = G^\circ \leq G \leq \mathrm{Sp}_D$, and so $G = \mathrm{Sp}_{A-1}$.

(c) Now we return to the general case, where we know only that $r \geq 4$. If $r \geq 7$, then we are done by (b).

Suppose that $A \geq 14$ if $2|AB$ and $A \geq 23$ if $2 \nmid AB$. In the former case, $r > 6$ by (6.7.5). In the latter case, $r > 6$ by (6.7.8). Thus we have $r \geq 7$, and so are again done by (b).

The rest of the proof is to analyze the remaining cases, in which we may assume

(6.7.9) $$4 \leq r \leq 6,\ 3 \leq A \leq 13 \text{ if } 2|AB, \text{ and } 3 \leq A \leq 21 \text{ if } 2 \nmid AB.$$

Suppose $A = 21$. Then $2 \nmid B$, and $C \in \{3, 7\}$. By (6.7.3) we have $A_0 \neq 3$, so $(A_0, C) = (7, 3)$ and $r \geq 6$ by (6.7.8). In view of (6.7.9), we now have $r = 6$, but $G^\circ \geq H^\circ = \mathrm{SL}_7$. So in fact $G^\circ = H^\circ = H^\circ_{\mathrm{inf}}$ and hence G° is reducible on V by (6.7.2), a contradiction.

Suppose $A \in \{3, 5, 7, 11, 13, 17, 19\} \cup \{2, 4, 8\}$. Since C is an odd proper divisor of A, in these cases we must have $C = 1$, violating (6.7.2).

Suppose $A = 15$. Then G° is a simple classical group of rank $4 \le r \le 6$ acting irreducibly on $V = \mathbb{C}^{14}$. This is impossible by [Lu].

Suppose $A = 12$. Then $(A_0, C) = (4, 3)$ and $r \ge 6$ by (6.7.5), whence $r = 6$. Now G° is a simple classical group of rank 6 acting irreducibly on $V = \mathbb{C}^{11}$. This is impossible by [Lu].

If $A = 10$, then $C = 5$ and $A_0 = 2$, violating (6.7.3).

Suppose $A = 9$. Then $(A_0, C) = (3, 3)$ by (6.7.3), so $2|AB$. Now G° is a simple classical group of rank $4 \le r \le 6$ acting irreducibly on $V = \mathbb{C}^8$, whence $G^\circ \cong \mathrm{Sp}_8$ or SO_8 by [Lu]. In either case, this contradicts Proposition 6.4.

Finally, if $A = 6$, then $C = 3$ and $A_0 = 2$, violating (6.7.3). □

Next we prove the following extension of [KT6, Theorem 11.1.3]:

Theorem 6.8. *Let $V = \mathbb{C}^D$ with $D \ge 6$, and let $G \le \mathrm{GL}(V)$ be a Zariski closed, irreducible subgroup, with $G^\circ \ne 1$ being semisimple. Suppose that G contains a subgroup G_1 which is one of the following groups.*

(a) *G_1 is the image of $\mathrm{Sp}_{2n}(q)$ in a nontrivial subrepresentation of degree D of a total Weil representation of degree q^n for some odd prime power $q = p^f$ and some $n \ge 1$. Furthermore, if $D = q^n$, assume that $q^n \ge 13$.*

(b) *G_1 is the image of $\mathrm{SU}_n(q)$ in a nontrivial subrepresentation of degree D of the total Weil representation of degree q^n for some prime power $q = p^f$ and some odd $n \ge 3$ with $(n, q) \ne (3, 2)$. Furthermore, if G_1 is reducible on V, assume that $V|_{G_1}$ contains a simple summand of dimension $(q^n - q)/(q + 1)$, and, in addition, $(n, q) \ne (3, 3)$.*

(c) *G_1 is the image of $2 \cdot \mathrm{J}_2$ in an irreducible representation of degree $D = 6$.*

(d) *G_1 is the image of $6_1 \cdot \mathrm{PSU}_4(3)$ in an irreducible representation of degree $D = 6$.*

(e) *G_1 is the image of $2 \cdot G_2(4)$ in an irreducible representation of degree $D = 12$.*

Then G° is a simple algebraic group acting irreducibly on V and $G^\circ > G_1$. Moreover, one of the following conclusions holds.

(i) *$G^\circ = \mathrm{SL}(V)$, $\mathrm{Sp}(V)$, or $\mathrm{SO}(V)$.*

(ii) *$D = 32$, $G_1 = \mathrm{SU}_5(2)$, and $G^\circ = \mathrm{Sp}_{10}$.*

(iii) *$(G^\circ, D) = (G_2, 7)$, and $G_1 = \mathrm{PSL}_2(13)$ or $\mathrm{SU}_3(3)$.*

(iv) *$(G^\circ, D) = (E_6, 27)$ and $G_1 = \mathrm{SL}_2(27)$.*

(v) *$(G^\circ, D) = (E_7, 56)$ and $G_1 = \mathrm{PSU}_3(8)$.*

Proof. (A) By assumption, $q^n \ge D \ge 6$ in (a) and $(n, q) \ne (3, 2)$ in (b), so G_1 is quasisimple. According to [KlL2, Table 5.2.A] and [Atlas], for the smallest index $P(G_1)$ of proper subgroups of G_1 we have $P(G_1) \ge q^n + 1 > D$ in case (a), unless $(n, q) = (1, 11)$, for which we have $D \le (q^n + 1)/2$ by hypothesis, and $P(G_1) \ge (q^n + 3)/2 > D$. Similarly, $P(G_1) \ge q^n + 1 > D$ in case (b), unless $(n, q) \ne (3, 5)$, in which case $P(G_1) = 50$. Furthermore, $P(G_1) = 100 > D$ in case (c), $P(G_1) = 112 > D$ in case (d), and $P(G_1) = 416 > D$ in case (e). Thus in all cases we have

$$P(G_1) > D \text{ or } (S, P(G_1), D) = (\mathrm{PSU}_3(5), 50, \ge 50), \tag{6.8.1}$$

where $S := G_1/\mathbf{Z}(G_1)$ is simple.

By [KlL1, Theorem 3], the smallest degree $e(G_1)$ of any nontrivial projective representation of G_1 (over $\mathbb{C}$) is at least the smallest degree $e(S)$ of any nontrivial projective representation of S (over $\mathbb{C}$). According to [KlL2, Table 5.3.A],

$$e(S) = (q^n - 1)/2 \ge (D - 1)/2 \ge \max(6, \sqrt{11D/4}) \tag{6.8.2}$$

in case (a), unless $D \leq 12$. If $6 \leq D \leq 12$ but $V|_{G_1}$ is irreducible, then $q^n \geq 11$ (as $D \geq 6$) and

$$e(S) = (q^n - 1)/2 \geq D - 1 \geq \max(5, \sqrt{4D}). \tag{6.8.3}$$

If $6 \leq D \leq 12$ but $V|_{G_1}$ is reducible, then $D = q^n \leq 11$, which is excluded by our hypothesis. Similarly,

$$e(S) = (q^n - q)/(q + 1) \geq \max(6, \sqrt{3D}) \tag{6.8.4}$$

in case (b), and

$$e(S) = D \geq \sqrt{6D} \geq 6 \tag{6.8.5}$$

in cases (c)–(e). Moreover, in all cases the smallest nontrivial projective representation of S is also a projective representation of G_1, so in fact we have

$$e(G_1) = e(S) > \sqrt{11D/4} > 4. \tag{6.8.6}$$

(A1) By assumption, G acts irreducibly on $V := \mathbb{C}^D$, and G_1 is quasisimple. Suppose that G fixes an imprimitive decomposition

$$V = V_1 \oplus V_2 \oplus \ldots \oplus V_m$$

with $m > 1$. Then $1 < m|D$ and $\dim(V_i) = D/m$ for all i.

Suppose we are in the case $P(G_1) > D$ of (6.8.1). Then every homomorphism $G_1 \to \mathsf{S}_m$ is trivial, and so the action of G_1 on the m summands V_i is trivial. In other words, G_1 stabilizes every V_i. If in addition $V|_{G_1}$ is irreducible, then V_1, being fixed by G_1, is equal to V, contrary to $m > 1$. So $V|_{G_1}$ is reducible. In particular, we are either in (a) with $D = q^n$, in which case $V|_{G_1}$ is a sum $W_1 \oplus W_2$ of two simple summands, W_1 of dimension $d := (q^n - 1)/2$ and W_2 of dimension $d + 1 = (q^n + 1)/2$, or in (b), in which case $V|_{G_1}$ is a sum $\oplus_{i=1}^{s}$ of $s > 1$ simple summands, W_1 of dimension $d := (q^n - q)/(q + 1)$ and $W_2, \ldots, W_s$ all of dimension $d + 1 = (q^n + 1)/(q + 1)$. In either case, because W_1 is a simple summand of multiplicity one in $V|_{G_1}$, we may assume that W_1 occurs in V_1 (and only in V_1). Since each W_i with $i > 1$ has dimension $d + 1$, we see that

$$\dim(V_1) \equiv -1 \pmod{d + 1}, \ \dim(V_2) \equiv 0 \pmod{d + 1}.$$

Thus $\dim(V_1) \neq \dim(V_2)$, a contradiction.

Suppose now that we are in the case $P(G_1) \leq D$ of (6.8.1), so that $G_1/\mathbf{Z}(G_1) = \mathrm{PSU}_3(5)$. The same arguments as above show that G_1 cannot act trivially on the set $\{V_1, \ldots, V_m\}$. As $P(G_1) = 50$, we must have that $m \geq 50$, and so $\dim(V_i) \leq 2$ as $D \leq 5^3$. But the simple summands of $V|_{G_1}$ has dimension 20 or 21, so no V_i can be fixed by G_1. Using [Atlas] we can check that every proper subgroup of G_1 has index 50 or $\geq 126 > m$. It follows that every G_1-orbit on $\{V_1, \ldots, V_m\}$ is of length 50, and hence $50|D$. On the other hand, by (6.8.1) and hypothesis, $D \in \{62, 83, 104, 125\}$, a contradiction.

(A2) We have shown that G acts primitively on V. Let Φ denote the representation of G on V. Next suppose that G_1 fixes a tensor decomposition

$$V = V_1 \otimes V_2$$

with $1 < \dim(V_1) \leq \dim(V_2)$. Then the quasisimple group G_1 admits a projective representation on V_1, of dimension $\leq \sqrt{D}$, whose image is either trivial, or a quasisimple cover of the simple group $S := G_1/\mathbf{Z}(G_1)$. By (6.8.6), every composition factor of the projective representation of G_1 on V_1 is trivial, and so the corresponding image of G_1 in $\mathrm{PGL}(V_1)$ is contained in a Borel subgroup which is solvable. As G_1 is quasisimple, this image is trivial, i.e. G_1 acts via scalars on V_1. Pulling the constants to the action of G_1 on V_2, for every $g \in G_1$ we can write

$$\Phi(g) = \mathrm{Id}_{\dim(V_1)} \otimes \Psi(g)$$

for a unique matrix $\Psi(g) \in \mathrm{GL}(V_2)$. Since $\Phi|_{G_1}$ is a linear representation, it follows that Ψ is a linear representation $G_1 \to \mathrm{GL}(V_2)$. Thus $\Phi|_{G_1}$ is the sum of $\dim(V_1) > 1$ copies of the representation Ψ. In particular, every simple summand of $V|_{G_1}$ occurs with multiplicity $\geq \dim(V_1) > 1$. But this contradicts our hypothesis on $V|_{G_1}$.

(A3) We have shown that G_1 cannot fix any tensor decomposition of V. Finally, suppose G_1 fixes a tensor induced decomposition

$$V = V_1 \otimes \ldots \otimes V_m \cong V_1^{\otimes m}$$

with $m \geq 2$ and $\dim(V_i) \geq 2$. Then

$$m \leq \log_2 D < P(G_1),$$

the latter inequality because of (6.8.1). 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.

Note that $\mathbf{Z}(G)^\circ \leq \mathbf{Z}(G^\circ)$ is finite since G° is semisimple. Thus $\mathbf{Z}(G)$ is finite. We have shown that (V, G) satisfies condition ($\mathbf{S}+$). By [KT3, Lemma 1.1], G° is a simple algebraic group acting irreducibly on V.

(B) By Schur's lemma, $\mathbf{C}_G(G^\circ) = \mathbf{Z}(G)$ is cyclic. Furthermore, $\mathrm{Out}(G^\circ)$ is a subgroup of S_3, hence solvable. It follows that G/G° is solvable. But G_1 is perfect, so $G_1 < G^\circ$.

Let r denote the rank of the simple algebraic group G°. We will now analyze each of the possibilities for G°.

(B1) Suppose G° is of type A_r. In this case, G° admits an irreducible projective complex representation Θ of dimension $r+1$ with finite cyclic kernel. Thus $\Theta|_{G_1}$ is now a nontrivial projective representation, and, arguing as in (A), we see that

$$r + 1 \geq e(G_1) \geq \sqrt{11D/4},$$

by (6.8.6). It follows that $r \geq 4$ and $D \leq 4(r+1)^2/11 < r(r+1)/2$. Applying [KlL2, Proposition 5.4.11], we conclude that the D-dimensional module V of G° is the natural module, or its dual and so $G^\circ = \mathrm{SL}_D$.

(B2) Suppose G° is of type B_r with $r \geq 2$. In this case, G° admits an irreducible projective complex representation Θ of dimension $2r+1$ with finite cyclic kernel and with image contained in PSO_{2r+1}. Thus $\Theta|_{G_1}$ is now a nontrivial projective representation, and hence

$$2r + 1 \geq e(G_1) \geq \sqrt{11D/4} \tag{6.8.7}$$

by (6.8.6). Now, if $r = 2$, then $e(G_1) = 5$, and so by (6.8.2)–(6.8.5) we must have that $G_1/\mathbf{Z}(G_1) = \mathrm{PSL}_2(11)$. Since $\mathrm{SL}_2(11)$ is the universal cover of $\mathrm{PSL}_2(11)$, Θ lifts to a 5-dimensional orthogonal representation of $\mathrm{SL}_2(11)$, which is impossible. So

$$r \geq 3 \text{ and } D \leq 4(2r+1)^2/11 < r(2r+1).$$

Applying [KlL2, Proposition 5.4.11], we see that either the D-dimensional module V of G° is the natural module of dimension $2r+1$ and so $G^\circ = \mathrm{SO}_D$, or $3 \leq r \leq 5$ and $D = 2^r$. It remains to look at the latter possibilities.

Note that if $D = 8$, then $G_1 = \mathrm{SL}_2(17)$ and $V|_{G_1}$ is irreducible of symplectic type. (Indeed, if we are in case (a), then, as $q^n \neq 8$, we have $(q^n \pm 1)/2 = D = 8$, whence $(n, q) = (1, 17)$ and so $G_1 = \mathrm{SL}_2(17)$ in an irreducible Weil representation. If we are in case (b), then $8 = D \geq (q^n - q)/(q+1)$, which is at least 10 if $n \geq 5$, and at least 12 if $n = 3$ but $q \geq 4$. So $(n, q) = (3, 3)$, and we quickly reach a contradiction.) However, in this case we have $e(G_1) = 8$ and $r = 3$, contrary to (6.8.7).

Similarly, if $D = 16$, 32, or 64, then either $(D, G_1) = (16, \mathrm{SL}_2(31))$, $(64, \mathrm{SL}_2(127))$ and $V|_{G_1}$ is irreducible, or $D = 32$ and $G_1 = \mathrm{SU}_5(2)$, or $D = 64$ and $G_1 = \mathrm{SU}_3(4)$. (Indeed, if we are in case (a), then, as $q^n \neq 16, 32, 64$, we have $(q^n \pm 1)/2 = D = 16$, 32, or 64, whence $(D, n, q) = (16, 1, 31)$ or $(64, 1, 127)$ and G_1 acts in an irreducible Weil representation. If we are in case (b), then $D \geq (q^n - q)/(q+1)$, which is at least 72 if $n \geq 9$, or $n = 7$ but $q \geq 3$, or $n = 5$ but $q \geq 4$, or $n = 3$ but $q \geq 9$. If $(n, q) = (7, 2)$, then $D \in \{42, 43, \geq 85\}$. If $(n, q) = (5, 3)$, then $D \in \{60, 61, \geq 121\}$. If $(n, q) = (5, 2)$, then $D \in \{10, 11, 21, 32\}$ by hypothesis, so $D = 32$. If $(n, q) = (3, 8)$, then $D \in \{56, 57, \geq 113\}$. If $(n, q) = (3, 7)$, then $D \in \{42, 43, \geq 85\}$. If $(n, q) = (3, 5)$, then $D \in \{20, 21, 41, 62, \geq 83\}$ by hypothesis. If $(n, q) = (3, 4)$, then by hypothesis $D \in \{12, 13, 25, 38, 51, 64\}$, so $D = 64$. If $(n, q) = (3, 3)$ then $D = 6, 7$ by hypothesis.)

Now, in the case $D = 16$ and $G_1 = \mathrm{SL}_2(31)$ we have $e(G_1) = 15$ and $r = 4$, contrary to (6.8.7).

In the case $D = 32$ and $G_1 = \mathrm{SU}_5(2)$, we have $G^\circ = \mathrm{Spin}_{11}$. The projection $G^\circ \to \mathrm{SO}_{11}$ has kernel of order 2 which must then intersect G_1 trivially since G_1 is simple. It follows that G_1 embeds in SO_{11}. But this is a contradiction, since every nontrivial complex representation of degree 11 of $\mathrm{SU}_5(2)$ is either irreducible non-self-dual, or a direct sum of a trivial representation and an irreducible representation of symplectic type (of degree 10) see [Atlas].

(B3) Suppose G° is of type D_r with $r \geq 4$. In this case, G° admits an irreducible projective complex representation Θ of dimension $2r$ with finite cyclic kernel and with image contained in PSO_{2r}. Thus $\Theta|_{G_1}$ is now a nontrivial projective representation, and hence

(6.8.8) $$2r \geq e(G_1) \geq \sqrt{11D/4}$$

by (6.8.6), so

$$D \leq 16r^2/11 < r(2r-1).$$

Applying [KlL2, Proposition 5.4.11], we see that either the D-dimensional module V of G° is (quasi-equivalent in the case $r = 4$ to) the natural module of dimension $2r$ and so $G^\circ \cong \mathrm{SO}_D$, or $4 \leq r \leq 7$ and $D = 2^{r-1}$. It remains to look at the latter possibilities.

If $(r, D) = (4, 8)$, then $G_1 = \mathrm{SL}_2(17)$ and $V|_{G_1}$ is of symplectic type, as shown in (B2). However, $V|_{G^\circ}$ is quasi-equivalent to the natural module, so it is of orthogonal type, a contradiction.

If $(r, D) = (5, 16)$, then $G_1 = \mathrm{SL}_2(31)$ as shown in (B2). However, in this case $e(G_1) = 15$ and $r = 5$, contrary to (6.8.8).

If $(r, D) = (6, 32)$, then $G_1 = \mathrm{SU}_5(2)$ as shown in (B2), and $G^\circ = \mathrm{Spin}_{12}$. The projection $G^\circ \to \mathrm{SO}_{12}$ has kernel of order 2 which must then intersect G_1 trivially since G_1 is simple. It follows that G_1 embeds in SO_{12}. But this is a contradiction, since every nontrivial complex representation of degree 12 of $\mathrm{SU}_5(2)$ is either a sum of of a trivial representation and a non-self-dual irreducible representation (of degree 11), or a sum of two copies of the trivial representation and an irreducible representation of symplectic type (of degree 10), see [Atlas].

If $(r, D) = (7, 64)$, then $G_1 = \mathrm{SU}_3(4)$ as shown in (B2), and $G^\circ = \mathrm{Spin}_{14}$. The projection $G^\circ \to \mathrm{SO}_{14}$ has kernel of order 2 which must then intersect G_1 trivially since G_1 is simple. It follows that G_1 embeds in SO_{14}. But this is a contradiction, since every nontrivial complex representation of degree 14 of $\mathrm{SU}_3(4)$ is either a sum of of a trivial representation and a non-self-dual irreducible representation (of degree 13), or a sum of two copies of the trivial representation and an irreducible representation of symplectic type (of degree 12), see [Atlas].

(B4) Suppose G° is of type C_r with $r \geq 3$. In this case, G° admits an irreducible projective complex representation Θ of dimension $2r$ with finite cyclic kernel and with image contained in PSp_{2r}. Thus $\Theta|_{G_1}$ is now a nontrivial projective representation, and hence (6.8.8) holds by (6.8.6), and so

$$D \leq 16r^2/11 < r(2r-1) - 1.$$

Applying [KlL2, Proposition 5.4.11], we see that either the D-dimensional module V of G° is the natural module of dimension $2r$ and so $G^\circ \cong \mathrm{Sp}_D$, or $3 \le r \le 5$ and $D = 2^r$, or $(r, D) = (3, 14)$. It remains to look at the latter possibilities.

If $D = 8$, then $G_1 = \mathrm{SL}_2(17)$ as shown in (B2). However, in this case we have $e(G_1) = 8$ and $r = 3$, contrary to (6.8.8).

If $D = 16$, then $G_1 = \mathrm{SL}_2(31)$ as shown in (B2). However, in this case we have $e(G_1) = 15$ and $r = 4$, contrary to (6.8.8).

If $D = 32$, then $G_1 = \mathrm{SU}_5(2)$ as shown in (B2), and this is recorded in conclusion (ii).

If $(r, D) = (3, 14)$, then this violates (6.8.8).

(B5) Suppose $G^\circ = G_2$. Then $G^\circ < \mathrm{SL}_7$, and so

$$e(G_1) \le 7, \tag{6.8.9}$$

whence $D \le 17$ by (6.8.6). Since $V|_{G^\circ}$ is irreducible, we must have $D = 7$ or 14 by [Lu].

Suppose $D = 7$. In case (a), (since $q^n \ge 13$ when $D = q^n$) we have $(q^n \pm 1)/2 = D = 7$, and so $(n, q) = (1, 13)$ and $G_1 = \mathrm{PSL}_2(13)$. In case (b), since $D \ge (q^n - q)/(q + 1)$ is at least 10 when $n \ge 5$ or $n = 3$ but $q \ge 4$, we have $(n, q) = (3, 3)$ and $G_1 = \mathrm{SU}_3(3)$. These two possibilities are recorded in conclusion (iii).

