RIGID LOCAL SYSTEMS AND FINITE SYMPLECTIC GROUPS

NICHOLAS M. KATZ AND PHAM HUU TIEP

Abstract. For certain powers q of odd primes p, and certain integers $n \geq 1$, we exhibit explicit rigid local systems on the affine line in characteristic $p > 0$ whose geometric and arithmetic monodromy groups are $\mathrm{Sp}(2n, q)$.

Contents

1. Introduction

Let p be an odd prime, q a power of p, $n \geq 1$ an integer, with $nq > 3$ (to exclude the case $n = 1, q = 3$ of $\mathrm{SL}(2, 3)$). After the trivial representation, the next lowest dimensional (complex, irreducible) representations of the finite group $\mathrm{Sp}(2n, q)$ are

two of dimension $(q^n - 1)/2$, the "small" ones, and
two of dimension $(q^n + 1)/2$, the "large" ones.

The second author gratefully acknowledges the support of the NSF (grant DMS-1665014). The paper is partially based upon work supported by the NSF under grant DMS-1440140 while the second author was in residence at the Mathematical Sciences Research Institute in Berkeley, California, during the Spring 2018 semester. It is a pleasure to thank the Institute for support, hospitality, and stimulating environments.

These four representations are called the "individual" Weil representations. A remarkable fact about these representations of these groups is this. If we write $q = p^a$, then we have inclusions of groups

$$\mathrm{SL}(2, p^{an}) = \mathrm{SL}(2, q^n) \hookrightarrow \mathrm{Sp}(2n, q) \hookrightarrow \mathrm{Sp}(2na, p),$$

and the restriction of any of the individual Weil representations of the big group $\mathrm{Sp}(2na, p)$ is one of the individual Weil representations of $\mathrm{SL}(2, p^a n)$ and of the intermediate group $\mathrm{Sp}(2n, q)$.

If $q \equiv 1(\bmod 4)$, all four individual Weil representations of $\mathrm{Sp}(2n, q)$ are self dual. Each of the small ones is a faithful representation toward $\mathrm{Sp}((q^n - 1)/2, \mathbb{C})$, and each of the large ones factors through a faithful representation of the simple group $\mathrm{PSp}(2n, q)$ toward $\mathrm{SO}((q^n+1)/2, \mathbb{C})$.

If $q \equiv 3(\bmod 4)$, none of the four is self dual: the two small ones are duals of each other, and the two large ones are duals of each other. If in addition $q^n \equiv 1(\bmod 4)$, then each of the small ones is faithful toward $\mathrm{SL}((q^n - 1)/2, \mathbb{C})$, and each of the large ones factors through a faithful representation of the simple group $\mathrm{PSp}(2n, q)$ toward $\mathrm{SL}((q^n+1)/2, \mathbb{C})$. If, on the other hand, $q^n \equiv 3(\bmod 4)$, then each of the small ones factors through a faithful representation of the simple group $\mathrm{PSp}(2n, q)$ toward $\mathrm{SL}((q^n - 1)/2, \mathbb{C})$, and each of the large ones is faithful toward $\mathrm{SL}((q^n + 1)/2, \mathbb{C})$.

All four representations have characters which take values in the (ring of integers of) the field $\mathbb{Q}(\sqrt{\epsilon_q q})$, for ϵ_q the sign defined by

$$\epsilon_q := (-1)^{(q-1)/2},$$

so that $\epsilon_q = 1$ when $q \equiv 1(\bmod 4)$, and $\epsilon_q = -1$ when $q \equiv 3(\bmod 4)$.

Thus when q is a square, all four individual Weil representations have integer traces. When q is not a square, the characters of the two small (respectively of the two large) individual Weil representations are Galois conjugates, by $\mathrm{Gal}(\mathbb{Q}(\sqrt{\epsilon_q q})/\mathbb{Q})$, of each other.

There is a unique "matching" of small and large as follows. If we name the two small representations Small_1 and Small_2, there is a unique naming the large ones as Large_1 and Large_2 so that each of the direct sums, called the total Weil representations Weil_1 and Weil_2,

$$\mathsf{Weil}_1 := \mathrm{Small}_1 \oplus \mathrm{Large}_1,$$
$$\mathsf{Weil}_2 = \mathrm{Small}_2 \oplus \mathrm{Large}_2,$$

has the property that for each element $g \in \mathrm{Sp}(2n, q)$, the square trace $(\mathrm{Trace}(\mathsf{Weil}_i(g)))^2$ is a power of $\pm q$. More precisely, as g runs over $\mathrm{Sp}(2n, q)$, we attain precisely the powers $\{(\epsilon_q q)^i\}_{0 \le i \le 2n}$.

Another characterization of the correct matching is the property that for each element $g \in \mathrm{Sp}(2n, q)$, the square absolute value $|\mathrm{Trace}(\mathsf{Weil}_i(g))|^2$ is a non-negative power of p.

Yet another characterization of the correct matching is the property that for each element $g \in \mathrm{Sp}(2n, q)$, the square absolute value $|\mathrm{Trace}(\mathsf{Weil}_i(g))|^2$ is a non-negative power of q. As g runs over $\mathrm{Sp}(2n, q)$, we attain precisely the powers $\{q^i\}_{0 \le i \le 2n}$. In fact, one knows that

$$|\mathrm{Trace}(\mathsf{Weil}_i(g))|^2 = q^{\dim_{\mathbb{F}_q}(\mathrm{Ker}(g-1))},$$

with Ker taken here in the tautological representation of $\mathrm{Sp}(2n, q)$ on a $2n$-dimensional symplectic space over $\mathbb{F}_q$, but we will not use this more precise information.

It will also be important to pay attention to the parity of the dimensions of the individual Weil representations. If $q^n \equiv 1 (\mathrm{mod}\, 4)$, then Small_i is even dimensional and Large_i is odd dimensional. If $q^n \equiv 3 (\mathrm{mod}\, 4)$, then Small_i is odd dimensional and Large_i is even dimensional. So for $i = 1, 2$ we name them Even_i and Odd_i accordingly:

(1) If $q^n \equiv 1 (\mathrm{mod}\, 4)$, then $\mathrm{Even}_i := \mathrm{Small}_i$ and $\mathrm{Odd}_i := \mathrm{Large}_i$.
(2) If $q^n \equiv 3 (\mathrm{mod}\, 4)$, then $\mathrm{Even}_i := \mathrm{Large}_i$ and $\mathrm{Odd}_i := \mathrm{Small}_i$.

The distinction is this. Each Even_i is a faithful representation of $\mathrm{Sp}(2n, q)$, while each Odd_i factors through a (necessarily faithful) representation of the simple group $\mathrm{PSp}(2n, q)$.

Now fix a prime $\ell \neq p$, and embeddings

$$\mathbb{Q}(\zeta_p) \subset \mathbb{Q}_\ell(\zeta_p) \subset \mathbb{C}.$$

We will work with ℓ-adic cohomology, over the coefficient field $\mathbb{Q}_\ell(\zeta_p)$.

We fix a nontrivial additive character ψ of the additive group of $\mathbb{F}_p$, We denote by χ_2 the quadratic character of $\mathbb{F}_p^\times$, extended by zero across $0 \in \mathbb{F}_p$. On the affine line $\mathbb{A}^1/\mathbb{F}_p$, we have the Artin-Schreier sheaf $\mathcal{L}_\psi$. On $\mathbb{G}_m/\mathbb{F}_p$, we have the Kummer sheaf $\mathcal{L}_{\chi_2}$, and its extension by zero to $\mathbb{A}^1/\mathbb{F}_p$ (which, when no confusion can arise, we will also denote $\mathcal{L}_{\chi_2}$.

We denote by $A_{\mathbb{F}_p} := A_{\psi,\mathbb{F}_p}$ the (negative of the) gauss sum

$$A_{\mathbb{F}_p} := -g(\psi_{-2}, \chi_2) := -\sum_{x \in \mathbb{F}_p^\times} \psi(-2x)\chi_2(x).$$

When we are dealing with a finite extension field $k/\mathbb{F}_p$, we use the nontrivial additive character $\psi_k := \psi \circ \mathrm{Trace}_{k/\mathbb{F}_p}$ of k and the quadratic character $\chi_{2,k} := \chi_2 \circ \mathrm{Norm}_{k/\mathbb{F}_p}$ of $k^\times$, extended by zero across $0 \in k$. We define

$$A_{\psi,k} := A_k := (A_{\mathbb{F}_p})^{\deg(\mathrm{k}/\mathbb{F}_\mathrm{p})} = -\sum_{x \in k^\times} \psi_k(-2x)\chi_{2,k}(x),$$

the last equality by the Hasse-Davenport relation.

When $n \geq 2$, we define three lisse sheaves on $\mathbb{A}^2/\mathbb{F}_p$, with coordinates (s,t). The first, lisee of rank $(q^n-1)/2$, is denoted

$$\mathcal{G}(\psi, n, q, \mathbb{1}).$$

The second, lisse of rank $(q^n+1)/2$, is denoted

$$\mathcal{G}(\psi, n, q, \chi_2).$$

The third, lisse of rank q^n, is simply the direct sum

$$\mathcal{W}(\psi, n, q) := \mathcal{G}(\psi, n, q, \mathbb{1}) \oplus \mathcal{G}(\psi, n, q, \chi_2).$$

Their trace functions are given as follows. For $k/\mathbb{F}_p$ a finite extension field, and $(s,t) \in \mathbb{A}^2(k)$, we have

$$\mathrm{Trace}(Frob_{k,(s,t)}|\mathcal{G}(\psi, n, q, \mathbb{1})) = (-1/A_k)\sum_{x\in k}\psi_k(x^{(q^n+1)/2}+sx^{(q+1)/2}+tx),$$

$$\mathrm{Trace}(Frob_{k,(s,t)}|\mathcal{G}(\psi, n, q, \chi_2)) = (-1/A_k)\sum_{x\in k}\psi_k(x^{(q^n+1)/2}+sx^{(q+1)/2}+tx)\chi_{2,k}(x),$$

and

$$\mathrm{Trace}(Frob_{k,(s,t)}|\mathcal{W}(\psi, n, q)) = (-1/A_k)\sum_{x\in k}\psi_k(x^{q^n+1}+sx^{q+1}+tx^2).$$

For compatibility with the Even and Odd nomenclature, we define

$\mathcal{G}_{\mathrm{odd}}(\psi, n, q) :=$ whichever of $\mathcal{G}(\psi, n, q, \mathbb{1})$ or $\mathcal{G}(\psi, n, q, \chi_2)$ has odd rank

$\mathcal{G}_{\mathrm{even}}(\psi, n, q) :=$ whichever of $\mathcal{G}(\psi, n, q, \mathbb{1})$ or $\mathcal{G}(\psi, n, q, \chi_2)$ has even rank

For compatibilty with the Small -Large dichotomy, we define

$$\mathcal{G}_{\mathrm{small}}(\psi, n, q) := \mathcal{G}(\psi, n, q, \mathbb{1}), \quad \mathcal{G}_{\mathrm{large}}(\psi, n, q) := \mathcal{G}(\psi, n, q, \chi_2).$$

At present, we are able to show the following two theorems.

Theorem 1.1. *Suppose that $n \geq 2$ is prime to p, and that $q = p^a$ with a prime to p. Then we have the following results.*

(i) *The geometric monodromy group G_{geom} of $\mathcal{G}_{\mathrm{even}}(\psi, n, q)$ is $\mathrm{Sp}(2n, q)$ in one of its individual even-dimensional Weil representations Even_i. After pullback to $\mathbb{A}^2/\mathbb{F}_q$, we have $G_{geom} = G_{arith}$.*
(ii) *The geometric monodromy group G_{geom} of $\mathcal{G}_{\mathrm{odd}}(\psi, n, q)$ is $\mathrm{PSp}(2n, q)$ in one of its individual odd-dimensional Weil representations Odd_i. After pullback to $\mathbb{A}^2/\mathbb{F}_q$, we have $G_{geom} = G_{arith}$.*
(iii) *The two local systems $\mathcal{G}_{\mathrm{even}}(\psi, n, q)$ and $\mathcal{G}_{\mathrm{odd}}(\psi, n, q)$ are correctly matched, in the sense that the geometric monodromy group of $\mathcal{W}(\psi, n, q)$ is $\mathrm{Sp}(2n, q)$ in one of its total Weil representations. After pullback to $\mathbb{A}^2/\mathbb{F}_q$, we have $G_{geom} = G_{arith}$.*

We next specialize $s \mapsto 1$, to obtain lisse sheaves $\mathcal{G}_1(\psi, n, q, \mathbb{1})$, $\mathcal{G}_1(\psi, n, q, \chi_2)$, and $\mathcal{W}_1(\psi, n, q)$ on $\mathbb{A}^1/\mathbb{F}_p$, whose trace functions at time $t \in k$, for $k/\mathbb{F}_p$ a finite extension field, are given by

$$\mathrm{Trace}(Frob_{k,t}|\mathcal{G}_1(\psi, n, q, \mathbb{1})) = (-1/A_k) \sum_{x \in k} \psi_k(x^{(q^n+1)/2} + x^{(q+1)/2} + tx),$$

$$\mathrm{Trace}(Frob_{k,t}|\mathcal{G}_1(\psi, n, q, \chi_2)) = (-1/A_k) \sum_{x \in k} \psi_k(x^{(q^n+1)/2} + x^{(q+1)/2} + tx)\chi_{2,k}(x),$$

and

$$\mathrm{Trace}(Frob_{k,t}|\mathcal{W}_1(\psi, n, q)) = (-1/A_k) \sum_{x \in k} \psi_k(x^{q^n+1} + x^{q+1} + tx^2).$$

These are the rigid local systems of the title.

As above, we define $\mathcal{G}_{1,\mathrm{even}}(\psi, n, q, \mathbb{1})$ and $\mathcal{G}_{1,,\mathrm{odd}}(\psi, n, q, \mathbb{1})$ by

$\mathcal{G}_{1,\mathrm{odd}}(\psi, n, q) :=$ whichever of $\mathcal{G}_1(\psi, \mathrm{n}, \mathrm{q}, \mathbb{1})$ or $\mathcal{G}_1(\psi, \mathrm{n}, \mathrm{q}, \chi_2)$ has odd rank,

$\mathcal{G}_{1,\mathrm{even}}(\psi, n, q) :=$ whichever of $\mathcal{G}_1(\psi, \mathrm{n}, \mathrm{q}, \mathbb{1})$ or $\mathcal{G};_1(\psi, \mathrm{n}, \mathrm{q}, \chi_2)$ has even rank.

Theorem 1.2. *Suppose that $n \geq 2$ is prime to p, and that $q = p^a$ with a prime to p. Then we have the following results.*

(i) *The geometric monodromy group G_{geom} of $\mathcal{G}_{1,\mathrm{even}}(\psi, n, q)$ is $\mathrm{Sp}(2n, q)$ in one of its even-dimensional individual Weil representations Even_i. After pullback to $\mathbb{A}^1/\mathbb{F}_q$, we have $G_{geom} = G_{arith}$.*

(ii) *The geometric monodromy group G_{geom} of $\mathcal{G}_{1,\mathrm{odd}}(\psi, n, q)$ is $\mathrm{PSp}(2n, q)$ in one of its odd-dimensional individual Weil representations Odd_i. After pullback to $\mathbb{A}^1/\mathbb{F}_q$, we have $G_{geom} = G_{arith}$.*

(iii) *The two local systems $\mathcal{G}_{1,\mathrm{even}}(\psi, n, q)$ and $\mathcal{G}_{1,\mathrm{odd}}(\psi, n, q)$ are correctly matched, in the sense that the geometric monodromy group of $\mathcal{W}_1(\psi, n, q)$ is $\mathrm{Sp}(2n, q)$ in one of its total Weil representations. After pullback to $\mathbb{A}^1/\mathbb{F}_q$, we have $G_{geom} = G_{arith}$.*

As the reader will see, we make fundamental use of the ideas and results of van der Geer and van der Flugt [vdG-vdV, §13, 364-367].

