Tunisian Journal of Mathematics
an international publication organized by the Tunisian Mathematical Society

# Rigid local systems and alternating groups

Robert M. Guralnick, Nicholas M. Katz and Pham Huu Tiep

2019 vol. 1 no. 3

msp

TUNISIAN JOURNAL OF MATHEMATICS
Vol. 1, No. 3, 2019
dx.doi.org/10.2140/tunis.2019.1.295

# Rigid local systems and alternating groups

Robert M. Guralnick, Nicholas M. Katz and Pham Huu Tiep

We show that some very simple to write one parameter families of exponential sums on the affine line in characteristic $p$ have alternating groups as their geometric monodromy groups.



## 1. Introduction

In earlier work Katz [2018] exhibited some very simple one parameter families of exponential sums which gave rigid local systems on the affine line in characteristic $p$ whose geometric (and usually, arithmetic) monodromy groups were $\mathrm{SL}_2(q)$, and he exhibited other such very simple families giving $\mathrm{SU}_3(q)$. (Here $q$ is a power of the characteristic $p$, and $p$ is odd.) In this paper, we exhibit equally simple families whose geometric monodromy groups are the alternating groups $\mathrm{Alt}(2q)$. We also determine their arithmetic monodromy groups. See Theorem 3.1 (Of course from the resolution [Raynaud 1994] of the Abhyankar conjecture, any finite simple group whose order is divisible by $p$ will occur as the geometric monodromy group of some local system on $\mathbb{A}^1/\overline{\mathbb{F}}_p$; the interest here is that it occurs in our particularly simple local systems.)

Guralnick was partially supported by NSF grant DMS-1600056 and Tiep was partially supported by NSF grant DMS-1840702. Guralnick would also like to thank the Institute for Advanced Study, Princeton for its support.
The authors are grateful to the referees for careful reading and helpful comments on the paper.
*MSC2010:* 11T23, 20D05.
*Keywords:* rigid local system, monodromy, alternating group.

In the earlier work of Katz, he used a theorem to Kubert to know that the monodromy groups in question were finite, then work of Gross [2010] to determine which finite groups they were. Here we do not have, at present, any direct way of showing this finiteness. Rather, the situation is more complicated and more interesting. Using some basic information about these local systems (see Theorem 6.1), the first and third authors prove a fundamental dichotomy: the geometric monodromy group is either $\mathrm{Alt}(2q)$ or it is the special orthogonal group $\mathrm{SO}(2q-1)$. The second author uses an elementary polynomial identity to compute the third moment as being 1 (see Theorem 7.1), which rules out the $\mathrm{SO}(2q-1)$ case. This roundabout method establishes the theorem. It would be interesting to find a "direct" proof that these local systems have integer (rather than rational) traces; this integrality is in fact equivalent to their monodromy groups being finite, see [Katz 1990, 8.14.6]. But even if one had such a direct proof, it would still require serious group theory to show that their geometric monodromy groups are the alternating groups.

## 2. The local systems in general

Throughout this paper, $p$ is an odd prime, $q$ is a power of $p$, $k$ is a finite field of characteristic $p$, $\ell$ is a prime $\neq p$,

$$\psi = \psi_k : (k, +) \to \mu_p \subset \overline{\mathbb{Q}}_\ell^\times$$

is a nontrivial additive character of $k$, and

$$\chi_2 = \chi_{2,k} : k^\times \to \pm 1 \subset \overline{\mathbb{Q}}_\ell^\times$$

is the quadratic character, extended to $k$ by $\chi_2(0) := 0$. For $L/k$ a finite extension, we have the nontrivial additive character

$$\psi_{L/k} := \psi_k \circ \mathrm{Trace}_{L/k}$$

of $L$, and the quadratic character $\chi_{2,L} = \chi_{2,k} \circ \mathrm{Norm}_{L/k}$ of $L^\times$, extended to $L$ by $\chi_{2,L}(0) = 0$.

On the affine line $\mathbb{A}^1/k$, we have the Artin–Schreier sheaf $\mathcal{L}_{\psi(x)}$. On $\mathbb{G}_m/k$ we have the Kummer sheaf $\mathcal{L}_{\chi_2(x)}$ and its extension by zero $j_!\mathcal{L}_{\chi_2(x)}$ (for $j : \mathbb{G}_m \subset \mathbb{A}^1$ the inclusion) on $\mathbb{A}^1/k$.

For an odd integer $n = 2d + 1$ which is prime to $p$, we have the rigid local system (rigid by [Katz 1996, 3.0.2 and 3.2.4])

$$\mathcal{F}(k, n, \psi) := FT_\psi(\mathcal{L}_{\psi(x^n)} \otimes j_!\mathcal{L}_{\chi_2(x)})$$

on $\mathbb{A}^1/k$. Let us recall the basic facts about it, see [Katz 2004, 1.3 and 1.4].

It is lisse of rank $n$, pure of weight one, and orthogonally self-dual, with its geometric monodromy group

$$G_{\text{geom}} \subset \mathrm{SO}(n, \overline{\mathbb{Q}}_\ell).$$

Recall that $G_{\text{geom}}$ is the Zariski closure in $\mathrm{SO}(n, \overline{\mathbb{Q}}_\ell)$ of the image of the geometric fundamental group $\pi_1(\mathbb{A}^1/\bar{k})$ in the representation which "is" the local system $\mathcal{F}(k, n, \psi)$. For ease of later reference, we recall the following fundamental fact.

**Lemma 2.1.** *For any lisse local system $\mathcal{H}$ on $\mathbb{A}^1/\bar{k}$, the subgroup $\Gamma_p$ of its $G_{\text{geom}}$ generated by elements of $p$-power order is Zariski dense.*

*Proof.* Denote by $N$ the Zariski closure of $\Gamma_p$ in $G_{\text{geom}}$. Then $N$ is a normal subgroup of $G_{\text{geom}}$. We must show that the quotient $M := G_{\text{geom}}/N$ is trivial.

To see this, we argue as follows. The local system $\mathcal{H}$ gives us a group homomorphism

$$\pi_1(\mathbb{A}^1/\bar{k}) \to G_{\text{geom}} \subset \mathrm{GL}(\mathrm{rank}(\mathcal{H}), \overline{\mathbb{Q}}_\ell)$$

with Zariski dense image. Under this homomorphism, the wild inertia group $P_\infty$ has finite image in $G_{\text{geom}}$ (because $\ell \neq p$). This image being a finite $p$ group in $G_{\text{geom}}$, it lies in $N$, and hence dies in $M := G_{\text{geom}}/N$. Therefore $M/M^0$ is a finite quotient of $\pi_1(\mathbb{A}^1/\bar{k})$ in which $P_\infty$ dies. So any irreducible representation of $M/M^0$ gives an irreducible local system on $\mathbb{A}^1/\bar{k}$ which is tame at $\infty$, hence trivial. Thus $M = M^0$ is connected. We next show that $M^{\text{red}} := M/\mathcal{R}_u$, the quotient of $M$ by its unipotent radical, is trivial. For this, it suffices to show that $M$ has no nontrivial irreducible representations. But any such representation is a local system on $\mathbb{A}^1/\bar{k}$ which is tamely ramified at $\infty$ (again because $P_\infty$ dies in $M$), so is trivial. Thus $M$ is unipotent. But $H^1(\mathbb{A}^1/\bar{k}, \overline{\mathbb{Q}}_\ell)$ vanishes, so any unipotent local system on $\mathbb{A}^1/\bar{k}$ is trivial, and hence $M$ is trivial. □

Let us denote by $A(k, n, \psi)$ the Gauss sum

$$A(k, n, \psi) := -\chi_2(n(-1)^d) \sum_{x \in k^\times} \psi(x)\chi_2(x).$$

By the Hasse–Davenport relation, for $L/k$ an extension of degree $d$, we have

$$A(L, n, \psi_{L/k}) = (A(k, n, \psi))^d.$$

The twisted local system

$$\mathcal{G}(k, n, \psi) := \mathcal{F}(k, n, \psi) \otimes A(n, k, \psi)^{-\deg}$$

is pure of weight zero and has

$$G_{\text{geom}} \subset G_{\text{arith}} \subset \mathrm{SO}(n, \overline{\mathbb{Q}}_\ell).$$

Concretely, for $L/k$ a finite extension, and $t \in L$, the trace at time $t$ of $\mathcal{G}(k, n, \psi)$ is

$$\begin{aligned}\mathrm{Trace}(\mathrm{Frob}_{t,L} \mid \mathcal{G}(k, n, \psi)) &= -(1/A(L, n, \psi_{L/k})) \sum_{x \in L^\times} \psi_{L/k}(x^n + tx)\chi_{2,L}(x) \\ &= -(1/A(L, n, \psi_{L/k})) \sum_{x \in L} \psi_{L/k}(x^n + tx)\chi_{2,L}(x),\end{aligned}$$

the last equality because the $\chi_2$ factor kills the $x = 0$ term.

Let us recall also [Katz 2004, 3.4] that the geometric monodromy group of $\mathcal{F}(k, n, \psi)$, or equivalently of $\mathcal{G}(k, n, \psi)$, is independent of the choice of the pair $(k, \psi)$.

To end this section, let us recall the relation of the local system $\mathcal{F}(k, n, \psi)$ to the hypergeometric sheaf

$$\mathcal{H}_n := \mathcal{H}(!, \psi; \text{all characters of order dividing } n; \chi_2).$$

According to [Katz 1990, 9.2.2], $\mathcal{F}(k, n, \psi)|\mathbb{G}_m$ is geometrically isomorphic to a multiplicative translate of the Kummer pullback $[n]^\star\mathcal{H}_n$. (An explicit descent of $\mathcal{F}(k, n, \psi)|\mathbb{G}_m$ through the $n$-th power map is given by the lisse sheaf on $\mathbb{G}_m$ whose trace function at time $t \in L^\times$, for $L/k$ a finite extension, is

$$t \mapsto -\sum_{x \in L^\times} \psi_{L/k}(x^n/t + x)\chi_{2,L}(x/t).$$

The structure theory of hypergeometric sheaves shows that this descent is, geometrically, a multiplicative translate of the asserted $\mathcal{H}_n$.)

## 3. The candidate local systems for Alt$(2q)$

In this section, we specialize the $n$ of the previous section to

$$n = 2q - 1 = 2(q - 1) + 1.$$

The target theorem is this:

**Theorem 3.1.** *Let $p$ be an odd prime, $q$ a power of $p$, $k$ a finite field of characteristic $p$, $\ell$ a prime $\neq p$, and $\psi$ a nontrivial additive character of $k$. For the $\ell$-adic local system $\mathcal{G}(k, 2q - 1, \psi)$ on $\mathbb{A}^1/k$, its geometric and arithmetic monodromy groups are given as follows*:

(1) $G_{\mathrm{geom}} = \mathrm{Alt}(2q)$ *in its unique irreducible representation of dimension* $2q - 1$.

(2) (a) *If $-1$ is a square in $k$, then* $G_{\mathrm{geom}} = G_{\mathrm{arith}} = \mathrm{Alt}(2q)$.