Suppose $D = 14$. In case (a) we have $(q^n \pm 1)/2 = D = 14$, and so $(n, q) = (1, 27)$ and $G_1 = \mathrm{SL}_2(27)$. This violates (6.8.9), since $e(G_1) = 13$. In case (b), $D \ge (q^n - q)/(q + 1)$ is at least 20 when $n \ge 7$, or $n = 5$ but $q \ge 3$, or $n = 3$ but $q \ge 5$. Now if $(n, q) = (5, 2)$ then $D \in \{10, 11, \ge 21\}$. If $(n, q) = (3, 4)$ then $D \in \{12, 13, \ge 25\}$. If $(n, q) = (3, 3)$, then $D \in \{6, 7\}$ by hypothesis.

(B6) Suppose $G^\circ = F_4$. Then $G^\circ < \mathrm{SL}_{26}$, and so

$$e(G_1) \le 26, \tag{6.8.10}$$

whence $D \le 245$ by (6.8.6). Since $V|_{G^\circ}$ is irreducible, we must have $D = 26$ or 52 by [Lu].

Suppose $D = 26$. In case (a) we have $(q^n \pm 1)/2 = D = 26$, and so $G_1 = \mathrm{SL}_2(53)$. But $\mathrm{SL}_2(53)$ cannot be embedded in F_4 by [GrR]. In case (b), $D \ge (q^n - q)/(q + 1)$ is at least 42 when $n \ge 7$, or $n = 5$ but $q \ge 3$, or $n = 3$ but $q \ge 7$. Now if $(n, q) = (5, 2)$ then $D \in \{10, 11, 21, 32\}$. If $(n, q) = (3, 5)$ then $D \in \{20, 21, \ge 41\}$. If $(n, q) = (3, 4)$ then $D \in \{12, 13, 25, \ge 38\}$. If $(n, q) = (3, 3)$, then $D \in \{6, 7\}$ by hypothesis.

Suppose $D = 52$. In case (a) we have $(q^n \pm 1)/2 = D = 52$, and so $G_1 = \mathrm{SL}_2(103)$. But $\mathrm{SL}_2(103)$ cannot be embedded in F_4 by [GrR]. In case (b), $D \ge (q^n - q)/(q + 1)$ is at least 56 if $n \ge 9$, or $n = 7$ but $q \ge 3$, or $n = 5$ but $q \ge 3$, or $n = 3$ but $q \ge 8$. If $(n, q) = (7, 2)$, then $D \in \{42, 43, \ge 85\}$. If $(n, q) = (5, 2)$ or $(3, 3)$ then $D \le 32$. If $(n, q) = (3, 7)$, then $D \in \{42, 43, \ge 85\}$. If $(n, q) = (3, 5)$, then $D \in \{20, 21, 41, \ge 62\}$ by hypothesis. If $(n, q) = (3, 4)$, then by hypothesis $D \in \{12, 13, 25, 38, 51, 64\}$.

(B7) Suppose $G^\circ = E_6$. Then G° admits an irreducible projective representation of degree 27, and so

$$e(G_1) \le 27$$

whence $D \le 265$ by (6.8.6). Since $V|_{G^\circ}$ is irreducible, we must have $D = 27$ or 78 by [Lu].

In case (a), $D = q^n$ or $(q^n \pm 1)/2$, so $G_1 = \mathrm{SL}_2(27)$ as recorded in (iv), or $\mathrm{SL}_2(53)$, which cannot be projectively embedded in E_6 by [GrR]. So we are in case (b). Since no $\mathrm{PSU}_n(q)$ with $n \ge 5$, or $n = 3$ but $q \ge 9$, can be embedded in E_8 by [GrR], we have $n = 3$ and $q \le 8$. If $(n, q) = (3, 8)$, then by hypothesis $D \in \{56, 57\}$ or $D \ge 113\}$ or $170 \le D \le 512$. If $(n, q) = (3, 7)$, then by hypothesis $D \in \{42, 43, \ge 85\}$. If $(n, q) = (3, 5)$, then $D \in \{20, 21, 41, 62, \ge 83\}$ by hypothesis. If $(n, q) = (3, 4)$, then by hypothesis $D \in \{12, 13, 25\}$ or $38 \le D \le 64$.

(B8) Suppose $G^\circ = E_7$. Then G° admits an irreducible projective representation of degree 56, and so

$$e(G_1) \leq 56,$$

whence $D \leq 1140$ by (6.8.6). Since $V|_{G^\circ}$ is irreducible, we must have $D = 56$, 133, or 912 by [Lu].

In case (a), $D = q^n$ or $(q^n \pm 1)/2$, so $G_1 = \mathrm{SL}_2(113)$ or $\mathrm{SL}_2(1813)$, neither of which can be projectively embedded in E_7 by [GrR]. So we are in case (b). Since no $\mathrm{PSU}_n(q)$ with $n \geq 5$, or $n = 3$ but $q \geq 9$, can be embedded in E_8 by [GrR], we have $n = 3$ and $q \leq 8$. If $(n,q) = (3,8)$, then by hypothesis $D \in \{56, 57, 113\}$ or $170 \leq D \leq 512$, so $D = 56$ and $G_1 = \mathrm{PSU}_3(8)$ as recorded in (v). If $(n,q) = (3,7)$, then by hypothesis $D \in \{42, 43, 85, 128\}$ or $171 \leq D \leq 343$. If $(n,q) = (3,5)$, then $D \leq 41$ or $62 \leq D \leq 125$ by hypothesis. If $(n,q) = (3,4)$, then by hypothesis $D \leq 51$ or $D = 64$.

(B9) Finally, suppose $G^\circ = E_8$. Then $G^\circ < \mathrm{SL}_{248}$, and so

$$e(G_1) \leq 248,$$

whence $D \leq 22365$ by (6.8.6). Since $V|_{G^\circ}$ is irreducible, we must have $D = 248$ or 3875 by [Lu].

In case (a), $D = q^n$ or $(q^n \pm 1)/2$, which is impossible. So we are in case (b). Since no $\mathrm{PSU}_n(q)$ with $n \geq 5$, or $n = 3$ but $q \geq 9$, can be embedded in E_8 by [GrR], we have $n = 3$ and $q \leq 8$. Now if $q \leq 5$ then $D \leq 125$. If $(n,q) = (3,8)$, then by hypothesis $D \leq 227$ or $284 \leq D \leq 512$. If $(n,q) = (3,7)$, then by hypothesis $D \leq 214$ or $257 \leq D \leq 343$. None of these values can fit the values 248 or 3875. □

Now we can prove the main result of this section. Recall that the systems $\mathcal{F}(A, B_1, \ldots, B_r, \mathbb{1})$ with finite G_{geom} are already classified in Theorem 11.2.4 of [KT6].

Theorem 6.9. *Consider the local system $\mathcal{F} := \mathcal{F}(A, B_1, \ldots, B_r, \mathbb{1})$ with $r \geq 1$ subject to* (4.0.1). *Suppose that $A \geq 7$ and that $G_{\mathrm{geom},\mathcal{F}}$ is infinite. Then the following statements hold.*

(i) *Suppose that $AB_1 \ldots B_r$ is even. Then $G^\circ_{\mathrm{geom},\mathcal{F}} = \mathrm{SL}_{A-1}$.*
(ii) *Suppose that $AB_1 \ldots B_r$ is odd. Then $G_{\mathrm{geom},\mathcal{F}} = \mathrm{Sp}_{A-1}$.*

Proof. If $k = 1$, then the result follows from Theorems 10.2.4 of 10.3.21 of [KT6]. Hence we will assume $r \geq 2$. Since $\gcd(A, B_1, \ldots, B_r) = 1$, there must be some i such that

$$2 \nmid C := \gcd(A, B_i).$$

Now if $\mathcal{F}(A, B_i, \mathbb{1})$ has infinite monodromy group, then we are done by Theorem 6.7.

It remains to consider the case in which $\mathcal{F}(A, B_i, \mathbb{1})$ has finite geometric monodromy group G_1. By Theorem 5.4(ii), we may assume that

$$(A/C, B_i/C) \neq (3, 1). \tag{6.9.1}$$

Let $G := G_{\mathrm{geom},\mathcal{F}}$. Applying Theorem 2.4 (with its $f(x)$ taken to be x^A, and its $b_1, \ldots, b_n$ taken to be $\{1, B_1, \ldots, B_{k-1}\}$), we see that $\mathcal{F}$ has

$$M_{2,2} = \limsup_{\#L \to \infty} \frac{\#\Sigma(L)}{(\#L)^2},$$

where Σ is the locus $\Sigma_1 = \Sigma_A = \Sigma_{B_1} = \ldots = \Sigma_{B_{k-1}} = 0$.

(b) Let p denote the characteristic of $\mathcal{F}$, and consider the case where $(A, B_r) = (p^n + 1, 1)$ for some $n \in \mathbb{Z}_{\geq 1}$. According to [KT6, Theorem 11.2.3], when $A = p^n + 1$, the local system $\mathcal{F}(A, B_1, \ldots, B_r, \mathbb{1})$ in characteristic $p \nmid AB_1 \ldots B_r$ can have finite G_{geom} only in the "van-der-Geer–van-der-Vlugt" situations, that is when $B_j = p^{m_j} + 1$ for $1 \leq j \leq r-1$, and either $B_r = p^{m_r} + 1$ with $m_r \geq 0$, or $B_r = 1$.

We apply Proposition 3.5 to $\mathcal{F}$. Suppose $p = 2$; in particular, $2 \nmid AB_1 \ldots B_r$. In the case of 3.5(b) we have $M_{2,2} = 3$ and hence $G = \mathrm{Sp}_{A-1}$. In the case of 3.5(d), which is "vdG-vdV", G is finite.

Suppose $p > 2$. In the case of 3.5(a), we have $M_{2,2} = 2$, and hence $G^\circ = \mathrm{SL}_{A-1}$. In the case of 3.5(c), which is again "vdG-vdV", G is finite.

(c) In the rest of the proof, we will assume that

$$\text{(6.9.2)} \qquad \text{If } A-1 \text{ is a } p\text{-power then } B_r \neq 1.$$

Moreover, using [KT6, Theorem 11.2.3], we may assume that some B_j is neither 1 nor a 2-power plus one when $p = 2$. Replacing B_i by this B_j, we may furthermore assume that

$$\text{(6.9.3)} \qquad \text{If } p = 2 \text{ and } A-1 \text{ is a 2-power then } B_i - 1 \text{ is not a 2-power.}$$

Let V denote the underlying representation of G, and apply Theorems 10.3.14 and 11.2.4 of [KT6] to G_1.

Suppose $C > 1$. Then, since C is odd, we are in case (iii) of [KT6, Theorem 11.2.4]. In particular, $V|_{G_1}$ is a sub-representation of the total Weil representation of $\mathrm{SU}_n(q)$ that contains the submodule $\mathcal{F}(A/C, B_i/C, \mathbb{1})$ of dimension $(q^n - q)/(q+1)$, for an odd integer $n \geq 3$ and a power $q = p^f$. Furthermore, $C|(q+1)$ by [KT6, Corollary 11.2.8(i)], and this rules out the possibility $(n, q) = (3, 3)$. If moreover $(n, q) = (3, 2)$, then we have $(A/C, B_i/C) = (3, 1)$, contrary to (6.9.1). Hence $(n, q) \neq (3, 2)$. Thus we fulfill hypothesis (b) of Theorem 6.8.

Suppose $C = 1$. Then [KT6, Theorem 11.2.4] implies that $\mathcal{F}(A, B_i, \mathbb{1})$ is as described in Theorems 10.2.6 and 10.3.13 of [KT6]. Next, assumption (6.9.1) rules out possibility (iv) of [KT6, Theorem 10.2.6], and assumption (6.9.2) rules out possibility (iii) of [KT6, Theorem 10.3.13]. Furthermore, in case (ii) of [KT6, Theorem 10.26] we have $(n, q) \neq (3, 2)$ because $A \geq 7$. Thus G_1 satisfies the hypothesis of Theorem 6.8 when $C = 1$ as well.

It follows that the semisimple group $G^\circ = G^\circ_{\mathrm{geom},\mathcal{F}}$ satisfies one of the conclusions of Theorem 6.8. In particular, $G^\circ > G_1$ acts irreducibly on V. Hence, by Proposition 6.4, $V|_{G^\circ}$ is not self-dual in case (i). Next we observe that none of the possibilities (ii) and (iv) of Theorem 6.8 cannot occur. Indeed, in the case of 6.8(ii) we have $(D, p, G_1, C) = (32, 2, \mathrm{SU}_5(2), 3)$. In such a case, by [KT6, Theorem 11.2.4], $A = 33$ and $B_i \in \{3, 9\}$, which is forbidden by (6.9.3). in the case of 6.8(iv) we have $(D, p, G_1, C) = (27, 3, \mathrm{SL}_2(27), 2)$, which is ruled out since C is odd.

Suppose G° satisfies Theorem 6.8(i), that is, $G^\circ = \mathrm{SL}(V)$, $\mathrm{Sp}(V)$, or $\cong \mathrm{SO}(V)$. In case (i), $V|_{G^\circ}$ is not self-dual, so we must have $G^\circ = \mathrm{SL}_D$. In case (b), V is symplectic self-dual, so $G^\circ = \mathrm{Sp}_D$.

Suppose G° satisfies Theorem 6.8(iii). Here $A = 8$, so $V|_{G^\circ}$ is not self-dual, contradicting the fact that the 7-dimensional module of G_2 is self-dual.

Finally, we consider the case when G° satisfies Theorem 6.8(v). Then we have $A = 57$, $C = 1$, $G_1 = \mathrm{PSU}_3(8)$, and Theorems 10.2.4 and 10.3.21 of [KT6] imply that $p = 2$ and $B_i = 1$ (and so $i = k$). As $p = 2$, all B_j are odd and hence $G \leq \mathrm{Sp}_{56}$. We will derive a contradiction by showing that $G = \mathrm{Sp}_{56}$ in this case. Indeed, recalling $k \geq 2$, we have that $B_1 > 1 = B_i$ and $\gcd(A, B_1)$ is odd. Replacing (A, B_i) by (A, B_1), we have $G^\circ = \mathrm{Sp}_{56}$ by the already established result. ☐

Finally, we remove the restriction $A \geq 7$ in Theorem 6.9:

Theorem 6.10. *Consider the local system $\mathcal{F} := \mathcal{F}(A, B_1, \ldots, B_r B_r, \mathbb{1})$ with $r \geq 1$ subject to* (4.0.1). *Suppose that $3 \leq A \leq 6$ and that $G_{\mathrm{geom},\mathcal{F}}$ is infinite. Then the following statements hold.*

(i) *Suppose that $AB_1 \ldots B_r$ is even. Then $G^\circ_{\mathrm{geom},\mathcal{F}} = \mathrm{SL}_{A-1}$.*
(ii) *Suppose that $AB_1 \ldots B_r$ is odd. Then $G_{\mathrm{geom},\mathcal{F}} = \mathrm{Sp}_{A-1}$.*

Proof. Denote $G := G_{\mathrm{geom},\mathcal{F}}$. If $k = 1$, then the result follows from Theorems 10.2.4 and 10.3.21 of [KT6]. Also, if $A = 3$, then $G^\circ \leq \mathrm{GL}_2$ is a semisimple algebraic group, whence $G^\circ = \mathrm{SL}_2$. Henceforth we assume

$$\text{(6.10.1)} \qquad k \geq 2, \ 4 \leq A \leq 6.$$

Suppose that for some i we have $A = 2B_i$ or $A = 3B_i$. In the latter case we have $A = 6$ because of (6.10.1). Hence Theorem 3.7 implies that $M_{2,2} = 2$ in both cases, when $G^\circ = \mathrm{SL}_{A-1}$ by Larsen's Alternative.

Next suppose that $B_1 = A - 1$; in particular $2|AB_1$. If $\mathcal{F}(A, B_1, \mathbb{1})$ has infinite geometric monodromy group H, then $H^\circ = \mathrm{SL}_{A-1}$ by [KT6, Theorem 10.3.21(i)]. As $\mathcal{F}(A, B_1, \mathbb{1})$ is a pullback of $\mathcal{F}$, it follows that $G^\circ = \mathrm{SL}_{A-1}$. If $\mathcal{F}(A, B_1, \mathbb{1})$ has finite geometric monodromy group, then $(A, B_1, p) = (5, 4, 3)$ by [KT6, Theorem 10.3.13]. In this case we have $\{B_2, \dots, B_r\} \subseteq \{1, 2\}$, and G is finite by [KT6, Theorem 11.2.3(vii)].

We now assume that

$$B_i \neq A - 1, A/2, A/3$$

and analyze the remaining cases.

(a) Suppose $A = 4$. Then $B_i \neq 2, 3$ and so $k < 2$, contrary to (6.10.1).

(b) Suppose $A = 5$. First we consider the case that $B_i = 2$ for some i, and let H denote the geometric monodromy group of $\mathcal{F}(A, B_i, \mathbb{1})$. If H is infinite, then $H^\circ = \mathrm{SL}_{A-1}$ by [KT6, Theorem 10.3.21(i)], whence $G^\circ = \mathrm{SL}_{A-1}$. If H is finite, then $(H, p) = (\mathrm{Sp}_4(3), 3)$ or $(2\mathsf{A}_7, 7)$ by [KT6, Theorem 10.3.13]. In both cases we have $M_{2,2}(H) = 2$, whence $M_{2,2}(\mathcal{F}) = 2$ and $G^\circ = \mathrm{SL}_4$.

In the remaining case, $B_i \neq 2, 4$, so $k \geq 2$ forces $(A, B_1, \dots, B_r) = (5, 3, 1)$ and $p \neq 3, 5$. If $p = 2$ then G is finite by [KT6, Theorem 11.2.3(ii)]. If $p > 5$, then $\mathcal{F}(5, 3, \mathbb{1})$ has Sp_4 as its G_{geom} by [KT6, Lemma 10.3.20]. As $\mathcal{F}$ is symplectic self-dual, we conclude that $G = \mathrm{Sp}_4$.

(c) Finally, assume $A = 6$. Then $B_i \neq 2, 3, 5$, so $k \geq 2$ forces $(A, B_1, \dots, B_r) = (6, 4, 1)$ and $p \geq 5$. Let H denote the geometric monodromy group of $\mathcal{F}(6, 1, \mathbb{1})$. If in addition $p \neq 5, 11$, then H is infinite by [KT6, Theorem 10.2.6], whence $H = \mathrm{SL}_5$ by [KT6, Theorem 10.2.4(i)], and we conclude that $G^\circ = \mathrm{SL}_5$.

Suppose $p = 5$. Then $M_{2,2} = 2$ by Proposition 3.5, whence $G^\circ = \mathrm{SL}_5$.

In the remaining case we have $p = 11$. Recall that G acts irreducibly on the underlying representation $V = \mathbb{C}^5$, of prime dimension $D = 5$. Since $G^\circ \neq 1$ is semisimple; in particular non-abelian, it must have some simple submodule of dimension > 1 on V, and so Clifford's theorem implies that G° is irreducible on V as well. Now $D = 5$ being prime forces G° to be simple, of rank ≤ 4. An inspection of [Lu] or use of Gabber's theorem [Ka2, 1.8] shows that either $G^\circ = \mathrm{SL}_5$, or $G^\circ = \mathrm{SL}_2$, or $G^\circ = \mathrm{SO}_5$. In the latter two cases, $V|_{G^\circ}$ is self-dual. Note that $G/\mathbf{C}_G(G^\circ) \hookrightarrow \mathrm{Out}(G^\circ) = 1$ and $\mathbf{C}_G(G^\circ)$ is abelian by Schur's lemma. So G/G° is abelian, and hence the simple $H = \mathrm{PSL}_2(11)$ must embed in G°. But this is a contradiction, since $V|_H$ is non-self-dual. Hence we conclude that $G^\circ = \mathrm{SL}_5$. (Alternatively, by considering the pullback $\mathcal{F}(6, 4, \mathbb{1})$ of $\mathcal{F}$ and its decomposition as $\mathcal{F}(3, 2, \mathbb{1}) \oplus \mathcal{F}(3, 2, \chi_2)$, we see by that $G^\circ_{\mathrm{geom}, \mathcal{F}(6,4,\mathbb{1})}$ projects onto SL_3. This rules out the possibilities SL_2 and SO_5 for G°). □

7. Multiparameter local systems with infinite monodromy. II

In this section, we are given a (possibly trivial) multiplicative character χ of (the multiplicative group of) a finite extension $L/\mathbb{F}_p$. We consider a local system $\mathcal{F}_\chi$ on $\mathbb{A}^r/L$ defined as follows. We are given a list of integers

$$A > B_1 > \ldots > B_r \geq 1, \quad p \nmid A \prod_i B_i, \ \gcd(A, B_1, \dots, B_r) = 1.$$

as in (4.0.1). For E/L a finite extension, and $(t_1, \dots, t_k) \in E^k$,

$$\mathrm{Trace}(\mathrm{Frob}_{(t_1,\dots,t_k),E} | \mathcal{F}_\chi) = (-1/\sqrt{\#L}) \sum_{x \in L} \psi_E(x^A + \sum_{i=2}^{k} t_i x^{B_i}) \chi_E(x).$$

Here we make a choice of $\sqrt{p} \in \overline{\mathbb{Q}_\ell}$, and define $\sqrt{\#L} := \sqrt{p}^{\deg(L/\mathbb{F}_p)}$. We adopt the usual convention that $\chi(0) = 0$ if $\chi \neq \mathbb{1}$, but $\mathbb{1}(0) = 1$. We will name this $\mathcal{F}_\chi$ as

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

when confusion about "which $\mathcal{F}_\chi$?" is possible. Recall from [KT5, 2.6] that such an $\mathcal{F}_\chi$ is geometrically irreducible.

In the previous sections, we determined $G^\circ_{\mathrm{geom},\mathcal{F}_\chi}$ for any $\mathcal{F}_\mathbb{1}$ whose G_{geom} is infinite. We now do the same for any $\mathcal{F}_\chi$ with $\chi \neq \mathbb{1}$ whose $G_{\mathrm{geom},\mathcal{F}_\chi}$ is infinite.