2. Group-theoretic information

In this section, we fix an integer $N \geq 1$, a prime p, and a factorization $N = AB$. We have inclusions of groups

$$\mathrm{SL}(2, p^N) \hookrightarrow \mathrm{Sp}(2A, p^B) \hookrightarrow \mathrm{Sp}(2N, p).$$

Moreover, the Galois group $\mathrm{Gal}(\mathbb{F}_{p^B}/\mathbb{F}_p)$ acts by entry-wise conjugation on $\mathrm{Sp}(2A, p^B)$. Denoting by C_B the cyclic group of order B, we thus have the semidirect product group $\mathrm{Sp}(2A, p^B) \rtimes C_B$, and we have inclusions

$$\mathrm{Sp}(2A, p^B) \hookrightarrow \mathrm{Sp}(2A, p^B) \rtimes C_B \hookrightarrow \mathrm{Sp}(2N, p).$$

To see this, start with the group $\mathrm{SL}(2, p^N)$, thought of as the automorphism group of the 2-dimensional $\mathbb{F}_{p^N}$-space $(\mathbb{F}_{p^N})^2$, with the symplectic form

$$< (a, b), (c, d) > := ad - bc.$$

Then think of this same space as a $2A$-dimensional $\mathbb{F}_{p^B}$-space, with symplectic form

$$< (a, b), (c, d) >_{\mathbb{F}_{p^B}} := \mathrm{Trace}_{\mathbb{F}_{p^N}/\mathbb{F}_{p^B}}(ad - bc).$$

Its automorphism group is $\mathrm{Sp}(2A, p^B)$. Now think of $\mathrm{Sp}(2N, p)$ as the automorphism group of $(\mathbb{F}_{p^N})^2$ as a $2N$-dimensional vector space over $\mathbb{F}_p$, with the symplectic form

$$< (a, b), (c, d) >_{\mathbb{F}_p} := \mathrm{Trace}_{\mathbb{F}_{p^N}/\mathbb{F}_p}(ad - bc).$$

Seen this way, the coordinate-wise action of $\mathrm{Gal}(\mathbb{F}_{p^N}/\mathbb{F}_{p^B})$ embeds this Galois group into $\mathrm{Sp}(2A, p^B)$.

Similarly, if we think of $\mathrm{Sp}(2A, p^B)$ as the automorphism group of $(\mathbb{F}_{p^B})^{2A}$ with the standard symplectic form

$$((x_i)_i, (y_i)_i)_{\mathbb{F}_{p^B}} := \sum_{j=1}^{A} (x_j y_{j+A} - x_{j+A} y_j),$$

and we think of $\mathrm{Sp}(2N, p)$ as the automorphism group of $(\mathbb{F}_{p^B})^{2A}$ as $\mathbb{F}_p$-space, with the symplectic form

$$((x_i)_i, (y_i)_i)_{\mathbb{F}_p} := \mathrm{Trace}_{\mathbb{F}_{p^B}/\mathbb{F}_p}(\sum_{j=1}^{A} (x_j y_{j+A} - x_{j+A} y_j)),$$

then the coordinate-wise action of $\mathrm{Gal}(\mathbb{F}_{p^B}/\mathbb{F}_p)$ embeds that Galois group into $\mathrm{Sp}(2N, p)$.

Given a divisor b of B, we denote by C_b the cyclic subgroup of C_B of order b. Thus for each divisor b of B, we have inclusions

$$\begin{aligned} \mathrm{SL}(2, p^N) \hookrightarrow \mathrm{Sp}(2A, p^B) \hookrightarrow \mathrm{Sp}(2A, p^B) \rtimes C_b \\ \hookrightarrow \mathrm{Sp}(2A, p^B) \rtimes C_B \hookrightarrow \mathrm{Sp}(2N, p). \end{aligned} \tag{2.0.1}$$

Similarly, we have inclusions of the projective groups

$$\begin{aligned} \mathrm{PSL}(2, p^N) \hookrightarrow \mathrm{PSp}(2A, p^B) \hookrightarrow \mathrm{PSp}(2A, p^B) \rtimes C_b \\ \hookrightarrow \mathrm{PSp}(2A, p^B) \rtimes C_B \hookrightarrow \mathrm{PSp}(2N, p). \end{aligned} \tag{2.0.2}$$

Theorem 2.1. *Suppose that $p^N \equiv 1 (\mathrm{mod}\, 4)$ (so that the even Weil representations land in $\mathrm{SL}((p^N-1)/2, \mathbb{C})$ and the odd ones land in $\mathrm{SL}((p^N+1)/2, \mathbb{C})$) and that $p^N \geq 9$. Then we have the following results.*

(i) *View $\mathrm{SL}(2, p^N)$ as sitting inside $\mathrm{SL}((p^N-1)/2, \mathbb{C})$ by one of its even Weil representations. Let G be a finite group sitting in*

$$\mathrm{SL}(2, p^N) \leq G < \mathrm{SL}((p^N-1)/2, \mathbb{C}).$$

Suppose further that G, so viewed, has all its traces in $\mathbb{Q}(\sqrt{\epsilon_p p})$. Then for some factorization $N = AB$ and for some divisor b of B, $G = \mathrm{Sp}(2A, p^B) \rtimes C_b$ as specified in (2.0.1).

(ii) *View $\mathrm{PSL}(2, p^N)$ as sitting inside $\mathrm{SL}((p^N+1)/2, \mathbb{C})$ by one of its odd Weil representations. Let G be a finite group sitting in*

$$\mathrm{PSL}(2, p^N) \leq G < \mathrm{SL}((p^N-1)/2, \mathbb{C}).$$

Suppose further that G, so viewed, has all its traces in $\mathbb{Q}(\sqrt{\epsilon_p p})$. Then for some factorization $N = AB$ and for some divisor b of B, G is $\mathrm{PSp}(2A, p^B) \rtimes C_b$ as specified in (2.0.2).

Theorem 2.2. *Suppose that $p^N \equiv 3 (\mathrm{mod}\, 4)$ (so that the even Weil representations land in $\mathrm{SL}((p^N+1)/2, \mathbb{C})$ and the odd ones land in $\mathrm{SL}((p^N-1)/2, \mathbb{C})$) and that $p^N \geq 11$. Then we have the following results.*

(i) *View $\mathrm{SL}(2, p^N)$ as sitting inside $\mathrm{SL}((p^N+1)/2, \mathbb{C})$ by one of its even Weil representations. Let G be a finite group sitting in*

$$\mathrm{SL}(2, p^N) \leq G < \mathrm{SL}((p^N-1)/2, \mathbb{C}).$$

Suppose further that G, so viewed, has all its traces in $\mathbb{Q}(\sqrt{\epsilon_p p})$. Then for some factorization $N = AB$ and for some divisor b of B, G is $\mathrm{Sp}(2A, p^B) \rtimes C_b$ as specified in (2.0.1).

(ii) *View $\mathrm{PSL}(2, p^N)$ as sitting inside $\mathrm{SL}((p^N-1)/2, \mathbb{C})$ by one of its odd Weil representations. Let G be a finite group sitting in*

$$\mathrm{PSL}(2, p^N) \leq G < \mathrm{SL}((p^N+1)/2, \mathbb{C}).$$

Suppose further that G, so viewed, has all its traces in $\mathbb{Q}(\sqrt{\epsilon_p p})$. Then for some factorization $N = AB$ and for some divisor b of B, G is $\mathrm{PSp}(2A, p^B) \rtimes C_b$ as specified in (2.0.2).

It is **not** true that given an embedding $\mathrm{Sp}(2n, q^m) \hookrightarrow \mathrm{Sp}(2nm, q)$ (by base change as above), the two distinct irreducible Weil characters of the same degree of $\mathrm{Sp}(2nm, q)$ would restrict to two distinct irreducible Weil characters of $\mathrm{Sp}(2n, q^m)$. However, the following is true:

Lemma 2.3. *Let q be an odd prime power and let $n, m \geq 1$. For a fixed degree $D := (q^{nm} \pm 1)/2$ and fixed irreducible Weil representations*

$$\Phi : \mathrm{Sp}(2n, q^m) \to \mathrm{SL}(D, \mathbb{C}),\ \ \Psi : \mathrm{Sp}(2nm, q) \to \mathrm{SL}(D, \mathbb{C}),$$

there exists an embedding $\Theta : \mathrm{Sp}(2n, q^m) \to \mathrm{Sp}(2nm, q)$ such that the representations Φ and $\Psi \circ \Theta$ of $\mathrm{Sp}(2n, q^m)$ are equivalent.

Proof. As discussed above, we can fix an embedding ι of $X := \mathrm{Sp}(2n, q^m)$ into $Y := \mathrm{Sp}(2nm, q)$. It is well known that $\Psi \circ \iota$ is an irreducible Weil representation of X of degree D. If $\Psi \circ \iota \cong \Phi$, then we can take $\Theta = \iota$. Otherwise, there is an outer diagonal automorphism α of X such that $\Psi \circ \iota \circ \alpha \cong \Phi$, in which case we take $\Theta = \iota \circ \alpha$. $\square$

Lemma 2.4. *Let $G = \mathrm{Sp}(2A, p^B) \rtimes C_b$ be as specified in* (2.0.1) *and consider the restriction of an irreducible Weil representation*

$$\Psi : \mathrm{Sp}(2N, p) \to \mathrm{SL}(D, \mathbb{C})$$

to G. Then G is generated by elements g with $\mathrm{Trace}(\Psi(g)) \neq 0$.

Proof. Let ψ denote the character of Ψ. We need to show that

$$H := \langle g \in G \mid \psi(g) \neq 0 \rangle$$

coincides with G. By [TZ2, Lemma 2.6], $\psi(t) \neq 0$ for any transvection $t \in \mathrm{Sp}(2A, p^B)$. It follows that H contains all transvections of $N := \mathrm{Sp}(2A, p^B)$, and so $H \geq N$. Next, since ψ is irreducible over $N \lhd G$, it follows from [Is, Lemma 8.14(c)] that $\sum_{y \in Nx} |\psi(y)|^2 = |N|$ for any coset Nx in G. In particular, there is some $h \in N$ such that $\psi(\sigma h) \neq 0$, where σ is a generator of C_b. Thus $H \ni \sigma h$, and so $H = G$. $\square$

Proof of Theorem 2.1 and Theorem 2.2. (a) Let $D = (p^N \pm 1)/2 \geq 4$ denote the dimension of the Weil representation in question, and let ψ denote the irreducible character of G acting on $V = \mathbb{C}^D$. First we show that $\mathbf{Z}(G)$ is of order 2, respectively 1, if D is even, respectively odd. Indeed, by Schur's lemma, any $z \in \mathbf{Z}(G)$ acts on V as a scalar γ, a primitive c^{th}-root of unity in $\mathbb{C}$ for some $c \geq 1$. By hypothesis,

$$Dc = \psi(z) \in \mathbb{Q}(\sqrt{\epsilon_p p}) \subseteq \mathbb{Q}(\exp(2\pi i/p)).$$

It follows that the Euler function φ takes value at most 2 at c, and so $c \in \{1, 2, 3, 4, 6\}$. Furthermore, c is coprime to p since $1 = \det(z) = c^D$. Hence $c = 1$ if $2 \nmid D$, and $c \leq 2$ if $2|D$, as claimed.

Inflating the representation to $\mathrm{SL}(2, p^N)$ in the case D is odd, we will assume that G contains $H := \mathrm{SL}(2, q)$ with $q := p^N$. In light of this inflation, we have shown that $\mathbf{Z}(G) = \mathbf{Z}(H) \cong C_2$.

(b) It is well known, see e.g. [KL, Table 5.2.A], that the smallest index $P(H)$ of proper subgroups of H is at least q if $q \neq 9$ and equals 6 if $q = 9$. Since H acts irreducibly on V, it follows that the $\mathbb{C}H$-module V is primitive.

Next suppose that G preserves a tensor decomposition $V = A \otimes_{\mathbb{C}} B$, with $\dim A, \dim B > 1$. Then H acts projectively and irreducibly on each of A and B. Again it is well known that the smallest dimension $e(H)$ of nontrivial irreducible, projective representations of H over fields of characteristic $\neq p$ is $(q-1)/2$ if $q \neq 9$ and 3 if $q = 9$. Since $e^2 > D$, it must be the case that H acts trivially projectively on at least one of A and B, but this contradicts the irreducibility hypothesis. Thus the $\mathbb{C}H$-module V is tensor indecomposable.

Suppose that G preserves a tensor induced decomposition $V = A_1 \otimes A_2 \otimes \ldots \otimes A_k \cong A_1^{\otimes k}$ for some $k > 1$. Clearly, $k < D < P(H)$, whence H cannot act transitively on $\{A_1, A_2, \ldots, A_k\}$. But this means that H preserves a tensor decomposition of V, contradicting the previous result. Thus the $\mathbb{C}G$-module V is not tensor induced.

Now we can apply [GT, Proposition 2.8] to (the image in $\mathrm{SL}(V)$ of) G to arrive at one of the three cases (i)–(iii) listed there. As G is finite and $\mathbf{Z}(\mathrm{SL}(V))$ is finite, case (i) cannot occur. Suppose we are in case (iii). Then $D = t^m$ for some prime r and some $m \geq 1$. In this case, $t \neq p$ and the action of H on a finite t-group E that acts irreducibly on V induces a homomorphism $\Phi : H \to \mathrm{Sp}(2m, t)$ with $\mathrm{Ker}(\Phi) \leq \mathbf{Z}(H)$. If $D \geq 5$, we see that $2m \leq t^m - 2 < (q-1)/2$, whereas the smallest degree of nontrivial irreducible representations of H over a field of characteristic t is $(q-1)/2$, yielding a contradiction. If $D = 4$, then we have necessarily $(p, N, t, m) = (3, 2, 2, 2)$. The proof of [GT, Proposition 2.8] shows that $G \lhd P$, where $P = \mathbf{Z}(P)E$ is a 2-group acting irreducibly on $V = \mathbb{C}^4$ and E is an extraspecial 2-group of order 2^5. By Schur's lemma, $\mathbf{Z}(P) \leq \mathbf{Z}(G) \cong C_2$ (as shown in (a)), whence $P = E = 2^{1+4}_{\pm}$. But this leads to a contradiction, since $H = \mathrm{SL}(2, 9)$ cannot act nontrivially on P.

We have shown that $S \lhd G/\mathbf{Z}(G) \leq \mathrm{Aut}(S)$ for some finite non-abelian simple group S. Furthermore, if $L = E(G)$ denotes the layer of G, then $L/\mathbf{Z}(L) \cong S$, and L acts irreducibly on V by [GT, Lemma 2.5]. In particular, the smallest dimension $e_{\mathbb{C}}(S)$ of nontrivial irreducible, projective complex representations of S satisfies

$$e_{\mathbb{C}}(S) \leq D. \tag{2.5.1}$$

Moreover, $H \leq L$ since H is perfect.