(b) *If $-1$ is not a square in $k$, then* $G_{\mathrm{arith}} = \mathrm{Sym}(2q)$, *the symmetric group, in its irreducible representation labeled by the partition* $(2, 1^{2q-2})$, *i.e.*,

$$(\text{the deleted permutation representation of } \mathrm{Sym}(2q)) \otimes \mathrm{sgn}\,.$$

**Remark 3.2.** The traces of elements of Alt($n$) (respectively of Sym($n$)) in its deleted permutation representation (respectively in every irreducible representation) are integers. One sees easily (look at the action of $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$) that the local system $\mathcal{G}(k, 2q-1, \psi)$ has traces which all lie in $\mathbb{Q}$, but as mentioned in the introduction, we do not know a direct proof that these traces all lie in $\mathbb{Z}$.

## 4. Basic facts about $\mathcal{H}_n$

In this section, we assume that $n \geq 3$ is odd and that $n(n-1)$ is prime to $p$. The geometric local monodromy at 0 is tame, and a topological generator of the tame inertia group $I(0)^{\mathrm{tame}}$, acting on $\mathcal{H}_n$, has as eigenvalues all the roots of unity of order dividing $n$.

The geometric local monodromy at $\infty$ is the direct sum

$$\mathcal{L}_{\chi_2} \oplus W, \quad W \text{ has rank } n-1, \text{ and all slopes } 1/(n-1).$$

Because $n$ is odd, the local system $\mathcal{H}_n$ is (geometrically) orthogonally self-dual, and $\det(\mathcal{H}_n)$ is geometrically trivial (because trivial at 0, lisse on $\mathbb{G}_m$, and all $\infty$ slopes are $\leq 1/(n-1) < 1$). Therefore $\det(W)$ is geometrically $\mathcal{L}_{\chi_2}$. From [Katz 1990, 8.6.4 and 8.7.2], we see that up to multiplicative translation, the geometric isomorphism class is determined entirely by its rank $n-1$ and its determinant $\mathcal{L}_{\chi_2}$. Because $n-1$ is even and prime to $p$, it follows that up to multiplicative translation, the geometric isomorphism class of $W$ is that of the $I(\infty)$-representation of the Kloosterman sheaf

$$\mathrm{Kl}_{n-1} := \mathrm{Kl}(\psi; \text{all characters of order dividing } n-1).$$

By [Katz 1988, 5.6.1], we have a global Kummer direct image geometric isomorphism

$$\mathrm{Kl}_{n-1} \cong [n-1]_\star \mathcal{L}_{\psi_{n-1}},$$

where we write $\psi_{n-1}$ for the additive character $x \mapsto \psi((n-1)x)$. Therefore, up to multiplicative translation, the geometric isomorphism class of $W$ is that of $[n-1]_\star \mathcal{L}_\psi$. Pulling back by $[n-1]$, which does not change the restriction of $W$ to the wild inertia group $P(\infty)$, we get

$$[n-1]^\star W \cong \bigoplus_{\zeta \in \mu_{n-1}} \mathcal{L}_{\psi(\zeta x)}.$$

A further pullback by $n$-th power, which also does not change the restriction of $W$ to $P(\infty)$, gives

$$[n-1]^\star [n]^\star W \cong \bigoplus_{\zeta \in \mu_{n-1}} \mathcal{L}_{\psi(\zeta x^n)}.$$

Thus we find that the $I(\infty)$ representation attached to a multiplicative translate[1] of $[n-1]^\star\mathcal{F}(k,n,\psi)$ is the direct sum

$$\mathbb{1}\bigoplus_{\zeta\in\mu_{n-1}}\mathcal{L}_{\psi(\zeta x^n)}=\bigoplus_{\alpha\in\mu_{n-1}\cup\{0\}}\mathcal{L}_{\psi(\alpha x^n)}.$$

This description shows that the image of $P(\infty)$ in the $I(\infty)$-representation attached to $\mathcal{F}(k,n,\psi)$ is an abelian group killed by $p$.

**Lemma 4.1.** *Let $L/\mathbb{F}_p$ be a finite extension which contains the $(n-1)$-st roots of unity. Denote by $V\subset L$ the additive subgroup of $L$ spanned by the $(n-1)$-st roots of unity. Denote by $V^\star$ the Pontryagin dual of $V$:*

$$V^\star:=\mathrm{Hom}_{\mathbb{F}_p}(V,\mu_p(\overline{\mathbb{Q}}_\ell)).$$

*Then the image of $P(\infty)$ in the $I(\infty)$-representation attached to $\mathcal{F}(k,n,\psi)$ is $V^\star$, and the representation restricted to $V^\star$ is the direct sum*

$$\mathbb{1}\bigoplus_{\zeta\in\mu_{n-1}(L)}(\textit{evaluation at }\zeta)=\bigoplus_{\alpha\in\mu_{n-1}(L)\cup\{0\}}(\textit{evaluation at }\alpha).$$

*Proof.* Each of the characters $\mathcal{L}_{\psi(\alpha x^n)}$ of $I(\infty)$ has order dividing $p$. Given an $n$-tuple of elements $(a_\alpha)_{\alpha\in\mu_{n-1}(L)\cup\{0\}}$, consider the character

$$\Lambda:=\bigotimes_{\alpha\in\mu_{n-1}(L)\cup\{0\}}(\mathcal{L}_{\psi(\alpha x^n)})^{\otimes a_\alpha}=\mathcal{L}_{\psi((\sum_{\alpha\in\mu_{n-1}(L)\cup\{0\}}a_\alpha\alpha)x^n)}.$$

The following conditions are equivalent:

(a) $\sum_{\alpha\in\mu_{n-1}(L)\cup\{0\}}a_\alpha\alpha=0$.

(b) The character $\Lambda$ is trivial on $I(\infty)$.

(c) The character $\Lambda$ is trivial on $P(\infty)$.

Indeed, it is obvious that (a) $\Longrightarrow$ (b) $\Longrightarrow$ (c). If (c) holds, then for

$$A:=\sum_{\alpha\in\mu_{n-1}(L)\cup\{0\}}a_\alpha\alpha,$$

we have that $\mathcal{L}_{\psi(Ax)}$ is trivial on $P(\infty)$, so is a character of $I(\infty)/P(\infty)=I(\infty)^{\mathrm{tame}}$, a group of order prime to $p$. But $\mathcal{L}_{\psi(Ax)}$ has order dividing $p$, so is trivial on $I(\infty)$, hence $A=0$.

This equivalence shows that the character group of the image of $P(\infty)$ is indeed the $\mathbb{F}_p$ span of the $\alpha$'s, i.e., it is $V$. The rest is just Pontryagin duality of finite abelian groups. □

[1]The referee has kindly explained to us that the results of [Fu 2010, Proposition 0.7, 0.8] allow one to make precise the multiplicative translates in the above paragraphs.

## 5. Basic facts about $\mathcal{H}_{2q-1}$

Taking $n = 2q - 1$, the geometric local monodromy at 0 of $\mathcal{H}_{2q-1}$ is tame, and a topological generator of the tame inertia group $I(0)^{\text{tame}}$, acting on $\mathcal{H}_n$, has as eigenvalues all the roots of unity of order dividing $2q - 1$.

Turning now to the action of $P(\infty)$, we have:

**Lemma 5.1.** *Denote by $\zeta_{2q-2} \in \mathbb{F}_{q^2}$ a primitive $(2q-2)$-th root of unity. In the $I(\infty)$-representation attached to $\mathcal{F}(k, 2q-1, \psi)$, the character group $V$ of the image of $P(\infty)$ is the $\mathbb{F}_p$-space*

$$V = \mathbb{F}_q \oplus \zeta_{2q-2}\mathbb{F}_q.$$

*Fix a nontrivial additive character $\psi_0$ of $\mathbb{F}_q$, and denote by $\psi_1$ the nontrivial additive character of $\mathbb{F}_{q^2}$ given by*

$$\psi_1 := \psi_0 \circ \mathrm{Trace}_{\mathbb{F}_{q^2}/\mathbb{F}_q}.$$

*Then the image $V^\star$ of $P(\infty)$ is itself isomorphic to $V$, and the representation of $P(\infty)$ is the direct sum of the characters*

$$\bigoplus_{\alpha \in \mathbb{F}_q} \psi_1(\alpha x) \oplus \bigoplus_{\beta \in \mathbb{F}_q^\times} \psi_1(\zeta_{2q-2}\beta x).$$

*Proof.* When $n = 2q-1$, then $n-1 = 2(q-1)$. The field $\mathbb{F}_{q^2}$ contains the $2(q-1)$-th roots of unity. The group $\mu_{2(q-1)}(\mathbb{F}_{q^2})$ contains the subgroup $\mu_{q-1}(\mathbb{F}_{q^2}) = \mathbb{F}_q^\times$ with index 2, the other coset being $\zeta_{2(q-1)}\mathbb{F}_q^\times$. Thus the $\mathbb{F}_p$ span of $\mu_{2(q-1)}(\mathbb{F}_{q^2})$ inside the additive group of $\mathbb{F}_{q^2}$ is indeed the asserted $V$. The characters $\psi_1(\alpha x)$, as $\alpha$ varies over $\mathbb{F}_q$, are each trivial on $\zeta_{2q-2}\mathbb{F}_q$ (because $\mathrm{Trace}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\zeta_{2q-2}) = 0$) and give all the additive characters of $\mathbb{F}_q$ (on which $\mathrm{Trace}_{\mathbb{F}_{q^2}/\mathbb{F}_q}$ is simply the map $x \mapsto 2x$). The characters $\psi_1(\zeta_{2q-2}\beta x)$, as $\beta$ varies over $\mathbb{F}_q$, are trivial on $\mathbb{F}_q$ (because $\mathrm{Trace}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\zeta_{2q-2}) = 0$) and give all the characters of $\zeta_{2q-2}\mathbb{F}_q$ (because $\zeta_{2(q-1)}^2$ lies in $\mathbb{F}_q^\times$). □

**Corollary 5.2.** *The image of $P(\infty)$ in the $I(\infty)$-representation attached to*

$$\mathcal{F}(k, 2q-1, \psi) \oplus \mathbb{1}$$

*is the direct sum*

$$V = \mathbb{F}_q \oplus \zeta_{2q-2}\mathbb{F}_q$$

*acting through the representation*

$$\mathrm{Reg}_{\mathbb{F}_q} \oplus \mathrm{Reg}_{\zeta_{2q-2}\mathbb{F}_q}.$$

## 6. Basic facts about the group $G_{\mathrm{geom}}$ for $\mathcal{F}(k, 2q-1, \psi)$

Recall that $G_{\mathrm{geom}}$ is the Zariski closure in $\mathrm{SO}(2q-1, \overline{\mathbb{Q}}_\ell)$ of the image of $\pi_1^{\mathrm{geom}} := \pi_1(\mathbb{A}^1/\overline{\mathbb{F}}_p)$ in the representation attached to $\mathcal{F}(k, 2q-1, \psi)$. Thus $G_{\mathrm{geom}}$ is an irreducible subgroup of $\mathrm{SO}(2q-1, \overline{\mathbb{Q}}_\ell)$.