We begin with the "easy" case.

Theorem 7.1. *Let χ be nontrivial. Suppose that for given data*

$$A > B_1 > \ldots > B_r \geq 1, \quad p \nmid A \prod_i B_i, \; \gcd(A, B_1, \ldots, B_r) = 1,$$

with $A \geq 3$, $k \geq 2$, and both $\mathcal{F}_\mathbb{1}$, $\mathcal{F}_\chi$ have infinite G_{geom}. Then we have the following results.

(i) *If $A \prod_i B_i$ is even, then $G^\circ_{\mathrm{geom},\mathcal{F}_\chi} = \mathrm{SL}_A$.*
(ii) *If $A \prod_i B_i$ is odd, $p \neq 2$, and χ is the quadratic character, then $G_{\mathrm{geom},\mathcal{F}_\chi} = \mathrm{SO}_A$.*
(iii) *If $A \prod_i B_i$ is odd, and $\chi^2 \neq \mathbb{1}$, then $G^\circ_{\mathrm{geom},\mathcal{F}_\chi} = \mathrm{SL}_A$.*

Proof. If $A \prod_i B_i$ is even and $G_{\mathrm{geom},\mathcal{F}_\mathbb{1}}$ is infinite, then $G^\circ_{\mathrm{geom},\mathcal{F}_\mathbb{1}} = \mathrm{SL}_{A-1}$ by Theorems 6.9 and 6.10. Therefore $M_{2,2}(\mathcal{F}_\mathbb{1}) = 2$. By Theorem 2.4, we have $M_{2,2}(\mathcal{F}_\chi) \leq M_{2,2}(\mathcal{F}_\mathbb{1})$. But for any local system of rank > 1, $M_{2,2} \geq 2$. Therefore $M_{2,2}(\mathcal{F}_\chi) = 2$. Given that $G_{\mathrm{geom},\mathcal{F}_\chi}$ is infinite, we must have $G^\circ_{\mathrm{geom},\mathcal{F}_\chi} = \mathrm{SL}_A$ by Larsen's Alternative [Ka3, 1.1.6],

If $A \prod_i B_i$ is odd and $G_{\mathrm{geom},\mathcal{F}_\mathbb{1}}$ is infinite, then $G_{\mathrm{geom},\mathcal{F}_\mathbb{1}} = \mathrm{Sp}_{A-1}$. Therefore $M_{2,2}(\mathcal{F}_\mathbb{1}) = 3$. Therefore $M_{2,2}(\mathcal{F}_\chi) \leq 3$, so either $M_{2,2}(\mathcal{F}_\chi) = 2$ or $M_{2,2}(\mathcal{F}_\chi) = 3$. If p is odd and χ is the quadratic character, then $\mathcal{F}_\chi$ is orthogonally self-dual (being self-dual because its traces are real, and being geometrically irreducible of odd rank). Thus we have an a priori inclusion $G_{\mathrm{geom},\mathcal{F}_\chi} \leq \mathrm{O}_A$. Given that $G_{\mathrm{geom},\mathcal{F}_\chi}$ is infinite, we must have $G^\circ_{\mathrm{geom},\mathcal{F}_\chi} = \mathrm{SO}_A$ by Larsen's Alternative [Ka3, 1.1.6]. Thus we have $\mathrm{SO}_D \leq G \leq \mathrm{O}_D$. But $\det(\mathcal{F})$ is lisse on $\mathbb{A}^k$ of order dividing 2, so must be geometrically trivial as $p \neq 2$.

Finally, we must treat the case when $A \prod_i B_i$ is odd, $G_{\mathrm{geom},\mathcal{F}_\mathbb{1}} = \mathrm{Sp}_{A-1}$, and $\chi^2 \neq \mathbb{1}$. When $\chi^2 \neq \mathbb{1}$ and A and all B_i are odd, we have $M_{2,2}(\mathcal{F}_\chi) < M_{2,2}(\mathcal{F}_\mathbb{1})$ by Theorem 2.4. Therefore $M_{2,2}(\mathcal{F}_\chi) = 2$ in this case, and we have $G^\circ_{\mathrm{geom},\mathcal{F}_\chi} = \mathrm{SL}_A$ by Larsen's Alternative [Ka3, 1.1.6]. ☐

It remains to treat cases with χ nontrivial in which $\mathcal{F}_\mathbb{1}$ has finite G_{geom} but $\mathcal{F}_\chi$ has infinite G_{geom}.

Theorem 7.2. *Consider the case of p arbitrary, $q = p^f$ for some $f \geq 1$, $r \geq 2$,*

$$n > m_1 > \ldots > m_{r-1} \geq 0$$

integers with $\gcd(n, m_1, \ldots, m_{r-1}) = 1$ and $\mathcal{F}_\chi$, $\chi \neq \mathbb{1}$, formed with

$$(A, B_1, \ldots, B_r) = (q^n + 1, q^{m_1} + 1, \ldots, q^{m_{r-1}} + 1, 1).$$

Then $G^\circ_{\mathrm{geom},\mathcal{F}_\chi} = \mathrm{SL}_A$.

Proof. The only purpose of the gcd hypothesis is to insure that our choice of q is correct. The fact that $B_r = 1$ insures the geometric irreducibility. We compute $M_{2,2}(\mathcal{F}_\mathbb{1})$ as the number of geometrically irreducible components of dimension 2 of the intersection $\Sigma_{A,B_1,\ldots,B_r}$ of the Fermat surfaces

$$\Sigma_d : x^d + y^d - z^d - w^d = 0$$

as d runs over the exponents $(A, B_1, \ldots, B_r)$. We have the obvious inclusion

$$\Sigma_{A,B_1,\ldots,B_r} \subseteq \Sigma_{A,B_r} = \Sigma_{1+q^n,1}.$$

Using the equation $\Sigma_1 = x + y - z - w = 0$, we may solve for w as $w = x + y - z$, and rewrite $\Sigma_{1+q^n,1}$ as the locus in the $\mathbb{A}^3$ of x, y, z of

$$x^{1+q^n} + y^{1+q^n} - z^{1+q^n} - (x + y - z)^{1+q^n} = 0.$$

Let us temporarily write

$$Q := q^n.$$

According to [KT6, Lemma 12.3.2], we have the following factorization in $\mathbb{F}_{Q^2}[x, y, z]$:

$$x^{1+Q} + y^{1+Q} - z^{1+Q} - (x + y - z)^{1+Q} = -(y - z) \prod_{A \in \mathbb{F}_{Q^2},\ A^Q = -A} (x + Ay - (A + 1)z).$$

In the special case $p = 2$, we get the identity in $\mathbb{F}_Q[x, y, z]$

(7.2.1) $$x^{1+Q} + y^{1+Q} - z^{1+Q} - (x + y - z)^{1+Q} = (y - z) \prod_{A \in \mathbb{F}_Q} (x + Ay - (A + 1)z).$$

Going back to x, y, z, w, these linear factors give the following $Q + 1$ affine planes in $\mathbb{A}^4$:

(7.2.2) $$(y = z, w = x),\ (x = z, w = y)$$

together with the $Q - 1$ planes P_A, one for each $A \in \mathbb{F}_{Q^2}$ with $A^{Q-1} = -1$, of equation

(7.2.3) $$P_A : (x = -Ay + (A + 1)z, w = -(A - 1)y + Az).$$

By [KT6, Theorem 11.2.3], $G_{\mathrm{geom},\mathcal{F}_\chi}$ is infinite, so it suffices to show that $M_{2,2}(\mathcal{F}_\chi) = 2$. The geometrically irreducible components of $\Sigma_{A,B_1,\ldots,B_r}$ are then among the planes above. So it suffices to show that for each $A \in \mathbb{F}_{Q^2}$ with $A^{Q-1} = -1$, the limsup over extensions E of L dies:

(7.2.4) $$\limsup_{E/L,\ \#E \to \infty} \frac{1}{(\#E)^2} \sum_{(x,y,z,w) \in P_A(E)} \chi(xy/zw) = 0.$$

We readily calculate on P_A, with coordinates y, z,

$$\begin{aligned} xy/zw &= (-Ay^2 + (A + 1)yz)/(-(A - 1)yz + Az^2) \\ &= (-A + (A + 1)z/y)/(-(A - 1)z/y + A(z/y)^2) \\ &= (-A + (A + 1)z/y)/((z/y)(-(A - 1) + A(z/y)). \end{aligned}$$

This is an expression in the quantity

$$T := z/y,$$

namely

$$(-A + (A + 1)T)/(T(-(A - 1) + AT)).$$

Thus

$$\sum_{(x,y,z,w) \in P_A(E)} \chi(xy/zw) = (\#E - 1) \sum_{T \in L} \chi(-A + (A + 1)T)\overline{\chi}(T(-(A - 1) + AT)).$$

So it suffices to show that for every $A \in \mathbb{F}_{Q^2}$ with $A^{Q-1} = -1$, this sum is $O(\sqrt{\#E})$.

Suppose first that p is odd. Then $Q + 1$ is even, hence A is neither 1 nor -1. Then the local system

$$\mathcal{L}_{\chi(-A+(A+1)T)} \otimes \mathcal{L}_{\overline{\chi}(T(-(A-1)+AT))}$$

is lisse of rank one on $\mathbb{P}^1 \setminus \{0, \infty, A/(A+1), A/(A-1)\}$, extended by direct image across the missing points, at each of which the ramification is tame but nontrivial. Then by the usual Weil estimate, this sum has absolute value at most $2\sqrt{\#E}$.

Suppose next that $p = 2$. Then for $A \neq 1$, the above argument gives the same bound $2\sqrt{\#E}$. In the case $A = 1$, local system is just $\mathcal{L}_{\overline{\chi}(T^2)} = \mathcal{L}_{\overline{\chi}^2(T)}$, But χ, being nontrivial in characteristic 2, has odd order, so $\chi^2 \neq \mathbb{1}$, and in this case the sum vanishes. ☐

Theorem 7.3. *Suppose given $r \geq 2$ and integers*

$$n > m_1 > \ldots > m_r \geq 0$$

with $\gcd(n, m_1, \ldots, m_r) = 1$ and $2|n \prod_i m_i$. Let p be a prime, $q = p^f$ with $f \geq 1$, $\kappa := \gcd(p-1, 2)$, and form the data

$$(A, B_1, \ldots, B_r) := ((q^n + 1)/\kappa, (q^{m_1} + 1)/\kappa, \ldots, (q^{m_r} + 1)/\kappa).$$

If $p = 2$, make the further assumption that $m_r \geq 1$. Then for $\mathcal{F} := \mathcal{F}(A, B_1, \ldots, B_r)$ and any χ with $\chi^\kappa \neq \mathbb{1}$, we have $G^\circ_{\mathrm{geom}, \mathcal{F}_\chi} = \mathrm{SL}_A$.

Proof. Because $\gcd(n, m_1, \ldots, m_r) = 1$ and $2|n \prod_i m_i$, there is some m_i whose parity is different from that of n: i.e., if n is even the gcd condition forces some m_i to be odd, and if n is odd, the evenness condition forces some m_i to be even. Pick one such $m := m_i$ such that n and m have opposite parities.

Next we show that

$$d := \gcd((q^n + 1)/\kappa, (q^m + 1)/\kappa) = 1. \tag{7.3.1}$$

Indeed, $e := \gcd(n, m)$ is odd as n and m_i have different parity. Let $k \in \{n, m\}$ be the one that is even. Then $q^k \equiv 1 \pmod 4$ when $p > 2$, and so $(q^k + 1)/\kappa$ is always odd and hence $2 \nmid d$. Suppose $d > 1$, and let $\ell > 2$ be any prime divisor of d. Then ℓ divides

$$\gcd(q^{2n} - 1, q^{2m_i} - 1) = q^{2e} - 1,$$

and so $\ell|(q^e - 1)$ or $\ell|(q^e + 1)$. In the former case, as $e|n$ and $ell > 2$ we have $\ell|(q^n - 1)/\kappa$ and so $(q^n + 1)/\kappa \equiv 2/\kappa \pmod \ell$, a contradiction. In the latter case, as $2 \nmid e$ and $2|k$ we have $k = 2le$ for some $l \in \mathbb{Z}_{\geq 1}$. Now $\ell|(q^{2e} - 1)$ and $(q^{2e} - 1)|(q^{2le} - 1)$, so we again have $(q^k + 1)/\kappa \equiv 2/\kappa \pmod \ell$, a contradiction.

By [KT6, Theorem 11.2.3], $G_{\mathrm{geom}, \mathcal{F}(A, B_i, \chi)}$ is infinite. Using (7.3.1) and applying Theorems 10.2.4 and 10.3.21 of [KT6], we obtain that $G^\circ_{\mathrm{geom}, \mathcal{F}(A, B_i, \chi)} = \mathrm{SL}_A$. Since $\mathcal{F}(A, B_i, \chi)$ is a pullback of $\mathcal{F}_\chi$, we conclude that $G^\circ_{\mathrm{geom}, \mathcal{F}_\chi} = \mathrm{SL}_A$. ☐

We now begin preparation for the SU case. We begin with an "axiomatic" result, which reveals the simple underlying mechanism.

Theorem 7.4. *Let p be a prime $A > B \geq 1$ a pair of odd, prime to p integers, $C := \gcd(A, B)$. Write $(A, B) ;= (A_0 C, B_0 C)$. Suppose that χ is a multiplicative character with $\chi^2 \neq \mathbb{1}$, with the following property: For every multiplicative character ρ with $\rho^C = \chi$, the local system $\mathcal{F}(A_0, B_0, \rho)$ has infinite G_{geom}.* [Indeed, it has $G_{\mathrm{geom}} = \mathrm{SL}_{A_0}$, in view of Theorems 10.2.4 and 10.3.21 of [KT6]. Notice that A_0, B_0 are both odd, so $A_0 - B_0 \geq 2$.] *Then*

$$\mathcal{F}(A, B, \chi) = \bigoplus_{\rho : \rho^C = \chi} \mathcal{F}(A_0, B_0, \rho)$$

has

$$G_{\mathrm{geom}, \mathcal{F}(A, B, \chi)} = \prod_{\rho : \rho^C = \chi} \mathrm{SL}_{A_0}.$$

Proof. For each ρ, pick a multiplicative character σ_ρ with

$$\sigma_\rho^{A_0} = \rho.$$

Then $\bigoplus_{\rho:\rho^C=\chi} \mathcal{F}(A_0, B_0, \rho)$ is geometrically isomorphic to the Kummer $[A_0]^\star$ pullback of the direct sum of hypergeometric sheaves

$$\bigoplus_{\rho:\rho^C=\chi} \mathcal{H}_{big,A_0,B_0,\sigma_\rho}.$$

Each constituent hypergeometric sheaf is of type (A_0, B_0), of odd rank $A_0 \geq 3$. As Kummer pullback does not change G°_{geom}, we see that each constituent hypergeometric sheaf has its $G^\circ_{\text{geom},\mathcal{H}} = \mathrm{SL}_{A_0}$. So it suffices to show that

$$G^\circ_{\text{geom},\bigoplus_{\rho:\rho^C=\chi}\mathcal{H}_{big,A_0,B_0,\sigma_\rho}} = \prod_{\rho:\rho^C=\chi} \mathrm{SL}_{A_0}.$$

For this, we apply Goursat-Kolchin-Ribet in the form [Ka2, 8.11.7.2]. We must show that for $\rho_1 \neq \rho_2$, there is no Kummer sheaf $\mathcal{L}_\Lambda$ such that $\mathcal{L}_\Lambda \otimes \mathcal{H}_{big,A_0,B_0,\sigma_{\rho_1}}$ is geometrically isomorphic to either $\mathcal{H}_{big,A_0,B_0,\sigma_{\rho_2}}$ or to its dual. [Notice that because $A_0 - B_0$ is even, the dual of $\mathcal{H}_{big,A_0,B_0,\sigma_{\rho_2}}$ is (with the same ψ) geometrically isomorphic to $\mathcal{H}_{big,A_0,B_0,\overline{\sigma_{\rho_2}}}$.]

We argue by contradiction. Suppose that

$$\mathcal{L}_\Lambda \otimes \mathcal{H}_{big,A_0,B_0,\sigma_{\rho_1}} \cong \mathcal{H}_{big,A_0,B_0,\sigma_{\rho_2}}.$$

Looking at the $I(0)$-representations of the two hypergeometrics, which are each $\mathsf{Char}(A_0)$, we first conclude that $\Lambda^{A_0} = \mathbb{1}$. From the definition of $\mathcal{H}_{big,A_0,B_0,\sigma_{\rho_1}}$, cf. [KT4, §3], we see that

$$\mathcal{L}_\Lambda \otimes \mathcal{H}_{big,A_0,B_0,\sigma_{\rho_1}} \cong \mathcal{H}_{big,A_0,B_0,\sigma_{\rho_1}/\Lambda^{B_0}}.$$

So if the purported isomorphism holds, then $\sigma_{\rho_1}/\Lambda^{B_0} = \sigma_{\rho_2}$. But their A_0 powers are ρ_1 and ρ_2 respectively, (because $\Lambda^{A_0} = \mathbb{1}$). But $\rho_1 \neq \rho_2$, the desired contradiction.

If instead we have

$$\mathcal{L}_\Lambda \otimes \mathcal{H}_{big,A_0,B_0,\sigma_{\rho_1}} \cong \mathcal{H}_{big,A_0,B_0,\overline{\sigma_{\rho_2}}}.$$

then we get the equality $\sigma_{\rho_1}/\Lambda^{B_0} = \overline{\sigma_{\rho_2}}$. But their A_0 powers are ρ_1 and $\overline{\rho_2}$. These cannot be equal, because their C powers are χ and $\overline{\chi}$ respectively, which are not equal, precisely because $\chi^2 \neq \mathbb{1}$. □

With this "axiomatic" result in hand, we now turn to the SU case directly. In preparation, observe that for any prime power $q > 1$ and any odd integer $n \geq 1$, the ratio $(q^n + 1)/(q + 1)$ is odd, indeed for $n \geq 3$ it is 1 mod $q(q-1)$.

Proposition 7.5. *Let p be a prime, $q = p^f$ with $f \geq 1$, $r \geq 2$, and*

$$n > m_1 > \ldots > m_r \geq 1$$

a sequence of odd integers with $\gcd(n, m_1, \ldots, m_r) = 1$. *Define*

$$(A, B_1, \ldots, B_r) := ((q^n + 1)/(q + 1), (q^{m_1} + 1)/(q + 1), \ldots, (q^{m_r} + 1)/(q + 1)).$$

Consider $\mathcal{F} := \mathcal{F}(A, B_1, \ldots, B_r, \chi)$ where $\chi^{q+1} \neq \mathbb{1}$. We have the following results.

(i) *If* $\gcd(n, m_i) = 1$ *for some i, then $G^\circ_{\text{geom},\mathcal{F}} = \mathrm{SL}_A$.*

(ii) *In general, with $c := \gcd(n, m_i)$ and $C := (q^c + 1)/(q + 1)$ we have*

$$G_{\text{geom},\mathcal{F}(A,B_i,\chi)} = \prod_{\rho:\rho^C=\chi} \mathrm{SL}_{A/C},$$

In particular, $G_{\text{geom},\mathcal{F}(A,B_i,\chi)}$ acts on $\mathcal{F}$ with C simple summands, none of which is self-dual and any two of which are neither isomorphic nor dual to each other.

Proof. The first assertion is easy, since $\gcd(A, B_i) = 1$ and so already the pullback $\mathcal{F}(A, B_i, \chi)$ has $G_{\rm geom} = {\rm SL}_A$ by Theorems 10.2.4 and 10.3.21 of [KT6]. For the second assertion, with $c = \gcd(n, m_i)$ and $Q = q^c$ we have

$$C = \gcd(A, B_i) = (Q+1)/(q+1), \quad (A, B_i) = (A_0C, B_0C),$$

where

$$A_0 = (Q^{n/c} + 1)/(Q+1), B_0 = (Q^{m_i/c} + 1)/(Q+1),$$

It remains only to remark that if $\chi^{q+1} \neq \mathbb{1}$ and $\rho^C = \chi$, then $\rho^{Q+1} = \rho^{C(q+1)} \neq \mathbb{1}$. Hence $\mathcal{F}(A_0, B_0, \rho)$ indeed has infinite $G_{\rm geom}$. Now if $p > 2$ then $2|(q+1)$ and so $\chi^2 \neq \mathbb{1}$, and if $p = 2$ then $\chi \neq \mathbb{1}$ implies $\chi^2 \neq \mathbb{1}$. The formula for $G_{{\rm geom},\mathcal{F}(A,B_i,\chi)}$ then follows from Theorem 7.4. The last statement also follows since each of the C simple summands $\mathcal{F}(A_0, B_0, \rho)$ is acted on by exactly one of the C simple factors ${\rm SL}_{A_0}$ as on its natural module (or its dual), and $A_0 \geq Q^2 - Q + 1 \geq 3$. □

Now we can complete the SU case:

Theorem 7.6. *Let p be a prime, $q = p^f$ with $f \geq 1$, $r \geq 2$, and*

$$n > m_1 > \ldots > m_r \geq 1$$

a sequence of odd integers with $\gcd(n, m_1, \ldots, m_r) = 1$. *Define*

$$(A, B_1, \ldots, B_r) := ((q^n + 1)/(q+1), (q^{m_1} + 1)/(q+1), \ldots, (q^{m_r} + 1)/(q+1)).$$

Consider $\mathcal{F} := \mathcal{F}(A, B_1, \ldots, B_r, \chi)$ with any χ where $\chi^{q+1} \neq \mathbb{1}$. Then $\mathcal{F}$ has $G^\circ_{{\rm geom},\mathcal{F}} = {\rm SL}_A$.

Proof. (a) Let $G := G_{{\rm geom},\mathcal{F}}$. If there is some i such that $\gcd(n, m_i) = 1$, then we are done by Proposition 7.5(i). Hence we may assume that

$$c_i := \gcd(n, m_i) > 1 \tag{7.6.1}$$

for all i. Since $r \geq 2$ and $2 \nmid nm_1 \ldots m_r$, this implies that

$$n \geq 15, \;\; n/c \geq 3. \tag{7.6.2}$$

for $c := c_r$. (Indeed, if $n < 15$, then either n is a prime or $n = 9$. In the former case $\gcd(n, m_1) = 1$, and in the latter case, $\gcd(n, m_2) = 1$, both violating (7.6.1).)

