THE SPARSITY OF CHARACTER TABLES OF HIGH RANK GROUPS OF LIE TYPE

MICHAEL J. LARSEN AND ALEXANDER R. MILLER

Abstract. In the high rank limit, the fraction of non-zero character table entries of finite simple groups of Lie type goes to zero.

1. Introduction

Let G be a finite group. Let G^G denote the set of conjugacy classes of G and $\mathrm{Irr}(G)$ the set of irreducible characters, so $k(G) = |G^G| = |\mathrm{Irr}(G)|$. A well-known theorem of Burnside asserts that if $\chi \in \mathrm{Irr}(G)$ and $\chi(1) > 1$, then there exists $g \in G$ such that $\chi(g) = 0$; in particular, there are zero entries in the character table of every non-abelian G. In fact, one can make much stronger statements about the subset of $G^G \times \mathrm{Irr}(G)$ determined by the vanishing condition, and there is a substantial literature devoted to such results. We are interested in the opposite extreme from abelian groups, namely groups for which almost all entries are zero.

We define the *sparsity* $\Sigma(G)$ to be the fraction of non-zero entries in the character table of G:

$$\Sigma(G) := \frac{|\{(g^G, \chi) \in G^G \times \mathrm{Irr}(G) \mid \chi(g) \neq 0\}|}{k(G)|\mathrm{Irr}(G)|}.$$

For finite simple groups of bounded rank, it is not too difficult to analyze the asymptotic behavior of $\Sigma(G)$. For instance,

$$\lim_{q \to \infty} \Sigma(L_2(q)) = \frac{1}{2}.$$

In this paper, we consider what happens when G ranges over finite simple groups of Lie type of unbounded rank. Our result is the following.

Theorem 1.1. *Given any sequence G_i of finite simple groups of Lie type with rank tending to ∞, $\lim_{i \to \infty} \Sigma(G_i) = 0$.*

To round out the story, it would be interesting to know whether $\Sigma(A_n) \to 0$ (or, equivalently, whether $\Sigma(S_n) \to 0$) as $n \to \infty$. This remains open. The numerical evidence [16] seems to point to a limit strictly between 0 and 1. Interestingly, Miller proved [15] that for random pairs $(\chi, g) \in \mathrm{Irr}(G) \times G$, the probability that $\chi(g) = 0$ goes to 1 as G ranges over symmetric groups.

2010 *Mathematics Subject Classification.* 20C33.

ML was partially supported by the NSF grant DMS-1702152. AM was partially supported by the Austrian Science Foundation.

The proof of Theorem 1.1 uses a trick of Burnside and roughly parallels that of [7]. Given a pair (g^G, χ), let

$$d_{g^G,\chi} := \frac{\chi(1)}{(\chi(1), |g^G|)}.$$

By [7], $\chi(g)$ is divisible by $d_{g^G,\chi}$ in a ring of cyclotomic integers. If $\alpha \neq 0$ is an algebraic integer, then the average of $|\alpha_i|^2$ over all conjugates α_i of α is at least 1 [6, p. 459]. Therefore, if α is divisible by a rational integer d, then the average is at least d^2. The multiset of values $\chi(g) \neq 0$ where $\chi(g)$ is divisible by some rational integer $d > D$ is stable under the action of $\mathrm{Gal}(\mathbb{Q}(\zeta_{|G|})/\mathbb{Q})$, so the average of $|\chi(g)|^2$ over all such values is greater than D^2. By the orthonormality of characters, the average of $|\chi(g)|^2$ over all pairs (χ, g) is 1. Of course, this average is over elements rather than conjugacy classes, so a key ingredient of the argument is Proposition 10.1, which implies that, for finite simple groups of Lie type, it does not make much difference which kind of average one takes. This is not true for alternating groups, since the partition associated to a randomly chosen element of S_n has $\log n + o(\log n)$ parts [3], while a typical partition of n has $(\pi^{-1}\sqrt{3/2} + o(1))\sqrt{n}\log n$ parts [2].