**Theorem 6.1.** *We have the following two results*:

(i) $G_{\mathrm{geom}}$ *is normalized by an element of* $\mathrm{SO}(2q-1, \overline{\mathbb{Q}}_\ell)$ *whose eigenvalues are all the roots of unity of order dividing* $2q-1$ *in* $\overline{\mathbb{Q}}_\ell$.

(ii) $G_{\mathrm{geom}}$ *contains a subgroup isomorphic to* $\mathbb{F}_q \oplus \mathbb{F}_q$, *acting through the virtual representation*

$$\mathrm{Reg}_{\mathrm{first}} \oplus \mathrm{Reg}_{\mathrm{second}} - \mathbb{1}.$$

*Proof.* The local system $\mathcal{F}(k, 2q-1, \psi)$ is, geometrically, a multiplicative translate of the Kummer pullback $[2q-1]^\star \mathcal{H}_{2q-1}$. Therefore $G_{\mathrm{geom}}$ is a normal subgroup of the group $G_{\mathrm{geom}}$ for $\mathcal{H}_{2q-1}$, so is normalized by any element of this possibly larger group. As already noted, local monodromy at 0 for $\mathcal{H}_{2q-1}$ is an element of the asserted type. This proves (i). Statement (ii) is just a repeating of what was proved in the previous lemma. □

## 7. The third moment of $\mathcal{F}(k, 2q-1, \psi)$ and of $\mathcal{G}(k, 2q-1, \psi)$

Let us recall the general set up. We are given a lisse $\mathcal{G}$ on a lisse, geometrically connected curve $C/k$. We suppose that $\mathcal{G}$ is $\iota$-pure of weight zero, for an embedding $\iota$ of $\overline{\mathbb{Q}}_\ell$ into $\mathbb{C}$. We denote by $V$ the $\overline{\mathbb{Q}}_\ell$-representation given by $\mathcal{G}$, and by $G_{\mathrm{geom}}$ the Zariski closure in $\mathrm{GL}(V)$ of the image of $\pi_1^{\mathrm{geom}}(C/k)$. For an integer $n \geq 1$, the $n$-th moment of $\mathcal{G}$ is the dimension of the space of invariants

$$M_n(\mathcal{G}) := \dim((V^{\otimes n})^{G_{\mathrm{geom}}}).$$

Recall [Katz 2005, 1.17.4] that we have an archimedean limit formula for $M_n(\mathcal{G})$ as the lim sup over finite extensions $L/k$ of the sums

$$(1/\#L) \sum_{t \in C(L)} (\mathrm{Trace}(\mathrm{Frob}_{t,L} \,|\mathcal{G}))^n,$$

which we call the empirical moments.

**Theorem 7.1.** *For the lisse sheaf* $\mathcal{G}(k, 2q-1, \psi)$ *on* $\mathbb{A}^1/k$, *we have*

$$M_3(\mathcal{G}(k, 2q-1, \psi)) = 1.$$

*Proof.* Fix a finite extension $L/k$. For $t \in L$, we have

$$\mathrm{Trace}(\mathrm{Frob}_{t,L} \,|\mathcal{G}(k, 2q-1, \psi)) \\ = (-1/A(L, 2q-1, \psi_{L/k})) \sum_{x\in L} \psi_{L/k}(x^{2q-1} + tx)\chi_{2,L}(x),$$

with the twisting factor given explicitly as

$$A(L, 2q-1, \psi_{L/k}) = -\chi_{2,L}(-1) \sum_{x\in L^\times} \psi_{L/k}(x)\chi_{2,L}(x).$$

Write $g_L$ for the Gauss sum

$$g_L := \sum_{x\in L^\times} \psi_{L/k}(x)\chi_{2,L}(x).$$

Then the empirical $M_3$ is the sum

$$(1/\#L)(\chi_{2,L}(-1)/g_L)^3 \sum_{t\in L} \sum_{x,y,z\in L} \psi_{L/k}\big(x^{2q-1} + y^{2q-1} + z^{2q-1} + t(x + y + z)\big) \cdot \chi_{2,L}(xyz)$$

$$= (\chi_{2,L}(-1)/g_L)^3 \sum_{x,y,z\in L, x+y+z=0} \psi_{L/k}\big(x^{2q-1} + y^{2q-1} + z^{2q-1}\big)\chi_{2,L}(xyz)$$

$$= (\chi_{2,L}(-1)/g_L)^3 \sum_{x,y\in L} \psi_{L/k}\big(x^{2q-1} + y^{2q-1} + (-x-y)^{2q-1}\big)\chi_{2,L}(xy(-x-y)).$$

The key is now the following identity.

**Lemma 7.2.** *In $\mathbb{F}_q[x, y]$, we have the identity*

$$x^{2q-1} + y^{2q-1} + (-x-y)^{2q-1} = xy(x+y) \prod_{\alpha\in\mathbb{F}_q\setminus\{0,-1\}} (x - \alpha y)^2.$$

*If we write $q = p^f$, then collecting Galois-conjugate terms this is*

$$xy(x+y) \prod_{h\in\mathcal{P}_f} h(x, y)^2,$$

*where $\mathcal{P}_f$ is the set of irreducible $h(x, y) \in \mathbb{F}_p[x, y]$ which are homogeneous of degree dividing $f$, monic in $x$, other than $x$ or $x + y$.*

*Proof.* Because $x^{2q-1} + y^{2q-1} + (-x-y)^{2q-1}$ is homogeneous of odd degree $2q-1$ and visibly divisible by $y$, it suffices to prove the inhomogeneous identity, that in $\mathbb{F}_q[x]$ we have

$$x^{2q-1} + 1 - (x+1)^{2q-1} = x(x+1) \prod_{\alpha\in\mathbb{F}_q\setminus\{0,-1\}} (x - \alpha)^2.$$

The left side

$$P(x) := x^{2q-1} + 1 - (x+1)^{2q-1}$$

has degree $2q-2$, and visibly vanishes at $x=0$ and at $x=-1$.

So it suffices to show that for each $\alpha \in \mathbb{F}_q \setminus \{0, -1\}$, $P(x)$ is divisible by $(x-\alpha)^2$. The key point is that for $\beta \in \mathbb{F}_q$, we have

$$\beta^{2q-1} = \beta,$$

and for $\alpha \in \mathbb{F}_q^\times$ we have

$$\alpha^{2q-2} = 1.$$

Thus for any $\beta \in \mathbb{F}_q$, we trivially have $P(\beta) = 0$. The derivative $P'(x)$ is equal to

$$P'(x) = -x^{2q-2} + (x+1)^{2q-2}.$$

So if both $\alpha$ and $\alpha+1$ lie in $\mathbb{F}_q^\times$, then $P'(\alpha) = -1+1 = 0$. □

With this identity in hand, we now return to the calculation of the empirical moment, which is now

$$(\chi_{2,L}(-1)/g_L)^3 \sum_{x,y \in L} \psi_{L/k}(xy(x+y) \prod_{h \in \mathcal{P}_f} h(x,y)^2) \chi_{2,L}(xy(-x-y)).$$

The set of $(x,y) \in \mathbb{A}^2(L)$ with $xy \neq 0$ and at which $\prod_{h \in \mathcal{P}_f} h(x,y) = 0$ has cardinality $(q-2)(\#L-1)$. So the empirical sum differs from the modified empirical sum

$$(\chi_{2,L}(-1)/g_L)^3 \sum_{x,y \in L} \psi_{L/k}(xy(x+y) \prod_{h \in \mathcal{P}_f} h(x,y)^2) \chi_{2,L}(xy(-x-y) \prod_{h \in \mathcal{P}_f} h(x,y)^2)$$

by a difference which is

$$(\chi_{2,L}(-1)/g_L)^3 \quad \big(\text{a sum of at most } (q-2)(\#L-1) \text{ terms, each of absolute value } 1\big).$$

So the difference in absolute value is at most $q/\sqrt{\#L}$, which tends to zero as $L$ grows (remember $q$ is fixed). The modified empirical sum we now rewrite as

$$(\chi_{2,L}(-1)/g_L)^3 \sum_{t \in L^\times} \psi_{L/k}(t) \chi_{2,L}(-t) N_L(t),$$

with $N_L(t)$ the number of $L$-points on the curve $\mathcal{C}_t$ given by

$$\mathcal{C}_t : xy(x+y) \prod_{h \in \mathcal{P}_f} h(x,y)^2 = t.$$

Because $xy(x+y) \prod_{h \in \mathcal{P}_f} h(x,y)^2$ is homogeneous of degree $2q-1$ prime to $p$ and is not a $d$-th power for any $d \geq 2$, the curves $\mathcal{C}_t$ are smooth and geometrically irreducible for all $t \neq 0$, see [Katz 1989, proof of 6.5]. Moreover, by the homogeneity, these curves are each geometrically isomorphic to $\mathcal{C}_1$, indeed the family become constant after the tame Kummer pullback $[2q-1]^\star$. Thus for the structural map $\pi : \mathcal{C} \to \mathbb{G}_m/\mathbb{F}_p$, $R^2\pi_!(\mathbb{Q}_\ell) = \mathbb{Q}_\ell(-1)$, $R^1\pi_!\mathbb{Q}_\ell$ is lisse of some rank $r$, tame at both 0 and $\infty$, and mixed of weight $\leq 1$, and all other $R^i\pi_!(\mathbb{Q}_\ell) = 0$.

So our modified empirical moment is

$$(\chi_{2,L}(-1)/g_L)^3 \sum_{t \in L^\times} \psi_{L/k}(t)\chi_{2,L}(-t)(\#L - \mathrm{Trace}(\mathrm{Frob}_{t,L} \mid R^1\pi_!\mathbb{Q}_\ell)$$
$$= (\chi_{2,L}(-1)/g_L)^3 \sum_{t \in L^\times} \psi_{L/k}(t)\chi_{2,L}(-t)(\#L)$$
$$- (\chi_{2,L}(-1)/g_L)^3 \sum_{t \in L^\times} \mathrm{Trace}\big(\mathrm{Frob}_{t,L} \mid \mathcal{L}_{\psi(t)} \otimes \mathcal{L}_{\chi_2(t)} \otimes R^1\pi_!\mathbb{Q}_\ell\big).$$

Remembering that $g_L^2 = \chi_{2,L}(-1)\#L$, we see that the first sum is $\chi_{2,L}(-1)$. We now show that the second sum is $O(1/\sqrt{\#L})$, or equivalently that the sum

$$\sum_{t \in L^\times} \mathrm{Trace}\big(\mathrm{Frob}_{t,L} \mid \mathcal{L}_\psi \otimes \mathcal{L}_{\chi_2} \otimes R^1\pi_!\mathbb{Q}_\ell\big)$$

is $O(\#L)$. By the Lefschetz trace formula [Grothendieck 1968], the second sum is

$$\mathrm{Trace}\big(\mathrm{Frob}_L \mid H_c^2(\mathbb{G}_m/\overline{\mathbb{F}_p}, \mathcal{L}_\psi \otimes \mathcal{L}_{\chi_2} \otimes R^1\pi_!\mathbb{Q}_\ell)\big)$$
$$- \mathrm{Trace}\big(\mathrm{Frob}_L \mid H_c^1(\mathbb{G}_m/\overline{\mathbb{F}_p}, \mathcal{L}_\psi \otimes \mathcal{L}_{\chi_2} \otimes R^1\pi_!\mathbb{Q}_\ell)\big).$$

The $H_c^2$ group vanishes, because the coefficient sheaf is totally wild at $\infty$ (this because it is $\mathcal{L}_\psi$ tensored with a lisse sheaf which is tame at $\infty$). The second sum is $O(\#L)$, by Deligne's fundamental estimate [Deligne 1980, 3.3.1] (because the coefficient sheaf is mixed of weight $\leq 1$, its $H_c^1$ is mixed of weight $\leq 2$).