We know by [KT5, 2.6] that $\mathcal{F}$ is geometrically irreducible, i.e. that G is an irreducible subgroup of ${\rm GL}_A = {\rm GL}(V)$ with $V := \mathcal{F}_{\overline{\eta}}$. By Proposition 7.5(ii), for each $1 \leq i \leq r$, G contains a semisimple subgroup

$$H_i \cong \bigl({\rm SL}_{(q^n+1)/(q^{c_i}+1)}\bigr)^{(q^{c_i}+1)/(q+1)}$$

of rank

$$\mathrm{R}_i = \frac{q^n - q^{c_i}}{q^{c_i}+1} \cdot \frac{q^{c_i}+1}{q+1} = \frac{q^n - q^{c_i}}{q+1}.$$

In particular,

$$\mathrm{R}_r = \frac{q^n - q^c}{q+1} \geq \frac{q^n - q^{n/3}}{q+1} > \frac{2A}{3}. \tag{7.6.3}$$

Furthermore, the H_i-module V is a direct sum of $(q^{c_i}+1)/(q+1)$ pairwise non-isomorphic simple summands, all of dimension

$$D_i := \frac{q^n + 1}{q^{c_i}+1}.$$

(b) Because $G^\circ \lhd G$, by Clifford's theorem we may express $V|_PG^\circ = n(\oplus_{j=1}^m W_j)$ as the sum of n copies each of pairwise non-isomorphic simple summands $W_1, \ldots, W_m$. Note that $G^\circ \geq H_i$ for all i. Now if $n > 1$, then some simple summand of $V|_{H_k}$ has multiplicity $\geq n$, contradicting the discussion in (a). Hence $n = 1$.

Next, the summands W_j are transitively permuted by G, so all have the same dimension

$$M = (q^n + 1)/m(q + 1).$$

Since $G^\circ \geq H_i$ and all simple summands of $V|_{H_i}$ have the same dimension D_i, we must have that $D_i|M$; equivalently, $(q^{c_i} + 1)/m(q + 1) \in \mathbb{Z}$ for all i. In turn, this implies that $m(q + 1)$ divides

$$\gcd\bigl(q^{c_1} + 1, q^{c_i} + 1, \ldots, q^{c_r} + 1\bigr) = q^e + 1,$$

where $e := \gcd(c_1, c_2, \ldots, c_r)$. As e divides $c_i = \gcd(n, m_i)$, we have e divides n and each m_i, and thus $e|\gcd(n, m_1, \ldots, m_r) = 1$. Thus $e = 1$ and so $m = 1$. We have shown that G° acts irreducibly on V.

(c) Recall from (7.6.3) that the semisimple group G° has rank $R \geq \mathrm{R}_r > 2A/3$. As shown in (b), G° acts irreducibly on V of dimension $A < 3R/2$, and

$$A = (q^n + 1)/(q + 1) \geq (2^{15} + 1)/3$$

by (7.6.2). Arguing as in part (a1) of the proof of Theorem 6.6, we conclude that G° is simple. The arguments in part (b) of the proof of Theorem 6.6, we then see that $G^\circ = \mathrm{SL}(V)$, $\mathrm{Sp}(V)$, or $\mathrm{SO}(V)$. In the two latter cases, the G°-module V is self-dual. Restricting to H_r, we see that some simple summand of the H_r-module V is either self-dual, or dual to another simple summand. This is however impossible by Proposition 7.5(ii). Hence $G^\circ = \mathrm{SL}_A$. □

Now we consider the remaining cases of an $\mathcal{F}_\chi$ on $\mathbb{A}^r/\overline{\mathbb{F}_p}$ with finite $G_{\mathrm{geom},\mathcal{F}_{\mathbb{1}}}$ and with $r \geq 2$. These remaining cases are listed in [KT6, Theorem 11.2.3]. They are

(i) $p = 2$, $r = 2$, $A = 13$, $B_1 = 3$, $B_2 = 1$, and $G = 2 \cdot G_2(4)$.
(ii) $p = 3$, $r = 2, 3$, $A = 7$, $\{B_1, \ldots, B_r\} \subseteq \{4, 2, 1\}$, and $G = 6_1 \cdot \mathrm{PSU}_4(3)$.
(iii) $p = 3$, $r = 2, 3$, $A = 5$, $\{B_1, \ldots, B_r\} \subseteq \{4, 2, 1\}$. Furthermore, $G = \mathrm{Sp}_4(3) \times 3$ if some B_i is 4, and $G = \mathrm{Sp}_4(3)$ otherwise.
(iv) $p = 5$, $A = 3$, $B_1 = 2$, $B_2 = 1$, and $G = \mathrm{SL}_2(5) \times 5$.

Each of these cases, with the exception of $\mathcal{F}(5, 2, 1)$ in characteristic $p = 3$, has the following property: for any $\chi \neq \mathbb{1}$, $\mathcal{F}_\chi$ has infinite G_{geom}. This is immediate from [KT6, Theorem 11.2.3], which lists all cases of an $\mathcal{F}_\chi$ with finite G_{geom}. In the exceptional case of $\mathcal{F} := \mathcal{F}(5, 2, 1)$ in characteristic $p = 3$, we have a Weil representation of degree 4 of $\mathrm{Sp}_4(3)$. In this case, $\mathcal{F}_{\chi_2}$ yields a Weil representation of degree 5 of $\mathrm{PSp}_4(3)$.

Theorem 7.7. *For any of the $\mathcal{F}$ listed above other than $\mathcal{F}(5, 2, 1)$ in characteristic $p = 3$, and any $\chi \neq \mathbb{1}$, $G^\circ_{\mathrm{geom},\mathcal{F}_\chi} = \mathrm{SL}_A$. In the exceptional case of $\mathcal{F}(5, 2, 1)$ in characteristic $p = 3$, the same is true for any χ with $\chi^2 \neq \mathbb{1}$.*

Proof. In cases (ii)–(iv), $G_{\mathrm{geom},\mathcal{F}_{\mathbb{1}}}$ has $M_{2,2} = 2$, whence the same holds for $\mathcal{F}_\chi$. As $G_{\mathrm{geom},\mathcal{F}_\chi}$ is infinite by the discussion preceding the theorem, we conclude $G^\circ_{\mathrm{geom},\mathcal{F}_\chi} = \mathrm{SL}_A$. In case (i), the pullback $\mathcal{F}(13, 3, \chi)$ has SL_{13} as its G_{geom} by Theorems 10.3.13 and 10.3.21 of [KT6], so we are done again. □

Now we can prove the first main result of the paper. Recall that local systems $\mathcal{F}(A, B_1, \ldots, B_r, \chi)$ with finite G_{geom} (and the corresponding G_{geom}) have been determined in [KT6, Theorem 11.2.3].

Theorem 7.8. *Consider the local system $\mathcal{F}_\chi := \mathcal{F}(A, B_1, \ldots, B_r, \chi)$ over $\mathbb{A}^r/\overline{\mathbb{F}_p}$ with $r \geq 1$ subject to (4.0.1), of dimension $D = A - 1$ if $\chi = \mathbb{1}$, and $D = A$ otherwise. Suppose that $D \geq 2$ and that $G := G_{\mathrm{geom},\mathcal{F}_\chi}$ is infinite. Then the following statements hold.*

(i) *If $AB_1 \dots B_r$ is even, then $G^\circ = \mathrm{SL}_D$.*
(ii) *If $AB_1 \dots B_r$ is odd and $\chi \neq \mathbb{1}, \chi_2$, then $G^\circ = \mathrm{SL}_D$.*
(iii) *If $AB_1 \dots B_r$ is odd and $\chi = \mathbb{1}$, then $G = \mathrm{Sp}_D$.*
(iv) *Suppose $AB_1 \dots B_r$ is odd, $p \neq 2$, and $\chi = \chi_2$. Then $G = \mathrm{SO}_D$, unless $(r, A, B_r) = (1, 7, 1)$, in which case we have $G = G_2$.*

Proof. If $k = 1$ and $A \geq 3$, then the result follows from Theorems 10.2.4 of 10.3.21 of [KT6]. If $A = 2$, then $\mathcal{F} = \mathcal{F}(2, 1, \chi)$, and $1 \neq G^\circ \leq \mathrm{GL}_2$ is semisimple, so $G^\circ = \mathrm{SL}_2$.

We next treat the cases $r \geq 2$ when $\mathcal{F}(A, B_1, \dots, B_r, \mathbb{1})$ has infinite G_{geom}. These cases result from Theorem 7.1.

Finally, assume that $r \geq 2$ and $\mathcal{F}(A, B_1, \dots, B_r, \mathbb{1})$ has finite G_{geom}. Applying [KT6, Theorem 11.2.3], we arrive at one of the possibilities considered in Theorems 7.2, 7.3, 7.6, and 7.7. ☐

We now consider the following variant. Given a finite field L of characteristic p, a multiplicative character χ of $L^\times$, and data $(A, B_1, \dots, B_r)$ subject to (4.0.1), we denote by $\mathcal{F}^\sharp(A, B_1, \dots, B_r, \chi)$ the local system on $(\mathbb{G}_m \times \mathbb{A}^r)/L$ whose trace function is given as follows: for E/L a finite extension, and $(s, t_1, \dots, t_r) \in E^\times \times E^r$,

$$\mathrm{Trace}(\mathrm{Frob}_{(s,t_1,\dots,t_r),E} | \mathcal{F}^\sharp(A, B_1, \dots, B_r, \chi)) = (-1/\sqrt{\#E}) \sum_{x \in E} (sx^A + \sum_i t_i x^{B_i}).$$

Theorem 7.9. *Consider $\mathcal{F}^\sharp_\chi := \mathcal{F}^\sharp(A, B_1, \dots, B_r, \chi)$ with $r \geq 1$ subject to (4.0.1), of dimension $D = A - 1$ if $\chi = \mathbb{1}$, and $D = A$ otherwise. Suppose that $D \geq 2$ and that $G := G_{\mathrm{geom}, \mathcal{F}^\sharp_\chi}$ is infinite. Then the following statements hold.*

(i) *If $AB_1 \dots B_r$ is even, then $G^\circ = \mathrm{SL}_D$.*
(ii) *If $AB_1 \dots B_r$ is odd and $\chi \neq \mathbb{1}, \chi_2$, then $G^\circ = \mathrm{SL}_D$.*
(iii) *If $AB_1 \dots B_r$ is odd and $\chi = \mathbb{1}$, then $G = \mathrm{Sp}_D$.*
(iv) *Suppose $AB_1 \dots B_r$ is odd, $p \neq 2$, and $\chi = \chi_2$. Then $G = \mathrm{O}_D$, unless $(r, A, B_r) = (1, 7, 1)$, in which case we have $G = \{\pm 1\} \times G_2$.*

Proof. We follow the idea behind [KT6, 8.5.1]. After the partial Kummer covering of $\mathbb{G}_m \times \mathbb{A}^r$ by itself,

$$[A, \mathrm{Id}] : (s, t_1, \dots, t_r) \mapsto (s^A, t_1, \dots, t_r),$$

the change of variable $x \mapsto x/s$, and the reparameterization $s \mapsto s, t_i \mapsto t_i s^{B_i}$, this pullback is just (the restriction to $\mathbb{G}_m \times \mathbb{A}^r$ of) the external tensor product $\mathcal{L}_{\overline{\chi}(s)} \otimes \mathcal{F}(A, B_1, \dots, B_r, \chi)$. Finite pullback doesn't change G°, nor does tensoring with a Kummer sheaf of finite order. In the case when $\chi = \mathbb{1}$ and $AB_1 \dots B_r$ is odd, $\mathcal{F}^\sharp_\chi$ is symplectic. So on the one hand its $G^\circ = \mathrm{Sp}_D$ while we also have $G \leq \mathrm{Sp}_D$. In the case when $p \neq 2$, $\chi = \chi_2$ and $AB_1 \dots B_r$ is odd, $\mathcal{F}^\sharp_\chi$ is orthogonal. So its $G^\circ = \mathrm{SO}_D$ while we also have $G \leq \mathrm{O}_D$. However, after the partial Kummer pullback $[A, \mathrm{Id}]^\star$, we obtain $\mathcal{L}_{\chi_2}(s) \otimes \mathcal{F}(A, B_1, \dots, B_r, \chi_2)$. Here $\mathcal{F}_{\chi_2}$ has odd rank A and trivial determinant, so this $[A, \mathrm{Id}]^\star \mathcal{F}^\sharp_{\chi_2}$ pullback has nontrivial determinant. Therefore $\mathcal{F}^\sharp_{\chi_2}$ must have nontrivial determinant. ☐

8. $M_{2,2}$ and finite symplectic and special unitary groups

In this section, we will determine the subgroups of $G = \mathrm{Sp}_{2n}(q)$ with $2 \nmid q$, and $G = \mathrm{SU}_n(q)$ with $2 \nmid n$, which have the same $M_{2,2}$ on an irreducible Weil representation of G. These results will allow us to determine G_{geom} for $\mathcal{F}(f, A, B)$, as defined in (1.0.4), in §11.

Let p be any odd prime and $q = p^f$. Then $G = \mathrm{Sp}_{2n}(q)$ has two *total Weil representations* of degree q^n, with characters $\xi + \eta$, and $\xi^* + \eta^*$, where $\xi \in \mathrm{Irr}(G)$ has degree $(q^n + 1)/2$, $\eta \in \mathrm{Irr}(G)$

has degree $(q^n-1)/2$, and * denotes the action of the outer automorphism of G_n induced by the conjugation by an element in $\mathrm{CSp}_{2n}(q) \smallsetminus \mathrm{Sp}_{2n}(q)\mathbf{Z}(\mathrm{CSp}_{2n}(q))$, cf. [TZ2], [KT1].

Theorem 8.1. [KT7, Theorem 2.1] *Assume $(n,q) \neq (1,3)$. Then the following statements hold for any irreducible Weil character $\theta = \xi, \xi^*, \eta, \eta^*$ of $G = \mathrm{Sp}_{2n}(q)$.*

(i) *If $n \geq 2$, or if $n = 1$ but $\theta \in \{\xi, \xi^*\}$, then*

$$M_{2,2}(\theta) = \begin{cases} (q+7)/4, & q \equiv 1 \pmod 4, \\ (q+5)/4, & q \equiv 3 \pmod 4. \end{cases}$$

(ii) *If $n = 1$ but $\theta \in \{\eta, \eta^*\}$, then $M_{2,2}$ drops by one, i.e.*

$$M_{2,2}(\theta) = \begin{cases} (q+3)/4, & q \equiv 1 \pmod 4, \\ (q+1)/4, & q \equiv 3 \pmod 4. \end{cases}$$

Theorem 8.2. *Let $q = p^f$ be a power of an odd prime p, $n \geq 1$, and $(n,q) \neq (1,3)$. Let H be a subgroup of $G = \mathrm{Sp}_{2n}(q)$ and θ be an irreducible Weil character of G, and suppose that*

$$M_{2,2}(H,\theta) = M_{2,2}(G,\theta).$$

Then either $H = G$, or one of the following cases occurs.

(i) *$(G, H, \theta(1)) = (\mathrm{Sp}_2(5), \mathrm{SL}_2(3), 2)$.*
(ii) *$(G, H, \theta(1)) = (\mathrm{Sp}_4(3), 2^{1+4}_- \cdot \mathsf{A}_5, 4)$.*

Proof. We argue by contradiction. If $H < G$, there exists a subgroup M with $H \leq M < G$ and M a maximal subgroup of G. We will show that this leads to a contradiction except in the two specified exceptional cases. For brevity, in this proof $\langle a \rangle$ (or $\langle a \rangle_i$ with some subscript i) will denote an irreducible character of G of degree $a \in \mathbb{Z}_{\geq 1}$. We will freely use the fact that $M_{2,2}(H,\theta) = M_{2,2}(G,\theta)$ implies that H, and so M, is irreducible on any irreducible constituent α of the G-character $\theta\bar{\theta}$. Moreover, $M_{1,1}(H,\theta) = M_{1,1}(G,\theta) = 1$ by [GT2, Lemma 3.1], so θ is irreducible over H and M as well.

(a) Here we consider the case $n = 1$. First suppose that $q = 5$. If $\theta \in \{\xi, \xi^*\}$, then

$$\theta\bar{\theta} = \langle 1 \rangle + \langle 3 \rangle + \langle 5 \rangle$$

as one can check using [GAP]. This implies that $\langle 5 \rangle$ is irreducible over M, and so $|M| \geq 26$, which is impossible by [Atlas]. If $\theta \in \{\eta, \eta^*\}$, then $\theta\bar{\theta} = \langle 1 \rangle + \langle 3 \rangle$ by [GAP]. Then $\langle 3 \rangle$ is irreducible on G, and so $|G| \geq 10$ and 3 divides $|G|$, whence $G \cong \mathrm{SL}_2(3)$ by [Atlas], as stated in (i).

Assume now that $9 \leq q \equiv 1 \pmod 4$. Using the character table of G [Do] one can check that

$$\xi\bar{\xi} = \langle 1 \rangle + \langle q \rangle + \langle \frac{q+1}{2} \rangle + \sum_{i=1}^{(q-5)/4} \langle q+1 \rangle_i, \;\; \eta\bar{\eta} = \langle 1 \rangle + \langle \frac{q+1}{2} \rangle + \sum_{i=1}^{(q-5)/4} \langle q+1 \rangle_i.$$

Similarly, if $7 \leq q \equiv 3 \pmod 4$, then

$$\xi\bar{\xi} = \langle 1 \rangle + \langle q \rangle + \sum_{i=1}^{(q-3)/4} \langle q+1 \rangle_i, \;\; \eta\bar{\eta} = \langle 1 \rangle + \sum_{i=1}^{(q-4)/4} \langle q+1 \rangle_i.$$

In both cases, some $\langle q+1 \rangle$ is irreducible over M, and so $|M| > (q+1)^2$, which is impossible by [BHR, Tables 8.1, 8.2].

(b) From now on, we will assume $n \geq 2$. According to [KT7, formulas (2.1.7) and (2.1.11)], we have

(8.2.1)
$$\begin{aligned}\xi\bar{\xi} &= \langle 1\rangle + \langle\frac{(q^n-1)(q^n+q)}{2(q-1)}\rangle + \langle\frac{q^{2n}-1}{2(q-1)}\rangle + \sum_{i=1}^{(q-5)/4}\langle\frac{q^{2n}-1}{q-1}\rangle_i,\\ \eta\bar{\eta} &= \langle 1\rangle + \langle\frac{(q^n+1)(q^n-q)}{2(q-1)}\rangle + \langle\frac{q^{2n}-1}{2(q-1)}\rangle + \sum_{i=1}^{(q-5)/4}\langle\frac{q^{2n}-1}{q-1}\rangle_i\end{aligned}$$

when $q \equiv 1 \pmod 4$, and

(8.2.2)
$$\begin{aligned}\xi\bar{\xi} &= \langle 1\rangle + \langle\frac{(q^n-1)(q^n+q)}{2(q-1)}\rangle + \sum_{i=1}^{(q-3)/4}\langle\frac{q^{2n}-1}{q-1}\rangle_i,\\ \eta\bar{\eta} &= \langle 1\rangle + \langle\frac{(q^n+1)(q^n-q)}{2(q-1)}\rangle + \sum_{i=1}^{(q-3)/4}\langle\frac{q^{2n}-1}{q-1}\rangle_i\end{aligned}$$

when $q \equiv 3 \pmod 4$. In particular, there exist (not necessarily distinct) $\gamma, \delta \in \mathrm{Irr}(G)$ such that

(8.2.3)
$$\frac{q^n+1}{2} \text{ divides } \gamma(1),\ \delta(1) = \frac{(q^n+\epsilon)(q^n-\epsilon q)}{2(q-1)} \text{ for some } \epsilon = \pm, \text{ and } \gamma|_M, \delta|_M \in \mathrm{Irr}(M).$$

Indeed, if $\theta \in \{\eta, \eta^*\}$ then we can choose $\gamma(1) = \delta(1) = (q^n+1)(q^n-q)/2(q-1)$. Suppose $\theta \in \{\xi, \xi^*\}$. Then we can choose $\gamma = \theta$ and $\delta(1) = (q^n-1)(q^n+q)/2(q-1)$.

Assume in addition that $n = 2$. Then (8.2.3) implies that $q(q^2+1)/2$ divides $|M|$. Using [BHR, Tables 8.12, 8.13] we now see that either $M = \mathrm{Sp}_2(q^2) \rtimes C_2$, or $q = 3$ and $M = 2_-^{1+4} \cdot \mathsf{A}_5$. In the former case, the degree of any irreducible character of M has p-part equal to 1 or q^2, contrary to the existence of δ in (8.2.3). In the latter case, suppose $\theta = \xi$. Then (8.2.2) shows that $\langle 24\rangle$ is irreducible on the image $2^4 \cdot \mathsf{A}_5$ of M in $G/\mathrm{Ker}(\theta)$. Hence 24 divides $|\mathsf{A}_5| = 60$ by Ito's theorem [Is, (6.15)], a contradiction. Thus $\theta(1) = \eta(1) = 4$, and using [GAP] we can check that $M_{2,2}(M,\theta) = 3 = M_{2,2}(G,\theta)$. Now, as $\mathbf{O}_2(M)H$ is irreducible on $\langle 15\rangle$, $\mathbf{O}_2(M)H/\mathbf{O}_2(M)$ is a subgroup of A_5 of order divisible by 15, whence $H\mathbf{O}_2(M) = M$. Working in M/Z where $Z := \mathbf{Z}(\mathbf{O}_2(M)) \cong C_2$ and noting that A_5 is irreducible on $\mathbf{O}_2(M)/Z \cong \mathbb{F}_2^4$, we see that either $ZH = M$ or $|ZH| = 2|\mathsf{A}_5| = 120$. The latter is however impossible as H is irreducible on $\langle 15\rangle$. So $ZH = M$, whence $H \geq [ZH, ZH] \geq [\mathbf{O}_2(M), \mathbf{O}_2(M)] = Z$. Thus $H = ZH = M$, and we arrive at (ii).