To show that $d_{g^G,\chi}$ is usually large, we show that for most choices of (g^G, χ), we can find a large Zsigmondy prime ℓ such $\mathrm{ord}_\ell |g^G| < \mathrm{ord}_\ell \chi(1)$. To do this, we need to have a good qualitative understanding of the degrees of irreducible characters of G. This is provided by the Lusztig theory. In the large q limit, regular semisimple elements and irreducible Deligne-Lusztig characters predominate, and it is relatively easy prove the needed estimates. For fixed q, we have to work harder, but most of what is needed is already available in work of Fulman-Guralnick [4, 5] and Larsen-Shalev [10].

We would like to thank the referee for a number of improvements, especially the argument about Suzuki and Ree groups in Theorem 10.2 below.

2. General framework

A key technical difficulty in implementing our strategy is that in counting conjugacy classes and characters, it is often easier to work not with G but with some closely related group. For instance, for $\mathrm{PSL}_n(\mathbb{F}_q)$, it is easier to study conjugacy classes of $\mathrm{SL}_n(\mathbb{F}_q)$ and characters of $\mathrm{PGL}_n(\mathbb{F}_q)$. To deal with these difficulties, we consider the following general situation. Suppose that we have maps of finite sets

$$\begin{array}{ccccc} \tilde{A} & \xrightarrow{f} & \mathcal{P} & \xleftarrow{g} & \tilde{B} \\ \phi \downarrow & & & & \downarrow \psi \\ A & & & & B \end{array} \tag{2.1}$$

and a subset $X \subset A \times B$. Our goal is to show that, under suitable conditions, $|X|$ is small compared to $|A \times B|$. We say $\mathcal{P}^\circ \subset \mathcal{P}$ and $A^\circ \subset A$ are *compatible*

if $f^{-1}(\mathcal{P}^\circ) = \phi^{-1}(A^\circ)$, and likewise for $\mathcal{P}^\circ$ and B°. In this case, we define $\tilde{A}^\circ \subset \tilde{A}$ (respectively $\tilde{B}^\circ \subset \tilde{B}$) to be this common inverse image.

In the intended application, A will be the set of conjugacy classes of a finite simple group G, B the set of irreducible characters of G, and X, which we want to prove small, will be the set of pairs (g^G, χ) for which $\chi(g) \neq 0$. The precise definitions of $\tilde{A}$, $\tilde{B}$, and $\mathcal{P}$ are given in §5. The definitions of the sets $A^\circ, \tilde{A}^\circ, B^\circ, \tilde{B}^\circ, \mathcal{P}^\circ$ depend on a single parameter as explained in §9.

Proposition 2.1. *There exists an absolute constant N with the following property. For all $\epsilon > 0$ there exists $\delta > 0$ such that given data (2.1), a subset $X \subset A \times B$, and compatible subsets $A^\circ \subset A$, $B^\circ \subset B$, and $\mathcal{P}^\circ \subset \mathcal{P}$ which are compatible and satisfy the following conditions, then $|X| \leq \epsilon |A \times B|$:*

(1) $|A^\circ| > (1-\delta)|A|$.
(2) $|B^\circ| > (1-\delta)|B|$.
(3) For $a_1 \in A^\circ$, $a_2 \in A$ we have $|\phi^{-1}(a_1)| \geq |\phi^{-1}(a_2)|$.
(4) For $b_1 \in B^\circ$, $b_2 \in B$ we have $|\psi^{-1}(b_1)| \geq |\psi^{-1}(b_2)|$.
(5) For all $n \geq N$, $\{P \in \mathcal{P} \mid |f^{-1}(P)| \geq n\}$ has less than $n^{-2}|\mathcal{P}|$ elements.
(6) For all $n \geq N$, $\{P \in \mathcal{P} \mid |g^{-1}(P)| \geq n\}$ has less than $n^{-2}|\mathcal{P}|$ elements.
(7) $|\mathcal{P}| \leq |\tilde{A}|$.
(8) $|\mathcal{P}| \leq |\tilde{B}|$.
(9) The set of pairs $(P_1, P_2) \in \mathcal{P}^\circ \times \mathcal{P}^\circ$ such that $(P_1, P_2) \in (f,g)((\phi,\psi)^{-1}(X))$ has cardinality less than $\delta|\mathcal{P}|^2$.