(c) Here we consider the possibility $S = \mathsf{A}_n$ for some $n \geq 5$. Indeed, if $q \geq 11$, then $n \geq P(H) = q$. It follows from [KL, Proposition 5.3.7] that

$$e_{\mathbb{C}}(S) = e_{\mathbb{C}}(\mathsf{A}_n) \geq n - 2 \geq q - 2 > (q+1)/2 > D,$$

contradicting (2.5.1). Suppose $q = 9$. Then $n \geq P(S) = 6$ and $n \leq 7$ as $\epsilon_C(\mathsf{A}_8) = 8 > D$. If $n = 7$, then using [CCNPW-Atlas] one can see that $L = 2\mathsf{A}_7$ and $\mathbb{Q}(\psi|_L) = \mathbb{Q}(\sqrt{-7})$, contrary to the assumptions. If $n = 6$, then one easily checks using [CCNPW-Atlas] that either $D = 5$ and

$$\mathsf{A}_6 \cong \mathrm{PSp}(2,9) \lhd G \leq \mathrm{PSp}(2,9) \rtimes C_2,$$

or $D = 4$ and

$$2\mathsf{A}_6 \cong \mathrm{Sp}(2,9) \lhd G \leq \mathrm{Sp}(2,9) \rtimes C_2.$$

Furthermore, if $S \not\cong \mathsf{A}_n$ (and $q = 9$ still), then the condition that L acts irreducibly on $\mathbb{C}^D$ with $D = 4, 5$ implies by inspecting [TZ1, Table I] and [CCNPW-Atlas] that either $(L, D) = (\mathrm{SL}(2,7), 4)$, or $(L, D) = (\mathrm{PSL}(2,11), 5)$, or $S = \mathrm{PSp}(4,3)$. The first two possibilities are ruled out since $\mathrm{PSL}(2,9)$ cannot be embedded in S or L. In the third case, we have $(G, D) = (\mathrm{PSp}(4,3), 5)$ or $(\mathrm{Sp}(4,3), 4)$, as stated. From now on we may assume that $q \geq 11$ and $D \geq 5$.

Next, suppose that S is a simple classical group of dimension d defined over $\mathbb{F}_s$ of prime characteristic $t \neq p$ (with d chosen minimal possible). Then $d \geq e(H) = (q-1)/2 \geq 5$. It follows from (2.5.1) that $e_{\mathbb{C}}(S) \leq d + 1 < d^2/2$. Hence [KL, Corollary 5.3.11] implies that $(S, d) = (\mathrm{SU}(5,2), 5)$, $(\Omega^{\pm}(8,2), 8)$, $(\mathrm{Sp}(6,2), 6)$. An inspection of character tables of universal covers of S rules out the existence of a complex irreducible character of degree D for L in the cases $S = \mathrm{SU}(5,2)$ and $\Omega^-(8,2)$. Suppose $S = \mathrm{Sp}(6,2)$. Then $(q-1)/2 \leq d = 6$, whence $q \in \{11, 13\}$ and so $H = \mathrm{SL}(2,q)$ cannot embed in L, a contradiction. Likewise, if $S = \Omega^+(8,2)$, then $(q-1)/2 \leq d = 8$, whence $q \in \{11, 13, 17\}$ and again $H = \mathrm{SL}(2,q)$ cannot embed in L, a contradiction.

Suppose that S is a simple exceptional group defined over $\mathbb{F}_s$ of prime characteristic $t \neq p$. Then the universal cover of S has a nontrivial irreducible representation of smallest possible degree $d \leq 248$ over $\overline{\mathbb{F}}_s$, and so $(q-1)/2 = e(H) \leq d$ yields $q \leq 497$. But then (2.5.1) implies that $e_{\mathbb{C}}(S) \leq (q+1)/2 \leq d+1 \leq 249$. The Landazuri–Seitz–Zalesskii bounds [KL, Table 5.3.A] now show that $(S, d) = (F_4(2), \leq 26)$, $({}^2F_4(2)', 26)$, $({}^3D_4(s \leq 3), 8)$, $(G_2(s \leq 5), \leq 7)$, $({}^2B_2(s \leq 32), 4)$. Among these groups, the only one that can have a projective irreducible complex representation of degree $D \leq d+1$ is $S = {}^2F_4(2)'$. In this case, $(q-1)/2 \leq d = 26$, $q \leq 53$. On the other hand, $(q+1)/2 \geq D \geq e_{\mathbb{C}}(S) = 26$, whence $q = 53$. But this is a contradiction, as $\mathrm{SL}(2,53)$ cannot embed in L.

(d) Now we consider the case S is a simple group of Lie type defined over a field $\mathbb{F}_s$ with $s = p^f$. We view $S = [\mathcal{G}^F, \mathcal{G}^F]$ for some Frobenius endomorphism $F : \mathcal{G} \to \mathcal{G}$ of a simple algebraic group $\mathcal{G}$ of adjoint type, defined over $\overline{\mathbb{F}}_p$. Recall that $H/\mathbf{Z}(H)$ contains a p'-element x of order $(q+1)/2$, and that $H/\mathbf{Z}(H) \hookrightarrow L/\mathbf{Z}(L) \cong S$. As shown in p. (i) of the proof of [GKT, Theorem 9.10],

$$|x| \leq (s+1)^r, \tag{2.5.2}$$

if r denotes the rank of $\mathcal{G}$. We will show that in most of the cases (2.5.2) contradicts the assumption

$$e_{\mathbb{C}}(S) \leq D = (q \pm 1)/2 \leq (q+1)/2 = |x|. \tag{2.5.3}$$

We will freely use various lower bounds on $e_{\mathbb{C}}(S)$ as recorded in [KL, Table 5.3.A] and [T, Table I]. First we consider the case where $V|_L$ is a Weil module and $S \in \{\mathrm{PSL}(n,s), \mathrm{PSU}(n,s)\}$ with $n \geq 3$, or $S = \mathrm{PSp}(2n,s)$ with $n \geq 1$.

(d1) If $S = \mathrm{PSL}(n,s)$ then

$$\dim V = (s^n - s)/(s-1),\ (s^n - 1)/(s-1)$$

is congruent to 0 or 1 modulo p, and so it can be equal to D only when $\dim V = (s^n - s)/(s-1)$ (and $p = 3$). But in this exception, $V|_L$ is an induced module, contradicting the primitivity of the $\mathbb{C}H$-module V.

(d2) Similarly, if $S = \mathrm{PSU}(n,s)$, then $V|_L$ can be a Weil module of dimension $D = (q \pm 1)/2$ only when $D = (q + (-1)^n)/2$, $p = 3$, and $\dim V = (s^n - (-1)^n)/(s+1)$. But in this case,

$$q = (2D - (-1)^n)_3 = (2s^{n-1} - 2s^{n-2} + \ldots \pm 2s^2 \pm (2s-3))_3 \leq s$$

(where X_p denotes the p-part of the integer X), and so

$$(s+1)/2 \geq D = (s^n - (-1)^n)/(s+1) \geq s(s-1),$$

a contradiction.

(d3) Suppose that $S = \mathrm{PSp}(2n,s)$. Then $V|_L$ can be a Weil module of dimension $(q \pm 1)/2$ only when

$$p^N = q = s^n = p^{nf}$$

and $\dim V = (s^n \pm 1)/2$. Again by Schur's lemma, $\mathbf{C}_G(L) = \mathbf{Z}(G) = \mathbf{Z}(H)$, and furthermore, the outer-diagonal automorphisms of L fuse the two Weil representations of degree D of L. It follows that $G/\mathbf{Z}(G)$ can induce only field automorphisms of L, and so G/L is a cyclic group of outer field automorphisms of order say $b|f$.

Assume that $2 \nmid D$. Then (after modding out by $\mathbf{Z}(H)$ that acts trivially on V) G embeds in $\mathrm{Aut}_1(S) \cong S \rtimes C_f$, where C_f is the group of (outer) field automorphisms of S. It follows that $G \cong S \rtimes C_b$. By

Lemma 2.3, we can embed $S = \mathrm{PSp}(2n, s)$ in $\mathrm{PSp}(2N, p)$ in such a way that $\psi|_S$ extends to a (fixed) Weil character of $\mathrm{PSp}(2N, p)$. Moreover, the normalizer of S in $\mathrm{PSp}(2N, p)$ induces $\mathrm{Aut}_1(S)$. Thus there is a subgroup $G_1 \leq \mathrm{PSp}(2N, p) < \mathrm{SL}(V)$, isomorphic to G and inducing the same automorphisms on S as G does. Note that all elements of G_1 have traces in $\mathbb{Q}(\sqrt{\epsilon_p p})$ while acting on V as so does $\mathrm{PSp}(2N, p)$. Suppose that $g \in G$ and $g_1 \in G_1$ induce the same automorphism on S. Then by Schur's lemma, $g = \lambda g_1$ for some $\lambda \in \mathbb{C}^\times$. Furthermore, $\lambda^D = 1$ and $\lambda \in \mathbb{Q}(\sqrt{\epsilon_p p})$, if we assume in addition that $\psi(g_1) \neq 0$. As $p \nmid D$ and D is odd, we conclude as in (a) that $\lambda = 1$. Note by Lemma 2.4 that we can generate G_1 by elements g_1 with $\psi(g_1) \neq 0$. It follows that $G = G_1$, that is, G is a subgroup $S \rtimes C_b$ of $\mathrm{PSp}(2N, p)$ (as specified in (2.0.2)).

Assume now that $2|D$. Then we have shown that $G \cong L{\cdot}C_b$ with $L \cong \mathrm{Sp}(2n, s)$. Again by Lemma 2.3, we can embed L in $\mathrm{Sp}(2N, p)$ in such a way that $\psi|_L$ extends to a (fixed) Weil character of $\mathrm{Sp}(2N, p)$. Moreover, the normalizer of L in $\mathrm{Sp}(2N, p)$ induces $\mathrm{Aut}_1(S)$. Furthermore, there is a subgroup $G_1 \leq \mathrm{Sp}(2N, p) < \mathrm{SL}(V)$, with $G_1 = \mathrm{Sp}(2n, s) \rtimes C_b$ as specified in (2.0.1) inducing the same automorphisms on S as G does. Note that all elements of G_1 have traces in $\mathbb{Q}(\sqrt{\epsilon_p p})$ while acting on V as so does $\mathrm{Sp}(2N, p)$. Suppose that $g \in G$ and $g_1 \in G_1$ induce the same automorphism on S. Then $h := g^{-1}g_1$ centralizes $S = L/\mathbf{Z}(L)$, and so $[h, L] \leq \mathbf{Z}(L)$ centralizes L. Now the Three Subgroups Lemma implies that $[h, L] = [h, [L, L]]$ is contained in $[[h, L], L] = 1$, i.e. h centralizes L. It then follows from Schur's lemma that $g = \lambda g_1$ for some $\lambda \in \mathbb{C}^\times$. We again have $\lambda^D = 1$ and $\lambda \in \mathbb{Q}(\sqrt{\epsilon_p p})$, if we assume in addition that $\psi(g_1) \neq 0$. As $p \nmid D$, we conclude as in (a) that $\lambda = \pm 1$. Note by Lemma 2.4 that we can generate G_1 by elements g_1 with $\psi(g_1) \neq 0$, and furthermore the central involution of L acts as -1 on V. It follows that $G = G_1$, and so G is a subgroup $L \rtimes C_b$ of $\mathrm{Sp}(2N, p)$ (as specified in (2.0.1)).

(e) We continue to assume that S is a simple classical group defined over a field $\mathbb{F}_s$ with $s = p^f$, and moreover, in view of (d), that $V|_L$ is not a Weil module if

$$S \cong \mathrm{PSL}(n, s),\ \mathrm{PSU}(n, s),\ \mathrm{PSp}(2n, s).$$

Suppose $S = \mathrm{PSL}(2, s)$; in particular, $s \neq 9$ as $\mathrm{PSL}(2, 9) \cong \mathsf{A}_6$. In view of (d), we may assume that $D = \dim V = s \pm 1$. On the other hand, $D = (q \pm 1)/2$, so $p = 3 = s = q$, contrary to the assumption that $q \geq 11$.

Next we consider the case $S = \mathrm{PSL}(3, s)$ or $\mathrm{PSU}(3, s)$. By Theorems 3.1 and 4.2 of [TZ1], we have

$$(s-1)(s^2-s+1)/3 \leq D \leq (s+1)^2,$$

yielding $s \in \{3, 5\}$. Now, any nontrivial $\chi \in \mathrm{Irr}(L)$ of degree $(q \pm 1)/2$ and at most $\leq (s+1)^2$ is a Weil character, which has been ruled out in (ii), unless $L = \mathrm{SU}(3, 3)$ and $D = 14$, forcing $q = 27$. But this is a contradiction, since 13 divides $|\mathrm{PSL}(2, 27)|$ but not $|\mathrm{SU}(3, 3)|$.

Suppose now that $S = \mathrm{PSL}(4, s)$ or $\mathrm{PSU}(4, s)$. For $s \geq 5$ we have

$$(s-1)(s^3-1)/2 \leq D \leq (s+1)^3,$$

which is impossible only when $s \leq 11$. If $s = 3$, then instead of (2.5.2) we have $|x| \leq 13$, ruling out all characters of $3'$-degree of L.

To finish off type A, assume now that $S = \mathrm{PSL}(n, s)$ or $\mathrm{PSU}(n, s)$ with $n \geq 5$. Then (2.5.2)–(2.5.3) imply

$$\frac{(s^n+1)(s^{n-1}-s^2)}{(s+1)(s^2-1)} \leq D \leq (s+1)^{n-1},$$

whence

$$s^{2n-3} < (s+1)^n < s^{51n/40}$$

(because $(s+1)/s \leq 4/3 < 3^{11/40}$), a contradiction as $n \geq 5$.

Suppose $S = P\Omega^{\pm}(2n, s)$ with $n \geq 4$. For $n \geq 5$ we get that

$$\frac{(s^n-1)(s^{n-1}-s)}{s^2-1} \leq e_{\mathbb{C}}(S) \leq D \leq (s+1)^n,$$

whence

$$s^{2n-3.1} < (s+1)^n < s^{51n/40},$$

a contradiction. If $n = 4$, then, since D is coprime to s, [Lu] implies that

$$D \geq (s^2+s+1)(s^2+1)(s-1)^2 > (s+1)^4,$$

contradicting (2.5.2)–(2.5.3).

Suppose $S = \mathrm{PSp}(2n, s)$ with $n \geq 2$ or $\Omega(2n+1, s)$ with $n \geq 3$. For $n \geq 3$ we have that

$$\frac{(s^n-1)(s^n-s)}{s^2-1} \leq D \leq (s+1)^n,$$

whence

$$s^{2n-2.1} < (s+1)^n < s^{51n/40},$$

a contradiction. If $n = 2$, then $S = \mathrm{PSp}(4, s)$, and we have

$$s(s-1)^2 \leq D \leq (s+1)^2,$$

forcing $s = 3$. In this case, instead of (2.5.2) we have $|x| \leq 5$, and L has no nontrivial non-Weil character of degree ≤ 5.

(f) Here we handle the cases where S is an exceptional group of Lie type over $\mathbb{F}_s$ with $s = p^f$. If S is of type E_6, ${}^2E_6$, E_7, or E_8, then

$$(s^5 + s)(s^6 - s^3 + 1) \le e_{\mathbb{C}}(S) \le D \le (s + 1)^8,$$

a contradiction. Similarly, if $S = F_4(s)$, then

$$s^8 - s^4 + 1 = e_{\mathbb{C}}(S) \le D \le (s + 1)^4,$$

which is impossible. Likewise, if $S = G_2(s)$ with $s \ge 5$, then

$$s^3 - 1 \le e_{\mathbb{C}}(S) \le D \le (s + 1)^2,$$

again a contradiction. Next, if $S = G_2(3)$, then instead of (2.5.2) we have $|x| \le 13$, and $e_{\mathbb{C}}(S) = 14$, a contradiction. If $S = {}^2G_2(s)$, then

$$s^2 - s + 1 = e_{\mathbb{C}}(S) \le D \le (s^0.5 + 1)^2,$$

again a contradiction. Finally, if $S = {}^3D_4(s)$, then since $D = \dim V$ is coprime to s, we see by [Lu] that

$$D \ge s^8 + s^4 + 1 > (s + 1)^4,$$

contradicting (2.5.2).