Next we consider the case $G = \mathrm{Sp}_6(5)$. By the choice of γ in (8.2.3), $|M|$ is divisible by $7 \cdot 31$. Inspecting [BHR, Tables 8.28, 8.29], we see that $M = \mathrm{Sp}_2(5^3) \rtimes C_3$. In this case, the degree of any irreducible character of M has p-part equal to 1 or q^3, contrary to the existence of δ in (8.2.3).

Assume now that $G = \mathrm{Sp}_6(3)$. As noted in the proof of (8.2.3) for $q = 3$, both θ and $\theta\bar{\theta} - 1_G$ are irreducible over M. This implies that $|M|$ is divisible by $7 \cdot 13$ and $\mathrm{Irr}(M)$ contains a character of degree ≥ 168. Inspecting [BHR, Tables 8.28, 8.29], we arrive at a contradiction.

(c) In the rest of the proof, we may assume that

(8.2.4)
$$n \geq 3 \text{ and } (n,q) \neq (3,3),\ (3,5).$$

Then $p^{2nf}-1$ admits a *large primitive prime divisor* ℓ in the sense of [F]. Note that $Q := (q^{2n}-1)_\ell$ divides $(q^n+1)/2$, and so Q divides $|M|$ by (8.2.3). Now we can apply [KT1, Theorem 4.6] to the subgroup $M < \mathrm{GL}_{2n}(q)$. If in addition

$$L := \mathbf{O}^{\ell'}(M)$$

is abelian, then again by Ito's theorem the irreducibility of $\gamma|_M$ implies that $\gamma(1)$ divides $|M/L$ and hence $\ell \nmid \gamma(1) = (q^n+1)/2$, a contradiction. Hence by [KT1, Theorem 4.6], there is a divisor $j < 2n$ of $2n$ such that we are in one of the following cases for L.

(c1) $j \leq 2n/3$ and $L \cong \mathrm{SL}_{2n/j}(q^j)$. Note that if $q^j = 3$ then $2n/j > 6$ by (8.2.4), and so $L \not\cong \mathrm{PSL}_4(3)$. Hence the smallest degree $d(L)$ of nontrivial irreducible complex characters of L satisfies

$$d(L) \geq (q^{2n} - q^j)/(q^j - 1) > q^{2n-j} > (q^n + 1)/2 > \eta(1)$$

by [TZ1, Theorem 1.1]. This forces the quasisimple subgroup L of G to be in the kernel of the Weil character η, which is absurd since $\mathrm{Ker}(\eta) \leq \mathbf{Z}(G) = C_2$.

(c2) $j|n$, $j \leq n/2$, and $L \cong \Omega^-_{2n/j}(q^j)$. Now if $j \leq n/4$ then

$$d(L) > q^{j(2n/j-3)} = q^{2n-3j} > (q^n + 1)/2 > \eta(1)$$

by [TZ1, Theorem 1.1], which leads to the contradiction $L \leq \mathrm{Ker}(\eta) \leq C_2$ as in (c1).

Suppose $j = n/3$. Then $(2n/j, q^j) \neq (6, 3)$ by (8.2.4). Hence $L = \Omega^-_6(q^j)$ is a cover of $\mathrm{PSU}_4(q^j) \not\cong \mathrm{PSU}_4(3)$, and so

$$d(L) \geq \frac{q^{4j} - q^j}{q^j + 1} > (q^{3j} + 1)/2 = (q^n + 1)/2 > \eta(1)$$

by [TZ1, Theorem 1.1]. This again yields the contradiction $L \leq \mathrm{Ker}(\eta) \leq C_2$ as in (c1).

In the remaining case $j = n/2$, we have $L \cong \Omega^-_4(q^{n/2}) \cong \mathrm{PSL}_2(q^n)$, see [KlL2, Proposition 2.9.1(v)]. Now, $d(\mathrm{PSL}_2(q^n)) = (q^n + 1)/2 > \eta(1)$ (as $q^n > 27$ by (8.2.4)), and this again forces $L \leq \mathrm{Ker}(\eta) \leq C_2$, a contradiction.

(c3) $j|n$, $L \cong \mathrm{Sp}_{2n/j}(q^j)$, and $L \lhd M \leq \mathbf{N}_G(L) = L \rtimes C_j$. Then we look at the character δ in (8.2.3). First suppose that $\epsilon = -$. As $n \geq 3$ by (8.2.4), $p^{(2n-2)f} - 1$ has a primitive prime divisor ℓ_1 by [Zs], and then ℓ_1 divides both $\delta(1)$ and $|M|$. Note that $\ell_1 \geq 2n - 1 > j$, so in fact ℓ_1 divides $|L|$. Hence we can find some $1 \leq i \leq n/j$ such that $\ell_1|(q^{2ij} - 1)$. The primitivity of ℓ_1 implies that $(n-1)|ij$, but $ij \leq n < 2(n-1)$. Thus $ij = n-1$, and so $j|\gcd(n, n-1) = 1$. We conclude that $j = 1$ and $L = G$, a contradiction.

Next we consider the case $\epsilon = +$. As before, $L < G$ implies that $j > 1$. Suppose first that $j = n$. Then $\mathrm{Sp}_2(q^n) = L \lhd M \leq L \cdot C_n$. It follows that the maximum degree of any $\alpha \in \mathrm{Irr}(M)$ is at most

$$n(q^n + 1) < \frac{(q^n + 1)(q^n - q)}{2(q - 1)} = \delta(1),$$

contrary to (8.2.3). So we have $j < n$; in particular $n \geq 4$. Hence $p^{(n-1)f} - 1$ has a primitive prime divisor ℓ_2 by [Zs]. Now ℓ_2 divides both $\delta(1)$ and $|M|$. Note that $\ell_2 \geq n > j$, so in fact ℓ_2 divides $|L|$. Hence we can find some $1 \leq i \leq n/j$ such that $\ell_2|(q^{2ij} - 1)$. The primitivity of ℓ_2 implies that $(n-1)|2ij$, but $2ij \leq 2n < 3(n-1)$. Thus $ij = (n-1)/2$ or $n-1$. It follows that $j|\gcd(n, n-1) = 1$, and so $j = 1$, again a contradiction.

(c4) $j = 2j_0 \in 2\mathbb{Z}$, $n/j_0 \geq 3$ is odd, $L \cong \mathrm{SU}_{n/j_0}(q^{j_0})$, and

$$L \lhd M \leq \mathbf{N}_G(L) \leq \mathrm{GU}_{n/j_0}(q^{j_0}) \rtimes C_j.$$

First suppose that $\theta(1) = \xi(1)$, and so $\epsilon = -$ in (8.2.3). As $n \geq 3$ by (8.2.4), $p^{(2n-2)f} - 1$ has a primitive prime divisor ℓ_1 by [Zs], and then ℓ_1 divides both $\delta(1)$ and $|M|$. Note that $\ell_1 \geq 2n-1 > j$, so in fact ℓ_1 divides $|L|$. Hence we can find some $1 \leq i \leq n/j_0$ such that $\ell_1|(q^{ij_0} - (-1)^i)$. The primitivity of ℓ_1 implies that $2(n-1)|2ij_0$, i.e. $(n-1)|ij_0$. But $ij_0 \leq n < 2(n-1)$, so $ij_0 = n-1$, and $j_0|\gcd(n, n-1) = 1$. In this case, $j_0 = 1$, and $i = n-1$ is even. Hence $\ell_1|(q^{ij_0} - 1)$, and so $2n-2$ divides $ij_0 = n-1$, a contradiction.

In the remaining case we have $\theta(1) = \eta(1)$. Since $L < \mathrm{Sp}_{2n/j_0}(q^{j_0})$, $\theta|_L$ is the restriction to L of a Weil character of degree $(q^n-1)/2$ of $\mathrm{Sp}_{2n/j_0}(q^{j_0})$, and so it is a sum of the unipotent Weil character of degree $(q^n - q^{j_0})/(q^{j_0}+1)$ and $(q^{j_0}-1)/2$ irreducible Weil characters, each of degree $(q^n+1)/(q^{j_0}+1)$. Since these characters are not of the same degree, $\theta|_M$ cannot be irreducible, a contradiction.

(c5) $(p, nf) = (3, 9)$ and $L/\mathbf{Z}(L) = \mathrm{PSL}_2(37)$. Here, since the smallest degree of nontrivial irreducible representations of L over $\overline{\mathbb{F}_3}$ is ≥ 18, we must have that $G = \mathrm{Sp}_{18}(3)$, $L = \mathrm{SL}_2(37) = M$. But then M cannot be irreducible on θ of degree $\geq (3^9-1)/2$.

(c6) $(p, nf) = (17, 6)$ and $L/\mathbf{Z}(L) = \mathrm{PSL}_2(13)$. Here, since the smallest degree of nontrivial irreducible representations of L over $\overline{\mathbb{F}_{17}}$ is ≥ 6, we must have that $G = \mathrm{Sp}_6(17)$, $L = \mathrm{SL}_2(13) = M$. But then M cannot be irreducible on θ of degree $\geq (17^3-1)/2$. ☐

Now let p be any prime, $q = p^f$, and $2 \nmid n \geq 5$. Then $G = \mathrm{SU}_n(q)$ has a *total Weil representation* of degree q^n, with character $\omega_n = \sum_{i=0}^{q} \zeta_{i,n}$, where $\zeta_{i,n} \in \mathrm{Irr}(G)$ has degree $(q^n + q(-1)^n)/(q+1)$ when $i = 0$ and $(q^n - (-1)^n)/(q+1)$ when $1 \leq i \leq q$, see e.g. [TZ2] and [KT2].

Theorem 8.3. [KT7, Theorem 3.4] *Assume $2 \nmid n$ and $n \geq 5$. Then for the irreducible Weil character $\theta = \zeta_{i,n}$ of $\mathrm{SU}_n(q)$, of degree $(q^n-q)/(q+1)$ if $i = 0$ and $(q^n+1)/(q+1)$ if $1 \leq i \leq q$, we have*

$$M_{2,2}(\theta) = \begin{cases} q+1, & i = 0, \text{ or } 2 \nmid q \text{ and } i = (q+1)/2, \\ q, & \text{otherwise.} \end{cases}$$

Theorem 8.4. *Let $q = p^f$ be a power of a prime p, $2 \nmid n \geq 3$ odd, and $(n, q) \neq (3, 2)$. Let H be a subgroup of $G = \mathrm{SU}_n(q)$ and θ be an irreducible Weil character of G, and suppose that*

$$M_{2,2}(H, \theta) = M_{2,2}(G, \theta).$$

Then $H = G$.

Proof. As in the proof of Theorem 8.2, we will assume that $H < G$ and let $H \leq M < G$ for a maximal subgroup M of G. We will also use the fact that $M_{2,2}(H,\theta) = M_{2,2}(G,\theta)$ implies that H, and so M, is irreducible on any irreducible constituent α of the G-characters θ^2 and $\theta\bar{\theta}$, as well as on θ itself.

(a) Here we consider the case $n = 3$. First suppose that $q = 3$, respectively $q = 4$. Using [GAP] we can check that $\theta\bar{\theta}$ has an irreducible constituent α with $\alpha(1) \geq 21$, respectively $\alpha(1) = 65$. On the other hand, $|M| \leq 216$, respectively $|M| \leq 960$ by [Atlas], so $\alpha|_M$ is reducible, a contradiction.

Assume now that $q \geq 5$. First we consider the case $\theta(1) = q^2 - q + 1$. Then $\theta(1)$ is divisible by ℓ, a primitive prime divisor of $p^{6f}-1$ by [Zs]. Using [BHR, Tables 8.5, 8.6], we see that $|M|$ can be divisible by ℓ only when $M = C_{\gcd 3,(q+1)} \times \mathrm{PSL}_2(7)$, $3 \cdot \mathsf{A}_6$, $3 \cdot \mathsf{A}_6 \cdot 2_3$, or $q = 5$ and $M = 3 \cdot \mathsf{A}_7$. The first three cases are however impossible, because M cannot have an irreducible character of odd degree $q^2 - q + 1 \geq 21$. In the last case, $\theta\bar{\theta}$ contains an irreducible constituent α of degree 126, and hence α is reducible over M by [Atlas].

It remains to consider the case $\theta(1) = q^2 - q$. Then $\theta|_M$ is irreducible; in particular, $|M| > q^2(q-1)^2$. Again using [BHR, Tables 8.5, 8.6] we can check that M must be a Borel subgroup of G. Note that the degree of any irreducible character of M is then equal to 1 or divisible by a fixed prime divisor r of $(q-1)/\gcd(3, q-1)$ [Geck]. However, any irreducible constituent of $\theta\bar{\theta} - 1_G$ has degree > 1, and at least one of them, say β, has degree coprime to r. Thus $\beta|_M$ is reducible, again a contradiction.

(b) From now on, we may assume $n \geq 5$, and write $\theta = \zeta_{i,n}$ with $0 \leq i \leq q$. Then the proof of Theorem 8.3 in [KT7] shows that θ^2 has an irreducible constituent

$$\gamma = C^{\circ}_{\chi_1^{(i)}},\ \text{of degree } \frac{(q^n+1)(q^{n-1}-1)}{(q+1)(q^2-1)},$$

when $i \neq 0$, and

$$\gamma = C^{\circ}_{\chi_{q-1}^{(1,q)}},\ \text{of degree } \frac{(q^n+1)(q^{n-1}-1)}{(q+1)^2},$$

when $i = 0$. As $\gamma|_M$ is irreducible, we always have

$$\gamma(1) \text{ divides } |M|. \tag{8.4.1}$$

As $n \geq 5$, $p^{2nf}-1$ admits a *large primitive prime divisor* ℓ in the sense of [F]. Note that $Q := (q^{2n}-1)_\ell$ divides $\gamma(1)$, and so Q divides $|M|$ by (8.4.1). Now we can apply [KT1, Theorem 4.6] to the subgroup $M < \mathrm{Sp}_{2n}(q)$. If in addition

$$L := \mathbf{O}^{\ell'}(M)$$

is abelian, then again by Ito's theorem the irreducibility of $\gamma|_M$ implies that $\gamma(1)$ divides $|M/L$ and hence $\ell \nmid \gamma(1)$, a contradiction. Hence by [KT1, Theorem 4.6], there is a divisor $j < 2n$ of $2n$ such that we are in one of the following cases for L.

(b1) $j \leq 2n/3$ and $L \cong \mathrm{SL}_{2n/j}(q^j)$. Note that if $q^j = 3$ then $2n/j = 2n \geq 10$, and so $L \not\cong \mathrm{PSL}_4(3)$. Hence, as in the proof of Theorem 8.2 we have

$$d(L) \geq (q^{2n}-q^j)/(q^j-1) > q^{2n-j} > (q^n+1)/(q+1) \geq \theta(1)$$

by [TZ1, Theorem 1.1]. This forces the quasisimple subgroup L of G to be in the kernel of the Weil character θ, which is absurd since $\mathrm{Ker}(\theta) \leq \mathbf{Z}(G)$.

(b2) $j|n$ and $L \cong \mathrm{Sp}_{2n/j}(q^j)$. Here, $j \neq n/2$ as $2 \nmid n$; furthermore, $q^j \geq 2^5$ if $j = n$, and $q^j \geq 2^3$ if $j = n/3$ (as $2 \nmid n \geq 5$). Hence

$$d(L) > (q^n-1)/2 > (q^n+1)/(q+1) \geq \theta(1)$$

by [TZ1, Theorem 1.1], which leads to the contradiction $L \leq \mathrm{Ker}(\theta) \leq \mathbf{Z}(G)$ as in (b1).

(b3) $j|n$, $j < n/2$ (recall $2 \nmid n$), and $L \cong \Omega^-_{2n/j}(q^j)$. Now if $j \leq n/4$ then

$$d(L) > q^{j(2n/j-3)} = q^{2n-3j} > (q^n+1)/(q+1) > \theta(1)$$

by [TZ1, Theorem 1.1], which again leads to the contradiction $L \leq \mathrm{Ker}(\theta) \leq \mathbf{Z}(G)$.

Suppose $j = n/3$. Then $q^j \geq 2^3$ as $2 \nmid n \geq 5$. Hence $L = \Omega^-_6(q^j)$ is a cover of $\mathrm{PSU}_4(q^j) \not\cong \mathrm{PSU}_4(3)$, and so

$$d(L) \geq \frac{q^{4j}-q^j}{q^j+1} > (q^{3j}+1)/2 > (q^n+1)/(q+1) > \theta(1)$$

by [TZ1, Theorem 1.1]. This again yields the contradiction $L \leq \mathrm{Ker}(\theta) \leq \mathbf{Z}(G)$.

(b4) $j = 2j_0 \in 2\mathbb{Z}$, $n/j_0 \geq 3$ is odd, $L \cong \mathrm{SU}_{n/j_0}(q^{j_0})$, and

$$L \lhd M \leq \mathbf{N}_G(L) \leq \mathrm{GU}_{n/j_0}(q^{j_0}) \rtimes C_j.$$

As $M < G = \mathrm{SU}_n(q)$, we have $j_0 > 1$. In particular, n is not prime, and so we may assume $n \geq 9$. It follows that $p^{(n-1)f}-1$ has a primitive prime divisor ℓ_1 [Zs], which then divides $|M|$ by (8.4.1). As $\ell_1 \geq n > j$, ℓ_1 divides $|\mathrm{GU}_{n/j_0}(q^{j_0})|$. Hence we can find some $1 \leq i \leq n/j_0$ such that $\ell_1|(q^{ij_0}-(-1)^i)$. The primitivity of ℓ_1 implies that $(n-1)|2ij_0$. But $2ij_0 \leq 2n < 3(n-1)$, so $ij_0 = n-1$ or $(n-1)/2$, and thus $j_0|\gcd(n,n-1) = 1$, a contradiction.

(b5) $(p, nf) = (3, 9)$ and $L/\mathbf{Z}(L) = \mathrm{PSL}_2(37)$. This case cannot however occur, since the smallest degree of nontrivial irreducible representations of L over $\overline{\mathbb{F}_3}$ is ≥ 18, and hence L cannot embed in $G = \mathrm{SU}_9(3)$. $\square$

9. $M_{2,2}$ and intersections of Fermat hypersurfaces

In this section, we fix a set $S = \{B_0, B_1, \ldots, B_r\}$ of integers

(9.0.1) $$B_0 > B_1 > \ldots > B_r \text{ with } r \geq 2 \text{ and } \gcd(S) := \gcd(B_0, B_1, \ldots, B_r) = 1.$$

We will sometimes write

$$A := B_0$$

when we wish to emphasize the largest B_i. We work in characteristic $p \nmid \prod_i B_i$, and choose a prime $\ell \neq p$ so that we can speak of ℓ-adic local systems. [For example, one might take for ℓ a prime which divides $\prod_i B_i$.]

In [KT6, 11.2.6], given a multiplicative character χ of $k^\times$ for $E/\mathbb{F}_p$ a finite extension, we introduced the local system

$$\mathcal{F}^\sharp(A, B_1, \ldots, B_r, \chi)$$

on $(\mathbb{G}_m \times \mathbb{A}^r)/E$ whose trace function is

$$(s, t_1, \ldots, t_r) \in L^\times \times L^r \mapsto \frac{-1}{\sqrt{\#L}} \sum_x \psi_L\big(sx^A + t_1 x^{B_1} + \ldots + t_k x^{B_r}\big)\chi(x).$$

We will denote this

$$\mathcal{F}^\sharp(S, \chi) := \mathcal{F}^\sharp(A, B_1, \ldots, B_r, \chi).$$

The pullback of $\mathcal{F}^\sharp$ to $s = 1$ is the local system $\mathcal{F}(A, B_1, \ldots, B_r, \chi)$ on $\mathbb{A}^k/E$ whose trace function is

$$(t_1, \ldots, t_k) \in L^k \mapsto \frac{-1}{\sqrt{\#L}} \sum_x \psi_L\big(x^A + t_1 x^{B_1} + \ldots + t_k x^{B_r}\big)\chi(x).$$

We will denote this

$$\mathcal{F}(S, \chi) := \mathcal{F}(A, B_1, \ldots, B_r, \chi).$$

As shown in §2, there is an intimate relationship between the $M_{2,2}$ of $\mathcal{F}(S, \chi)$ and the number $N(S, p)$ of geometrically irreducible components Z of dimension 2 of the $\overline{\mathbb{F}_p}$-locus

$$\Sigma(S) := \cap_{i=0}^r \Sigma_{B_i},$$

where Σ_{B_i} is the Fermat hypersurface $x^{B_i} + y^{B_i} = z^{B_i} + w^{B_i}$ in $\mathbb{A}^4(x, y, z, w)$. As an application of the results of the preceding sections, we will be able to completely determine this invariant $N(S, p)$.

In fact, $N(S, p)$ is related to $M_{2,2}$ of a more general kind of multi-parameter local system. Consider a partition of S as

$$S = S_0 \sqcup T, \#T = 2, \; T = \{a, b\}, \; a < b.$$

and a polynomial $f(x) = \sum_i c_i x^i \in E[x]$ for which

$$\{i | c_i \neq 0\} = S_0.$$

In a more cumbersome expression, we assume that

$$f(x) = \sum_{B_i \in S_0} c_{B_i} x^{B_i}, \text{ all } c_{B_i} \neq 0.$$

We now consider the two-parameter family $\mathcal{F}(f,a,b,\chi)$ on $\mathbb{A}^2/E$ if $A := B_0 \in S_0$, respectively on $(\mathbb{G}_m \times \mathbb{A}^1)/E$ if $a < b = A := B_0$, whose trace function at L-valued points is

$$(s,t) \mapsto -\sum_x \psi_L(sx^b + tx^a + f(x))\chi(x).$$

The following theorem is a recapitulation of Theorems 2.3 and 2.6, see also Corollary 2.5. Remember that $\#S \geq 3$ in this section.