Proof. By conditions (3) and (4), every (ϕ,ψ)-fiber over $A^\circ \times B^\circ$ has cardinality at least

$$\frac{|\tilde{A} \times \tilde{B}|}{|A \times B|}.$$

Let $x = |X|/|A \times B|$. Then by conditions (1) and (2),

$$|X \cap (A^\circ \times B^\circ)| > (x - 2\delta)|A \times B|,$$

so

$$|(\phi,\psi)^{-1}(X) \cap (\tilde{A}^\circ \times \tilde{B}^\circ)| = |(\phi,\psi)^{-1}(X \cap (A^\circ \times B^\circ))| > (x-2\delta)|\tilde{A} \times \tilde{B}|. \tag{2.2}$$

Let $\mathcal{P}_{f,n}$ denote the set of elements $P \in \mathcal{P}^\circ$ such that $|f^{-1}(P)| = n$. Let $M \geq N$. By condition (5),

$$\begin{aligned} \Big| \bigcup_{n \geq M} f^{-1}(\mathcal{P}_{f,n}) \Big| &= \sum_{n \geq M} n|\mathcal{P}_{f,n}| \\ &= M|\{P \in \mathcal{P}^\circ \mid |f^{-1}(P)| \geq M\}| + \sum_{i=1}^{\infty} |\{P \in \mathcal{P}^\circ \mid |f^{-1}(P)| \geq M+i\}| \\ &\leq \frac{|\mathcal{P}|}{M} + \sum_{i=1}^{\infty} \frac{|\mathcal{P}|}{(M+i)^2} \leq \frac{2|\mathcal{P}|}{M}. \end{aligned} \tag{2.3}$$

Likewise, condition (6) implies

$$|\bigcup_{n\geq M} g^{-1}(\mathcal{P}_{g,n})| \leq \frac{2|\mathcal{P}|}{M}.$$

By inequality (2.2) and conditions (7) and (8), the subset of $(\phi,\psi)^{-1}(X)$ consisting of elements which map by (f,g) to

$$\{P \in \mathcal{P}^\circ \mid |f^{-1}(P)| < M\} \times \{P \in \mathcal{P}^\circ \mid |g^{-1}(P)| < M\}$$

has more than

$$(x - 2\delta - 4M^{-1})|\mathcal{P}|^2$$

elements. On this set the map (f,g) takes at most M^2 elements to any given element, so the cardinality of the image by (f,g) is at least

$$\frac{(x - 2\delta - 4M^{-1})|\mathcal{P}|^2}{M^2}.$$

By condition (9), this must be less than $\delta|\mathcal{P}|^2$, so $x < M^2\delta + 2\delta + 4M^{-1}$. By choosing M larger than N and $8/\epsilon$, we get $x < \epsilon$ if $\delta < \frac{\epsilon}{2M^2+4}$. □

3. Subexponential sequences

In this section, we prove some basic facts about subexponential sequences that will be useful for checking the hypotheses of Proposition 2.1.

We say that a sequence $a_1, a_2, \ldots$ of nonnegative integers is *subexponential* if for all $\gamma > 1$ we have $\lim_{n\to\infty} \gamma^{-n} a_n = 0$. This is equivalent to the condition that $\sum_n a_n z^n$ converges in the open unit disk. It is clear from this criterion that the coefficients of the product of power series with subexponential coefficients again has subexponential coefficients. From the definition, it is clear that the termwise product of subexponential sequences is again subexponential.