(g) It remains to consider the case S is one of 26 sporadic simple groups. We will search for $\chi \in \mathrm{Irr}(L)$ where $\chi(1) = (q \pm 1)/2$ with $q||S|$, and, moreover, S has an element of order $(q + 1)/2$. Possible cases are for $(L, q, \chi(1))$ are:

- $(J_2, 27, 14)$, but then 13 divides $|\mathrm{PSL}(2, 27)|$ but not $|J_2|$;
- $(6Suz, 12, 25)$. Here, $\mathrm{PSL}(2, 25) \hookrightarrow S$, but $|\mathbf{Z}(L)| = 6$ is too big;
- $(2Co_1, 24, 49)$, but S does not have any element of order 25. $\square$

Recall [Zs] that if $a \ge 2$ and $n \ge 2$ are any integers with $(a, n) \ne (2, 6)$, $(2^k - 1, 2)$, then $a^n - 1$ has a *primitive prime divisor*, that is, a prime divisor ℓ that does not divide $\prod_{i=1}^{n-1}(a^i - 1)$; write $\ell = \mathrm{ppd}(a, n)$ in this case. Furthermore, if in addition $a, n \ge 3$ and $(a, n) \ne (3, 4)$, $(3, 6)$, $(5, 6)$, then $a^n - 1$ admits a *large primitive prime divisor*, i.e. a primitive prime divisor ℓ where either $\ell > m + 1$ (whence $\ell \ge 2m + 1$), or $\ell^2|(a^m - 1)$, see [F2].

Theorem 2.6. *Let $q = p^f$ be a power of an odd prime p and let $d \ge 2$. If $d = 2$, suppose that $p^{df} - 1$ admits a primitive prime divisor $\ell > 5$. If $d \ge 3$, suppose in addition that $(p, df) \ne (3, 4)$, $(3, 6)$, $(5, 6)$, so that $p^{df} - 1$ admits a large primitive prime divisor ℓ, in which case we choose such an ℓ to maximize the ℓ-part of $p^{df} - 1$. Let $W = \mathbb{F}_q^d$ and let G be a subgroup of $\mathrm{GL}(W) \cong \mathrm{GL}(d, q)$ of order divisible by the ℓ-part $Q := (q^d - 1)_\ell$ of $q^d - 1$. Then either $L := \mathbf{O}^{\ell'}(G)$ is a cyclic ℓ-group of order Q, or there is a divisor $j < d$ of d such that one of the following statements holds.*

(i) $L = \mathrm{SL}(W_j) \cong \mathrm{SL}(d/j, q^j)$, $d/j \geq 3$, *and* W_j *is* W *viewed as a* d/j*-dimensional vector space over* $\mathbb{F}_{q^j}$.
(ii) $2j|d$, W_j *is* W *viewed as a* d/j*-dimensional vector space over* $\mathbb{F}_{q^j}$ *endowed with a non-degenerate symplectic form, and* $L = \mathrm{Sp}(W_j) \cong \mathrm{Sp}(d/j, q^j)$.
(iii) $2|jf$, $2 \nmid d/j$, W_j *is* W *viewed as a* d/j*-dimensional vector space over* $\mathbb{F}_{q^j}$ *endowed with a non-degenerate Hermitian form, and* $L = \mathrm{SU}(W_j) \cong \mathrm{SU}(d/j, q^{j/2})$.
(iv) $2j|d$, $d/j \geq 4$, W_j *is* W *viewed as a* d/j*-dimensional vector space over* $\mathbb{F}_{q^j}$ *endowed with a non-degenerate quadratic form of type* $-$, *and* $L = \Omega(W_j) \cong \Omega^-(d/j, q^j)$.
(v) $(p, df, L/\mathbf{Z}(L)) = (3, 18, \mathrm{PSL}(2, 37))$, $(17, 6, \mathrm{PSL}(2, 13))$.

Proof. (a) We proceed by induction on $d \geq 2$. For the induction base $d = 2$, note that $L \leq G \cap \mathrm{SL}(2, q)$. The list of maximal subgroups of $\mathrm{SL}(2, q)$ is well known. Using this list, one easily checks that either $L \cong C_Q$, or (i) holds with $j = 1$.

(b) For the induction step $d \geq 3$, we will assume that $L \not\cong C_Q$, and apply the main result of [GPPS] to see that G is one of the groups described in Examples 2.1–2.9 of [GPPS].

If G is described in Example 2.1 of [GPPS], then $a_0 = 1$ since $\ell = \mathrm{ppd}(p, df)$. Furthermore, one of (i)–(iv) holds, with $j = 1$.

Next, as ℓ does not divide the order of any (maximal) parabolic subgroup of $\mathrm{GL}(W) \cong \mathrm{GL}(d, q)$, G must act irreducibly on W, and so cannot be any of the groups in Example 2.2 of [GPPS]. Likewise, the condition $\ell||G|$ rules out all the groups listed in Example 2.3 of [GPPS]. Suppose G is one of the groups described in Example 2.5 of [GPPS]. Then $d = 2^m = \ell - 1$ (and ℓ is a Fermat prime). Since ℓ is a large primitive prime divisor, $\ell^2|(q^d - 1)$ and so ℓ^2 divides $|G|$. On the other hand, $|G|$ divides $(q-1)2^{1+2m} \cdot |\mathrm{Sp}(2m, 2)|$ and so it is not divisible by $\ell^2 = (2^m + 1)^2$, a contradiction.

(c) Suppose G is among the groups described in Example 2.4 of [GPPS]. Again, as $\ell = \mathrm{ppd}(p, df)$, G can appear only in Example 2.4(b) of [GPPS]. Thus there is a divisor $1 < j|d$ and W is endowed with the structure of a d/j-dimensional vector space W_j over $\mathbb{F}_{q^j}$, and $G \leq \mathrm{GL}(W_j) \rtimes C_j$, where C_j is the group of field automorphisms of $\mathbb{F}_{q^j}$ over $\mathbb{F}_q$. Note that $j \leq d \leq df < \ell$, so $L \leq \mathrm{GL}(W_j) \cong \mathrm{GL}_{d/j}(q^j)$ has order divisible by $Q = ((q^j)^{d/j} - 1)_\ell = Q$. If $j = d$, then $L \cong C_Q$, contrary to our assumption. If $d/j = 2$, then $q^j > q$ is not a Mersenne prime, and so the induction base implies that (i) holds with $j = d/2$. If $d/j \geq 3$, then we still have $(p, (d/j)jf) = (p, df) \neq (3, 4)$, $(3, 6)$, $(5, 6)$, and moreover $d/j < d$. The induction hypothesis then implies that one of (i)–(iv) holds.

(d) In Examples 2.6–2.9 of [GPPS], $S \lhd G/(G \cap Z) \leq \mathrm{Aut}(S)$ for some non-abelian simple group S, where $Z := \mathbf{Z}(\mathrm{GL}(d,q)) \cong C_{q-1}$ and the full inverse image N of S in G acts absolutely irreducibly on W.

In Example 2.6 of [GPPS] we have $S = \mathsf{A}_n$; in particular, $\ell \leq n$. First, in Example 2.6(a) of [GPPS] we have $n-2 \leq d \leq n-1$, and so $\ell \geq d+1 \geq n-1 > n/2$, whence $\ell^2 \nmid |G|$. As ℓ is a large primitive prime divisor, we then have $\ell \geq 2d+1 > n$ and so $\ell \nmid |G|$, a contradiction. In Examples 2.6(b), (c) of [GPPS], we must have that $\ell = d+1 \in \{5,7\}$ and $n \leq 7$. It follows that $\ell^2 \nmid |G|$, contradicting the choice of ℓ to be a large primitive prime divisor.

In Example 2.7 of [GPPS], S is a sporadic simple group. Furthermore, we have that $\ell = d+1$ and $\ell^2 \nmid |G|$, contradicting the largeness of ℓ.

In Example 2.8 of [GPPS], S is a simple group of Lie type in the same characteristic p. But then the condition $\ell = \mathrm{ppd}(p, df)$ with $p > 2$ rules out this case.

In Example 2.9 of [GPPS], S is a simple group of Lie type in characteristic $\neq p$. If S appears in Table 7 of [GPPS], then $\ell = d+1$ and $\ell^2 \nmid |G|$, again contradicting the largeness of ℓ. Finally, assume that S appears in Table 8 of [GPPS]. Using the fact that ℓ is a large prime divisor of $p^{df} - 1$, we can again rule out all cases except for the case $(d, \ell, S) = ((\ell-1)/2, \ell, \mathrm{PSL}_2(\ell))$. In this case, $|G|_\ell = \ell = 2d+1$. To handle this last case, we use a strengthening [Tr, Theorem 3.2.2] of the main result of [F2], proved by A. MacLaughlin and S. Trefethen. This result asserts that ℓ can be chosen so that $(p^{df}-1)_\ell > 2df+1$, unless $(p, df) = (3, 18)$, respectively $(17, 6)$, where $\ell = 37$, 13, respectively. This leads to the two exceptions listed in (v) (as it is easy to see that $L/\mathbf{Z}(L) \cong S$ in these situations). $\square$

Theorem 2.7. *Suppose G is a finite irreducible subgroup of $\mathrm{SL}((p^N+1)/2, \mathbb{C})$, and suppose that, so viewed, G has all its traces in $\mathbb{Q}(\sqrt{\epsilon_p p})$. Suppose in addition that $p \geq 13$ if $N = 1$ and that $(p, N) \neq (3,2)$, $(3,3)$, $(5,3)$. Then we have the following results.*

(i) *Suppose that $(p^N+1)/2$ is even and G lies in the image, under an even Weil representation, of $\mathrm{Sp}(2N, p)$ in $\mathrm{SL}((p^N+1)/2, \mathbb{C})$. Then one of the following statements holds.*
   (a) *G contains $\mathrm{SL}(2, p^N)$ in one of its even Weil representations, and hence for some factorization $N = AB$ and for some divisor b of B, G is $\mathrm{Sp}(2A, p^B) \rtimes C_b$.*

(b) *$p = 3$, N is odd, G contains $L = \mathrm{SU}(N,3) = \mathbf{O}^2(G) < G$ as a normal subgroup (and induces a graph automorphism on L).*

(ii) *If $(p^N + 1)/2$ is odd, suppose G lies in the image, under an odd Weil representation, of $\mathrm{PSp}(2N,p)$ in $\mathrm{SL}((p^N+1)/2, \mathbb{C})$. Then G contains $\mathrm{PSL}(2,p^N)$ in one of its odd Weil representations, and hence for some factorization $N = AB$ and for some divisor b of B, G is $\mathrm{PSp}(2A, p^B) \rtimes C_b$.*

Proof. (a) First we consider the case $N = 1$. Then $(p^N + 1)/2 \geq 7$ according to our assumption. The maximal subgroups of $\mathrm{SL}(2,p)$ are well known, and none of them can have a complex irreducible representation of degree $(p+1)/2$. Hence $G = \mathrm{SL}(2,p)$ in (i) and $G = \mathrm{PSL}(2,p)$ in (ii).

(b) From now on we assume $N > 1$ and let $W = \mathbb{F}_p^{2N}$ denote the natural module for $\mathrm{Sp}(2N,p)$. By [F2] there is a large primitive prime divisor $\ell = \mathrm{ppd}(p, 2N)$, and we choose such an ℓ to maximize $(p^{2N} - 1)_\ell$. Note that $|G|$ is divisible by $D := (p^N + 1)/2$. Inflating the representation of $\mathrm{PSp}(2N,p)$ in (ii) to $\mathrm{Sp}(2N,p)$, we may assume that G is a subgroup of $\mathrm{Sp}(2N,p)$, of order divisible by $(p^{2N} - 1)_\ell$. Now we can apply Theorem 2.6 to $G < \mathrm{GL}(2N,p)$ to determine the structure of $L = \mathbf{O}^{\ell'}(G)$. First note that if L is cyclic, then by Ito's theorem [Is, (6.15)], any irreducible complex character of G has degree coprime to ℓ, and so G cannot act irreducibly on $V := \mathbb{C}^D$. The same argument shows that L cannot act trivially on V. Let $d(L)$ denote the smallest degree of nontrivial complex irreducible representations of L.

(c) Suppose we are in case (v) of Theorem 2.6. Then $S \lhd G/\mathbf{Z}(G) \leq \mathrm{Aut}(S) \cong S \cdot C_2$, $S = \mathrm{PSL}(2,\ell)$ with $\ell = 37$, respectively 13. It is easy to see that G cannot have a complex irreducible representation of degree $(3^9 + 1)/2$, $(17^3 + 1)/2$, respectively.

Next suppose that we are in case (i), so that $L \cong \mathrm{SL}(2N/j, p^j)$. Then $2N/j \geq 3$, and, according to [TZ1, Theorem 1.1], $d(L) > p^{j(2N/j-1)} = p^{2N-j} > D$, and so L acts trivially on V, a contradiction.

Assume now that we are in case (iv), so that $L \cong \Omega^-(2N/j, p^j)$. If $2N/j \geq 8$, then by [TZ1, Theorem 1.1], $d(L) > p^{j(2N/j-3)} > p^N > D$. If $2N/j = 6$, then L is a cover of $\mathrm{PSU}(6, p^j)$, and so $d(L) \geq (q^4 - 1)/(q + 1) > (q^3 + 1)/2 = D$ for $q := p^j$. If $2N/j = 4$, then $L \cong \mathrm{PSL}(2, q^2)$ for $q := p^j = p^{N/2}$, and so $d(L) = (q^2 + 1)/2 = (p^N + 1)/2 = D$. In all cases, L cannot embed in $\mathrm{Sp}(2N,p)$, since $\mathrm{Sp}(2N,p)$ has an irreducible complex representation of degree $D - 1$ with kernel of order ≤ 2.

(d) Suppose we are in case (ii) of Theorem 2.6. Note that the central involution j of $L = \mathrm{Sp}(W_j)$ acts as the scalar -1 and so coincides with the central involution of $\mathrm{Sp}(2N,p)$. Hence, if D is even, then j acts as -1 on V, and if $2 \nmid D$ then j acts trivially on V. The complex irreducible representations of degree $\leq D$ are classified in [TZ1, Theorem 5.2], and together with the described action of j on V, it implies that L acts irreducibly on V, via one of its two Weil representations of degree D. By Schur's lemma, $\mathbf{C}_G(L)$ acts via scalars on V, and so it is contained in $\mathbf{Z}(\mathrm{Sp}(2N,p)) = \langle j \rangle$. It follows that $\mathbf{C}_G(L) = \mathbf{Z}(G) = \langle j \rangle$ and so $G/\mathbf{Z}(G) \leq \mathrm{Aut}(L)$. Note that the outer diagonal automorphism of L fuses the two Weil representations of degree D of L, whereas all field automorphisms stabilize each of these Weil representations. Thus $G = \langle L, \sigma \rangle$, where σ is a field automorphism of order say $b|B$, as stated.

(e) Finally, suppose we are in case (iii) of Theorem 2.6, so that $L = \mathrm{SU}(W_j) \cong \mathrm{SU}(m,q)$ with $q := p^{j/2}$ and $2 \nmid m := 2N/j \geq 3$. Recall [TZ2, §4] that L has $q+1$ complex irreducible Weil characters $\zeta^i_{m,q}$, $0 \leq i \leq q$, of degree $(q^m-q)/(q+1)$ for $i=0$ and $(q^m+1)/(q+1) = 2D/(q+1)$ for $i > 0$. As $L \lhd G$, all irreducible summands of the $\mathbb{C}L$-module V have common dimension $e|D$. If $m \geq 5$, then any nontrivial non-Weil irreducible character of L has degree $> (q^m+1) = 2D$, see [TZ1, Theorem 4.1]. If $m = 3$, then $q \neq 3$ as $(p,N) \neq (3,3)$, and one can check using [Geck] that any nontrivial non-Weil irreducible character of L has degree not dividing D. Furthermore, $(q^m-q)/(q+1)$ does not divide D either. We have therefore shown that $e = (q^m+1)/(q+1)$ and furthermore

$$\psi|_L = \sum_{j=1}^{(q+1)/2} \zeta^{i_j}_{m,q} \tag{2.7.1}$$

with $q \geq i_1, \ldots, i_{(q+1)/2} > 0$ (not necessarily distinct), if ψ denotes the character of $\mathrm{Sp}(2N,p)$ afforded by V.