Theorem 9.1. *For any χ, any partition $S = S_0 \sqcup T$ as above and any f whose set of exponents is S_0, the following three local systems*

$$\mathcal{F}^\sharp(S,\chi),\ \mathcal{F}(S,\chi),\ \mathcal{F}(f,a,b,\chi)$$

have the same geometric $M_{2,2}$ as each other. This common $M_{2,2}$ is the number $N(S,\chi)$ of geometrically irreducible components Z of dimension 2 of the $\overline{\mathbb{F}_p}$-locus $\Sigma(S)$ with the property that on the dense open set $xyzw \neq 0$ of Z, the rank one local system $\mathcal{L}_{\chi(xy)\overline{\chi}(zw)}$ is geometrically trivial. In particular, when $\chi = \mathbb{1}$, the common $M_{2,2}$ is $N(S,\mathbb{1}) = N(S,p)$ of geometrically irreducible components Z of dimension 2 of the $\overline{\mathbb{F}_p}$-locus $\Sigma(S)$.

Recall the definitions 4.1 and 4.2 of a data $S = \{B_0, \dots, B_r\}$ to be p-finite, respectively strongly p-finite.

Theorem 9.2. *Given a set $S = \{B_0, B_1, \dots, B_r\}$ subject to (9.0.1) and a prime $p \nmid \prod_{i=0}^k B_i$. The following statements holds for the number $N(S,p)$ of geometrically irreducible components Z of dimension 2 of the $\overline{\mathbb{F}_p}$-locus $\Sigma(S)$.*

(i) *Suppose that S is either strongly p-finite or not p-finite. Then $N(S,p)$ is 2 if $2|\prod_{i=0}^k B_i$, and 3 otherwise.*
(ii) *Suppose that S is p-finite, but not strongly p-finite, i.e. we are in 4.1(i) with $q \geq 7$, 4.1(ii) with $q > 2$ and furthermore $2 \nmid nm_1 \dots m_{r-1}$ if $p > 2$, 4.1(iii) with $q > 2$, or 4.1(iv) with $q > 2$. In the case of 4.1(i), $N(S,p)$ equals $(q+7)/4$ if $q \equiv 1 \pmod 4$ and $(q+5)/4$ if $q \equiv 3 \pmod 4$. In the cases of 4.1(ii)–4.1(iv), $N(S,p) = q+1$.*

Proof. By Theorem 9.1, $N(S,p)$ is just the $M_{2,2}$ of the local system $\mathcal{F}(S,\mathbb{1})$ of rank $D = B_0 - 1$. Now the statements follow from Theorem 4.3 if S is strongly p-finite.

Suppose next that S is not p-finite. By Theorem 4.3, $\mathcal{F}(S,\mathbb{1})$ has infinite G_{geom}, whence $G^\circ_{\mathrm{geom}} = \mathrm{SL}_D$ if $2||\prod_{i=0}^r B_i$ and $G_{\mathrm{geom}} = \mathrm{Sp}_D$ otherwise (note that in the latter case $B_0 \geq 5$ as $k \geq 2$, and hence $D \geq 4$). It follows that the conclusion of (i) holds.

Finally, we consider the case where S is p-finite, but not strongly p-finite. By Theorem 4.3, $\mathcal{F}(S,\mathbb{1})$ has finite G_{geom}, which is determined in [KT6, Theorem 11.2.3]. In the case of 4.1(i), we have $B_0 = (q^n+1)/2$ with $n \geq 2$, and G_{geom} is the image of $\mathrm{Sp}_{2n}(q)$ in a Weil representation of degree $D = (q^n-1)/2$ by [KT6, Theorem 11.2.3(i)], so the conclusion of (ii) follows from Theorem 8.1. In the case of 4.1(iv), we have $B_0 = (q^n+1)/(q+1)$ with $2 \nmid n \geq 5$, and G_{geom} is the image of $\mathrm{SU}_n(q)$ in a Weil representation of degree $D = (q^n-q)/(q+1)$ by [KT6, Theorem 11.2.3(iii)], whence $N(S,p) = M_{2,2} = q+1$ by Theorem 8.3. In the case of 4.1(ii) we have $B_0 = q^n+1$, $B_i = q^{m_i}+1$ for $1 \leq i \leq r-1$, $B_r = 1$, and furthermore $2 \nmid nm_1 \dots m_{r-1}$ if $p > 2$. In this case, $N(S,p) = q+1$ by Corollary 3.6. In the case of 4.1(iii) we have $B_0 = q^n+1$ and $B_i = q^{m_i}+1$ for $1 \leq i \leq k$ with $q = 2^f > 2$ and $n > 2$. In this case, $G_{\mathrm{geom}} = 2_-^{1+2nf} \cdot \Omega^-_{2n}(q)$ by [KT6, Theorem 11.2.3(ii)], and the proof of [GT2, Lemma 5.1] shows that $N(S,p) = M_{2,2} = q+1$, the number of $\Omega^-_{2n}(q)$ orbits on the vectors of its natural module $\mathbb{F}_q^{2n}$. ☐

10. Two-parameter specializations of multi-parameter local systems

In this and the next sections, we will use our results on $M_{2,2}$ to determine the geometric monodromy groups of the two-parameter families $\mathcal{F}(f,a,b)$, $1 \le a < b < \deg(f)$, with f monic and Artin-Schreier reduced, obtained as the specializations of the multi-parameter local systems $\mathcal{F}(A, B_1, \ldots, B_r)$, as defined in (1.0.4) given the data (1.0.2).

Theorem 10.1. *Let $p = 2$ and consider the data (1.0.2) with $r \ge 3$, $\gcd(n, m_1, \ldots, m_r) = 1$, and*

$A = 2^n + 1$, $B_i = 2^{m_i} + 1$, $1 \le i \le r-1$, and either $B_r = 2^{m_r} + 1$ with $m_r \ge 1$ or $(B_r, m_r) = (1, 0)$.

Then the following statements hold for the geometric monodromy group $G = G_{\rm geom}$ of the local system $\mathcal{F} = \mathcal{F}(f,a,b)$ defined in (1.0.4), with $a = B_i < b = B_j$.

(i) *Either $G = 2^{1+2n}_- \cdot \Omega^-_{2n}(2)$ or $G = 2^{1+2n}_- \cdot \mathrm{SU}_n(2)$.*
(ii) *If $B_r = 1$ and $2 \nmid nm_1 \ldots m_{r-1}$, then $G = 2^{1+2n}_- \cdot \mathrm{SU}_n(2)$.*
(iii) *If $2|n$, then $G = 2^{1+2n}_- \cdot \Omega^-_{2n}(2)$.*

Proof. Note that $\mathcal{F}$ is a pullback of the local system $\tilde{\mathcal{F}} := \mathcal{F}(A, B_1, \ldots, B_r)$; furthermore,

$$\text{Either } n \ge 4, \text{ or } (A, B_1, \ldots, B_r) = (9, 5, 3, 1). \tag{10.1.1}$$

By Theorems 9.1 and 9.2, both $\mathcal{F}$ and $\tilde{\mathcal{F}}$ have $M_{2,2} = 3$; moreover, G embeds in the (finite) geometric monodromy group $\tilde{G} < \mathrm{Sp}_{2^n}(\mathbb{C})$ of $\tilde{\mathcal{F}}$. Now we can apply [GT2, Theorem 1.5] and use the assumption $n \ge 3$ to conclude that

$$E = 2^{1+2n}_- \lhd G \le \mathbf{N}_{\mathrm{Sp}_{2^n}(\mathbb{C})}(E) = E \cdot \mathrm{O}^-_{2n}(2); \tag{10.1.2}$$

furthermore, $G/E \le \mathrm{O}(V)$ is transitive on the set of $2^{n-1}(2^n+1)$ (nonzero) isotropic vectors and the set of $(2^n+1)(2^{n-1}-1)$ anisotropic vectors of the natural module $V = \mathbb{F}_2^{2n}$ of $\mathrm{O}^-_{2n}(2)$. In particular,

$$|G/E| \text{ is divisible by } 2^{n-1} \cdot \mathrm{lcm}(2^n+1, 2^{n-1}-1). \tag{10.1.3}$$

Moreover, the semidirect product $V \rtimes (G/E)$ acts on the point set of V as a rank 3 affine permutation group with point stabilizer G/E. By [Li, Theorem], we arrive at one of the following possibilities for G/E.

(a) G/E is in one of the 'exceptional' cases listed in [Li, Theorem, part (C)]. Here, $n = 3$, 4 or 6, so the lengths of the orbits of G/E on $V \smallsetminus \{0\}$, which are the so-called subdegrees for $V \rtimes (G/E)$ must be $27, 36$, or $119, 136$, or $2015, 2080$, respectively. But those subdegrees do not match the subdegrees listed in [Li, Table 14].

(b) G/E is in one of the 'extraspecial' cases listed in [Li, Theorem, part (B)]. Here we have $n = 3$, so $(A, B_1, \ldots, B_r) = (9, 5, 3, 1)$ by (10.1.1). Furthermore, G/E is a subgroup of $\mathrm{O}^-_6(2)$ that normalizes an extraspecial 3-group $3^{1+2}_\pm$; in particular, G/E cannot contain $\Omega^-_6(2)$. Using the list of maximal subgroups of $\mathrm{O}^-_6(2)$ [Atlas] and the fact that $|G/E|$ is divisible by 27, we now see that G/E is solvable, and hence G is solvable. Next, since $\mathcal{F}$ is a pullback of the local system $\mathcal{F}_{9531}$, by Theorem 4.4(ii) we have

$$G \le \tilde{G} = E_3 \cdot \Omega^-_6(2),$$

where $E_3 \cong E = 2^{1+6}_-$, and $\mathbf{Z}(E_3) = \mathbf{Z}(E)$ acts via ± 1 in the underlying representation. Since G is solvable, E_3G is a solvable subgroup of $\mathrm{Sp}_{2^n}(\mathbb{C})$, for which we have

$$3 = M_{2,2}(\mathrm{Sp}_{2^n}(\mathbb{C})) \le M_{2,2}(E_3G) \le M_{2,2}(G) = 3, \tag{10.1.4}$$

and hence $M_{2,2}(E_3G) = 3$. Now the arguments in part (d) of the proof of Theorem 4.4, with G_1 replaced by G and E replaced by E_3, show that, first, $E_3G = E_3 \cdot \mathrm{SU}_3(2)$, and, secondly, either $E_3 \cap G = \mathbf{Z}(E_3) = \mathbf{Z}(E)$ or $G \geq E_3$. In the former case,

$$|G| = |E_3 \cap G| \cdot |E_3G/E_3| = 2|\mathrm{SU}_3(2)| = 3^3 \cdot 2^4,$$

which is a contradiction since G contains E of order 2^7. So $G \geq E_3$, and hence $G = E_3 \cdot \mathrm{SU}_3(2)$.

(c) G/E is in one of the infinite families listed in [Li, Theorem, part (A)]. First, we may have that

$$G/E \leq \Gamma_1(2^{2n}) \cong C_{2^{2n}-1} \cdot C_{2n};$$

in particular, $4 \nmid |G/E|$ if $2 \nmid n$. This rules out the case $2 \nmid n \geq 3$ since 2^{n-1} divides $|G/E|$ by (10.1.3). Assume now that $2|n \geq 4$. By [Zs], $2^{n-1}-1$ admits a primitive prime divisor ℓ, for which we have $\ell > n$, ℓ divides $|G/E|$ by (10.1.3), but not $2n(2^{2n}-1)$, a contradiction.

In the imprimitive case, by [Li, Table 12] the subdegrees are $(2^n-1)^2$ and $2(2^n-1)$, none of which is divisible by 4, whereas one of the subdegrees of G/E is divisible by 2^{n-1}.

In the tensor product case, according to [Li, Table 12] the subdegrees are $(q+1)(q^m-1)$ and $q(q^{m-1}-1)(q^m-1)$ with $q^m = 2^n$. Since the even subdegree of G/E has 2-part equal to 2^{n-1}, we get $2^{n-1} = q$. As $n \geq 3$, we have $q^{2m} = 2^{2n} \leq 2^{3(n-1)} = q^3$, whence $m = 1 = q$, a contradiction.

In all the remaining cases, we again match up the subdegrees listed in [Li, Table 12] to the ones of G/E and compare the 2-part of the even subdegree. First, in the case $G/E \rhd \mathrm{SL}_a(q)$ we either have $q^{2a} = 2^{2n}$ and $q = 2^{n-1}$, which is impossible as shown in the preceding case, or $a = 2$, $q^6 = 2^{2n}$, and $q = 2^{n-1}$, which is also impossible, or $a = 5$, $q^{10} = 2^{2n}$, and $q = 2^{n-1}$, which is absurd.

In the case $G/E \rhd {}^2B_2(q)$ we have $q^4 = 2^{2n}$ and $q = 2^{n-1}$, which is impossible since $n \geq 3$.

In the case $G/E \rhd \Omega^+_{10}(q)$ we have $q^{16} = 2^{2n}$ and $q = 2^{n-1}$, which is impossible.

Suppose $G/E \rhd \mathrm{Sp}_6(q)$. Then $q^8 = 2^{2n}$ and $q = 2^{n-1}$, whence $(n,q) = (4,2)$. But then the subdegrees are $135, 120$ but not $136, 119$.

Suppose $G/E \rhd \Omega^\epsilon_{2a}(q)$. Then $q^{2a} = 2^{2n}$ and $q^{a-1} = 2^{n-1}$, whence $(a,q) = (n,2)$. Now the even subdegree is $2^{n-1}(2^n - \epsilon)$, so $\epsilon = -$.

Suppose $G/E \rhd \mathrm{SU}_a(q)$. Then $q^{2a} = 2^{2n}$ and $q^{a-1} = 2^{n-1}$, whence $(a,q) = (n,2)$. Now the even subdegree is $2^{n-1}(2^n - (-1)^n)$, so $2 \nmid n$.

To summarize, with replacing E by E_3 in the case $(A, B_1, \ldots, B_r) = (9,5,3,1)$ if necessary, we have shown that

(10.1.5) $$\text{Either } G/E \rhd \Omega^-_{2n}(2), \text{ or } 2 \nmid n \text{ and } G/E \rhd \mathrm{SU}_n(2).$$

Now, suppose that we have the first possibility in (10.1.5). Then $\Omega^-_{2n}(2) \lhd G/E \leq \mathrm{O}^-_{2n}(2)$ by (10.1.2). On the other hand, G injects in the geometric monodromy group $\tilde{G}$ of $\tilde{\mathcal{F}}$, which is isomorphic to a subgroup of $2^{1+2n}_- \cdot \Omega^-_{2n}(2)$ by [KT6, Theorem 11.2.3(ii)] when $n \geq 4$ and Theorem 4.4(ii) when $n = 3$. Comparing the orders of G and $\tilde{G}$, we conclude that $G/E = \Omega^-_{2n}(2)$ and that $\tilde{G} \cong 2^{1+2n}_- \cdot \Omega^-_{2n}(2)$. The latter conclusion implies by by [KT6, Theorem 11.2.3(ii)] when $n \geq 4$ and Theorem 4.4(ii) when $n = 3$ that either $B_r > 1$, or $B_r = 1$ but $2|nm_1 \ldots m_r$.

Next suppose that $2 \nmid nm_1 \ldots m_{r-1}$ and $B_r = 1$; in particular, $n \geq 4$ since $n, r \geq 3$. Then G injects in the geometric monodromy group $\tilde{G}$ of $\tilde{\mathcal{F}}$, which is isomorphic to $2^{1+2n}_- \cdot \mathrm{SU}_n(2)$, by [KT6, Theorem 11.2.3(ii)]. Again comparing the orders of G and $\tilde{G}$, we see that $G/E = \mathrm{SU}_n(2)$ in (10.1.5), and hence (ii) follows.

Finally, assume that we have the second possibility in (10.1.5), so $2 \nmid n$, and, in addition, either $B_r > 1$, or $B_r = 1$ but $2|m_1 \ldots m_{r-1}$. Then G injects in the geometric monodromy group $\tilde{G}$ of $\tilde{\mathcal{F}}$, which is $E_3 \cdot S$ by [KT6, Theorem 11.2.3(ii)] when $n \geq 4$ and Theorem 4.4(ii) when $n = 3$, where

$E_3 \cong E = 2_-^{1+2n}$ and $S \cong \Omega_{2n}^-(2)$. Certainly, $E_3G \leq \tilde{G} < \mathrm{Sp}_{2^n}(\mathbb{C})$ still has $M_{2,2} = 3$, see (10.1.4). So the preceding arguments but applied to E_3G show that (10.1.5) also holds for E_3G:

$$\text{Either } E_3G/E_3 \rhd \Omega_{2n}^-(2), \text{ or } E_3G/E_3 \rhd \mathrm{SU}_n(2).$$

In the former case, we have $E_3G = \tilde{G}$, and so the composition factors of G are $\Omega_{2n}^-(2)$ and C_2, all present. But this contradicts the fact that $G/E \rhd \mathrm{SU}_n(2)$ (which yields a composition factor $\mathrm{PSU}_n(2)$ when $n \geq 4$ and C_3 when $n = 3$). So we must have that

$$E_3G/E_3 \rhd \mathrm{SU}_n(2). \tag{10.1.6}$$

Recall that E_3G/E_3 is a subgroup of $S = \Omega(W)$, where $W := E_3/\mathbf{Z}(E_3) = \mathbb{F}_2^{2n}$ carries the quadratic form $x\mathbf{Z}(E_3) \mapsto x^2$ and symplectic form $(x\mathbf{Z}(E_3), y\mathbf{Z}(E_3)) \mapsto [x,y]$, both invariant under the normal subgroup $G_1 := \mathrm{SU}_n(2)$ of E_3G/E_3. Assuming $n > 3$ and applying [KT6, Proposition 8.4.1], we obtain that

$$E_3G/E_3 \leq \mathbf{N}_{\mathrm{O}(W)}(G_1) = \mathrm{GU}(W_1) \rtimes \mathrm{Gal}(\mathbb{F}_4/\mathbb{F}_2),$$

where $W_1 := \mathbb{F}_4^n$. Working from a standard basis for the Hermitian form on W_1 (over $\mathbb{F}_4$) back to a Witt basis of W (over $\mathbb{F}_2$), one can readily check that the Galois automorphism $\alpha \mapsto \alpha^2$ of $\mathbb{F}_4$ induces (in that standard basis) an element of $\mathrm{O}(W)$ which is a product of n reflections. Since $2 \nmid n$, this element is **not** in $S = \Omega(W)$. On the other hand, since $\mathrm{O}(W)$ has index 2 over S and $2 \nmid n \geq 5$, $\mathrm{GU}(W_1) \leq S$. It follows that $E_3G/E_3 \leq \mathbf{N}_S(G_1) \cong \mathrm{GU}_n(2)$. Now we can use the fact that $G = \mathbf{O}^{2'}(G)$ to conclude that

$$E_3G/E_3 = \mathrm{SU}_n(2). \tag{10.1.7}$$

Suppose now that $n = 3$. Then, using (10.1.6) and the fact that E_3G/E_3 is transitive on both the nonzero singular vectors and the non-singular vectors of the quadratic space $\mathbb{F}_2^6$, and arguing as in part (b) (recalling that $\mathbf{O}_3(\mathrm{SU}_3(2)) = 3_+^{1+2}$), we see that (10.1.7) holds in this case as well.

We have therefore shown that $|G| \leq |E_3G| = |E_3| \cdot |\mathrm{SU}_n(2)| = |E| \cdot |\mathrm{SU}_n(2)|$. But $G/E \rhd \mathrm{SU}_n(2)$ by (10.1.5), so in fact $G/E = \mathrm{SU}_n(2)$. $\square$

In some special instances of the case where $2|m_1 \dots m_r$ but $2 \nmid n$ of Theorem 10.1, we can also prove that $\mathcal{F}(f,a,b)$ has $G_{\mathrm{geom}} = E \cdot \Omega_{2n}^-(2)$. [Also see Theorem 11.7 about the "generic" situation.] To do this, we first prove a general statement.

Proposition 10.2. *Let $k/\mathbb{F}_p$ be an finite extension, $f(x) \in k[x]$ a polynomial of degree A with $p \nmid A$, and a an integer*

$$1 < a < A, \; p \nmid a.$$

Denote by $\mathcal{F}_{f,a}$ the lisse sheaf on $\mathbb{A}^1$ whose trace function at a point $t \in L$, for L/k a finite extension, is

$$(-1/\sqrt{\#L}) \sum_{x \in L} \psi_L(f(x) + tx^a).$$

Then the following statements hold for its G_{geom}.

(i) *G_{geom}, indeed its $I(\infty)$, contains elements of order a. In particular, G_{geom} is not a finite p-group.*

(ii) *Assume in addition that $\gcd(A,a) = 1$. Then G_{geom} contains a subquotient of order $(A-a)_{p'}$.*

Proof. (i) Up to a Tate twist $(1/2)$, $\mathcal{F}_{f,a}$ is the Fourier Transform of the Kummer direct image $[a]_\star(\mathcal{L}_{\psi(f)})$:

$$\mathcal{F}_{f,a} = \mathrm{FT}_\psi(\mathcal{G}) \text{ for } \mathcal{G} := [a]_\star(\mathcal{L}_{\psi(f)}).$$

The sheaf $\mathcal{G}$ is lisse of rank a on $\mathbb{G}_m$, its $I(0)$-representation is $\oplus_{\chi:\chi^a=\mathbb{1}}\mathcal{L}_\chi$, and its $I(\infty)$-representation has all slopes $A/a > 1$. By Laumon's theory of local Fourier Transform, cf. [Ka2, 7.4.2, 7.4.4(2)], the $I(\infty)$-representation of $\mathcal{F}_{f,a}$ is the direct sum

$$\mathrm{FT}_\psi\mathrm{loc}(0,\infty)(\mathcal{G}_{|I(0)}/\overline{\mathbb{Q}_\ell}) \oplus \mathrm{FT}_\psi\mathrm{loc}(\infty,\infty)(\mathcal{G}_{|I(\infty)}).$$

The first factor is $\oplus_{\chi:\chi^a=\mathbb{1},\chi\neq\mathbb{1}}\mathcal{L}_\chi$. Thus the subgroup $I(\infty) \leq G_{\mathrm{geom}}$ contains elements of order a.