Lemma 3.1. *If $(a_i)_{i=1,2,\ldots}$ is subexponential, then the sequence A_m of coefficients of the formal power series*

$$A(z) := \prod_{i=1}^{\infty} (1 - z^i)^{-a_i} = \sum_m A_m z^m$$

is likewise subexponential.

Proof. As $a_i \geq 0$ for all i,

$$A^{(n)}(z) := \prod_{i=1}^{n} (1 - z^i)^{-a_i} = \sum_{m=0}^{\infty} A_m^{(n)} z^m$$

has nonnegative coefficients, and for each $m \geq 0$, the sequence $(A_m^{(n)})_{n=1,2,\ldots}$ is nondecreasing. Therefore, for any $z_0 \in (0,1)$, the sequence $(A^{(n)}(z_0))_{n=1,2,\ldots}$

is nondecreasing. As $A_m = A_m^{(n)}$, for all $n \geq m$, we have

$$A^{(n)}(z_0) \geq \sum_{m=0}^{n} A_m z_0^m.$$

Thus, if $A(z)$ converges at $z = z_0$, then $\lim_{n\to\infty} A^{(n)}(z_0)$ exists and equals $A(z_0)$, and conversely, if $\lim_{n\to\infty} A^{(n)}(z_0)$ exists, then its limit is an upper bound for the increasing sequence of partial sums of $\sum_{m=0}^{\infty} A_m z_0^m$, so this series converges.

As $\lim_{z\downarrow 0} \frac{\log(1-z)}{z} = -1$, the function $\frac{\log(1-z)}{z}$ is bounded on every interval of the form $(0, a] \subset (0, 1)$. Applying this for $a = z_0$, we obtain

$$\log A^{(n)}(z_0) = \sum_{i=1}^{n} -a_i \log(1 - z_0^i) < C \sum_{i=1}^{n} a_i z_0^i,$$

where C depends on z_0 but not on n. As a_i is subexponential, the right hand side in this inequality is bounded independent of n, so the sequence $A^{(n)}(z_0)$ is bounded, so it converges. □

In particular, when $a_i = 1$ for all i, we obtain the well-known fact that the partition function $p(n)$ is subexponential.

Lemma 3.2. *Let $(a_i)_{i=1,2,\ldots}$ and $(b_i)_{i=1,2,\ldots}$ be two sequences of positive integers such that a_i is subexponential and b_i is arbitrary. Define c_k to be the maximum of $\prod_j a_j^{e_j}$ as $1^{e_1}2^{e_2}\cdots$ ranges over all partitions of k with $e_i \leq b_i$ for all i. Then c_k is subexponential.*

Proof. For all $\epsilon > 0$, there exists r such that $a_i < (1+\epsilon)^i$ for $i > r$. Thus

$$c_k < a_1^{b_1} \cdots a_r^{b_r} (1+\epsilon)^k.$$

□

4. Counting polynomials

In this section, we introduce several sets of polynomials which are candidates for the set $\mathcal{P}$ in Proposition 2.1.

For $P(x) \in \mathbb{F}_{q^2}[x]$ a monic polynomial with non-zero constant term, we define

$$P^*(x) := \bar{P}(0)^{-1} x^{\deg P} \bar{P}(1/x), \tag{4.1}$$

where $\bar{P}$ is the polynomial obtained from P by applying the q-Frobenius automorphism to each coefficient. In particular, if $P(x) \in \mathbb{F}_q[x]$, then $P^*(x) = P(0)^{-1} x^{\deg P} P(1/x)$. Note that $P^*(x)$ is a monic polynomial of the same degree as P. If $P(x) = \prod_i (x - r_i)$, then