Recall that $L \lhd G \leq \mathrm{GL}(W)$ and L acts irreducibly (although not necessarily absolutely) on W, since $\ell||L|$. Hence $\mathbf{C}_{\mathrm{End}(W)}(L)$ is a finite division ring; in fact it is $\mathbb{F}_{q^2}$. Let $H < \mathrm{GL}(W)$ be the central product of $\mathrm{U}(W_j)$ and $\mathbf{Z}(\mathrm{GL}(W_j)) \cong C_{q^2-1}$, whose intersection is precisely $\mathbf{Z}(\mathrm{U}(W_j))$. Then H induces all inner-diagonal automorphisms of L, and $H \rtimes C_j < \mathrm{GL}(W)$ induces all automorphisms of L. Since $\mathbf{C}_{\mathrm{End}(W)}(L) = \{0\} \cup \mathbf{Z}(\mathrm{GL}(W_j))$, we have shown that $G \leq \mathbf{N}_{\mathrm{GL}(W)}(L) = H \rtimes C_j$.

Next we observe that each $\zeta^i_{m,q}$ extends to $\mathrm{U}(W_j)$ and then to H, and furthermore H/L is abelian (as $[H,H] = L$). In particular, $\zeta^{i_j}_{m,q}$ extends to $G \cap H$, and furthermore any irreducible character of $G \cap H$ lying above $\zeta^{i_j}_{m,q}$ is in fact an extension of it by Gallagher's theorem [Is, (6.17)]. Since $\psi|_G$ is irreducible, it follows by Clifford's theorem that

$$(p^{j/2}+1)/2 = (q+1)/2 = \psi(1)/\zeta^{i,j}_{m,q}(1) \leq [G : G \cap H] \leq j.$$

This is possible only when $(p, j) = (3, 2)$, $N = m$, $L = \mathrm{SU}(N, 3)$. In this case, the above analysis shows that $[G : G \cap H] = 2$ and so G induces an outer graph automorphism of L, as well as $L = \mathbf{O}^2(G) < G$. One can check that V is indeed irreducible over the subgroup $\mathrm{U}(N, 3)\cdot 2$ of $\mathrm{Sp}(2N, 3)$ when $N \geq 3$ is odd. □

Remark 2.8. (i) Note that the cases $(p, N) = (3, 2)$, $(3, 3)$, and $(5, 3)$ are real exceptions to Theorem 2.7. Indeed, $\mathrm{PSp}(4, 3)$ contains a subgroup $G = 2^4 \rtimes \mathsf{A}_5$ that acts irreducibly on $\mathbb{C}^5$, see [CCNPW-Atlas].

Next, we show that $\mathrm{Sp}(6, 3) < \mathrm{SL}(14, \mathbb{C})$ contains a subgroup $G \cong \mathrm{SL}(2, 13)$ that acts irreducibly on $\mathbb{C}^{14}$. First, according to [CCNPW-Atlas], $\mathrm{PSp}(6, 3)$ contains a maximal subgroup $\bar{G} \cong \mathrm{PSL}(2, 13)$. As $\mathrm{PSL}(2, 13)$ does not any nontrivial representation of degree 6 over a field of characteristic 3, the full inverse image G of $\bar{G}$ in $\mathrm{Sp}(6, 3)$ is isomorphic to $\mathrm{SL}(2, 13)$, with the central involution equal to the central involution j of $\mathrm{Sp}(6, 3)$. In particular, j acts as the scalar -1 on $\mathbb{C}^{14}$. Inspecting the complex representations of $\mathrm{SL}(2, 13)$ with j acting as -1 in [CCNPW-Atlas], we see that $\mathrm{SL}(2, 13)$ acts irreducibly on $\mathbb{C}^{14}$, as stated.

Likewise, we claim that $\mathrm{PSp}(6, 5) < \mathrm{SL}(63, \mathbb{C})$ contains a subgroup $G \cong J_2$ that acts irreducibly on $\mathbb{C}^{63}$. Indeed, according to [JLPW], $2J_2$ has a faithful irreducible representation of degree 6 over $\mathbb{F}_5$ of symplectic type, yielding an embedding $2J_2 \hookrightarrow \mathrm{Sp}(6, 5)$, with an involution a having trace 4 and an element b of order 3 having trace 0. This leads to an embedding $G \cong J_2$ into $\mathrm{PSp}(6, 5)$. Observe that a is conjugate to the element h_{-1} in [TZ2, Lemma 2.6], and so a has trace 15 on $\mathbb{C}^{63}$. Next, $W = [b, W] \oplus \mathbf{C}_W(b)$, where $\mathbf{C}_W(b)$ is of dimension 2, and b has no nonzero fixed point on the non-degenerate space $[b, W] \cong \mathbb{F}_5^4$. Using [JLPW] one can check that $\mathrm{Sp}([b, W]) \cong \mathrm{Sp}(4, 5)$ has one conjugacy class of such elements of order 3. Hence $\mathrm{Sp}(W) \cong \mathrm{Sp}(6, 5)$ has exactly one conjugacy class of elements of order 0 with trace 0. Thus we may assume that b belongs to a Levi subgroup $\mathrm{GL}(3, 5)$ of the stabilizer of a totally isotropic subspace $W_1 \cong \mathbb{F}_5^3$ of W in $\mathrm{Sp}(W)$, and that b acts on W_1 with trace 0 and determinant 1. Arguing as in the proof of [TZ2, Lemma 2.6] we see that b has trace 0 on $\mathbb{C}^{63}$. The determined traces of a and b on $\mathbb{C}^{63}$ allow one to prove using the character table of J_2 that J_2 is irreducible on $\mathbb{C}^{63}$.

(ii) We also note Case (i)(b) does not arise in Theorem 2.7 if we require in addition that G has no nontrivial p'-quotient.

3. Finiteness of the arithmetic monodromy of $\mathcal{W}(\psi, n, q)$, d'aprés van der Geer and van der Flugt

The local system $\mathcal{W}(\psi, n, q)$ is pure of weight zero and lisse of rank q^n on $\mathbb{A}^2/\mathbb{F}_p$. Its trace function, at time $(s,t) \in \mathbb{A}^2(k)$, for $k/\mathbb{F}_p$ a finite extension field, is the exponential sum

$$(-1/A_k)\sum_{x \in k} \psi_k(x^{q^n+1} + sx^{q+1} + tx^2).$$

Think of (s,t) as fixed in $A^2(k)$. Write this sum as

$$(-1/A_k)\sum_{x \in k} \psi_k(xR(x)),$$

with $R(x)$ the additive, $\mathbb{F}_q$-linear polynomial

$$R(x) = R_{(s,t)}(x) := x^{q^n} + sx^q + tx.$$

When k is a finite extension of $\mathbb{F}_q$, we can write this sum as

$$(-1/A_k)\sum_{x \in k} \psi_{\mathbb{F}_q}(\mathrm{Trace}_{k/\mathbb{F}_q}(xR(x))).$$

The insight of van der Geer and van der Flugt [vdG-vdV, & 13] is to then view

$$\mathrm{Trace}_{k/\mathbb{F}_q}(xR(x))$$

as a quadratic form on k, viewed as an $\mathbb{F}_q$ vector space; it is the quadratic form attached to the symmetric bilinear form

$$(x,y)_R := \mathrm{Trace}_{k/\mathbb{F}_q}(xR(y) + yR(x)).$$

As they explain [vdG-vdV, 13.1], the $\mathbb{F}_q$ vector space

$$W_R := \{x \in k | (x,y)_R = 0 \text{ for all y} \in \text{k}\}$$

is precisely the set of zeroes in k of the polynomial

$$E_R(x) := x^{q^{2n}} + s^{q^n}x^{q^{n+1}} + 2t^{q^n}x^{q^n} + s^{q^{n-1}}x^{q^{n-1}} + x.$$

At this point, we invoke the following lemma.

Lemma 3.1. *Let p be an odd prime, α an element of $\mathbb{Z}[\zeta_p][1/p]$ and $\overline{\alpha}$ its complex conjugate (i.e., the image of α under the Galois automorphism $\zeta_p \mapsto \zeta_p^{-1}$). Then α lies in $\mathbb{Z}[\zeta_p]$ if and only if $\alpha\overline{\alpha}$ lies in $\mathbb{Z}[\zeta_p]$.*

Proof. If α lies in $\mathbb{Z}[\zeta_p]$, then so does $\overline{\alpha}$. For the converse, use the fact that in the field $\mathbb{Q}(\zeta_p)$, there is a unique place over p, whose normalized valuation $\mathrm{ord_p}$ has $\mathrm{ord_p}(\zeta_\mathrm{p} - 1) = 1/(\mathrm{p}-1)$. By uniqueness, we have

$$\mathrm{ord_p}(\alpha) = \mathrm{ord_p}(\overline{\alpha}),$$

and hence

$$\mathrm{ord_p}(\alpha\overline{\alpha}) = 2\mathrm{ord_p}(\alpha).$$

But for $\alpha \in \mathbb{Z}[\zeta_p][1/p]$, α lies in $\mathbb{Z}[\zeta_p]$ if and only if $\mathrm{ord_p}(\alpha) \geq 0$. □

The sum

$$(-1/A_k)\sum_{x\in k}\psi_{\mathbb{F}_q}(\mathrm{Trace}_{k/\mathbb{F}_q}(R(x)x))$$

visibly lies in $\mathbb{Z}[\zeta_p][1/p]$ (the only possible nonintegrality is from the $1/A_k$ factor, whose square is $\pm 1/\#k$).

The key calculation is due to [vdG-vdV].

Lemma 3.2. *For $k/\mathbb{F}_q$ a finite extension field, $(s,t) \in \mathbb{A}^2(k)$, and $R := R_{(s,t)}$, the square absolute value of our exponential sum is given by*

$$|(-1/A_k)\sum_{x\in k}\psi_{\mathbb{F}_q}(\mathrm{Trace}_{k/\mathbb{F}_q}(R(x)x))|^2 = \#W_R = q^{\dim_{\mathbb{F}_q}(W_R)}.$$

Proof. We have

$$|(-1/A_k)\sum_{x\in k}\psi_{\mathbb{F}_q}(\mathrm{Trace}_{k/\mathbb{F}_q}(R(x)x))|^2 =$$

$$= (1/\#k)\sum_{x,y\in k}\psi_{\mathbb{F}_q}(\mathrm{Trace}_{k/\mathbb{F}_q}(xR(x) - yR(y))) =$$

(make the substitution $(x,y) \mapsto (x+y,y)$)

$$= (1/\#k)\sum_{x\in k}\psi_{\mathbb{F}_q}(\mathrm{Trace}_{k/\mathbb{F}_q}(xR(x))\sum_{y\in k}\psi_{\mathbb{F}_q}(\mathrm{Trace}_{k/\mathbb{F}_q}(xR(y)+yR(x))).$$

The inner sum is $\#k$ if x lies in W_R, and the inner sum vanishes if x does not lie in W_R (for in that case $y \mapsto \psi_{\mathbb{F}_q}(\mathrm{Trace}_{k/\mathbb{F}_q}(xT(y)+yR(x)))$ is a nontrivial additive character of k). Therefore our square absolute value is

$$\sum_{x\in W_R}\psi_{\mathbb{F}_q}(\mathrm{Trace}_{k/\mathbb{F}_q}(xR(x)).$$

But for $x \in W_R$, the quadratic form $\mathrm{Trace}_{k/\mathbb{F}_q}(xR(x))$ vanishes identically (as it is one half of $\mathrm{Trace}_{k/\mathbb{F}_q}(xR(y)+yR(x))|_{y=x}$). □

Proposition 3.3. *Given the data (ψ, n, q), there exists an integer D such that for any finite extension field $k/\mathbb{F}_p$, and for any $(s,t) \in \mathbb{A}^2(k)$, all eigenvalues of the Frobenius automorphism*

$$Frob_{k,(s,t)}|\mathcal{W}(\psi, n, q)$$

are roots of unity of order dividing D.

Proof. We have shown that the traces of the lisse sheaf $\mathcal{W}(\psi, n, q)$ at all points $(s,t) \in \mathbb{A}^2(k)$, for all finite extensions $k/\mathbb{F}_q$, are algebraic integers, in fact lie in $\mathbb{Z}[\zeta_p]$. For an arbitrary extension $k/\mathbb{F}_p$, and fixed $(s,t) \in \mathbb{A}^2(k)$, denote by A the endomorphism $Frob_{k,(s,t)}|\mathcal{W}(\psi, n, q)$. Some finite extension L/k contains $\mathbb{F}_q$. Fix one such L. Then for $r := \deg(L/k)$, $A^r = Frob_{L,(s,t)}|\mathcal{W}(\psi, n, q)$. As L is a finite extension of $\mathbb{F}_q$, all powers of A^d have traces in $\mathbb{Z}[\zeta_p]$. By the usual "consider the poles of $d/dT(\log(\det(1 - TA^d))$" argument, cf. [Ax, top of page 256], all the eigenvalues of A^d are algebraic integers, and hence all the eigenvalues of A are algebraic integers.

These algebraic integers are pure of weight zero, hence are roots of unity. The characteristic polynomial of A has coefficients in $\mathbb{Q}(\zeta_p)$, hence in $\mathbb{Q}_\ell(\zeta_p)$ for any pre-chosen $\ell \neq p$. So each of these roots of unity lies in an extension field of $\mathbb{Q}_\ell(\zeta_p)$ of degree at most q^n. As $\mathbb{Q}_\ell(\zeta_p)$ has only finitely many extensions of each degree inside $\overline{\mathbb{Q}_\ell}$, it follows that all these roots of unity lie in a single finite extension E_λ of $\mathbb{Q}_\ell(\zeta_p)$. In such an E_λ, the group of roots of unity is finite. The order of this group serves as the D of the corollary. $\square$

Corollary 3.4. *Given the data (ψ, n, q), there exists an integer D such that for any finite extension field $k/\mathbb{F}_p$, and for any $(s,t) \in \mathbb{A}^2(k)$, the Frobenius automorphism*

$$Frob_{k,(s,t)}|\mathcal{W}(\psi, n, q)$$

has D'th power the identity.

Proof. Indeed, the lisse sheaf $\mathcal{W}(\psi, n, q)$ is the ψ-component of the H^1 of a family of Artin-Schreier curves, so by Weil [Weil, middle paragraph on p. 72, and last complete sentence on p. 80] each $Frob_{k,(s,t)}|\mathcal{W}(\psi, n, q)$ is (over $\overline{\mathbb{Q}_\ell}$) diagonalizable. $\square$

Putting this all together, we get the following theorem.

Theorem 3.5. *The groups G_{geom} and G_{arith} for $\mathcal{W}(\psi, n, q)$ on $\mathbb{A}^2/\mathbb{F}_p$ are finite, as are the groups G_{geom} and G_{arith} for each of its direct summands $\mathcal{G}_{\mathrm{odd}}(\psi, n, q)$ and $\mathcal{G}_{\mathrm{even}}(\psi, n, q)$.*

Proof. It suffices to prove the statement for $\mathcal{W}(\psi, n, q)$, since the groups for its direct summands are quotients of those for $\mathcal{W}(\psi, n, q)$. Since we have the inclusion $G_{geom} \subset G_{arith}$, it suffices to prove that G_{arith} is finite. The group $G_{arith} \subset \mathrm{GL}(q^n, \overline{\mathbb{Q}_\ell})$ is an algebraic group in which, by Chebotarev, every element has order dividing D. Therefore D kills the Lie algebra $\mathrm{Lie}(G_{arith})$, and hence G_{arith} is finite. $\square$

4. Determining the monodromy of $\mathcal{W}(\psi, n, q)$, of $\mathcal{G}_{\mathrm{even}}(\psi, n, q)$, and of $\mathcal{G}_{\mathrm{odd}}(\psi, n, q)$

We first establish a fundamental rationality property of our local systems.