Thus the empirical moment is $\chi_{2,L}(-1)$ plus an error term which, as $L$ grows, is $O(1/\sqrt{\#L})$. So the lim sup is 1, as asserted. □

## 8. Exact determination of $G_{\mathrm{arith}}$

**Theorem 8.1.** *Suppose known that $\mathcal{G}(k, 2q-1, \psi)$ has $G_{\mathrm{geom}} = \mathrm{Alt}(2q)$. Then its $G_{\mathrm{arith}}$ is as asserted in Theorem 3.1, namely it is* $\mathrm{Alt}(2q)$ *if $-1$ is a square in $k$, and is* $\mathrm{Sym}(2q)$ *if $-1$ is not a square in $k$.*

*Proof.* For $q > 3$, the outer automorphism group of $\mathrm{Alt}(2q)$ has order 2, induced by the conjugation action of $\mathrm{Sym}(2q)$. Therefore the normalizer of $\mathrm{Alt}(2q)$ in $\mathrm{SO}(2q-1)$ (viewed there by its deleted permutation representation) is the group $\mathrm{Sym}(2q)$ (viewed in $\mathrm{SO}(2q-1)$ by (deleted permutation representation) $\otimes$ sgn). If $q = 3$, the automorphism group is slightly bigger but the stabilizer of the character of the deleted permutation module is just $\mathrm{Sym}(2q)$. (Indeed, either of the exotic automorphisms of Alt(6) maps the cycle (123) to an element which in Sym(6) is conjugate to (123)(456). The element (123) has trace 2, whereas (123)(456) has trace $-1$ (both viewed in SO(5) by the deleted permutation representation)). Since we have a priori inclusions

$$G_{\mathrm{geom}} = \mathrm{Alt}(2q) \lhd G_{\mathrm{arith}} \subset \mathrm{SO}(2q-1),$$

the only choices for $G_{\mathrm{arith}}$ are $\mathrm{Alt}(2q)$ or $\mathrm{Sym}(2q)$.

Denoting by $V$ the representation of $G_{\mathrm{arith}}$ given by $\mathcal{G}(k, 2q-1, \psi)$, the action of $G_{\mathrm{arith}}$ on the line

$$\mathbb{L} := (V^{\otimes 3})^{G_{\mathrm{geom}}}$$

is a character of $G_{\mathrm{arith}}/G_{\mathrm{geom}}$. We claim that this character is the sign character sgn of $G_{\mathrm{arith}} \subset \mathrm{Sym}(2q)$. To see this, we argue as follows.

For any $n \geq 3$, denoting by $V_n$ the deleted permutation representation of $\mathrm{Sym}(n+1)$, one knows that

$$(V_n^{\otimes 3})^{\mathrm{Sym}(n+1)} = (V_n^{\otimes 3})^{\mathrm{Alt}(n+1)}$$

is one dimensional. (Indeed, if $S^\lambda$ denotes the complex irreducible representation of $\mathrm{Sym}(n+1)$ labeled by the partition $\lambda$ of $n+1$, then $V_n = S^{(n,1)}$ and $\mathrm{sgn} = S^{(1^{n+1})}$. An application of the Littlewood–Richardson rule to

$$S^\lambda \otimes \mathrm{Ind}_{\mathrm{Sym}(n)}^{\mathrm{Sym}(n+1)}(S^{(n)}) = S^\lambda \oplus (S^\lambda \otimes V_n)$$

yields

$$V_n \otimes V_n = S^{(n+1)} \oplus S^{(n,1)} \oplus S^{(n-1,2)} \oplus S^{(n-1,1^2)}$$

see [Fulton and Harris 1991, Exercise 4.19]. Further similar applications of the Littlewood–Richardson rule then show that $V_n \otimes V_n \otimes V_n$ contains the trivial representation $S^{(n+1)}$ once but does not contain sgn.) Hence that the action of $\mathrm{Sym}(n+1)$ on

$$((V_n \otimes \mathrm{sgn})^{\otimes 3})^{\mathrm{Alt}(n+1)}$$

is $\mathrm{sgn}^3 = \mathrm{sgn}$. Taking $n = 2q-1$, we get the claim.

Now apply Deligne's equidistribution theorem, in the form [Katz and Sarnak 1999, 9.7.10]. It tells us that if $G_{\mathrm{arith}}/G_{\mathrm{geom}}$ has order 2 instead of 1, then the Frobenii $\mathrm{Frob}_{t,L}$ as $L$ runs over larger and larger extensions of $k$ of even (respectively odd) degree become equidistributed in the conjugacy classes of $G_{\mathrm{arith}}$ lying in $G_{\mathrm{geom}}$ (respectively lying in the other coset $G_{\mathrm{arith}} \setminus G_{\mathrm{geom}}$). If $-1$ is not a square in $k$, then $\chi_L(-1) = -1$ for all odd degree extensions $L/k$, and the empirical third moment over all odd degree extensions will be $-1 + O(1/\sqrt{\#L})$, by the proof of Theorem 7.1, whereas the empirical moment will be $1 + O(1/\sqrt{\#L})$ over even degree extensions. So if $-1$ is not a square in $k$, then $G_{\mathrm{arith}} = \mathrm{Sym}(2q)$. If $-1$ is a square in $k$, then every empirical moment will be $1 + O(1/\sqrt{\#L})$, and hence $G_{\mathrm{arith}} = \mathrm{Alt}(2q) = G_{\mathrm{geom}}$.

## 9. Identifying the group

In this section, we use the information obtained earlier to identify the group. We choose a field embedding $\overline{\mathbb{Q}}_\ell \subset \mathbb{C}$, so that we may view $G := G_{\text{geom}}$ as an algebraic group over $\mathbb{C}$.

So let $p$ be an odd prime with $q$ a power of $p$. We start by assuming that $G$ is an irreducible, Zariski closed subgroup of $\mathrm{SO}(2q-1, \mathbb{C}) = \mathrm{SO}(V)$ such that $G$ contains $Q$, an elementary abelian subgroup of order $q^2$. Moreover, we assume that we may write $Q = Q_1 \times Q_2$ with $|Q_1| = |Q_2| = q$ so that $V = V_0 \oplus V_1 \oplus V_2$, where $V_0$ is a trivial $Q$-module, $V_0 \oplus V_i$ is the regular representation for $Q_i$ and $Q_i$ acts trivially on the other summand. Moreover, we assume that $G$ is a quasi-$p$ group (in the sense that the subgroup generated by its $p$-elements is Zariski dense), see Lemma 2.1.

**Lemma 9.1.** *$V$ is tensor indecomposable for $Q_1$. More precisely, $V \neq X_1 \otimes X_2$, where the $X_i$ are $Q_1$-modules each of dimension $\geq 2$.*

*Proof.* We argue by contradiction. Suppose $V = X_1 \otimes X_2$ with each $X_i$ of (necessarily odd) dimensional $\geq 2$. Let $\chi_{X_i}$ be the character of $Q_1$ on $X_i$. So $\chi_{X_1} = a_0\mathbb{1} + \sum a_\chi \chi$ and $\chi_{X_2} = b_0\mathbb{1} + \sum b_\chi \chi$, where the $\chi$ are the nontrivial characters of $Q_1$.

We first reduce to the case when both $a_0, b_0$ are nonzero. The multiplicity of the trivial character of $Q_1$ in $V$ is $q$, so we have

$$q = a_0 b_0 + \sum_\chi a_\chi b_{\overline{\chi}}.$$

So either $a_0 b_0$ is nonzero, and we are done, or for some nontrivial $\chi$ we have $a_\chi b_{\overline{\chi}}$ nonzero. In this latter case, replace $X_1$ by $X_1 \otimes \overline{\chi}$ and $X_2$ by $X_2 \otimes \chi$.

Since each nontrivial character $\chi$ of $Q_1$ occur exactly once in $V$, for each such $\chi$ we have

$$1 = a_0 b_\chi + a_\chi b_0 + \sum_{\rho \neq \chi} a_\rho b_{\chi\bar{\rho}}.$$

In particular we have the inequalities

$$a_0 b_\chi \leq 1, \quad a_\chi b_0 \leq 1.$$

Because $a_0, b_0$ are both nonzero, we infer that if $a_\chi \neq 0$, then $a_\chi = b_0 = 1$ (respectively that if $b_\chi \neq 0$, then $a_0 = b_\chi = 1$). It cannot be the case that all $a_\chi$ vanish, otherwise $X_1$ is the trivial module of dimension $> 1$. This is impossible so long as $X_2$ is nontrivial, as each nontrivial character of $Q_1$ occurs in $V$ exactly once. But if all $a_\chi$ and all $b_\chi$ vanish, then $V$ is the trivial $Q_1$ module, which it is not. Therefore $a_0 = 1$ and, similarly, $b_0 = 1$, and all $a_\chi, b_\chi$ are either 0 or 1. Now use again that the multiplicity of the trivial character of $Q_1$ in $V$ is $q$, so we have

$$q = a_0 b_0 + \sum_{\chi} a_\chi b_{\bar{\chi}}.$$

This is possible only if all $a_\chi$ and all $b_\chi$ are 1. But then each $X_i$ has dimension $q$, which is impossible, as the product of their dimensions is $2q-1$. □

**Lemma 9.2.** *The following statements hold for $G$:*

(i) *$G$ preserves no nontrivial orthogonal decomposition of $V$.*

(ii) *$V$ is not tensor induced for $G$.*

*Proof.* We first prove (i). We argue by contradiction. Suppose that

$$V = W_1 \perp \cdots \perp W_r \quad \text{with } r > 1.$$

Because $G$ acts irreducibly, $G$ transitively permutes the $W_i$, and all the $W_i$ have the same odd dimension $d$ (because $2q-1=rd$). Since $r$ divides $2q-1$, $\gcd(r, p)=1$, so the $p$-group $Q$ fixes at least one of the $W_i$, say $W_1$. Because $r > 1$, there are other orbits of $Q$ on the set of blocks. Any of these has cardinality some power of $p$, so the corresponding direct sum of $W_i$'s has odd dimension. As $2q-1$ is odd, there must be evenly many other orbits, so at least three orbits in total. In each $Q$-stable odd-dimensional orthogonal space, $Q$ lies in a maximal torus of the corresponding SO group, so has a fixed line. Hence $\dim V^Q \geq 3$, contradiction.