$$P^*(x) = \prod_i (x - 1/\bar{r}_i) = \prod_i (1 - r_i^{-q}).$$

Therefore, if $P = P^*$, then the roots of P, taken with multiplicity, form a union of orbits in $\bar{\mathbb{F}}_q^{\times}$ under the map $x \mapsto x^{-q}$. Any orbit under this map is

stable by the q^2-Frobenius, so if $P(x)$ is irreducible in $\mathbb{F}_{q^2}[x]$, its roots form a single orbit under $x \mapsto x^{-q}$. If $P(x) \in \mathbb{F}_q[x]$ and P is irreducible as a polynomial over $\mathbb{F}_q$, then it may form one orbit or two mutually reciprocal orbits.

Following [10], we denote by $\mathcal{L}_n(q)$ the set of monic polynomials $P(x) \in \mathbb{F}_q[x]$ of degree n such that $P(0) = (-1)^n$. We define by $\mathcal{U}_n(q)$ the set of monic polynomials $P(x) \in \mathbb{F}_{q^2}[x]$ of degree n such that $P = P^*$ and $P(0) = (-1)^n$. When n is even, we denote by $\mathcal{O}_n(q)$ the set of monic polynomials $P(x) \in \mathbb{F}_q[x]$ of degree n such that $P = P^*$ and $P(0) = 1$. For $c \in \mathbb{F}_q^\times$, we denote by $\mathcal{L}_{n,c}(q)$ the set of monic polynomials $P(x) \in \mathbb{F}_q[x]$ of degree n such that $P(0) = c$. Likewise, for $c \in \mathbb{F}_{q^2}^\times$ with $c\bar{c} = 1$, let $\mathcal{U}_{n,c}(q)$ denote the set of monic polynomials $P(x) \in \mathbb{F}_{q^2}[x]$ of degree n such that $P = P^*$ and $P(0) = c$.

Lemma 4.1. *Let r be a positive integer and q a prime power. Then*

$$|\mathcal{L}_{r+1}(q)| = |\mathcal{U}_{r+1}(q)| = |\mathcal{O}_{2r}(q)| = q^r.$$

Proof. In each case, the leading coefficient and the constant coefficient are fixed. For $\mathcal{L}_{r+1}(q)$, the remaining r coefficients can be chosen independently from $\mathbb{F}_q$. For $\mathcal{U}_{r+1}(q)$, if $0 < i < (r+1)/2$, the x^i coefficient can be any element of $\mathbb{F}_{q^2}$ and it uniquely determines the x^{r+1-i} coefficient. That finishes the $\mathcal{U}$ case if $r+1$ is odd. If it is even, the $x^{\frac{r+1}{2}}$ coefficient can be any element of $\mathbb{F}_q$, so again $|\mathcal{U}_{r+1}(q)| = q^r$. For $\mathcal{O}_{2r}(q)$, the x^i coefficients can be chosen independently from $\mathbb{F}_q$ for $0 < i \leq r$, and the x^i coefficient determines the x^{2r-i} coefficient. □

Proposition 4.2. *There exists a positive real sequence $(\epsilon_i)_{i=1,2,\dots}$ tending to 0 such that all of the following statements hold for all integers $r \geq 1$.*

1. *Let $n = r+1$. If $m > \sqrt{n}$ and $c \in \mathbb{F}_q^\times$, then the number of elements in $\mathcal{L}_{n,c}(q)$ with an irreducible factor whose degree is divisible by m is less than $\epsilon_r|\mathcal{L}_{n,c}(q)|$. Likewise, the number of elements with an irreducible factor whose degree is $> \sqrt{n}$ and divides $\ell - 1$ for some prime divisor ℓ of n is less than $\epsilon_r|\mathcal{L}_{n,c}(q)|$.*
2. *Let $n = r+1$. If $m > \sqrt{n}$ and $c \in \mathbb{F}_{q^2}^\times$ with $c\bar{c} = 1$, then the number of elements in $\mathcal{U}_{n,c}(q)$ with an irreducible factor whose degree is divisible by m is less than $\epsilon_r|\mathcal{U}_{n,c}(q)|$. Likewise, the number of elements with an irreducible factor whose degree is $> \sqrt{n}$ and divides $\ell - 1$ for some prime divisor ℓ of n is less than $\epsilon_r|\mathcal{U}_{n,c}(q)|$.*
3. *Let $n = 2r$. If $m > \sqrt{n}$, then the number of elements in $\mathcal{O}_n(q)$ with an irreducible factor whose degree is divisible by m is less than $\epsilon_r|\mathcal{O}_n(q)|$.*