Lemma 4.1. *The local systems $\mathcal{G}_{\mathrm{even}}(\psi, n, q)$, and $\mathcal{G}_{\mathrm{odd}}(\psi, n, q)$ have all their Frobenius traces in the quadratic field $\mathbb{Q}(\sqrt{\epsilon_p p})$.*

Proof. We must show that for any square $a \in \mathbb{F}_p^\times$, replacing ψ by ψ_a does not change the traces. [The normalizing factor $A_{\mathbb{F}_p} := -g(\psi_{-2}, \chi_2)$ is equal to $-g(\psi_{-2a}, \chi_2)$, precisely because a is a square.] These traces are

$$(-1/A_k) \sum_{x \in k} \psi_k(x^{(q^n+1)/2} + sx^{(q+1)/2} + tx)$$

and

$$(-1/A_k) \sum_{x \in k} \psi_k(x^{(q^n+1)/2} + sx^{(q+1)/2} + tx)\chi_{2,k}(x).$$

Using ψ_a instead, these traces become

$$(-1/A_k) \sum_{x \in k} \psi_k(ax^{(q^n+1)/2} + sax^{(q+1)/2} + tax)$$

and

$$(-1/A_k) \sum_{x \in k} \psi_k(ax^{(q^n+1)/2} + sax^{(q+1)/2} + tax)\chi_{2,k}(ax).$$

The key point is that, because a is a square $a \in \mathbb{F}_p^\times$, we have

$$a^{(q^n+1)/2} = aa^{(q^n-1)/2} = a, \text{ and } \mathrm{a}^{(\mathrm{q}+1)/2} = \mathrm{aa}^{(\mathrm{q}-1)/2} = \mathrm{a}.$$

So these ψ_a sums are obtained from the original ones by the change of variable $x \mapsto ax$. ☐

We next check the determinants of our local systems

Lemma 4.2. *Suppose $p \equiv 1 (\mathrm{mod}\, 4)$. Then we have the following results.*

- (i) *The arithmetic monodromy group G_{arith} for $\mathcal{G}_{\mathrm{even}}(\psi, n, q)$ lies in* $\mathrm{Sp}((q^n - 1)/2, \mathbb{C})$.
- (ii) *The arithmetic monodromy group G_{arith} for $\mathcal{G}_{\mathrm{odd}}(\psi, n, q)$ lies in* $\mathrm{SO}((q^n + 1)/2, \mathbb{C})$.

Proof. The first statement is proven in [Ka-MMP, 3.10.1]. The second statement is proven in [Ka-NG2, 1.7]. In that second reference, one is to use ψ_a for $a = (-1)^{(q^n-1)/4}((q^n + 1)/2)$, but this a mod squares in $\mathbb{F}_p^\times$ is indeed -2. ☐

Lemma 4.3. *Suppose $q \equiv 3(\mathrm{mod}\, 4)$. Denote by r_{even} (respectively r_{odd}) whichever of $(q^n \pm 1)/2$ is even (respectively odd). Thus r_{even} is the rank of $\mathcal{G}_{\mathrm{even}}(\psi, n, q)$ and r_{odd} is the rank of $\mathcal{G}_{\mathrm{odd}}(\psi, n, q)$. Then we have the following results.*

(i) *The arithmetic monodromy group G_{arith} for $\mathcal{G}_{\mathrm{even}}(\psi, n, q)$ lies in $\mathrm{SL}(r_{\mathrm{even}}, \mathbb{C})$.*
(ii) *The arithmetic monodromy group G_{arith} for $\mathcal{G}_{\mathrm{odd}}(\psi, n, q)$ lies in $\mathrm{SL}(r_{\mathrm{odd}}, \mathbb{C})$.*
(iii) *The arithmetic monodromy group G_{arith} for $\mathcal{W}(\psi, n, q)$ lies in $\mathrm{SL}(q^n, \mathbb{C})$.*

Proof. Let us denote the determinants in question by

$$\mathcal{D}_{\mathrm{even}} := \det(\mathcal{G}_{\mathrm{even}}(\psi, n, q)),\ \mathcal{D}_{\mathrm{odd}} := \det(\mathcal{G}_{\mathrm{even}}(\psi, n, q)),\ \mathcal{D}_{\mathcal{W}} := \det(\mathcal{W}(\psi, n, q)).$$

These are each lisse of rank one and pure of weight zero on $\mathbb{A}^2/\mathbb{F}_p$. Because $\mathcal{W}$ is the direct sum, we have

$$\mathcal{D}_{\mathcal{W}} \cong \mathcal{D}_{\mathrm{even}} \otimes \mathcal{D}_{\mathrm{odd}}.$$

So it suffices to show any two of the three assertions of the lemma.

Suppose first we are in characteristic $p \geq 5$. The only roots of unity in $\mathbb{Q}(\sqrt{\epsilon_p p})$ are ± 1. Because both $\mathcal{G}_{\mathrm{even}}(\psi, n, q)$ and $\mathcal{G}_{\mathrm{odd}}(\psi, n, q)$ have all their Frobenius traces in $\mathbb{Q}(\sqrt{\epsilon_p p})$, so also do their determinants. On the other hand, these determinants are, point by point, roots of unity (being, in fact, D'th roots of unity for some fixed D). Therefore the Frobenius determinants all lie in ± 1, and hence each of $\mathcal{D}_{\mathrm{even}} := \det(\mathcal{G}_{\mathrm{even}}(\psi, n, q))$ and $\mathcal{D}_{\mathrm{odd}} := \det(\mathcal{G}_{\mathrm{even}}(\psi, n, q))$ is lisse of rank one on $\mathbb{A}^2/\mathbb{F}_p$ with $\mathcal{D}_{\mathrm{even}}^{\otimes 2}$ and $\mathcal{D}_{\mathrm{odd}}^{\otimes 2}$ arithmetically, and hence geometrically trivial. But $\pi_1(\mathbb{A}^2/\overline{\mathbb{F}_p})$ has no nontrivial prime to p quotients. Therefore both $\mathcal{D}_{\mathrm{even}}$ and $\mathcal{D}_{\mathrm{odd}}$ are geometrically trivial. So to check that they are arithmetically trivial as well, it suffices to check at a single $\mathbb{F}_p$ point of $\mathbb{A}^2$. We check at the origin. The result is then, with some tedium, checked to be a special case of [KT-gpconj, 2.3].

It remains to treat the case of characteristic $p = 3$. We will do this by giving a proof of the lemma which is valid in all odd characteristics. First, it suffices to prove that two of the three $\mathcal{D}_{\mathcal{W}}, \cong \mathcal{D}_{\mathrm{even}}, \otimes \mathcal{D}_{\mathrm{odd}}$ are geometrically constant. Then both $\mathcal{D}_{\mathrm{even}}$ and $\otimes \mathcal{D}_{\mathrm{odd}}$ are geometrically constant, and we then verify their arithmetic triviality by checking at a single point, just as in the paragraph above.

We will use the Hasse-Davenport argument, cf. [D-H, §3, II, pp. 162-165] or [Ka-MG, pp. 53-54], and apply it to $\mathcal{W}(\psi, n, q)$ and to whichever of the $\mathcal{G}$ is $\mathcal{G}(\psi, n, q, \mathbb{1})$. Their trace functions, at a point

$(s,t) \in \mathbb{A}^2(k)$, are given by the expressions

$$(-1/A_k)\sum_{x\in k}\psi_k(x^{(q^n+1)/2}+sx^{(q+1)/2}+tx)$$

and

$$(-1/A_k)\sum_{x\in k}\psi_k(x^{q^n+1}+sx^{q+1}+tx^2).$$

In both cases, the polynomial $f(x)$ being summed inside the ψ is of the form

$$f(x) := x^m + \sum_{i=1}^{d} a_i x^i$$

with $m \geq 5$ prime to p and with $d < m/2$.

In terms of the L-function for $\mathcal{L}_{\psi_k(fx))}$, the determinant of $-Frob$ on $H^1_c(\mathbb{A}^1/\overline{k}, \mathcal{L}_{\psi_k(fx))})$ is the coefficient of T^{m-1}. Using the additive expression of the L-series, we see that this coefficient is expressed in terms of the Newton symmetric functions $N_1, \ldots, N_m$ of the first $m-1$ elementary symmetric functions $s_1, \ldots, s_{m-1}$, as

$$\sum_{s1,\ldots,s_{m-1}\in k}\psi_k(N_m(s1,\ldots,s_{m-1})+\sum_{i=1}^{d}a_iN_i(s1,\ldots,s_i)).$$

[We have used the fact that N_i is a polynomial in $s_1, \ldots, s_i$.] Thus the variables $s_{m-1}, s_{m-2}, \ldots, s_{d+1}$ occur only in the N_m term. In the polynomial N_m, these variables occur in the form

$$(-1)^m m s_{m-i}s_i + s_{m-i}(\text{a polynomial in variables } s_j \text{ with } j < i),$$

for $m - j > m/2$. When m is even, the variable $s_{m/2}$ occurs as

$$(-1)^m(m/2)s_{m/2}^2 + s_{m/2}(\text{a polynomial in variables } s_j \text{ with } j < m/2),$$

Summing over s_{m-1}, we get $\#k$ times the sum of the terms with $s_1 = 0$, and this sum is independent of the value of s_{m-1}, so it is

$$(\#k)\sum_{s_2\ldots,s_{m-2}\in k}\psi_k(N_m(0,s_2,\ldots,s_{m-2},0)+\sum_{i=1}^{d}a_iN_i(0,s_2,\ldots,s_i)).$$

Summing then over s_{m-2}, we get $\#k$ times the sum of these terms with $s_2 = 0$ as well, thus

$$(\#k)^2\sum_{s_3\ldots,s_{m-3}\in k}\psi_k(N_m(0,0,s_3,\ldots,s_{m-3},0,0)+\sum_{i=1}^{d}a_iN_i(0,0,s_3,\ldots,s_i)).$$

Continuing in this way, we get

$$(\#k)^{(m-1)/2} \text{ if } m \text{ is odd}, (\#k)^{(m-2)/2} \sum_{s_{m/2} \in k} \psi_k((m/2)s_{m/2}^2) \text{ if } m \text{ is even.}$$

As for the determinant of $Frob$ itself on $H^1_c(\mathbb{A}^1/\overline{k}, \mathcal{L}_{\psi_k(fx))})$, it is therefore

$$(\#k)^{(m-1)/2} \text{ if } m \text{ is odd}, (\#k)^{(m-2)/2}(-\sum_{s_{m/2} \in k} \psi_k((m/2)s_{m/2}^2)) \text{ if } m \text{ is even.}$$

This expression, independent of choices of the coefficients $a_1, \ldots, a_d$ of the polynomial $f(x)$, establishes the asserted geometric constance. $\square$

At this point, we recall a key result from [KT-gpconj, 17.2] about the local systems $\mathcal{G}_{0,\text{even}}(\psi, n, q)$ and $\mathcal{G}_{0,\text{odd}}(\psi, n, q)$ obtained by specializing $s \mapsto 0$ in $\mathcal{G}_{\text{even}}(\psi, n, q)$ and $\mathcal{G}_{\text{odd}}(\psi, n, q)$.

Theorem 4.4. *Suppose $q = p^a$, p an odd prime, and $q > 3$. We have the following results.*

(i) *The group G_{geom} for $\mathcal{G}_{0,\text{even}}(\psi, n, q)$ is $\mathrm{SL}(2, q^n)$ in one of its even Weil representations.*

(ii) *The group G_{geom} for $\mathcal{G}_{0,\text{odd}}(\psi, n, q)$ is $\mathrm{PSL}(2, q^n)$ in one of its odd Weil representations.*

We now combine this result with Theorems 2.1 and 2.2, to obtain the following corollary.

Corollary 4.5. *Suppose $q = p^a$, p an odd prime, and na is prime to p. Suppose also that $n \geq 2$. We have the following results.*

(i) *The group G_{geom} for $\mathcal{G}_{\text{even}}(\psi, n, q)$ is one of the groups $\mathrm{Sp}(2A, p^B)$ in one of its even Weil representations, for some factorization of na as $na = AB$.*

(ii) *The group G_{geom} for $\mathcal{G}_{\text{odd}}(\psi, n, q)$ is one of the groups $\mathrm{PSp}(2C, p^D)$ in one of its odd Weil representations, for some factorization of na as $na = CD$.*

Proof. To prove (i), we argue as follows. By the determinant lemma above, the group G_{geom} for $\mathcal{G}_{\text{even}}(\psi, n, q)$ lies in the relevant SL group $\mathrm{SL}(r_{\text{even}}, \mathbb{C})$, and it contains $\mathrm{SL}(2, q^n)$, the geometric monodromy group of the pullback local system $\mathcal{G}_{0,\text{even}}(\psi, n, q)$. By Theorems 2.1 and 2.2, G_{geom} is one of the groups $\mathrm{Sp}(2A, p^B) \rtimes C_b$ for some divisor b of B. By hypothesis, na is prime to p, and hence b, a divisor of $na = AB$, is prime to p. Because $\mathcal{G}_{\text{even}}(\psi, n, q)$ is lisse on $\mathbb{A}^2/\overline{\mathbb{F}_p}$, its G_{geom} has no nontrivial prime to p quotient, and hence $b = 1$.

Repeat essentially the same argument to prove (ii). $\square$

Proposition 4.6. *In the above corollary, we have* $(A, B) = (C, D)$, *and* G_{geom} *for* $\mathcal{W}(\psi, n, q)$ *is the diagonal image of* $\mathrm{Sp}(2A, p^B)$ *in the product group* $\mathrm{Sp}(2A, p^B) \times \mathrm{PSp}(2A, p^B)$.

Proof. The group $G_{geom,\mathcal{W}}$ is a subgroup of the product $\mathrm{Sp}(2A, p^B) \times \mathrm{PSp}(2C, p^D)$ which maps onto each factor. The group $\mathrm{PSp}(2C, p^D)$ is simple, and the only quotient groups of $\mathrm{Sp}(2A, p^B)$ are itself, the simple group $\mathrm{PSp}(2A, p^B)$, and the trivial group. If $(A, B) \neq (C, D)$, we argue by contradiction. By Goursat's lemma, $G_{geom,\mathcal{W}}$ would be the product group $\mathrm{Sp}(2A, p^B) \times \mathrm{PSp}(2C, p^D)$. From the known character table of $\mathrm{SL}(2, q^n)$, for any of its individual Weil representations there are elements of trace zero. So in the product group $\mathrm{Sp}(2A, p^B) \times \mathrm{PSp}(2C, p^D)$ (indeed already in the subgroup $\mathrm{SL}(2, q^n) \times \mathrm{PSL}(2, q^n)$), there are elements whose traces are zero in both summands of any given representation of $\mathrm{Sp}(2A, p^B) \times \mathrm{PSp}(2C, p^D)$ of the form

(an even Weil rep. of $\mathrm{Sp}(2A, p^B) \oplus$ an odd Weil rep. of $\mathrm{PSp}(2C, p^D)$.

On the other hand, we have shown that over all extension fields $k/\mathbb{F}_q$, all Frobenius traces have square absolute value in the set $\{q^d\}_{d=0,\ldots,2n}$. In other words, if we compute $G_{arith,\mathcal{W}}$ after extending scalars to $\mathbb{A}^1/\mathbb{F}_q$, all of its traces have square absolute value in this set. Therefore all elements in the subgroup $G_{geom,\mathcal{W}}$ have traces whose square absolute value lies in this set. In particular, $G_{geom,\mathcal{W}}$ contains no elements of trace zero. This contadiction shows that $(A, B) = (C, D)$.