We next show that $V$ is not tensor induced. We argue by contradiction. If $V$ is tensor induced, write $V = W \otimes \cdots \otimes W$ (with $f \geq 2$ tensor factors, $\dim W < \dim V$). Then $Q_1$ must act transitively on the set of tensor factors (otherwise the representation for $Q_1$ is tensor decomposable and the previous lemma gives a contradiction).

So by Jordan's theorem [1872] (see also [Serre 2003, Theorem 4]), there exists an element $y \in Q_1$ that acts fixed point freely on the set of the $f$ tensor factors. All such elements are conjugate in the wreath product $\mathrm{GL}(W) \wr \mathrm{Sym}(f)$ and we have

$$\chi_V(y) = (\dim W)^{f/p}.$$

(Indeed, after replacing $y$ by a $\mathrm{GL}(W)\wr\mathrm{Sym}(f)$-conjugate, the situation is this. Each orbit of $\langle y\rangle$ on the set of tensor factors has length $p$, and $y$ acts on each corresponding $p$-fold self-product of $W$, indexed by $\mathbb{F}_p$, by mapping $\bigotimes_i w_i$ to $\bigotimes_i w_{i+1}$. In terms of a basis $B := \{e_j\}_{j=1,\dots,\dim W}$ of W, the only diagonal entries of the matrix of $y$ on this $W^{\otimes p}$ are given by the $\dim W$ vectors $e \otimes e \otimes \cdots \otimes e$ with $e \in B$.) On the other hand, we have $\chi_V(y) = q-1$ for any nonzero element $y$ of $Q_1$. Thus, if $d = \dim W$, we have $d^{f/p} = q-1$. Thus, $\dim V = d^f = (q-1)^p > 2q-1$, a contradiction. □

**Corollary 9.3.** *Let $L \leq \mathrm{SO}(V)$ be any subgroup containing $G$ and let $1 \neq N \lhd L$. Then $N$ acts irreducibly on $V$.*

*Proof.* We argue by contradiction. Note that the conclusions of Lemmas 9.1 and 9.2 also hold for $L$.

(i) Because $N$ is normal in $L$, $V$ is completely reducible for $N$. Let $V_1, \ldots, V_r$ be the distinct $N$-isomorphism classes of $N$-irreducible submodules of $V$. Because $V$ is $L$-self-dual, it is a fortiori $N$-self-dual. Therefore the set of $V_i$ is stable by passage to the $N$-dual, $V_i \mapsto V_i^\star$. The group $L$ acts transitively on the set of the $V_i$. Either every $V_i$ is $N$-self-dual, or none is (the $L$-conjugates of an $N$-self-dual representation are $N$-self-dual).

When we write $V$ as the direct sum of its $N$-isotypic ("homogeneous" in the terminology of [Curtis and Reiner 1962, 49.5]) components,

$$V = W_1 \oplus \cdots \oplus W_r,$$

then for some integer $e \geq 1$ we have $N$-isomorphisms

$$W_i \cong eV_i := \text{ the direct sum of } e \text{ copies of } V_i.$$

If $r > 1$ and all the $W_i$ are self-dual, then this is an orthogonal decomposition (because for $i \neq j$, the inner product pairing of (any) $V_i$ with (any) $V_j$ is an $N$-homomorphism from $V_i$ to $V_j^\star \cong V_j$, so vanishes). This contradicts Lemma 9.2.

Suppose $r > 1$ and no $V_i$ is self-dual. Then the $V_i$ occur in pairs of duals. Therefore both $r$ and $\dim V$ are even, again a contradiction.

(ii) We have shown that $r = 1$ and $e > 1$, i.e., $V \cong eV_1$. Now we apply Clifford's theorem, see [Curtis and Reiner 1962, Theorem 51.7]. Thus $L$ preserves the $N$-isomorphism class of $V_1$, and so we get an irreducible projective representation $L \mapsto \mathrm{PGL}(V_1) = \mathrm{PSL}(V_1)$, and $V$ as a projective representation of $L$ is $V_1 \otimes X$ with $L$ acting (projectively) irreducibly on $X$ through $L/N$, and $X$ of dimension $e$. Furthermore, the two factor sets associated to these two projective representations can be chosen to be inverses to each other (as functions $L \times L \to \mathbb{C}^\times$), because the tensor product $V_1 \otimes X = V$ is a linear representation of $Q_1$. Since $e \dim V_1 = \dim V = 2q - 1$, both $e$ and $n = \dim V_1$ are coprime to $p$.

We now claim that, restricted to $Q_1$, each of the tensor factors $V_1$ and $X$ lifts to a genuine linear representation. Indeed, using the fact that $\mathrm{PGL}(n, \mathbb{C}) = \mathrm{PSL}(n, \mathbb{C})$ and the short exact sequence

$$1 \to \mu_n \to \mathrm{SL}(n, \mathbb{C}) \to \mathrm{PSL}(n, \mathbb{C}) \to 1,$$

the obstruction for $(V_1)|_{Q_1}$, which is given by the first factor set restricted to $Q_1$, lies in the cohomology group $H^2(Q_1, \mu_n)$. As $p \nmid n$ while $Q_1$ is a $p$-group, this cohomology group vanishes; and so the first factor set restricted to $Q_1$ is cohomologically trivial. As the second set is the inverse of the first set, it is also cohomologically trivial. Thus the $Q_1$-module $V$ is tensor decomposable, contradicting Lemma 9.1. □

We next show that $G$ is finite. It is convenient to use one more fact about $G$. There is a subgroup $A$ (namely the group $G_{\mathrm{geom}}$ for the hypergeometric sheaf $\mathcal{H}_{2q-1}$) of $\mathrm{SO}(V)$ such that $G$ is normal in $A$, $A/G$ is cyclic of order dividing $2q-1$ and $A$ contains an element $x$ of order $2q-1$ with distinct eigenvalues on $V$.

We also use the fact that $G$ has a nontrivial fixed space on $V \otimes V \otimes V$ (Theorem 7.1).

**Theorem 9.4.** *$G$ is finite.*

*Proof.* Suppose not. Let $N$ be any nontrivial normal (closed) subgroup of $G$. By Corollary 9.3, $N$ is irreducible on $V$.

(i) Let $G^0$ be the identity component of $G$. We now show that $G^0$ is a simple algebraic group. Taking $N = G^0$, we have that $G^0$ acts irreducibly and hence is semisimple (as it lies in $\mathrm{SO}(V)$). Moreover, the center of $G^0$ is trivial (because it consists of scalars in $\mathrm{SO}(V)$). Therefore if $G^0$ is not simple, it is the product of adjoint groups $L_j$, $1 \le j \le t$ (namely the adjoint forms of the factors of its universal cover), and $V$ is the (outer) tensor product $V = \bigotimes_{j=1}^{t} V_j$ of nontrivial irreducible $L_j$-modules $V_j$. By [Guralnick and Tiep 2008, Corollary 2.7], $G$ permutes these tensor factors $V_j$. This action is transitive, otherwise we contradict Lemma 9.1. But this implies that $V$ is tensor induced for $G$, contradicting Lemma 9.2. Thus $G^0$ is a simple algebraic group.

(ii) Because the subgroup of $G$ generated by its $p$-elements is Zariski dense, the finite group $G/G^0$ is generated by its $p$-elements. As $p$ is odd, it follows that either $G = G^0$ is a simple algebraic group or $p = 3$ and $G^0 = D_4(\mathbb{C})$. (In all other cases, the outer automorphism group, i.e., the automorphism group of the Dynkin diagram of $G^0$, has order at most 2.) Since $A/G$ has odd order, it follows that $A \le G^0$ as well, unless $G^0 = D_4(\mathbb{C})$ and 3 divides $2q-1$.

Suppose first that $A$ is connected and so a simple algebraic group. Then it contains a semisimple element $x$ acting with distinct eigenvalues. This implies that a maximal torus has all weight spaces of dimension at most 1. Moreover, the module is in the root lattice (since it is odd dimensional and orthogonal). By a result of Howe [1990] (see also [Panyushev 2004, Table]), it follows if $G \neq \mathrm{SO}(V)$, then either $G = G_2(\mathbb{C})$ with $\dim V = 7$ or $G = \mathrm{PGL}_2(\mathbb{C})$. If $\dim V = 7$, then $q = 4$, a contradiction. If $G = \mathrm{PGL}_2(\mathbb{C})$, then any finite abelian subgroup of odd order is cyclic and so $Q$ does not embed in $G$.

So $G = \mathrm{SO}(V)$. However, $\mathrm{SO}(V)$ has no nonzero fixed points on $V \otimes V \otimes V$ and this contradicts Theorem 7.1.

Thus, it follows that $A$ is disconnected. So the connected component is $D_4(\mathbb{C})$ and this acts irreducibly on $V$. If $D_4(\mathbb{C})$ contains the element of order $2q-1$, then a maximal torus has all weight space of dimension 1 and again using [Howe 1990], we obtain a contradiction. If not, then 3 divides $2q-1$, whence $p \geq 5$ and $Q \leq D_4(\mathbb{C})$. Any elementary abelian $p$-subgroup of $D_4(\mathbb{C})$ is contained in a torus and so again we see that the connected component has all weight spaces of dimension at most 1 and we obtain the final contradiction using [Howe 1990]. □

Let $F^*(X)$ denote the generalized Fitting subgroup of a finite group $X$ (so $X$ is almost simple precisely when $F^*(X)$ is a nonabelian simple group).

**Corollary 9.5.** *$A$ and $G$ are almost simple and $F^*(A) = F^*(G)$ acts irreducibly on $V$.*

*Proof.* Let $N$ be a minimal normal subgroup of $G$. By Corollary 9.3, $N$ acts irreducibly, and so by Schur's lemma $\boldsymbol{C}_A(N) = \boldsymbol{Z}(N) = 1$ as $A < \mathrm{SO}(V)$ with $\dim V$ odd. So $N$ is nonabelian, and so, being a minimal normal subgroup, it is a direct product of nonabelian simple groups. Arguing as in part (i) of the proof of Theorem 9.4, we see that $N$ is nonabelian simple (otherwise the module $V$ would be tensor induced). As $\boldsymbol{C}_G(N) = 1$, we see that $N \lhd G \leq \mathrm{Aut}(N)$, and so $G$ is almost simple and $F^*(G) = N$.

Now, as $G \lhd A$, $A$ normalizes $N$. Again since $\boldsymbol{C}_A(N) = 1$ we have that $N \lhd A \leq \mathrm{Aut}(N)$, and so $A$ is almost simple and $F^*(A) = N$. □

We next observe:

**Lemma 9.6.** *$F^*(G)$ is not a sporadic simple group.*

*Proof.* Notice that both $G$ and $A$ are generated by elements of odd order ($p$-elements for $G$, these and elements of order $2q-1$ for $A$). On the other hand, we have $S \leq G \leq A \leq \mathrm{Aut}(S)$ for $S = F^*(G)$. One knows [Conway et al. 1985] that if $S$ is sporadic, then $|\mathrm{Out}(S)| \leq 2$. Therefore, if $S$ is a sporadic simple group, then $G = A = S$. The result now follows easily from information in [Conway et al. 1985]. Namely, we observe that if $q$ is an odd prime power with $q^2$ dividing $|G|$, then $G$ has no irreducible representation of dimension $2q-1$. □

We next consider the case $F^*(G) = \mathrm{Alt}(n)$. First note $\mathrm{Alt}(5)$ contains no noncyclic elementary abelian groups of odd order and so is ruled out. Since $2q-1$ is odd, we see that if $G = \mathrm{Alt}(n)$, then $A = G = \mathrm{Alt}(n)$ (as the outer automorphism group of $\mathrm{Alt}(n)$ is a 2-group).