Proof. A monic irreducible polynomial over $\mathbb{F}_q$ of degree k corresponds to a q-Frobenius orbit of length k in $\bar{\mathbb{F}}_q^\times$. Any such orbit is contained in the $(q^k - 1)$-roots of 1 in $\bar{\mathbb{F}}_q$, so there are less than q^k/k such polynomials.

Therefore, the number of monic polynomials of degree n with constant term c and an irreducible factor of degree k is less than $\frac{q^{n-1}}{k}$. Summing over multiples of m, the number of monic polynomials of degree n with constant term c and an irreducible factor whose degree lies in $m\mathbb{Z}$ is less than

$$\sum_{1\le i\le n/m} \frac{q^{n-1}}{mi} < \frac{q^r(1+\log n)}{m} = \frac{|\mathcal{L}_{n,c}(q)|(1+\log n)}{m},$$

which gives the first claim in part (1). For the second claim, we note that n has at most one prime divisor $\ell > \sqrt{n}$. So it suffices to prove that the sum of $1/m$ over divisors m of n which are larger than $\sqrt{n}$ is $o((1+\log n)^{-1})$. This follows from the fact that the total number of divisors of any integer n is $n^{o(1)}$.

For (2), we proceed in the same way, using the fact that $|\mathcal{U}_{n,c}(q)| = q^{n-1}$. If $Q \in \mathcal{U}_{n,c}(q)$ and P divides Q, then P^* divides Q. It follows that if $P \neq P^*$, then any element of $\mathcal{U}_{n,c}(q)$ divisible by P is the product of PP^* and a polynomial in $\mathcal{U}_{n-2k,cP(0)^{q-1}}$. If $P = P^*$, then any element of $\mathcal{U}_{n,c}(q)$ divisible by P is the product of P and an element of $\mathcal{U}_{n-k,cP(0)^{-1}}$. The first case gives less than

$$\frac{q^{2k}}{k} q^{n-2k-1} = \frac{q^r}{k}$$

elements of $\mathcal{U}_{n,c}(q)$.

For the second term, every monic irreducible degree k polynomial $P(x) \in \mathbb{F}_{q^2}[x]$ such that $P = P^*$ corresponds to a length-k orbit

$$r, r^{-q}, r^{q^2}, \dots, r^{(-q)^k} = r,$$

so r is a $(q^k - (-1)^k)$-root of 1. If $k \ge 2$, the $q+1$ fixed points of $x \mapsto x^{-q}$ do not belong to such an orbit, so the number of orbits is again less than q^k/k, thus contributing less than

$$\frac{q^k}{k} q^{n-k-1} = \frac{q^r}{k}$$

elements of $\mathcal{U}_{n,c}(q)$. The argument therefore goes through as before.

For (3), we follow (2). The number of elements in $\mathcal{O}_n(q)$ is q^r. If a monic polynomial $P(x) \in \mathbb{F}_q[x]$ satisfies $P \neq P^*$ and P divides $Q \in \mathcal{O}_n(q)$, then Q is the product of PP^* and an element of $\mathcal{O}_{n-2k}(q)$. For $k \ge 2$, a monic irreducible polynomial P of degree k satisfying $P = P^*$ must be of even degree, and every element of $\mathcal{O}_n(q)$ divisible by P is the multiple of P by an element of $\mathcal{O}_{n-k}(q)$. By the proof of [10, Prop. 2.6], the number of irreducible monic polynomials of degree $k \ge 4$ satisfying $P = P^*$ is the same as the number of monic irreducible polynomials of degree $k/2$, and for $k = 2$, the number is at most $q-1$. Thus, the argument goes through as before.