Now $G_{geom,\mathcal{W}}$ is a subgroup of $\mathrm{Sp}(2A, p^B) \times \mathrm{PSp}(2A, p^B)$ which maps onto each factor. So again by Goursat's lemma, either $G_{geom,\mathcal{W}}$ is the diagonal image of $\mathrm{Sp}(2A, p^B)$ in $\mathrm{Sp}(2A, p^B) \times \mathrm{PSp}(2A, p^B)$, or it is the full product group. The above "trace zero" argument shows that the product group is not possible. ☐

Lemma 4.7. *Suppose* $q = p^a$, p *an odd prime, and* na *is prime to* p. *Suppose also that* $n \geq 2$. *After extension of scalars to* $\mathbb{A}^2/\mathbb{F}_{q^n}$, *we have* $G_{arith} = G_{geom}$ *for each of* $\mathcal{G}_{\mathrm{even}}(\psi, n, q)$, $\mathcal{G}_{\mathrm{odd}}(\psi, n, q)$, *and* $\mathcal{W}(\psi, n, q)$.

Proof. Apply Theorems 2.1 and 2.2 to the relevant G_{arith} groups. The normalizer of $\mathrm{Sp}(2A, p^B)$ in $\mathrm{Sp}(2AB, p)$ is $\mathrm{Sp}(2A, p^B) \rtimes C_B$, and the normalizer of $\mathrm{PSp}(2A, p^B)$ in $\mathrm{PSp}(2AB, p)$ is $\mathrm{PSp}(2A, p^B) \rtimes C_B$. Thus for $\mathcal{G}_{\mathrm{even}}(\psi, n, q)$ we have

$$G_{geom} = \mathrm{Sp}(2A, p^B) \hookrightarrow G_{arith} \hookrightarrow \mathrm{Sp}(2A, p^B) \rtimes C_B,$$

and for $\mathcal{G}_{\mathrm{even}}(\psi, n, q)$ we have

$$G_{geom} = \mathrm{PSp}(2A, p^B) \hookrightarrow G_{arith} \hookrightarrow \mathrm{PSp}(2A, p^B) \rtimes C_B.$$

Thus in both cases G_{geom} has index dividing B, and hence dividing $an = AB$ in G_{arith}. So in both cases we attain $G_{arith} = G_{geom}$ after extension of scalars to $\mathbb{F}_{p^B}$, and hence to the larger field $\mathbb{F}_{p^{an}} = \mathbb{F}_{q^n}$. Then $G_{arith,\mathcal{W}}$ is a subgroup of $\mathrm{Sp}(2A, p^B) \times \mathrm{PSp}(2A, p^B)$ which maps onto each factor. Now repeat the "trace zero" argument, to show that $G_{arith,\mathcal{W}}$ is the the diagonal image of $\mathrm{Sp}(2A, p^B)$ in this product. In particular, $G_{arith,\mathcal{W}}$ is equal to $G_{geom,\mathcal{W}}$. □

Theorem 4.8. *Suppose $q = p^a$, p an odd prime, and na is prime to p. Suppose also that $n \geq 2$. After extension of scalars to $\mathbb{A}^2/\mathbb{F}_{q^n}$, the local systems $\mathcal{G}_{\mathrm{even}}(\psi, n, q)$ and $\mathcal{G}_{\mathrm{odd}}(\psi, n, q)$ are correctly matched in the sense that $\mathcal{W}(\psi, n, q)$ is a total Weil representation, and their respective geometric (and arithmetic) monodromy groups are* $\mathrm{Sp}(n, q)$, $\mathrm{PSp}(n, q)$, $\mathrm{Sp}(n, q)$.

Proof. From Lemma 3.2, the square absolute values of the traces of elements of $G_{geom,\mathcal{W}}$ are powers of q, hence powers of p, hance $\mathcal{W}(\psi, n, q)$ does indeed incarnate a total Weil representation. These square absolute values will then be all the powers $\{p^{Bd}\}_{d=0,\ldots,2A}$ of p^B. Therefore p^B, being the trace of some element of $G_{geom,\mathcal{W}}$, is itself a power of q. Therefore p^B is q^f for the least $f \geq 1$ such that q^f is the square absolute value of the trace of some element of $G_{geom,\mathcal{W}} = G_{arith,\mathcal{W}}$.

So it suffices to exhibit a point $(s, t) \in \mathbb{A}^2(\mathbb{F}_{q^n})$ at which

$$|\mathrm{Trace}(Frob_{\mathbb{F}_{q^n},(s,t)}|\mathcal{W}(\psi, n, q)|^2 = q.$$

We will show that $(1, -2)$ is such a point.

Recall that for $(s, t) \in \mathbb{A}^2(\mathbb{F}_{q^n})$, this square absolute value is the cardinality of the set of zeroes in $\mathbb{F}_{q^n}$ of the polynomial

$$x^{q^{2n}} + s^{q^n} x^{q^{n+1}} + 2t^{q^n} x^{q^n} + s^{q^{n-1}} x^{q^{n-1}} + x.$$

If we choose s, t both to lie in $\mathbb{F}_q$, the $\mathbb{F}_{q^n}$ zeroes are the zeroes $x \in \mathbb{F}_{q^n}$ of

$$x + sx^q + 2tx + sx^{q^{-1}} + x,$$

or, raising to the q'th power, the the zeroes $x \in \mathbb{F}_{q^n}$ of

$$2x^q + sx^{q^2} + 2tx^q + sx.$$

Let us denote by F the operator

$$F(x) := x^q,$$

the q^{th} power arithmetic Frobenius. Then our equation becomes

$$(sF^2 + (2 + 2t)F + s)(x) = 0.$$

Take $s = 1, t = -2$. The equation becomes

$$(F - 1)^2(x) = 0.$$

We will show that the only $\mathbb{F}_{q^n}$ solutions are $x \in \mathbb{F}_q$. To see this, put $y := (F - 1)(x)$. Then $(F - 1)(y) = 0$, i.e., y lies in $\mathbb{F}_q$. Then we seek $x \in \mathbb{F}_{q^n}$ such that $(F - 1)(x) = y$ For $y = 0$, the solutions of $(F - 1)(x) = y$ are all $x \in \mathbb{F}_q$. For any fixed $y \neq 0$ in $\mathbb{F}_q$, any solution x of $(F - 1)(x) = y$, i.e., any solution of

$$x^q - x = y,$$

lies in a degree p extension of $\mathbb{F}_q$. By hypothesis n is prime to p, so for $y \neq 0$ in $\mathbb{F}_q$, the equation $(F - 1)(x) = y$ has no solutions in $\mathbb{F}_{q^n}$. □

Corollary 4.9. *Hypotheses as in Theorem 4.8, each of the local systems $\mathcal{G}_{\text{even}}(\psi, n, q)$, $\mathcal{G}_{\text{odd}}(\psi, n, q)$, and $\mathcal{W}(\psi, n, q)$ has $G_{geom} = G_{arith}$ after extension of scalars to $\mathbb{A}^2/\mathbb{F}_q$.*

Proof. In Lemma 4.7 we proved that these equalities of G_{geom} with G_{arith} take place after extension of scalars to $\mathbb{A}^2/\mathbb{F}_{p^B}$, and in Theorem 4.8 we proved that $p^B = q$. □

5. Changing the choice of ψ to ψ_2; which Weil representation?

Recall that $\mathrm{Sp}(2n, q)$ has two "small" Weil representations, of dimension $(q^n - 1)/2$, and two "large" ones, of dimension $(q^n + 1)/2$, with a matching of small and large imposed by the total Weil representation. We have shown that for any choice of nontrivial additive character of $\mathbb{F}_p$, the local systems $\mathcal{G}_{\text{even}}(\psi, n, q)$ and $\mathcal{G}_{\text{odd}}(\psi, n, q)$ incarnate a correctly matched pair, with geometric monodromy groups respectively $\mathrm{Sp}(2n, q)$ and $\mathrm{PSp}(2n, q)$.

Theorem 5.1. *We have the following results.*

(i) *Suppose 2 is a square in $\mathbb{F}_q$ (i.e., suppose q is ± 1 mod 8). Then pulled back to $\mathbb{A}^2/\mathbb{F}_q$, there exist arithmetic isomorphisms of local systems*

$$\mathcal{G}_{\text{even}}(\psi, n, q) \cong \mathcal{G}_{\text{even}}(\psi_2, n, q), \quad \mathcal{G}_{\text{odd}}(\psi, n, q) \cong \mathcal{G}_{\text{odd}}(\psi_2, n, q).$$

(ii) *Suppose 2 is not a square in $\mathbb{F}_q$. Then $\mathcal{G}_{\text{even}}(\psi, n, q)$ and $\mathcal{G}_{\text{odd}}(\psi, n, q)$ incarnate the other correctly matched pair.*

Proof. Suppose first that 2 is a square in $\mathbb{F}_q$. Then over extensions $k/\mathbb{F}_q$, the normalizing factor $A_{\psi_2,k} = A_{\psi,k}$. Inside the exponential sum, the substitution $x \mapsto 2x$ turns the ψ sum into the ψ_2 sum, simply because

$$2^{(q^n+1)/2} = 2^{(q^n-1)/2}2 = \chi_{2,\mathbb{F}_{q^n}}(2) = 2,\ 2^{(q+1)/2} = 2^{(q-1)/2}2 = \chi_{2,\mathbb{F}_q}(2) = 2,$$

and over over extensions $k/\mathbb{F}_q$, we have $\chi_{2,k}(2x) = \chi_{2,k}(x)$.

Suppose now that 2 is not a square in $\mathbb{F}_q$. It suffices to show that $\mathcal{G}(\psi, n, q, \mathbb{1})$ is not geometrically isomorphic to $\mathcal{G}(\psi_2, n, q, \mathbb{1})$. In fact, we will show that even after specializing $s \mapsto 1$, the resulting local systems $\mathcal{G}_1(\psi, n, q, \mathbb{1})$ and $\mathcal{G}_1(\psi_2, n, q, \mathbb{1})$ are not geometrically isomorphic. Geometrically, we can ignore the normalizing factors. Then $\mathcal{G}_1(\psi, n, q, \mathbb{1})$ is the Fourier transform FT_ψ of $\mathcal{L}_{\psi(x^{(q^n+1)/2}+x^{(q+1)/2})}$.

We now express $\mathcal{G}_1(\psi_2, n, q, \mathbb{1})$ as an FT_ψ. Its trace function (again ignoring the normalizing factor) at $t \in \mathbb{A}^1(k)$ is

$$-\sum_{x \in k} \psi(2x^{(q^n+1)/2} + 2x^{(q+1)/2} + 2tx) =$$

(remembering that $2^{(q+1)/2} = -2$, and that $2^{(q^n+1)/2} = 2(-1)^n$)

$$= -\sum_{x \in k} \psi((-1)^n(2x)^{(q^n+1)/2} - (2x)^{(q+1)/2} + t(2x)) =$$

$$= -\sum_{x \in k} \psi((-1)^n x^{(q^n+1)/2} - x^{(q+1)/2} + tx).$$

Thus $\mathcal{G}_1(\psi_2, n, q, \mathbb{1})$ is the Fourier transform FT_ψ of $\mathcal{L}_{\psi((-1)^n x^{(q^n+1)/2} - x^{(q+1)/2})}$. As the two inputs

$$\mathcal{L}_{\psi(x^{(q^n+1)/2}+x^{(q+1)/2})} \text{ and } \mathcal{L}_{\psi((-1)^{\mathrm{n}}\mathrm{x}^{(\mathrm{q}^{\mathrm{n}}+1)/2}-\mathrm{x}^{(\mathrm{q}+1)/2})}$$

are visibly not geometrically isomorphic, neither are their FT_ψ outputs. $\square$

We now invoke a fundamental result of Guralnick, Magaard, and Tiep [GMT, Theorem 1.1, (ii) and (iii)]. Recall that 2 is a square in $\mathbb{F}_q$ if and only if q is $\pm 1 (\mathrm{mod}\, 8)$. So their result gives

Theorem 5.2. *Suppose $q = p^a$, p an odd prime, and na is prime to p. Suppose also that $n \geq 2$. On $\mathbb{A}^2/\mathbb{F}_p$, there exists geometric isomorphism of local systems*

$$Sym^2(\mathcal{G}_{\mathrm{small}}(\psi, n, q)) \cong \Lambda^2(\mathcal{G}_{\mathrm{large}}(\psi_2, n, q)),$$

$$Sym^2(\mathcal{G}_{\mathrm{small}}(\psi_2, n, q)) \cong \Lambda^2(\mathcal{G}_{\mathrm{large}}(\psi, n, q)).$$

Pulled back to $\mathbb{A}^2/\mathbb{F}_{q^n}$, these exist as arithmetic isomorphisms.

Proof. For the geometric isomorphisms, this is immediate from Theorem 4.8 and [GMT, 1.1, (ii) and (iii)], because in view of Theorem 4.8 it is a statement about the representation theory of G_{geom}. Pulled back to $\mathbb{A}^2/\mathbb{F}_{q^n}$, we know that $G_{geom} = G_{airth}$, so we have an equality of all Frobenius traces over extension fields of $\mathbb{F}_{q^n}$, as every such Frobenius lies in G_{geom}. □

6. Specializing $s \mapsto 1$

Specializing $s \mapsto 1$, we get the following corollary of Theorem 5.2.

Corollary 6.1. *Suppose $q = p^a$, p an odd prime, and na is prime to p. Suppose also that $n \geq 2$. On $\mathbb{A}^1/\mathbb{F}_p$, there exists geometric isomorphism of local systems*

$$Sym^2(\mathcal{G}_{1,\text{small}}(\psi, n, q)) \cong \Lambda^2(\mathcal{G}_{1,\text{large}}(\psi_2, n, q)),$$
$$Sym^2(\mathcal{G}_{1,\text{small}}(\psi_2, n, q)) \cong \Lambda^2(\mathcal{G}_{1,\text{large}}(\psi, n, q)).$$

Pulled back to $\mathbb{A}^2/\mathbb{F}_{q^n}$, these exist as arithmetic isomorphisms.

When we specialize$s \mapsto 1$, the groups G_{geom} and G_{arith} can only shrink. Each of the local systems

$$\mathcal{G}_{1,\text{small}} := \mathcal{G}_{1,\text{small}}(\psi, n, q)$$

and

$$\mathcal{G}_{1,\text{large}} := \mathcal{G}_{1,\text{large}}(\psi, n, q)$$

is geometrically irreducible (thanks to the Fourier Transform description). In view of Theorem 4.8, we get

Proposition 6.2. *Suppose $q = p^a$, p an odd prime, and na is prime to p. Suppose also that $n \geq 2$. We have the following results, which we now express in terms of $\mathcal{G}_{1,\text{even}}$ and $\mathcal{G}_{1,\text{odd}}$.*

(i) *After extension of scalars to $\mathbb{A}^1/\mathbb{F}_{q^n}$, we have inclusions of geometric and arithmetic monodromy groups*

$$G_{geom,\mathcal{G}_{1,\text{even}}} \subset G_{arith,\mathcal{G}_{1,\text{even}}} \subset G_{arith,\mathcal{G}_{\text{even}}} = \mathrm{Sp}(n, q).$$

(ii) *The restriction to $G_{geom,\mathcal{G}_{1,\text{even}}}$ of the even Weil representation of of $\mathrm{Sp}(n, q)$ is irreducible (this being the taulogical representation of the geometrically irreducible local system $\mathcal{G}_{1,\text{even}}$).*

(iii) *After extension of scalars to $\mathbb{A}^1/\mathbb{F}_{q^n}$, we have inclusions of geometric and arithmetic monodromy groups*

$$G_{geom,\mathcal{G}_{1,\text{odd}}} \subset G_{arith,\mathcal{G}_{1,\text{odd}}} \subset G_{arith,\mathcal{G}_{\text{odd}}} = \mathrm{PSp}(n, q).$$

(iv) *The restriction to $G_{geom,\mathcal{G}_{1,\text{odd}}}$ of the odd Weil representation of of $\mathrm{PSp}(n, q)$ is irreducible (this being the taulogical representation of the geometrically irreducible local system $\mathcal{G}_{1,\text{odd}}$).*

We now combine this result with Theorem 2.7.