**Theorem 9.7.** *Let $\Gamma = \mathrm{Alt}(n)$ with $n \geq 6$. Suppose that $x \in \Gamma$ has odd order and $V$ is an irreducible $\mathbb{C}[\Gamma]$-module such that $x$ acts as a semisimple regular element on $V$. Then one of the following holds*:

(i) *$V$ is the deleted permutation module of dimension $n-1$* (i.e., the nontrivial irreducible constituent of $\mathbb{C}^{\mathrm{Alt}(n)}_{\mathrm{Alt}(n-1)}$), *and $x$ is either an $n$-cycle* (*for $n$ odd*) *or a product of two disjoint cycles of coprime lengths* (*for $n$ even*); *or*

(ii) $n = 8$, *$x$ has order* 15 *and* $\dim V = 14$.

*Proof.* First note that if $V$ is the deleted permutation module of dimension $n-1$, an element with 3 or more disjoint cycles has at least a two-dimensional fixed space on $V$. Next assume that $x$ has two disjoint cycles of lengths $a$ and $b$ which are not coprime. Then $x$ affords a 2-dimensional eigenspace on $\mathbb{C}^n$ for an eigenvalue $\lambda$, a primitive $\gcd(a, b)$-th root of unity in $\mathbb{C}$. As $\lambda \neq 1$ and $V$ is obtained from $\mathbb{C}^n$ by modding out the trivial eigenspace of $\mathrm{Sym}(n)$, it follows that $x$ has a two-dimensional eigenspace on $V$ as well.

Next we observe that if $x$ is semisimple regular on $V$, then the order of $x$ is at least $\dim V$. This proves the result for $6 \leq n \leq 14$ by inspection of the odd order elements and dimensions of the irreducible modules, aside from the case $n = 8$ and $\dim V = 14$ (note that $\mathrm{Alt}(8)$ contains an element of order 15). Recall that $\mathrm{Alt}(8) \cong \mathrm{GL}_4(2)$ and it acts 2-transitively on the nonzero vectors. The only irreducible module of dimension 14 is the irreducible summand of the permutation module of dimension 15. In this case $x$ has a single orbit in the permutation representation and so $x$ is semisimple regular on $V$.

Now assume that $n \geq 15$.

Suppose first that $x$ has at most three nontrivial cycles. Then the order of $x$ is less than $(n/3)^3 = n^3/27$ and so $\dim V < n^3/27$. Let $W$ be a complex irreducible $\mathrm{Sym}(n)$-module whose restriction to $\mathrm{Alt}(n)$ contains $V|_{\mathrm{Alt}(n)}$. Since $2 \leq \dim W < 2n^3/27$, it follows by [Rasala 1977, Result 3] that $W \cong S^\lambda$ or $S^\lambda \otimes \mathrm{sgn}$, where $S^\lambda$ is the Specht module labeled by the partition $\lambda$ of $n$, with $\lambda = (n-1, 1)$, $(n-2, 2)$, or $(n-2, 1, 1)$. Restricting back to $\mathrm{Alt}(n)$, we see that $V|_{\mathrm{Alt}(n)} = S^\lambda|_{\mathrm{Alt}(n)}$.

Note that

$$\dim S^{(n-2,1,1)} = (n-1)(n-2)/2, \quad \dim S^{(n-2,2)} = n(n-3)/2.$$

It is straightforward to see that the dimension of the fixed space of $x$ on either of these modules is at least two dimensional, a contradiction. Hence $\lambda = (n-1, 1)$ and $V|_{\mathrm{Alt}(n)}$ is the deleted permutation module of dimension $n-1$.

We now induct on $n$. The base case $n \leq 14$ has already done. We may assume that $x$ has at least four nontrivial cycles (each of odd length, as $x$ has odd order). View $x \in J := \mathrm{Alt}(a) \times \mathrm{Alt}(b)$. where the projection into $\mathrm{Alt}(b)$ is a $b$-cycle and so the projection into $\mathrm{Alt}(a)$ is a product of at least three disjoint cycles. Thus, $a \geq 9$. Let $W$ be an irreducible $J$-submodule of $V$ with $\mathrm{Alt}(a)$ acting nontrivially. So $W = W_1 \otimes W_2$ with $W_1$ an irreducible $\mathrm{Alt}(a)$-module. Then $x$ must be multiplicity free on each $W_i$ and by induction $x$ can have at most two cycles in $\mathrm{Alt}(a)$, a contradiction. □

Note that the previous result does fail for $n = 5$. Alt(5) has a 5-dimensional representation in which an element of order 5 has all eigenvalues occurring once. Thus if $G = \mathrm{Alt}(n)$, we see that $n = 2q$ and $V$ is the deleted permutation module.

**Corollary 9.8.** *If $G = G_{\mathrm{geom}}$ is an alternating group* $\mathrm{Alt}(n)$ *for some $n$, then $n = 2q$.*

Finally, we consider the case where $G$ is an almost simple finite group of Lie type, defined over $\mathbb{F}_s$, where $s = s_0^f$ is a power of a prime $s_0$. Let us denote

$$S := F^*(G) = F^*(A).$$

Recall that $S$ is simple, irreducible on $V$, and $\mathbf{Z}(S) = 1$ by Corollary 9.5. We will freely use information on character tables of simple groups available in [Conway et al. 1985; GAP 2004], as well as degrees of complex irreducible characters of various quasisimple groups of Lie type available in [Lübeck 2007]. Finally, we will also use bounds on the smallest degree $d(S)$ of nontrivial complex irreducible representations of $S$ as listed in [Tiep 2003, Table 1].

**Theorem 9.9.** *Suppose $s_0 \neq p$. Then $S \cong \mathrm{Alt}(m)$ with $m \in \{5, 6, 8\}$.*

*Proof.* (i) Assume the contrary. We will exploit the existence of the subgroup $Q \leq G$. Recall that the *p-rank* $m_p(G)$ is the largest rank of elementary abelian $p$-subgroups of $G$. Furthermore,

$$\mathrm{Aut}(S) \cong \mathrm{Inndiag}(S) \rtimes \Phi_S \Gamma_S, \tag{9.9.1}$$

where $\mathrm{Inndiag}(S)$ is the subgroup of inner-diagonal automorphisms of $S$, $\Phi_S$ is a subgroup of field automorphisms of $S$ and $\Gamma_S$ is a subgroup of graph automorphisms of $S$, as defined in [Gorenstein et al. 1998, Theorem 2.5.12]. As $F^*(G) = S$, we can embed $G$ in $\mathrm{Aut}(S)$. Now, given an elementary abelian $p$-subgroup $P < G$ of rank $m_p(G)$, we can define a normal series

$$1 \leq P_1 \leq P_2 \leq P,$$

where $P_1 = P \cap \mathrm{Inndiag}(S)$ and $P_2 = P \cap (\mathrm{Inndiag}(S) \rtimes \Phi_S)$. As $\Phi_S$ is cyclic and $P$ is elementary abelian, $P_2/P_1$ has order 1 or $p$. Set $e = 1$ if $S \cong P\Omega_8^+(s)$ and $p = 3$, and $e = 0$ otherwise. Then $|P/P_2| \leq p^e$.

Next we bound $|P_1|$ when $S$ is not a Suzuki–Ree group. Let $\Phi_j(t)$ denote the $j$-th cyclotomic polynomial in the variable $t$, and let $m$ denote the multiplicative order of $s$ modulo $p$, so that $p \mid \Phi_m(s)$. Note that we can find a simple algebraic group $\mathcal{G}$ of adjoint type defined over $\overline{\mathbb{F}}_s$ and a Frobenius endomorphism $F : \mathcal{G} \to \mathcal{G}$

such that $\mathrm{Inndiag}(S) \cong \mathcal{G}^F$. Letting $r$ denote the rank of $\mathcal{G}$, then one can find $r$ positive integers $k_1, \dots, k_r$ and $\epsilon_1, \dots, \epsilon_r = \pm 1$ such that

$$|\mathrm{Inndiag}(S)| = s^N \prod_{j \geq 1} \Phi_j(s)^{n_j} = s^N \prod_{i=1}^{r} (s^{k_i} - \epsilon_i)$$

for suitable integers $N$, $n_j$. Then, according to [Gorenstein et al. 1998, Theorem 4.10.3(b)], $|P_1| \leq p^{n_m}$. Let $\varphi(\,\cdot\,)$ denote the Euler function, so $\deg(\Phi_m) = \varphi(m)$. Inspecting the integers $k_1, \dots, k_r$, one sees that $n_m \leq r/\varphi(m)$. It follows that

$$|P_1| \leq \Phi_m(s)^{n_m} \leq ((s+1)^{\varphi(m)})^{r/\varphi(m)} \leq (s+1)^r.$$

In fact, one can verify that this bound on $|P_1|$ also holds for Suzuki–Ree groups. Putting all the above estimates together, we obtain that

$$q^2 = |Q| \leq |P| \leq (s+1)^{r+1+e}. \tag{9.9.2}$$

We will show that this upper bound on $q$ contradicts the lower bound

$$2q - 1 = \dim V \geq d(S) \tag{9.9.3}$$

in most of the cases. Let $f^*$ denote the odd part of the integer $f$.

(ii) First we handle the case when $S$ is of type $D_4$ or ${}^3D_4$. Here, $q \leq (s+1)^3$ by (9.9.2). On the other hand, $d(S) \geq s(s^4 - s^2 + 1)$, contradicting (9.9.3) if $s \geq 3$. If $s = 2$, then $\Phi_S \Gamma_S = C_3$, and so instead of (9.9.2) we now have that $q^2 \leq 3^5$, whence $q \leq 13$, $2q - 1 \leq 25 < d(S)$, again a contradiction.

From now on we may assume $e = 0$.

Next we consider the case $S = \mathrm{PSL}_2(s)$. Then $\mathrm{Out}(S) = C_{\gcd(2,s-1)} \times C_f$, and $m_p(S) \leq 1$. It follows that $Q$ is not contained in $S$ but in $S \rtimes C_f$ and $3 \leq p \mid f^*$, and furthermore $q^2 = |Q| \leq (s+1) f^*$. As $d(S) \geq (s-1)/2$, (9.9.3) now implies that

$$s + 1 = s_0^f + 1 \leq 16 f^*,$$

a contradiction if $s_0 \geq 5$, or $s_0 = 3$ and $f \geq 5$, or $s_0 = 2$ and $f \geq 7$. If $s_0 = 3$ and $f \leq 4$, then $f^* = 3 = f = p$, forcing $p = s_0$, a contraction. Suppose $s_0 = 2$ and $f \leq 6$. If $p = 5$, then $f^* = 5$ and $m_p(G) = 1$, ruling out the existence of $Q$. If $p = 3$, then $f = 3, 6$, whence $q^2 \leq 9$ and $2q - 1 \leq 5 < d(S)$.