(ii) The $I(\infty)$-representation of $\mathcal{G}$ has rank a, and all slopes A/a. By Laumon's result [Ka2, 7.4.1(1)],the second factor $\mathrm{FT}_\psi\mathrm{loc}(\infty,\infty)(\mathcal{G}_{|I(\infty)})$ has rank $A-a$ and all slopes $A/(A-a)$. If $\gcd(A,a)=1$, one knows [Ka1, 1.1.4] that the second factor is $I(\infty)$-irreducible, and one knows further that denoting by $(A-a)_{p'}$ the p' part of $A-a$, the second factor is the Kummer induction $[(A-a)_{p'}]_\star W$ of an irreducible $I(\infty)$-representation of dimension the p part of $A-a$. This description of the second factor makes visible the group $\mu_{(A-a)_{p'}}$ as a quotient of the wild part of the $I(\infty)$-representation of $\mathcal{F}_{f,a}$. □

Corollary 10.3. *Consider the case $2 \nmid n$ of Theorem 10.1. Assume that some $m \in \{m_i, m_j\}$ is even and strictly positive. Then $\mathcal{F}(f,a,b)$ has $G_{\mathrm{geom}} = 2_-^{1+2n} \cdot \Omega_{2n}^-(2)$.*

Proof. For definiteness, we will assume $m = m_i$, so that $a = 2^m+1$. By Theorem 10.1, it suffices to prove that $|G_{\mathrm{geom}}|$ is divisible by some odd prime which does not divide $|\mathrm{SU}_n(2)|$.

First consider the case $m > n/2$. Applying Proposition 10.2(i) to the pullback $t=1$ of $\mathcal{F}(f,a,b)$, we see that $|G_{\mathrm{geom}}|$ is divisible by 2^m+1. Since $2m_i \neq 6$, $2^{2m}-1$ has a primitive prime divisor ℓ by [Zs]. Then ℓ certainly divides both 2^m+1 and $|G_{\mathrm{geom}}|$. Suppose ℓ divides $|\mathrm{SU}_n(2)|$. Then there is some $1 \leq k \leq n$ such that ℓ divides $2^k-(-1)^k$. In particular, $\ell|(2^{2k}-1)$. The primitivity of ℓ implies that $2m$ divides $2k$. But $2m > n$ and $2k \leq 2n$, so $k=m$. It follows that ℓ divides $2^k-(-1)^k = 2^m-1$, contradicting the choice of ℓ. Thus ℓ does not divide $|\mathrm{SU}_n(2)|$, as desired.

Assume now that $2 \leq m < n/2$. Suppose that some prime r divides both 2^n+1 and 2^m+1. Then r divides $\gcd(2^{2n}-1, 2^{2m}-1) = 2^{2e}-1$ for $e := \gcd(n,m)$. As $2 \nmid n$, e is odd, and so $2e$ divides m. But in this case, r divides 2^m-1 and so cannot divide 2^m+1, a contradiction. Thus 2^n+1 and 2^m+1 are coprime. Hence, by Proposition 10.2(ii) applied to the pullback $t=1$ of $\mathcal{F}(f,a,b)$, $|G_{\mathrm{geom}}|$ is divisible by $2^{n-m}-1$. Note that $n \geq 3$ and $n-m > n/2$ is odd, so $n-m \geq 3$. By [Zs], $2^{n-m}-1$ admits a primitive prime divisor ℓ_1. Suppose ℓ_1 divides $|\mathrm{SU}_n(2)|$. Then there is some $1 \leq k \leq n$ such that ℓ_1 divides $2^k-(-1)^k$. In particular, $\ell_1|(2^{2k}-1)$. The primitivity of ℓ_1 implies that $n-m$ divides $2k$, and hence $n-m$ divides k since $n-m$ is odd. But $2(n-m) > n \geq k$, so $k = n-m$. It follows that ℓ_1 divides $2^k-(-1)^k = 2^{n-m}+1$, contradicting the choice of ℓ_1. Thus ℓ_1 does not divide $|\mathrm{SU}_n(2)|$, and we are done in this case as well. □

11. Semicontinuity

First we recall some results from [Ka2, 8.17, 8.18].

The situation we consider is the following. We are given a normal connected affine noetherian scheme $S = \mathrm{Spec}\,(A)$ with A a noetherian normal integral domain with fraction field K, and a chosen algebraic closure $\overline{K}$ of K. Thus $\mathrm{Spec}\,(K)$ is a generic point η of S, and $\mathrm{Spec}\,(\overline{K})$ is a geometric generic point $\overline{\eta}$ of S. We are given X/S a smooth S-scheme of relative dimension D, with geometrically connected fibres, and $\phi \in X(S)$ a section of X/S. Then $\phi(\overline{\eta})$ is a geometric generic point of X. We are given a finite group G and a surjective homomorphism

$$\pi_1(X, \phi(\overline{\eta})) \twoheadrightarrow G.$$

For each geometric point s of S, $\phi(s)$ is a geometric point of X_s (and also of X). We have a continuous group homomorphism

$$\pi_1(X_s, \phi(s)) \to \pi_1(X, \phi(s)) \cong \pi_1(X, \phi(\overline{\eta})).$$

This last isomorphism is only canonical up to inner automorphism of the target group $\pi_1(X, \phi(\overline{\eta}))$. By composition, we get a group homomorphism

$$\pi_1(X_s, \phi(s)) \to G$$

which is well defined up to inner automorphism of G. This applies in particular with s taken to be $\overline{\eta}$. We are interested in how the image of $\pi_1(X_s, \phi(s))$ in G compares with the image of $\pi_1(X_{\overline{\eta}}, \phi(\overline{\eta}))$ in G: when are these two subgroups of G conjugate in G? Let us denote these image groups G_s and $G_{\overline{\eta}}$.

Theorem 11.1. *There exists a dense open set $U \subset S$ such that for any geometric point $s \in U$, G_s and $G_{\overline{\eta}}$ are conjugate subgroups of G. Moreover, for any geometric point $s \in S$, G_s is conjugate to a subgroup of $G_{\overline{\eta}}$.*

Proof. We first reduce to the case when $G_{\overline{\eta}} = G$.

Consider the scheme X_η, a smooth K-scheme, and compare it to the smooth $\overline{K}$-scheme $X_{\overline{\eta}}$. We have the π_1 short exact sequence

$$1 \to \pi_1(X_{\overline{\eta}}, \phi(\overline{\eta})) \to \pi_1(X_\eta, \phi(\overline{\eta})) \to \mathrm{Gal}(\overline{K}/K) \to 1.$$

The scheme X_η has the same function field as X, so the canonical map is surjective:

$$\pi_1(X_\eta, \phi(\overline{\eta})) \twoheadrightarrow \pi_1(X, \phi(\overline{\eta})).$$

Thus the image of $\pi_1(X_\eta, \phi(\overline{\eta}))$ is G, while the image of $\pi_1(X_{\overline{\eta}}, \phi(\overline{\eta}))$ is a normal subgroup H of G, with G/H the Galois group of some finite Galois extension L/K. View $X_{\overline{\eta}}$ as $X \otimes_A \overline{K}$. Then for the finite Galois extension L/K, $\pi_1(X_{\overline{\eta}}, \phi(\overline{\eta}))$ and $\pi_1(X \otimes_A L, \phi(\overline{\eta}))$ have the same image H.

Now replace S by T:=the normalization of S in L (i.e., the Spec of the integral closure of A in L), replace X by $X_T := X \times_S T$, and replace ϕ by the section ϕ_T (in terms of the finite map $f : T \to S$, ϕ_T is $(\phi \circ f) \times id_T$ as map to $X \times_S T$). In this new situation, the image H of $\pi_1((X_T)_{\phi_T(\overline{\eta})}, \phi_T(\overline{\eta}))$ is equal to the image of $\pi_1(X_T, \phi_T(\overline{\eta}))$. Because L/K is separable (being Galois), one knows that $f : T \to S$ is both finite and surjective. Being finite, it is proper. Thus f is closed. Hence the image of a dense open set $V = T \smallsetminus Z$ of T contains the dense open set $U := S \smallsetminus f(Z)$ of S.

Returning to the original notation (X, S, ϕ, G), this completes reduction to the case when $G_{\overline{\eta}} = G$, for G the image of $\pi_1(X, \phi(\overline{\eta}))$. In this case, every G_s is visibly (conjugate to) a subgroup of G (by the homomorphism

$$\pi_1(X_s, \phi(s)) \to \pi_1(X, \phi(s)) \cong \pi_1(X, \phi(\overline{\eta})).$$

Let $E \to X$ denote the finite etale G-covering classified by the surjection

$$\pi_1(X, \phi(\overline{\eta})) \twoheadrightarrow G.$$

Precisely because this is a surjection, E is connected. Being finite etale over X, which is in turn smooth over the normal scheme S, we see that E is itself smooth over S, of relative dimension d. Let us denote by

$$g : E \to S$$

the structural morphism.

Then E_s is a finite etale G-covering of X_s, but it may not be connected. One has $G_s = G$ if and only if E_s, which is smooth over s of dimension d, is itself connected (or equivalently geometrically irreducible, being smooth over s). [Indeed, the index of G_s in G is the number of geometrically irreducible components of E_s.]

For any prime ℓ invertible on S, the $\mathbb{F}_\ell$-rank of the stalk at s of $R^{2d}g_!(\mathbb{F}_\ell)$ is the number of geometrically irreducible components of E_s. By general constructibility theorems, $R^{2d}g_!(\mathbb{F}_\ell)$ is a constructible sheaf on S, so on a dense open set has constant rank. But at the generic point $\overline{\eta}$, the rank is one (precisely because $G_{\overline{\eta}} = G$). Therefore the rank is one on some dense open set U. Thus for every $s \in U$, we have $G_s = G$. [If there is no prime ℓ invertible on S, pick any two distinct primes, say $2, 3$, and work separately on $S[1/2]$ and on $S[1/3]$.] For a more direct proof, see [EGA, 9.7.8] or [StPr, Lemma 37.27.5]. □

Corollary 11.2. *Hypotheses and notations as in Theorem 11.1, suppose that for some geometric point $s_0 \in S$, $G_{s_0} = G$. Then $G_{\overline{\eta}} = G_{s_0} = G$, and hence there exists a dense open set U of S such that we have $G_s = G$ for every geometric point $s \in S$.*

Proof. We have the inclusion, up to conjugation, $G_{s_0} \subset G_{\overline{\eta}}$. We also have the inclusion $G_{\overline{\eta}} \subset G$, simply via the map $\pi_1(X_{\overline{\eta}}, \phi(\overline{\eta})) \to \pi_1(X, \phi(\overline{\eta}))$. Thus $G = G_{s_0} \subset G_{\overline{\eta}} \subset G$, whence $G_{\overline{\eta}} = G$, and we apply Theorem 11.1. □

Here is a particular instance of Corollary 11.2.

Proposition 11.3. *Let p be a prime, $q = p^f$, χ a (possibly trivial) multiplicative character of $\mathbb{F}_q^\times$, $r \geq 2$ an integer, and let $A > B_1 > \ldots > B_r \geq 1$ be integers with $\gcd(A, B_1, \ldots, B_r) = 1$ and $p \nmid AB_1 \ldots B_r$. Consider the local system $\mathcal{F}(A, B_1, \ldots, B_r, \chi)$ on $\mathbb{A}^r/\mathbb{F}_q$ with trace function for any finite extension $L/\mathbb{F}_q$*

$$(t_1, \ldots, t_r) \in L^r \mapsto -\frac{1}{\sqrt{\#L}} \sum_x \psi_L\big(x^A + t_1 x^{B_1} + \ldots + t_r x^{B_r}\big)\chi(x),$$

in characteristic p, of rank $D = A - 1$ if $\chi = \mathbb{1}$ and $D = A$ otherwise, with geometric monodromy group $G = G_{\mathrm{geom}}$. Given a choice $i_0 \in [1, k]$ and a polynomial $f(x) \in \overline{\mathbb{F}_p}[x]$ of the form

$$f(x) = \sum_{1 \leq i \leq r,\, i \neq i_0} a_i x^{B_i},$$

denote by $\mathcal{F}(A, B_{i_0}, f, \chi)$ the local system on $\mathbb{A}^1/K_f$ for $K_f := \mathbb{F}_q(\text{all coefficients of } f)$ whose trace function, for any finite extension L/K_f is

$$t \in L \mapsto -\frac{1}{\sqrt{\#L}} \sum_x \psi_L\big(x^A + t x^{B_{i_0}} + f(x)\big)\chi(x),$$

and by $\mathcal{F}(A, B_{i_0}, f = 0, \chi)$ the local system on $\mathbb{A}^1/\mathbb{F}_q$ whose trace function, for any finite extension $L/\mathbb{F}_q$ is

$$t \in L \mapsto -\frac{1}{\sqrt{\#L}} \sum_x \psi_L\big(x^A + t x^{B_{i_0}}\big)\chi(x).$$

Suppose that $\mathcal{F}(A, B_1, \ldots, B_r, \chi)$ has finite geometric monodromy group G, and that the specialized local system $\mathcal{F}(A, B_{i_0}, f = 0, \chi)$ has the same geometric monodromy group G. Then in the $\mathbb{A}^{r-1}/\mathbb{F}_p$ of possible f, there is an open dense set $U \subset \mathbb{A}^{r-1}$ such that for any $f \in U$, the specialized local system $\mathcal{F}(A, B_{i_0}, f = 0, \chi)$ has the same geometric monodromy group G.

Here are some examples. In the first two of these examples, we are given $r + 1$ integers

$$n > m_1 > \ldots > m_r \geq 0$$

with $2 | nm_1 \ldots m_r$, $\gcd(n, m_1, \ldots, m_r) = 1$.

(i) $p = 2$, $q = 2^f$, $A = q^n + 1$, $r \ge 2$, $B_i = q^{m_i} + 1$ for $1 \le i < r$, and either ($m_r > 0$, $B_r = q^{m_r} + 1$) or ($B_r = 1$, $m_r = 0$, and $2|nm_1 \ldots m_{r-1}$). Suppose that $2|nm_{i_0}$ and $\gcd(n, m_{i_0}) = 1$. Then $\mathcal{F}(A, B_{i_0}, f = 0, \mathbb{1})$ has the same geometric monodromy group G as does $\mathcal{F}(A, B_1, \ldots, B_r, \mathbb{1})$, namely the group $2_-^{1+2nf} \cdot \Omega_{2n}^-(q)$. Simplest example: $i_0 = 1$ and $m_1 = n-1$. The calculations of the monodromy groups are Theorem 11.2.3 (ii) and Theorem 10.3.13(iii) of [KT6] for $q^n > 8$ and Theorem 4.4 for $q^n = 4, 8$.

(ii) $p > 2$, $q = p^f$, χ is either $\mathbb{1}$ or the quadratic character χ_2, $A = (q^n + 1)/2$, $B_i = (q^{m_i} + 1)/2$, $1 \le i \le k$, where $n > m_1 > \ldots > m_r \ge 0$ are integers with $2|nm_1 \ldots m_r$, $\gcd(n, m_1, \ldots, m_r) = 1$, and $\chi = \mathbb{1}$ or $\chi = \chi_2$. Suppose that $2|nm_{i_0}$ and $\gcd(n, m_{i_0}) = 1$. Then $\mathcal{F}(A, B_{i_0}, f = 0, \chi)$ has the same geometric monodromy group G as does $\mathcal{F}(A, B_1, \ldots, B_r, \chi)$, namely the image of $\mathrm{Sp}_{2n}(q)$ in one of its irreducible Weil representations of degree D, with $D = A - 1$ for $\chi = \mathbb{1}$ and $D = A$ for $\chi = \chi_2$. Simplest example: $i_0 = 1$ and $m_1 = n-1$. The calculations of the monodromy groups are Theorem 11.2.3 (i) and Theorem 10.3.13(i) of [KT6].

(iii) p arbitrary, $q = p^f$. In this third example, $n > m_1 > \ldots > m_r \ge 1$ are all odd, and $\gcd(n, m_1, \ldots, m_r) = 1$, χ is a character of $\mathbb{F}_{q^2}^\times$ of order dividing $q + 1$. Suppose that $\gcd(n, m_{i_0}) = 1$. Then $\mathcal{F}(A, B_{i_0}, f = 0, \chi)$ has the same geometric monodromy group G as does $\mathcal{F}(A, B_1, \ldots, B_r, \chi)$, namely the image of $\mathrm{SU}_n(q)$ in a Weil representation of degree D, with $D = A - 1$ for $\chi = \mathbb{1}$ and $D = A$ for $\chi \ne \mathbb{1}$. Simplest example: $i_0 = 1$ and $m_1 = n - 2$. The calculations of the monodromy groups are Theorem 11.2.3 (iii) and Theorem 10.3.13(ii) of [KT6].

Remark 11.4. In the above examples, we need the existence of an index i_0 such that $\gcd(n, m_{i_0}) = 1$. So we have nothing to say about one-parameter specializations in cases such as $(n, m_1, \ldots m_r) = (6, 3, 2)$ or $(15, 6, 5, 3)$ or $(30, 5, 3, 2)$.

A second problem is that in the examples, although we know G_{geom} for an open dense set U of f's, we do not know which subgroups of G_{geom} can occur for f's not in U, nor for which f these smaller groups occur.

Next we consider some one- and two-parameter systems in characteristic $p = 2$. We begin with a lemma on generalized Pink–Sawin sheaves.

Lemma 11.5. *Let p be a prime, $n \ge 1$ an integer, $k/\mathbb{F}_p$ a finite extension, and $f(x) \in k[x]$ a polynomial of the form*

$$f(x) = \sum_{i=1}^{n} a_i x^{1+p^i}, \quad a_n \in k^\times.$$

Denote by $\mathcal{F}_f$ the lisse sheaf on $\mathbb{A}^1/k$ whose trace function at a point $t \in L$, for L/k a finite extension, is

$$t \mapsto (-1/\sqrt{\#L}) \sum_{x \in L} \psi_L(f(x) + tx),$$

i.e., $\mathcal{F}_f$ is, up to the Tate twist $(1/2)$ which makes it pure of weight zero, the Fourier Transform $FT_\psi(\mathcal{L}_{\psi(f)})$. Then there exists an explicit finite extension L_0/k such that for every finite extension L_1/L_0, and every $t \in L_1$,

$$|\mathrm{Trace}(\mathrm{Frob}_{t,L_1}|\mathcal{F}_f)|^2 = p^{2n}.$$

Proof. This is an instance of the argument of [vdG-vdV, Section 5]. Write

$$f(x) = xR(x)$$

for $R(x)$ the additive polynomial $\sum_{i=1}^n a_i x^{p^i}$. Then

$$|\mathrm{Trace}(\mathrm{Frob}_{t,L_1}|\mathcal{F}_f)|^2 = (1/\#L_1)\sum_{x,y\in L_1}\psi_{L_1}(xR(x)+tx-yR(y)-ty) =$$

(substituting $(x,y)\mapsto(x+y,y)$ and remembering that $R(x+y)=R(x)+R(y)$)

$$= (1/\#L_1)\sum_{x,y\in L_1}\psi((x+y)R(x+y)+tx+ty-yR(y)-ty) =$$

$$= (1/\#L_1)\sum_{x\in L_1}\psi_{L_1}(xR(x)+tx)\sum_{y\in L}\psi_L(yR(x)+xR(y)).$$

For the inner sum, the $\mathrm{Trace}_{L_1/\mathbb{F}_p}$ of $yR(x)+xR(y)$ is equal to the $\mathrm{Trace}_{L_1/\mathbb{F}_p}$ of

$$y(\sum_i a_i x^{p^i}) + y(\sum_i (a_i x)^{p^{-1}}).$$

Let us denote by

$$W_R(L_1) := \{x\in L_1|(\sum_i a_i x^{p^i}) + (\sum_i (a_i x)^{p^{-i}}).$$

Equivalently, $W_R(L_1)$ is the set of zeroes in L_1 of the additive polynomial

$$P_R(x) := \sum_{i=1}^n a_i x^{p^{n+i}} + \sum_{i=1}^n a_i^{p^{n-i}} x^{p^{n-i}}.$$

The sum

$$(1/\#L_1)\sum_{y\in L_1}\psi_{L_1}(yR(x)+xR(y)) = (1/\#L_1)\sum_{y\in L_1}\psi_{L_1}(yP_R(x)),$$

which is 1 if $P_R(x)=0$, and zero otherwise.