Theorem 6.3. *Suppose $q = p^a$, p an odd prime, and na is prime to p. Suppose also that $n \geq 2$. We have the following results.*

(i) *Suppose $(q^n + 1)/2$ is even. Then $\mathcal{G}_{1,\mathrm{large}} = \mathcal{G}_{1,\mathrm{even}}(\psi, n, q)$ has*

$$\mathrm{SL}(2, q^n) \subset G_{geom,\mathcal{G}_{1,\mathrm{even}}} \subset G_{arith,\mathcal{G}_{1,\mathrm{even}}} \subset \mathrm{Sp}(n, q).$$

For some factorization $na = AB$, we have $G_{geom,\mathcal{G}_{1,\mathrm{even}}} = \mathrm{Sp}(2A, p^B)$, and after extension of scalars to $\mathbb{A}^1/\mathbb{F}_{q^n}$, we have

$$G_{geom,\mathcal{G}_{1,\mathrm{even}}} = G_{arith,\mathcal{G}_{1,\mathrm{even}}}.$$

(ii) *Suppose $(q^n + 1)/2$ is odd, and that $q^n \neq 3^2$, 5^3. Then $\mathcal{G}_{1,\mathrm{large}} = \mathcal{G}_{1,\mathrm{odd}}(\psi, n, q)$ has*

$$\mathrm{PSL}(2, q^n) \subset G_{geom,\mathcal{G}_{1,\mathrm{odd}}} \subset G_{arith,\mathcal{G}_{1,\mathrm{odd}}} \subset \mathrm{PSp}(n, q).$$

For some factorization $na = CD$, we have $G_{geom,\mathcal{G}_{1,\mathrm{odd}}} = \mathrm{Sp}(2C, p^D)$, and after extension of scalars to $\mathbb{A}^1/\mathbb{F}_{q^n}$, we have

$$G_{geom,\mathcal{G}_{1,\mathrm{odd}}} = G_{arith,\mathcal{G}_{1,\mathrm{even}}}.$$

(iii) *Suppose $q^n = 3^2$ or 5^3. The above statement* (ii) remains true.

Proof. The first assertion of (i) and (ii) is immediate from Theorem 2.7, remembering that the G_{geom} groups have no nontrivial prime to p quotients, cf. the proof of Corollary 4.5. The second statement is proven as in the proof of Lemma 4.7.

It remains to prove (iii).

We first consider the case $q^n = 3^2$. Here we look at maximal subgroups $G < \mathrm{PSp}(4, 3)$ on which an odd Weil representation, toward $\mathrm{SL}(5, \mathbb{C})$, remains irreducible. If G contains $\mathrm{PSL}(2, 9)$, we are done. The other possibility is $G = 2^4 \rtimes \mathsf{A}_5$. This group is best seen using the isomorphism $\mathsf{A}_5 \cong \mathrm{SL}(2, 4)$ as the affine special linear group $\mathbb{F}_4^2 \rtimes \mathrm{SL}(2, 4)$. In this case, G_{geom} for $\mathcal{G}_{1,\mathrm{odd}}(\psi, 2, 3)$ is either this G or it is $\mathrm{PSp}(4, 3)$. In the latter case, we are done. If G_{geom} is G, then also G_{arith} is G (because G is its own normalizer in $\mathrm{SL}(5, \mathbb{C})$). A computer calculation shows that over $\mathbb{F}_9$, the traces of $\mathcal{G}_{1,\mathrm{odd}}(\psi, 2, 3)$ lie in $\mathbb{Z}[\zeta_3]$ but do **not** lie in $\mathbb{Z}$. On the other hand, all traces of G in its unique five-dimensional irreducible representation lie in $\mathbb{Z}$.

We now turn the case $q^n = 5^3$. Here we look at maximal subgroups $G < \mathrm{PSp}(6, 5)$ on which an odd Weil representation, toward $\mathrm{SL}(63, \mathbb{C})$, remains irreducible. When G contains $\mathrm{PSL}(2, 5^3)$, we are done. The other possibility is that $G = J_2$. In this case, G_{geom} for $\mathcal{G}_{1,\mathrm{odd}}(\psi, 3, 5)$ is either J_2 or it is $\mathrm{PSp}(6, 5)$. In the latter case, we are done. If G_{geom} is J_2, then also G_{arith} is J_2 (because J_2 is its own normalizer in $\mathrm{SL}(63, \mathbb{C})$).

A computer calculation shows that over $\mathbb{F}_{25}$, the traces of $\mathcal{G}_{1,\mathrm{odd}}(\psi, 3, 5)$ lie in $\mathbb{Z}[\zeta_5]^+$ but do **not** lie in $\mathbb{Z}$. On the other hand, all traces of J_2 in its unique 63-dimensional irreducible representation lie in $\mathbb{Z}$. $\square$

We now make use of Corollary 6.1, applied to our local systems using ψ_2.

Theorem 6.4. *Suppose $q = p^a$, p an odd prime, and na is prime to p. Suppose also that $n \geq 2$. We have the following results.*

(i) *Suppose $(q^n + 1)/2$ is even. For some factorization $na = AB$, $\mathcal{G}_{1,\mathrm{small}} = \mathcal{G}_{1,\mathrm{odd}}(\psi, n, q)$ has*

$$G_{geom,\mathcal{G}_{1,\mathrm{odd}}} = \mathrm{PSp}(2A, p^B).$$

After extension of scalars to $\mathbb{A}^1/\mathbb{F}_{q^n}$, we have

$$G_{geom,\mathcal{G}_{1,\mathrm{odd}}} = G_{arith,\mathcal{G}_{1,\mathrm{odd}}}.$$

(ii) *Suppose $(q^n + 1)/2$ is odd. For some factorization $na = CD$, $\mathcal{G}_{1,\mathrm{large}} = \mathcal{G}_{1,\mathrm{even}}(\psi, n, q)$ has*

$$G_{geom,\mathcal{G}_{1,\mathrm{even}}} = \mathrm{Sp}(2C, p^D).$$

After extension of scalars to $\mathbb{A}^1/\mathbb{F}_{q^n}$, we have

$$G_{geom,\mathcal{G}_{1,\mathrm{even}}} = G_{arith,\mathcal{G}_{1,\mathrm{even}}}.$$

Proof. Suppose first $(q^n + 1)/2$ is even. Then

$$\mathcal{G}_{1,\mathrm{large}}(\psi_2, n, q) = \mathcal{G}_{1,\mathrm{even}}(\psi_2, n, q),$$

and by Corollary 6.1, we have

$$\Lambda^2(\mathcal{G}_{1,\mathrm{even}}(\psi_2, n, q)) \cong Sym^2(\mathcal{G}_{1,\mathrm{odd}}(\psi, n, q).$$

Therefore $Sym^2(\mathcal{G}_{1,\mathrm{odd}}(\psi, n, q)$ has its G_{geom} (and its G_{arith}, after extension of scalars to $\mathbb{A}^1/\mathbb{F}_{q^n}$) equal to $\mathrm{PSp}(2A, p^B)$ for some factorization $na = AB$. The G_{geom} for $sG_{1,\mathrm{odd}}(\psi, n, q)$ itself is therefore either $\mathrm{PSp}(2A, p^B)$ or a double covering of $\mathrm{PSp}(2A, p^B)$, so either the product $\mathrm{PSp}(2A, p^B) \times \pm 1$ or $\mathrm{Sp}(2A, p^B)$. It cannot be $\mathrm{Sp}(2A, p^B)$, because $\mathrm{Sp}(2A, p^B)$ has no faithful irreducible representation of odd dimension $(q^n - 1)/2$. It cannot be the product $\mathrm{PSp}(2A, p^B) \times \pm 1$ because G_{geom} has no nontrivial prime to p quotient.

Suppose now that $(q^n + 1)/2$ is odd. Then

$$\mathcal{G}_{1,\mathrm{large}}(\psi_2, n, q) = \mathcal{G}_{1,\mathrm{odd}}(\psi_2, n, q),$$

and by Corollary 6.1, we have

$$\Lambda^2(\mathcal{G}_{1,\mathrm{odd}}(\psi_2, n, q) \cong Sym^2(\mathcal{G}_{1,\mathrm{even}}(\psi, n, q)).$$

Therefore $Sym^2(\mathcal{G}_{1,\text{even}}(\psi,n,q)$ has its G_{geom} (and its G_{arith}, after extension of scalars to $\mathbb{A}^1/\mathbb{F}_{q^n}$) equal to $\mathrm{PSp}(2C,p^D)$ for some factorization $na = CD$. The G_{geom} for $sG_{1,\text{even}}(\psi,n,q)$ itself is therefore either $\mathrm{PSp}(2C,p^D)$ or a double covering of $\mathrm{PSp}(2C,p^D)$, so either the product $\mathrm{PSp}(2C,p^D)\{\times\pm 1\}$ or $\mathrm{Sp}(2C,p^D)$. It cannot be $\mathrm{PSp}(2C,p^D)$, because $\mathrm{PSp}(2C,p^D)$ has no irreducible representation of even dimension $(q^n-1)/2$. It cannot be the product $\mathrm{PSp}(2C,p^D)\times\{\pm 1\}$ because G_{geom} has no nontrivial prime to p quotient. □

Proposition 6.5. *In the above theorem, we have* $(A,B) = (C,D)$, *and* G_{geom} *for* $\mathcal{W}_1(\psi,n,q)$ *is the diagonal image of* $\mathrm{Sp}(2A,p^B)$ *in the product group* $\mathrm{Sp}(2A,p^B)\times\mathrm{PSp}(2A,p^B)$.

Proof. Repeat the proof of Proposition 4.6. □

Lemma 6.6. *Suppose* $q = p^a$, *p an odd prime, and na is prime to p. Suppose also that* $n \geq 2$. *After extension of scalars to* $\mathbb{A}^1/\mathbb{F}_{q^n}$, *we have* $G_{arith} = G_{geom}$ *for each of* $\mathcal{G}_{1,\text{even}}(\psi,n,q)$, $\mathcal{G}_{1,\text{odd}}(\psi,n,q)$, *and* $\mathcal{W}_1(\psi,n,q)$.

Proof. Repeat the proof of Lemma 4.7. □

Theorem 6.7. *Suppose* $q = p^a$, *p an odd prime, and na is prime to p. Suppose also that* $n \geq 2$. *After extension of scalars to* $\mathbb{A}^1/\mathbb{F}_{q^n}$, *the local systems* $\mathcal{G}_{1,\text{even}}(\psi,n,q)$ *and* $\mathcal{G}_{1,\text{odd}}(\psi,n,q)$ *are correctly matched in the sense that* $\mathcal{W}_1(\psi,n,q)$ *is a total Weil representation, and their respective geometric (and arithmetic) monodromy groups are* $\mathrm{Sp}(n,q)$, $\mathrm{PSp}(n,q)$, $\mathrm{Sp}(n,q)$.

Proof. Repeat the proof of Theorem 4.8 (with the point $(1,-2)$ replaced by the point $t=-2$). □

Corollary 6.8. *Hypotheses as in Theorem 6.7, each of the local systems* $\mathcal{G}_{1,\text{even}}(\psi,n,q)$, $\mathcal{G}_{1,\text{odd}}(\psi,n,q)$, *and* $\mathcal{W}_1(\psi,n,q)$ *has* $G_{geom} = G_{arith}$ *after extension of scalars to* $\mathbb{A}^1/\mathbb{F}_q$.

Proof. The argument of Lemma 4.7 gives this equality after extension of scalars to $A^1/\mathbb{F}_{p^B}$, and Theorem 6.7 shows that $q = p^B$. □

Remark 6.9. It is plausible that Theorems 1.1 and 1.2 in fact remain valid for $n \geq 2$ and $q = p^a$ **without** the hypotheses that that both n and a be prime to p. Using the character tables in Magma, and the calculation of the traces over a few small finite fields of our local systems $\mathcal{G}_{1,\text{odd}}(\psi,n,q)$ and $\mathcal{G}_{\text{odd}}(\psi,n,q)$, we have checked that part (ii) of each of the Theorems 1.1 and 1.2 remains valid in each of the three special cases $(p=n=3, a=1)$, $(p=n=3, a=2)$, and $(p=n=5, a=1)$. But even to do the cases $(p=n, a=1)$ or $(p=n, a=2)$ for higher p, much less the general case, would seem to require new ideas.

References

[Ax] Ax, J., Zeroes of polynomials over finite fields, *Amer. J. Math.* **86** (1964), 255–261.

[CCNPW-Atlas] Conway, J., Curtis, R., Norton, S., Parker, R., Wilson, R., *Atlas of Finite Groups*, Oxford University Press, Oxford, 1985.

[D-H] Davenport, H., and Hasse, H., Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen, *J. Reine Angew. Math.* **172** (1934), 151–182.

[F2] Feit, W., On large Zsigmondy primes, *Proc. Amer. Math. Soc.* **102** (1988), 28–36.

[Geck] Geck, M., Irreducible Brauer characters of the 3-dimensional special unitary groups in non-describing characteristic, *Comm. Algebra* **18** (1990), 563–584.

[GKT] Guralnick, R. M., Katz, N., Tiep, P. H., Rigid local systems and alternating groups, preprint.

[GMT] Guralnick, R. M., Magaard, K., Tiep, P. H., Symmetric and alternating powers of Weil representations of finite symplectic groups, *Bull. Inst. Math. Acad. Sinica* (to appear).

[GPPS] Guralnick, R. M., Penttila, T., Praeger, C., Saxl, J., Linear groups with orders having certain large prime divisors, *Proc. London Math. Soc.* **78** (1999), 167–214.

[GT] Guranick, R. M., Tiep, P. H., Symmetric powers and a conjecture of Kollár and Larsen, *Invent. Math.* **174** (2008), 505–554.

[Is] Isaacs, I. M., *Character Theory of Finite Groups*, AMS-Chelsea, Providence, 2006.

[JLPW] Jansen, C., Lux, K., Parker, R. A., Wilson, R. A., *An ATLAS of Brauer Characters*, Oxford University Press, Oxford, 1995.

[Ka-MG] Katz, N., On the monodromy groups attached to certain familiies of exponential sums, *Duke Math. J.* **34** (1987), 41–56.

[KL] Kleidman, P. B., Liebeck, M. W., *The Subgroup Structure of the Finite Classical Groups*, London Math. Soc. Lecture Note Ser. **129**, Cambridge University Press, 1990.

[Ka-MMP] Katz, N., *Moments, Monodromy, and Perversity: a Diophantine Perspective*, Annals of Mathematics Studies, **159**, Princeton University Press, Princeton, NJ, 2005, viii+475 pp.

[Ka-NG2] Katz, N., Notes on G2, determinants, and equidistribution, *Finite Fields Appl.* **10** (2004), 221–269.

[KT-gpconj] Katz, N., with an appendix by Tiep, P.H., Rigid local systems on $\mathbb{A}^1$ with finite monodromy, available at `math.princeton.edu/~nmk/gpconj106.pdf`.

[Lu] Lübeck, F., Character degrees and their multiplicities for some groups of Lie type of rank < 9, `http://www.math.rwth-aachen.de/~Frank.Luebeck/chev/DegMult/index.html`.

[T] Tiep, P. H., Low dimensional representations of finite quasisimple groups, Proceedings of the London Math. Soc. Symposium "Groups, Geometries, and Combinatorics", Durham, July 2001, A. A. Ivanov et al eds., World Scientific, 2003, N. J. 277–294.

[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.

[Tr] Trefethen, S., *Non-abelian Composition Factors of m-rational Groups*, Ph. D. Thesis, University of Arizona, 2016.

[vdG-vdV] van der Geer, G., van der Vlugt, M., Reed-Muller codes and supersingular curves. I, *Compos. Math.* **84** (1992), 333–367.

[Weil] Weil, A., *Courbes Algébriques et Variétés Abeliennes*, Hermann, Paris, 1971, reprinting of volumes 1041 and 1064 of the series Actualités scientifiques et industrielles, 1948.

[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