Suppose that $S = {}^2B_2(s)$ or ${}^2G_2(s)$ with $s \geq 8$. Since $m_p(S) \leq 1$, we see that $q^2 \leq (s+1) f$, contradicting (9.9.3) as $d(S) \geq (s-1)\sqrt{s/2}$.

Now we consider the remaining cases with $r = 2$. Then $q \leq (s+1)^{\frac{3}{2}}$ by (9.9.2). This contradicts (9.9.3) if $S = G_2(s)$ (and $s \geq 3$), as $d(S) \geq s^3 - 1$. Similarly, $S \not\cong \mathrm{PSL}_3(s)$ with $s \geq 5$ and $S \not\cong \mathrm{PSU}_3(s)$ with $s \geq 8$. If $S = \mathrm{PSp}_4(s)$, then the case $2 \nmid s \geq 19$ is ruled out since $d(S) \geq (s^2 - 1)/2$, and similarly the case $2 | s \geq 8$ is ruled out since $d(S) = s(s-1)^2/2$. In the remaining cases, $\Phi_S \Gamma_S$ is a 2-group, and so $Q \le S$, $q^2 \le (s+1)^2$, $q \le s+1$. Now $\mathrm{PSL}_3(s)$ and $\mathrm{PSU}_3(s)$ with $s \ge 4$ are ruled out by (9.9.3), and the same for $\mathrm{PSp}_4(s)$ with $s \ge 4$. Note that when $s = 3$, $q \ge 4$ and so $\gcd(q, 2s) \ne 1$, a contradiction. If $S = \mathrm{SL}_3(2)$, then $q = 3$ and $S$ has no irreducible character of degree $2q - 1$. Finally, $\mathrm{Sp}_4(2)' \cong \mathrm{Alt}(6)$.

Next we handle the groups with $r = 3$. Here $q \le (s+1)^2$ by (9.9.2). Then (9.9.3) implies that $s \le 5$. In this case, $\mathrm{Out}(S)$ is a 2-group, and so $Q \le S$ and $q \le (s+1)^{\frac{3}{2}}$ by (9.9.2). Using (9.9.3), we see that $s \le 3$. The remaining groups $S$ cannot occur, since $S$ does not have a real-valued complex irreducible character of degree $2q - 1$.

(iii) From now we may assume that $r \ge 4$ (and $S$ is not of type $D_4$ or ${}^3D_4$). First we consider the case $s = 2$. If $S = \mathrm{SL}_n(2)$ with $n \ge 5$, then since $\mathrm{Out}(S) = C_2$, the arguments in (i) show that $q^2 \le 3^{n-1}$. This contradicts (9.9.3), since $d(S) = 2^n - 2$. Suppose $S = \mathrm{SU}_n(2)$ with $n \ge 7$. Note by [Tiep and Zalesskii 1996, Theorem 4.1] that the first three nontrivial irreducible characters of $S$ are Weil characters and either non-real-valued or of even degree, and the next characters have degree at least $(2^n - 1)(2^{n-1} - 4)/9$. Hence (9.9.3) can be improved to

$$2q - 1 \ge (2^n - 1)(2^{n-1} - 4)/9,$$

which is impossible since $q^2 \le 3^n$ by (9.9.2). If $S = \mathrm{PSU}_n(2)$ with $n = 5, 6$, then $q^2 \le 3^6$, and $S$ has no nontrivial real-valued irreducible character of odd degree $\le 2q-1 \le 53$. If $S = {}^2F_4(2)'$ or $F_4(2)$, then $q^2 \le 3^5$, $q \le 13$, and $S$ has no nontrivial real-valued irreducible character of odd degree $\le 2q - 1 \le 25$.

Suppose $S = \mathrm{Sp}_{2n}(2)$ or $\Omega^{\pm}_{2n}(2)$. Then $\mathrm{Out}(S)$ is a 2-group (recall $S$ is not of type $D_4$), and so $q^2 \le 3^n$. On the other hand, $d(S) \ge (2^n - 1)(2^{n-1} - 2)/3$, contradicting (9.9.3). Finally, if $S$ is of type $E_8$, $E_7$, $E_6$, or ${}^2E_6$, then $q^2 \le 3^8$ whereas $d(S) > 2^{10}$, again contradicting (9.9.3).

(iv) Suppose that $S = \mathrm{PSp}_{2n}(s)$ with $n \ge 4$ and $2 \nmid s \ge 3$. Then by (9.9.2) and (9.9.3) we have

$$(s^n - 1)/2 \le 2q - 1 \le 2(s+1)^{(n+1)/2} - 1,$$

implying $n \le 5$ and $s = 3$. In this case, inspecting the order of $\mathrm{PSp}_{10}(3)$ we see that $q^2 \le 121$, and so $2q - 1 \le 21 < d(S)$, a contradiction.

Next suppose that $S = \mathrm{PSU}_n(3)$ with $n \ge 5$. Then $q \le 2^n$ and $d(S) \ge (3^n - 3)/4$, and so (9.9.3) implies that $n = 5$. In this case, inspecting the order of $\mathrm{SU}_5(3)$ we see that $q^2 \le 61$, and so $2q - 1 \le 13 < d(S)$, again a contradiction.

Now we may assume that $r \ge 4$, $s \ge 3$, $S \not\cong \mathrm{PSp}_{2n}(s)$ if $2 \nmid s$, and moreover $s \ge 4$ if $S \cong \mathrm{PSU}_n(s)$. Then one can check that $d(S) \ge s^r \cdot (51/64)$ (with equality attained exactly when $S \cong \mathrm{PSU}_5(4)$). Hence (9.9.2) and (9.9.3) imply that

$$(51/64)^2 \cdot s^{2r} \le d(S)^2 \le (2q-1)^2 < 4(s+1)^{r+1} \le 4 \cdot (4s/3)^{r+1},$$

and so

$$(3s/4)^{r-1} < 4 \cdot (64/51)^2 \cdot (4/3)^2,$$

which is impossible for $r \geq 4$. □

**Theorem 9.10.** *Suppose $s_0 = p$. Then $S \cong \mathrm{Alt}(6)$.*

*Proof.* (i) Assume the contrary. We now exploit the existence of the element $x \in A$ of order $2q - 1$ which has simple spectrum on $V$. As before, we can embed $A$ in $\mathrm{Aut}(S)$ and again use the decomposition (9.9.1). Let $\langle y \rangle = \langle x \rangle \cap \mathrm{Inndiag}(S)$. We also view $S = \mathcal{G}^F$ for some Frobenius endomorphism $F : \mathcal{G} \to \mathcal{G}$ of a simple algebraic group $\mathcal{G}$ of adjoint type, defined over $\overline{\mathbb{F}}_p$. Note that $y$ is an $F$-stable semisimple element in $\mathcal{G}$, hence it is contained in an $F$-stable maximal torus $\mathcal{T}$ of $\mathcal{G}$ by [Digne and Michel 1991, Corollary 3.16]. It follows that $|y| \leq |\mathcal{T}^F| \leq (s+1)^r$, if $r$ is the rank of $\mathcal{G}$. Set $e = 3$ if $S$ is of type $D_4$ or ${}^3D_4$, and $e = 1$ otherwise. Then the decomposition (9.9.1) shows that

$$|x|/|y| \leq ef^*,$$

where $f^*$ denotes the odd part of $f$ as before (and $s = p^f$). We have thus shown that

$$2q - 1 = |x| \leq (s+1)^r ef^*. \tag{9.10.1}$$

We will frequently use the following remark:

$$\text{either} \quad f = 1 \text{ and } s \geq 3f^*, \quad \text{or} \quad s \geq 9f^*. \tag{9.10.2}$$

We will show that in most of the cases (9.10.1) contradicts (9.9.3). First we handle the case $S$ is of type $D_4$ or ${}^3D_4$, whence $d(S) \geq s(s^4 - s^2 + 1)$. Hence (9.10.1) and (9.10.2) imply that

$$s(s^4 - s^2 + 1) \leq 2q - 1 \leq s(s+1)^4/3$$

if $f > 1$, a contradiction. If $f = 1$, then since $2q - 1 = \dim V$ is coprime to $2s$, we see by [Lübeck 2007] that

$$2q - 1 > s^7/2 > 3(s+1)^4,$$

contradicting (9.10.1).

(ii) From now on we may assume that $e = 1$. Next we rule out the case where $V|_S$ is a Weil module of $S \in \{\mathrm{PSL}_n(s), \mathrm{PSU}_n(s)\}$ with $n \geq 3$, or $S = \mathrm{PSp}_{2n}(s)$ with $n \geq 2$. Indeed, in this case, 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 cannot be equal to $2q-1$. Similarly, if $S=\mathrm{PSU}_n(s)$, then $V|_S$ can be a Weil module of dimension $2q-1$ only when $2\,|\,n$ and $\dim V=(s^n-1)/(s+1)$. In this case,

$$q=(2q-1)_p=((s^n+s)/(s+1))_p=s$$

(where $N_p$ denotes the $p$-part of the integer $N$), and so $2s-1=(s^n+s)/(s+1)$, a contradiction. Likewise, if $S=\mathrm{PSp}_{2n}(s)$, then $V|_S$ can be a Weil module of dimension $2q-1$ only when $p=3$ and $\dim V=(s^n+1)/2$. In this case,

$$s^n=(2\dim V-1)_p=(4q-3)_p,$$

and so $q=3$ and $n=2$. One can show that $\mathrm{PSp}_4(3)$ does possess a complex irreducible module of dimension $2q-1=5$, with an element $x$ of order 5 with simple spectrum on $V$ and a subgroup $Q\cong C_3^2$ with desired prescribed action on $V$; however, any such module is not self-dual. Henceforth, for the aforementioned possibilities for $S$ we may assume that $\dim V\geq d_2(S)$, the next degree after the degree of Weil characters. Note that $d_2(S)$ for these simple groups $S$ is determined in Theorems 3.1, 4.1, and 5.2 of [Tiep and Zalesskii 1996].

(iii) Suppose $S=\mathrm{PSL}_2(s)$; in particular, $s\neq 9$. Assume $f\geq 4$. As $\mathrm{Out}(S)=C_{2,s-1}\times C_f$, we see that $q^2\leq sf_p<s^2/20$, whereas $2q-1\geq d(S)\geq(s-1)/2$, a contradiction. If $f\leq 3$ but $f_p>1$, then $f=p=3$, $s=3^3$, $q^2\leq sf=3^4$, forcing $q=9$. But then $S=\mathrm{PSL}_2(27)$ has no irreducible character of degree $2q-1=17$. Thus $f_p=1$, $q^2\leq s$, and so (9.9.3) implies that $s\leq 17$. As $s\neq 9$, we see that $m_p(G)=m_p(S)=1$, contradicting the existence of $Q$.