Take for L_0 a field containing $\mathbb{F}_{p^2}$ all the p^{2n} roots of $P_R(x)$. [Notice that the highest degree term of $P_R(x)$ is $a_n x^{p^{2n}}$ and its lowest degree term is $a_n x$, so its derivative is the nonzero constant a_n, and hence $P_R(x)$ has p^{2n} distinct zeroes over $\overline{\mathbb{F}_p}$]. Then

$$|\mathrm{Trace}(\mathrm{Frob}_{t,L_1}|\mathcal{F}_f)|^2 = \sum_{x\in W_R(L_1}\psi_{L_1}(xR(x)+tx).$$

One checks that the map $x\mapsto\psi_{L_1}(xR(x)+tx)$ is a μ_p valued character of the finite abelian group $W_R(L_1)$, so the sum $\sum_{x\in W_R(L_1)}\psi_{L_1}(xR(x)+tx)$ is either 0, if the character is nontrivial, or is $\#W_R(L_1)$. But over any extension L_1/L_0, $W_R(L_1)=W_R(L_0)$, whose cardinality is p^{2n}. ☐

Corollary 11.6. *Keep the notation and assumption of Lemma 11.5. For every finite extension L_1/L_0 and every $t\in L_1$, $\mathrm{Trace}(\mathrm{Frob}_{t,L_1}|\mathcal{F}_f)$ is either 0 or $\pm p^n\zeta$ for some $\zeta\in\mu_p$.*

Proof. The trace lies in $\mathbb{Z}[\zeta_p]$ and divides p^{2n} in that ring, so is a unit at all places outside p, while at the unique place over p of $\mathbb{Q}(\zeta_p)$ it and its complex conjugate each have absolute value p^n. By the product formula, this trace, divided by p^n, is an element of $\mathbb{Z}[\zeta_p]$ all of whose absolute values (at **all** places) are 1, hence is a root of unity in $\mathbb{Z}[\zeta_p]$. ☐

Theorem 11.7. *Let $p=2$, $q=p^f$, $r\geq 2$, $n>m_1>\ldots>m_r\geq 0$, $\gcd(n,m_1,\ldots,m_r)=1$, $2|nm_1\ldots m_r$, and $A=q^n+1$, $B_i=q^{m_i}+1$, $1\leq i\leq r-1$, and either $B_r=q^{m_r}+1$ with $m_r\geq 1$ or $(B_r,m_r)=(1,0)$. Recall, see* [KT6, Theorem 11.2.3(ii)] *and Theorem 4.4, that the local system $\mathcal{F}_{\mathrm{up}} := \mathcal{F}(A,B_1,\ldots,B_r)$ has $G_{\mathrm{geom},\mathcal{F}_{\mathrm{up}}} =: G_{\mathrm{up}}$ equal to $2_-^{1+2nf}\rtimes\mathrm{SU}_n(q)$ if $B_r=1$ and $2\nmid nm_1\ldots m_{r-1}$, and $2_-^{1+2nf}\cdot\Omega_{2n}^-(q)$ otherwise. Assume in addition that $(q,r,n,m_1,m_2)\neq$*

$(2,2,3,1,0)$. *Fix a choice of* $1 \le i \le j \le r$. *If* $i = j$, *set* $d := 1$. *If* $i < j$, *set* $d := 2$ *and assume* $r \ge 3$. *For* f *in the space* $\mathbb{A}^{r-d}$ *of all polynomials*

$$f(x) = \sum_{1 \le k \le r,\, k \ne i,j} c_k x^{B_k},$$

denote by $\mathcal{F}(A, B_i, B_j, f)$ *the local system on* $\mathbb{A}^d$ *whose trace function is*

$$t \in L \mapsto \frac{-1}{\sqrt{\#L}} \sum_{x \in L} \psi_L\big(x^A + tx^{B_i} + f(x)\big)$$

when $i = j$ *and*

$$(s,t) \in L^2 \mapsto \frac{-1}{\sqrt{\#L}} \sum_{x \in L} \psi_L\big(x^A + tx^{B_i} + sx^{B_j} + f(x)\big)$$

when $i < j$. *Then one of the following statements holds.*

(i) *There is an open dense set* $U \subset \mathbb{A}^{r-d}$ *such that for any* $f \in U$, $\mathcal{F}(A, B_i, B_j, f)$ *has* $G_{\rm geom}$ *the group* $G_{\rm up}$.
(ii) $i = j$, *and for all* $f \in \mathbb{G}_m^{r-1}$, $\mathcal{F}(A, B_i, B_i, f)$ *has* $G_{\rm geom}$ *the extraspecial* 2*-group* 2_-^{1+2nf}.

In particular, conclusion (i) *holds if* $i < j$. *Moreover, conclusion* (ii) *holds if and only if* $i = j$ *and* $B_i = 1$.

Proof. We first note that each $\mathcal{F}(A, B_i, B_j, f)$ is a pullback of $\mathcal{F}_{\rm up}$, so its $G_{{\rm geom},\mathcal{F}(A,B_i,B_j,f)}$ is a subgroup of $G_{\rm up}$, well defined up to conjugacy in $G_{\rm up} = E \cdot S$, where $E = 2_-^{1+2nf}$ and $S = {\rm SU}_n(q)$, respectively $S = \Omega_{2n}^-(q)$. We further note that, so long as all coefficients of f are nonzero, the group $G_{{\rm geom},\mathcal{F}(A,B_i,B_j,f)}$ is an irreducible subgroup of ${\rm Sp}_{q^n}(\mathbb{C})$, cf. [KT4, Prop. 2.4]. By the specialization Theorem 11.1, there is a subgroup $G_0 \le G_{\rm up}$, well defined up to conjugacy in $G_{\rm up}$, and a dense open set $U \subset \mathbb{A}^{r-d}$ such that for every $f \in U$, $G_{{\rm geom},\mathcal{F}(A,B_i,B_j,f)}$ is conjugate to G_0. Concretely, there is a nonzero polynomial $P(x_k \mid 1 \le k \le r,\ k \ne i,j)$ in $r-d$ variables over $\overline{\mathbb{F}_q}$ such that any $f(x) = \sum_{1 \le i \le m,\, i \ne i,js} c_i x^{B_i}$ with $P(c_k \mid 1 \le k \le r,\ k \ne i,j) \ne 0$ lies in U. Let us denote $U_{\rm up} \subset \mathbb{A}^r$ (with coordinates $(s_1, \ldots, s_r)$) the dense open set on which $P(s_k \mid 1 \le k \le r,\ k \ne i,j) \ne 0$. Replacing P by $P \prod_{k \ne i,j} x_k$, we reduce to the case when every $f \in U$ has all coefficients nonzero, and hence for every $f \in U$, $G_{{\rm geom},\mathcal{F}(A,B_i,B_j,f)}$ is an irreducible subgroup of ${\rm Sp}_{q^n}(\mathbb{C})$. In particular, the group G_0 is an irreducible subgroup of ${\rm Sp}_{q^n}(\mathbb{C})$.

Because $U_{\rm up} \subset \mathbb{A}^r$ is a dense open set, $\mathcal{F}_{\rm up}$ on $\mathbb{A}^r$ and $\mathcal{F}_{\rm up}|_{U_{\rm up}}$ on $U_{\rm up}$ have the same $G_{\rm geom}$, namely $G_{\rm up}$. Both $G_{\rm up}$ and the arithmetic group $G_{{\rm arith},\mathcal{F}_{\rm up},\mathbb{F}_2}$ are finite, with $G_{\rm up} \lhd G_{{\rm arith},\mathcal{F}_{\rm up}} \le {\rm Sp}_{q^n}(\mathbb{C})$, with the quotient $G_{{\rm arith},\mathcal{F}_{\rm up},\mathbb{F}_2}/G_{\rm up}$ a finite cyclic group. In the case $S = \Omega_{2n}^-(q)$, one knows that

$$\mathbf{N}_{{\rm Sp}_{q^n}(\mathbb{C})}(G_{\rm up}) \le E \cdot {\rm O}_{2n}^-(q) \cdot C_f$$

contains $G_{\rm up}$ with index dividing $2f$. In the case $S = {\rm SU}_n(q)$, our assumptions imply that $(n,q) \ne (3,2)$, whence S is simple and

$$\mathbf{N}_{{\rm Sp}_{q^n}(\mathbb{C})}(G_{\rm up}) \le E \cdot {\rm GU}_n(q) \cdot C_{2f}$$

contains $G_{\rm up}$ with index dividing $2f(n+1)$, see [KT6, Proposition 8.4.1(b2)]. [For completeness, we note that when $S = {\rm SU}_n(q)$ with $(n,q) = (3,2)$, $G_{{\rm arith},\mathcal{F}_{\rm up},\mathbb{F}_2}$ has index 2 over $G_{{\rm geom},\mathcal{F}_{\rm up}}$ by Theorem 4.4(iii).]

Thus over any extension $L/\mathbb{F}_{q^{2n+2}}$, $G_{{\rm arith},\mathcal{F}_{\rm up},L} = G_{\rm up}$. By the finite group version [KaS, Theorem 9.7.13] of Deligne's equidistribution theorem, applied to $\mathcal{F}_{\rm up}|_{U_{\rm up}}$, over any sufficiently large finite extension $L/\mathbb{F}_{q^{2n+2}}$, every element $\gamma \in G_{\rm up}$ is conjugate to some Frobenius ${\rm Frob}_{(s_1,\ldots s_r),L}$ with $(s_1,\ldots,s_r) \in U_{\rm up}(L)$. Such a Frobenius is ${\rm Frob}_{s_i,s_j,L}$ on $\mathcal{F}(A,B_i,B_j,f)$ for

$$f(x) = \sum_{1\le k\le m,\, k\neq i,j} s_k x^{B_k}.$$

Now view $G_{{\rm geom},\mathcal{F}(A,B_i,B_j,f)}$ as a subgroup of $G_{\rm up}$. Then ${\rm Frob}_{s_i,s_j,L}$ lies in $G_{{\rm arith},\mathcal{F}(A,B_i,B_j,f)}$, so normalizes $G_{{\rm geom},\mathcal{F}(A,B_i,B_j,f)}$. But $G_{{\rm geom},\mathcal{F}(A,B_i,B_j,f)}$ is conjugate in $G_{\rm up}$ to G_0, and hence, every conjugacy class in $G_{\rm up}$ contains an element that normalizes G_0. Thus the normalizer $\mathbf{N}_{G_{\rm up}}(G_0)$ of G_0 in $G_{\rm up}$ meets every conjugacy class in $G_{\rm up}$. Therefore

$$\mathbf{N}_{G_{\rm up}}(G_0) = G_{\rm up},$$

whence

$$G_0 \lhd G_{\rm up}.$$

In particular, EG_0/E is a normal subgroup of the simple group $G_{\rm up}/E \cong S$, whence $EG_0 = E$ or $EG_0 = G_{\rm up}$. Note that any proper subgroup of E has order $\le q^{2n}$ and so cannot be irreducible on $\mathbb{C}^{q^n}$, and thus the only irreducible subgroup of E is E itself. Furthermore, $M_{2,2}(E) = q^{2n} > q+1$, whereas $G_{{\rm geom},\mathcal{F}(A,B_i,B_j,f)}$ with $i<j$ has the same $M_{2,2}$ as that of $G_{\rm up}$, which is equal to $q+1$, by Theorems 9.1 and 9.2. Hence in the former case, we must have that $G_0 = E$, $i=j$, and furthermore $B_i = 1$ by Proposition 10.2, and thus conclusion (ii) holds by Theorem 11.1.

In the latter case, $(E\cap\mathbf{Z}(E)G_0)/\mathbf{Z}(E)$ is a normal subgroup in $G_{\rm up}/\mathbf{Z}(E) = (E/\mathbf{Z}(E)\cdot S$ contained in $E/\mathbf{Z}(E)$. But S acts irreducibly on $E/\mathbf{Z}(E) = \mathbb{F}_2^{2nf}$, so either $E\cap\mathbf{Z}(E)G_0 = \mathbf{Z}(E)$ or $\mathbf{Z}(E)G_0 \ge E$. However, since $EG_0 = G_{\rm up}$ and $G_0 \lhd G_{\rm up}$, the first possibility leads to $G_{\rm up}/\mathbf{Z}(E) \cong E/\mathbf{Z}(E)\times S$, which is impossible. So $\mathbf{Z}(E)G_0 \ge E$, in which case we have

$$G_0 = [G_0,G_0] = [\mathbf{Z}(E)G_0, \mathbf{Z}(E)G_0] \ge [E,E] = \mathbf{Z}(E)$$

(since $\mathbf{Z}(E) = \mathbf{Z}(G_{\rm up})$), whence $G_0 = \mathbf{Z}(E)G_0 = EG_0 = \tilde{G}$ and (i) holds.

Assume now that $i=j$ and $B_i = 1$. By Corollary 11.6, $\varphi(x) \in \{\pm q^n, 0\}$ for all $x \in G_0$, where φ denotes the character of the underlying representation. It follows that $[\varphi,\varphi]_{G_0} = q^{2n}|\mathbf{Z}(G_0)|/|G_0|$. As $\mathbf{Z}(G_0) = \mathbf{Z}(E) \cong C_2$ and $\varphi \in {\rm Irr}(G_0)$, we conclude that $|G_0| = 2q^{2n} = |E|$, and hence $G_0 = E$. □

Here is the odd-p analogue of the above result:

Theorem 11.8. *Let $p>2$, $q=p^f$, $r\ge 2$, $n > m_1 > \ldots > m_{r-1} > 0$, $\gcd(n,m_1,\ldots,m_{r-1}) = 1$, and $A = q^n+1$, $B_i = q^{m_i}+1$, $1\le i\le r-1$, and $B_r = 1$. Recall, see* [KT6, Theorem 11.2.3(i-bis)], *that the local system $\mathcal{F}_{\rm up} := \mathcal{F}(A,B_1,\ldots,B_r)$ has $G_{{\rm geom},\mathcal{F}_{\rm up}} =: G_{\rm up}$ equal to $p_+^{1+2nf} \rtimes {\rm SU}_n(q)$ if $2 \nmid nm_1\ldots m_{r-1}$, and $p_+^{1+2nf} \rtimes {\rm Sp}_{2n}(q)$ otherwise. Fix a choice of $1\le i\le j\le r$. If $i=j$, set $d:=1$. If $i<j$, set $d:=2$ and assume $r\ge 3$. For f in the space $\mathbb{A}^{r-d}$ of all polynomials*

$$f(x) = \sum_{1\le k\le r,\, k\neq i,j} c_k x^{B_k},$$

denote by $\mathcal{F}(A,B_i,B_j,f)$ the local system on $\mathbb{A}^d$ whose trace function is

$$t\in L \mapsto \frac{-1}{\sqrt{\#L}}\sum_{x\in L}\psi_L\big(x^A + tx^{B_i} + f(x)\big)$$

when $i=j$ and

$$(s,t)\in L^2 \mapsto \frac{-1}{\sqrt{\#L}}\sum_{x\in L}\psi_L\big(x^A + tx^{B_i} + sx^{B_j} + f(x)\big)$$

when $i<j$. Then one of the following statements holds.

(i) *There is an open dense set* $U \subset \mathbb{A}^{r-d}$ *such that for any* $f \in U$, $\mathcal{F}(A, B_i, B_j, f)$ *has* $G_{\rm geom}$ *the group* $G_{\rm up}$.

(ii) $i = j$, *and for all* $f \in \mathbb{G}_m^{r-1}$, $\mathcal{F}(A, B_i, B_i, f)$ *has* $G_{\rm geom}$ *the extraspecial p-group* p_+^{1+2nf}.

In particular, conclusion (i) *holds if* $i < j$. *Moreover, conclusion* (ii) *holds if and only if* $i = j$ *and* $B_i = 1$.

Proof. We can follow the proof of Theorem 11.7 almost verbatim. Note that since $n \geq 2$, $S = \mathrm{Sp}_{2n}(q)$, respectively $\mathrm{SU}_n(q)$ with $2 \nmid n$, is quasisimple. We also use the fact that $G_{\mathrm{geom},\mathcal{F}(A,B_i,B_j,f)}$ has no nontrivial p'-quotient to show that, if G_0 is contained in $E\mathbf{Z}(S)$ then $G_0 \leq E$ for $E = p_+^{1+2nf}$. □

We can be much more precise in the quasisimple case:

Theorem 11.9. *Let* p *be a prime,* $q = p^f$, $r \geq 2$. *Suppose that either*

(a) $p > 2$, $n > m_1 > \ldots > m_r \geq 0$ *with* $2 | n m_1 \ldots m_r$, $\gcd(n, m_1, \ldots, m_r) = 1$, $A = (q^n + 1)/2$, $B_i = (q^{m_i} + 1)/2$, $1 \leq i \leq r$, *and* $\chi = \mathbb{1}$ *or* χ_2; *or*

(b) $n > m_1 > \ldots > m_r \geq 1$ *with* $2 \nmid n m_1 \ldots m_r$, $\gcd(n, m_1, \ldots, m_r) = 1$, $A = (q^n + 1)/(q + 1)$, $B_i = (q^{m_i} + 1)/(q + 1)$, $1 \leq i \leq r$, *and* $\chi^{q+1} = \mathbb{1}$.

Recall, see [KT6, Theorem 11.2.3(i), (iii)], *that the local system* $\mathcal{F}_{\rm up} := \mathcal{F}(A, B_1, \ldots, B_r, \chi)$ *has* $G_{\mathrm{geom},\mathcal{F}_{\rm up}} =: G_{\rm up}$ *equal to the image of* $S := \mathrm{Sp}_{2n}(q)$ *in case* (a) *and* $S := \mathrm{SU}_n(q)$ *in case* (b), *in a Weil representation of degree* $D = \mathrm{rank}(\mathcal{F}_{\rm up})$. *Fix a choice of* $1 \leq i \leq j \leq r$. *If* $i = j$, *set* $d := 1$. *If* $i < j$, *set* $d := 2$ *and assume* $r \geq 3$. *For* f *in the space* $\mathbb{A}^{r-d}$ *of all polynomials*

$$f(x) = \sum_{1 \leq k \leq r,\, k \neq i,j} c_k x^{B_k},$$

denote by $\mathcal{F}(A, B_i, B_j, f, \chi)$ *the local system on* $\mathbb{A}^d$ *whose trace function is*

$$t \in L \mapsto \frac{-1}{\sqrt{\#L}} \sum_{x \in L} \psi_L\big(x^A + t x^{B_i} + f(x)\big)\chi(x)$$

when $i = j$ *and*

$$(s, t) \in L^2 \mapsto \frac{-1}{\sqrt{\#L}} \sum_{x \in L} \psi_L\big(x^A + t x^{B_i} + s x^{B_j} + f(x)\big)\chi(x)$$

when $i < j$. *Then we have the following results.*

(i) *If* $i = j$, *there is an open dense set* $U \subset \mathbb{A}^{r-1}$ *such that for any* $f \in U$, $\mathcal{F}(A, B_i, B_j, f, \chi)$ *has* $G_{\rm geom}$ *the group* $G_{\rm up}$.

(ii) *In the case* $i < j$, *for any* $f \in (\mathbb{G}_m)^{r-2}$, *i.e., for any* f *having all coefficients nonzero,* $\mathcal{F}(A, B_i, B_j, f, \chi)$ *has* $G_{\rm geom}$ *the group* $G_{\rm up}$.

Proof. To prove (i), we follow the proof of Theorem 11.7 almost verbatim. In the Sp case, we have $n > m_1 > m_2 \geq 0$, so $n \geq 2$, and $\mathrm{Sp}_{2n}(q)$ is quasisimple for any odd q. In the SU case, we have $n > m_1 > m_2 \geq 1$ are all odd, so $n \geq 5$, and $\mathrm{SU}_n(q)$ is again quasisimple. We also use the fact that $G_{\mathrm{geom},\mathcal{F}(A,B_i,B_j,f,\chi)}$ is irreducible on $\mathcal{F}(A, B_i, B_j, f, \chi)$ of rank $D > 1$ to see that G_0 cannot be contained in the image of $\mathbf{Z}(S)$.

To prove (ii), we use the fact that when $i < j$, for any f all of whose coefficients are nonzero, $\mathcal{F}(A, B_i, B_j, f, \chi)$ has the same $M_{2,2}$ as $\mathcal{F}_{\rm up}$, cf. Theorem 2.3 and Corollary 2.5. The result is then immediate from Theorem 8.2 in the Sp case (since $r \geq 3$ implies $n \geq 3$ here), and from Theorem 8.4 in the SU case (since $r \geq 3$ implies $n \geq 7$ here). □

References

[Atlas] 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. With computational assistance from J. G. Thackray. Oxford University Press, Eynsham, 1985.

[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.

[De2] Deligne, P., La conjecture de Weil II, *Pub. Math. I.H.E.S.* **52** (1981), 313–428.

[Do] Dornhoff, L., Group representation theory, Dekker, New York, 1971.

[EGA] Grothendieck, A., Elements de géométrie algébrique (rédigés avec la collaboration de Jean Dieudonné): IV. Étude locale des schémas et des morhismes de schémas, Troisième partie, Pub. Math. IHES, tome 28 (1966), pp. 5.-255

[F] Feit, W., On large Zsigmondy primes, *Proc. Amer. Math. Soc.* **102** (1988), 28–36.

[GAP] The GAP group, GAP - groups, algorithms, and programming, Version 4.4, 2004, `http://www.gap-system.org`.

[Geck] Geck, M., Irreducible Brauer characters of the 3-dimensional special unitary groups in non-describing characteristic, *Comm. Algebra* **18** (1990), 563–584.

[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.

[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.

[HM] Hiss, G. and Malle, G., Low-dimensional representations of quasi-simple groups, *LMS J. Comput. Math.* **4** (2001), 22–63.

[Is] Isaacs, I. M., Character Theory of Finite Groups, AMS-Chelsea, Providence, 2006.

[Ka1] Katz, N., Gauss sums, Kloosterman sums, and monodromy groups, Annals of Mathematics Studies, **116**. Princeton Univ. Press, Princeton, NJ, 1988. ix+246 pp.

[Ka2] Katz, N., Exponential sums and differential equations. Annals of Mathematics Studies, **124**. Princeton Univ. Press, Princeton, NJ, 1990. xii+430 pp.

[Ka3] 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.

[Ka4] Katz, N., Moments, Monodromy, and Perversity. Annals of Mathematics Studies, **159**. Princeton University Press, Princeton, NJ, 2005. viii+475 pp.

[KaS] 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., and Tiep, P.H., Rigid local systems and finite symplectic groups, *Finite Fields Appl.* **59** (2019), 134–174.

[KT2] Katz, N., and Tiep, P.H., Moments of Weil representations of finite special unitary groups, *J. Algebra* **561** (2020), 237–255.

[KT3] Katz, N., and Tiep, P.H., Monodromy groups of Kloosterman and hypergeometric sheaves, *Geom. Funct. Analysis* **31** (2021), 562–662.

[KT4] 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.

[KT5] Katz, N., and Tiep, P.H., Hypergeometric sheaves and finite symplectic and unitary groups, *Cambridge J. Math.* **9** (2021), 577–691.

[KT6] Katz, N., and Tiep, P.H., Exponential sums, hypergeometric sheaves, and monodromy groups, (submitted).

[KT7] Katz, N., and Tiep, P.H., On a conjecture of Miyamoto, (in preparation).

[KlL1] Kleidman, P. B., and Liebeck, M. W., On a theorem of Feit and Tits, *Proc. Amer. Math. Soc.* **107** (1989), 315–322.

[KlL2] 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.

[L] Lang, S., Algebra, Third Edition, Addison-Wesley, 1993, xv+906pp.

[Li] Liebeck, M. W., The affine permutation groups of rank three, *Proc. London 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.

[StPr] Stacks Project, `https://stacks.math.columbia.edu`

[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.

[vdG-vdV] van der Geer, G., van der Vlugt, M., Reed-Muller codes and supersingular curves. I, *Compos. Math.* **84** (1992), 333–367.

[Zs] Zsigmondy, K., Zur Theorie der Potenzreste, *Monatsh. Math. Phys.* **3** (1892), 265–284.

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`