Next we consider the case $S=\mathrm{PSL}_3(s)$ or $\mathrm{PSU}_3(s)$. If $f>1$, then (9.9.3)–(9.10.2) imply

$$(s-1)(s^2-s+1)/3\leq d_2(S)\leq 2q-1\leq(s+1)^2s/9,$$

which is impossible. Thus $f=1$, whence

$$(s-1)(s^2-s+1)/3\leq d_2(S)\leq 2q-1\leq(s+1)^2,$$

yielding $s\leq 5$. But if $s=3$ or 5, then any nontrivial $\chi\in\mathrm{Irr}(S)$ of odd degree coprime to $s$ is a Weil character, which has been ruled out in (ii).

Suppose now that $S=\mathrm{PSL}_4(s)$ or $\mathrm{PSU}_4(s)$. For $s\geq 5$ we have

$$(s-1)(s^3-1)/2\leq d_2(S)\leq 2q-1\leq(s+1)^3s/3,$$

which is possible only when $s\leq 11$. Thus $3\leq s\leq 11$, whence $f^*=1$, and so

$$(s-1)(s^3-1)/2\leq d_2(S)\leq 2q-1\leq(s+1)^3,$$

leading to $s=3$. If $s=3$, then any odd-order element in $G$ has order $\leq 13$, whereas $d(S)=21$, contradicting (9.9.3).

To finish off type $A$, assume now that $S=\mathrm{PSL}_n(s)$ or $\mathrm{PSU}_n(s)$ with $n\geq 5$. Then (9.9.3)–(9.10.2) imply

$$\frac{(s^n+1)(s^{n-1}-s^2)}{(s+1)(s^2-1)}\leq d_2(S)\leq 2q-1\leq (s+1)^{n-1}s/3,$$

whence

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

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

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

$$\frac{(s^n-1)(s^{n-1}-s)}{s^2-1}\leq d(S)\leq 2q-1\leq (s+1)^n f\leq (s+1)^n s/3,$$

whence

$$s^{2n-3.1}<(s+1)^n s/3<s^{51n/40},$$

a contradiction. If $n=4$, then $S=P\Omega^-_8(s)$. In this case, since $2q-1$ is coprime to $2s$, [Lübeck 2007] implies that

$$2q-1\geq (s^4+1)(s^2-s+1)/2>(s+1)^4 s/3,$$

again a contradiction.

Suppose $S=\mathrm{PSp}_{2n}(s)$ with $n\geq 2$ or $\Omega_{2n+1}(s)$ with $n\geq 3$. Using the bound $2q-1\geq d_2(S)$ for $S=\mathrm{PSp}_{2n}(s)$ and $2q-1\geq d(S)$ otherwise, we get for $n\geq 3$ that

$$\frac{(s^n-1)(s^n-s)}{s^2-1}\leq 2q-1\leq (s+1)^n f\leq (s+1)^n s/3,$$

whence

$$s^{2n-2.1}<(s+1)^n s/3<s^{51n/40},$$

a contradiction. If $n=2$, then $S=\mathrm{PSp}_4(s)$, and we have

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

forcing $q\leq 9$. If $5\leq q\leq 9$, then since the degree $2q-1=\dim V$ is coprime to $2s$, we again get $2q-1>300\geq (s+1)^2 s/3$. Finally, $\mathrm{PSp}_4(3)$ has no nontrivial non-Weil character of degree coprime to 6.

(v) If $S$ is of type $E_6$, ${}^2E_6$, $E_7$, or $E_8$, then

$$(s^5+s)(s^6-s^3+1)\leq d(S)\leq 2q-1\leq (s+1)^8 f\leq (s+1)^8 s/3,$$

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

$$s^8-s^4+1=d(S)\leq 2q-1\leq (s+1)^4 s/3,$$

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

$$s^3 - 1 \leq d(S) \leq 2q - 1 \leq (s+1)^2 s/3,$$

again a contradiction. Next, if $S = G_2(3)$, then $2q - 1 \leq 16$ cannot be a degree of an irreducible character of $S$. Finally, if $S = {}^2G_2(s)$, then

$$s^2 - s + 1 = d(S) \leq 2q - 1 \leq (s+1)f \leq (s+1)s/3,$$

again a contradiction since $s \geq 27$. □

Our proof is now concluded by applying Theorem 9.7. □

## References

[Conway et al. 1985] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *Atlas of finite groups: maximal subgroups and ordinary characters for simple groups*, Oxford University Press, Eynsham, 1985. MR Zbl

[Curtis and Reiner 1962] C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, Pure and Applied Mathematics **XI**, Interscience, New York, 1962. MR Zbl

[Deligne 1980] P. Deligne, "La conjecture de Weil, II", *Inst. Hautes Études Sci. Publ. Math.* **52** (1980), 137–252. MR Zbl

[Digne and Michel 1991] F. Digne and J. Michel, *Representations of finite groups of Lie type*, London Mathematical Society Student Texts **21**, Cambridge University Press, 1991. MR Zbl

[Fu 2010] L. Fu, "Calculation of $\ell$-adic local Fourier transformations", *Manuscripta Math.* **133**:3-4 (2010), 409–464. MR Zbl

[Fulton and Harris 1991] W. Fulton and J. Harris, *Representation theory: a first course*, Graduate Texts in Mathematics **129**, Springer, 1991. MR Zbl

[GAP 2004] *GAP — Groups, Algorithms, and Programming, Version 4.4*, The GAP Group, 2004, available at https://www.gap-system.org.

[Gorenstein et al. 1998] D. Gorenstein, R. Lyons, and R. Solomon, *The classification of the finite simple groups*, vol. 3, Mathematical Surveys and Monographs **40**, American Mathematical Society, Providence, RI, 1998. MR Zbl

[Gross 2010] B. H. Gross, "Rigid local systems on $\mathbb{G}_m$ with finite monodromy", *Adv. Math.* **224**:6 (2010), 2531–2543. MR Zbl

[Grothendieck 1968] A. Grothendieck, "Formule de Lefschetz et rationalité des fonctions $L$", pp. 31–45 in *Dix exposés sur la cohomologie des schémas*, Adv. Stud. Pure Math. **3**, North-Holland, Amsterdam, 1968. MR Zbl

[Guralnick and Tiep 2008] R. M. Guralnick and P. H. Tiep, "Symmetric powers and a problem of Kollár and Larsen", *Invent. Math.* **174**:3 (2008), 505–554. MR Zbl

[Howe 1990] R. Howe, "Another look at the local $\theta$-correspondence for an unramified dual pair", pp. 93–124 in *Festschrift in honor of I. I. Piatetski-Shapiro on the occasion of his sixtieth birthday, I* (Ramat Aviv, Israel, 1989), Israel Math. Conf. Proc. **2**, Weizmann, Jerusalem, 1990. MR Zbl

[Jordan 1872] C. Jordan, "Recherches sur les substitutions", *Journal de Mathématiques Pures et Appliquées* **17** (1872), 351–367. Zbl

[Katz 1988] N. M. Katz, *Gauss sums, Kloosterman sums, and monodromy groups*, Annals of Mathematics Studies **116**, Princeton University Press, 1988. MR Zbl

[Katz 1989] N. M. Katz, "Perversity and exponential sums", pp. 209–259 in *Algebraic number theory*, Adv. Stud. Pure Math. **17**, Academic Press, Boston, 1989. MR Zbl

[Katz 1990] N. M. Katz, *Exponential sums and differential equations*, Annals of Mathematics Studies **124**, Princeton University Press, 1990. MR Zbl

[Katz 1996] N. M. Katz, *Rigid local systems*, Annals of Mathematics Studies **139**, Princeton University Press, 1996. MR Zbl

[Katz 2004] N. M. Katz, "Notes on $G_2$, determinants, and equidistribution", *Finite Fields Appl.* **10**:2 (2004), 221–269. MR Zbl

[Katz 2005] N. M. Katz, *Moments, monodromy, and perversity: a Diophantine perspective*, Annals of Mathematics Studies **159**, Princeton University Press, 2005. MR Zbl

[Katz 2018] N. Katz, "Rigid local systems on $\mathbb{A}^1$ with finite monodromy", preprint, 2018, available at http://www.math.princeton.edu/~nmk/gpconj114.pdf. With an appendix by P. H. Tiep. To appear in *Mathematika*.

[Katz and Sarnak 1999] N. M. Katz and P. Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, American Mathematical Society Colloquium Publications **45**, American Mathematical Society, Providence, RI, 1999. MR Zbl

[Lübeck 2007] F. Lübeck, "Character degrees and their multiplicities for some groups of Lie type of rank $< 9$", web site, 2007, available at http://www.math.rwth-aachen.de/~Frank.Luebeck/chev/DegMult/index.html.

[Panyushev 2004] D. I. Panyushev, "Weight multiplicity free representations, $\mathfrak{g}$-endomorphism algebras, and Dynkin polynomials", *J. London Math. Soc.* (2) **69**:2 (2004), 273–290. MR Zbl

[Rasala 1977] R. Rasala, "On the minimal degrees of characters of $S_n$", *J. Algebra* **45**:1 (1977), 132–181. MR Zbl

[Raynaud 1994] M. Raynaud, "Revêtements de la droite affine en caractéristique $p > 0$ et conjecture d'Abhyankar", *Invent. Math.* **116**:1-3 (1994), 425–462. MR Zbl

[Serre 2003] J.-P. Serre, "On a theorem of Jordan", *Bull. Amer. Math. Soc.* (*N.S.*) **40**:4 (2003), 429–440. MR Zbl

[Tiep 2003] P. H. Tiep, "Low dimensional representations of finite quasisimple groups", pp. 277–294 in *Groups, combinatorics & geometry* (Durham, NC, 2001), edited by A. A. Ivanov et al., World Sci. Publ., River Edge, NJ, 2003. MR Zbl

[Tiep and Zalesskii 1996] P. H. Tiep and A. E. Zalesskii, "Minimal characters of the finite classical groups", *Comm. Algebra* **24**:6 (1996), 2093–2167. MR Zbl

Received 5 Oct 2017. Revised 3 Apr 2018.

ROBERT M. GURALNICK:
guralnic@usc.edu
Department of Mathematics, University of Southern California, Los Angeles, CA 90089-2532, United States

NICHOLAS M. KATZ:
nmk@math.princeton.edu
Department of Mathematics, Princeton University, Fine Hall, Princeton, NJ 08544-1000, United States

PHAM HUU TIEP:
tiep@math.rutgers.edu
Department of Mathematics, Rutgers University, Piscataway, NJ 08854-8019, United States

# Tunisian Journal of Mathematics

msp.org/tunis





The Tunisian Journal of Mathematics is an international publication organized by the Tunisian Mathematical Society (http://www.tms.rnu.tn) and published in electronic and print formats by MSP in Berkeley.

See inside back cover or msp.org/tunis for submission instructions.

The subscription price for 2019 is US $315/year for the electronic version, and $370/year (+$20, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Tunisian Journal of Mathematics (ISSN 2576-7666 electronic, 2576-7658 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

TJM peer review and production are managed by EditFlow® from MSP.

PUBLISHED BY

**mathematical sciences publishers**

**nonprofit scientific publishing**

http://msp.org/

# Tunisian Journal of Mathematics

2019 vol. 1 no. 3