□

For any monic polynomial $P(x)$ over a field F, we define $\rho(P)$ to be the sum $\sum_{i=1}^{j} b_i(a_i-1)$, where $P = P_1^{a_1}\cdots P_j^{a_j}$, and the P_i are pairwise distinct monic irreducible polynomials over F of degree b_i. For a perfect field F, $\rho(P)$ does not change if F is replaced by a field extension.

Lemma 4.3. *Let m and n be positive integers.*

1. *The number of polynomials $P \in \mathcal{L}_n(q)$ with $\rho(P) \geq m$ is less than $2q^{-m/2}|\mathcal{L}_n(q)|$.*
2. *The number of polynomials $P \in \mathcal{U}_n(q)$ with $\rho(P) \geq m$ is less than $4q^{-m/2}|\mathcal{U}_n(q)|$.*
3. *If n is even, the number of polynomials $P \in \mathcal{O}_n(q)$ with $\rho(P) \geq m$ is less than $2q^{-m/4}|\mathcal{O}_n(q)|$.*

Proof. Recall that $P = \prod_{i=1}^{j} P_i^{a_i}$, and let

$$Q = \prod_{i=1}^{j} P_i^{\lfloor a_i/2 \rfloor}, \ R = \frac{P}{Q^2}.$$

For claim (2) (resp. (3)), if $P_i^* = P_j$, then $a_i = a_j$, so the multiplicities of P_i and P_j in Q (or in R) are the same. Therefore, $Q \in \mathcal{U}_{\deg Q, Q(0)}(q)$ and $R \in \mathcal{U}_{\deg R, P(0)Q(0)^{-2}}(q)$ (resp. $Q \in \mathcal{O}_{\deg Q}(q)$ and $R \in \mathcal{O}_{\deg R}(q)$.) As

$$\sum_i b_i \lfloor a_i/2 \rfloor \geq \frac{1}{2}\sum_i b_i(a_i-1),$$

we have $\deg Q \geq \rho(P)/2$ and $2\deg Q + \deg R = n$.

For $\mathcal{L}_n(q)$, the total number of possibilities for (Q, R) with $\rho(P) \geq m$ is therefore at most

$$\sum_{i \geq m/2} q^i q^{n-2i-1} < 2q^{n-1-m/2}.$$

For $\mathcal{U}_n(q)$, there are $q+1$ elements $c \in \mathbb{F}_{q^2}$ with $c\bar{c} = 1$, and for each of these $|\mathcal{U}_{k,c}| = q^{k-1}$, so the total number of possibilities for (Q, R) with $\rho(P) \geq m$ is at most

$$\sum_{i \geq m/2} (q+1) q^{i-1} q^{n-2i-1} < 4q^{n-1-m/2}.$$

For $\mathcal{O}_n(q)$, the number of possibilities is at most

$$\sum_{i \geq m/2} q^{i/2} q^{(n-2i)/2} < 2q^{n/2-m/4}.$$

□

With a_i, b_i, and j as above, we define

$$\alpha(P) := \frac{\prod_{i=1}^{j}(1+q^{-b_i})}{1-q^{-1}}.$$

Lemma 4.4. *For all $\epsilon > 0$ there exists M such that for all $n \geq 1$ and all prime powers q:*

(1) *The number of polynomials* $P \in \mathcal{L}_n(q)$ *with* $\alpha(P) < (1+q^{-1})^M$ *is greater than* $(1-\epsilon)|\mathcal{L}_n(q)|$.
(2) *The number of polynomials* $P \in \mathcal{U}_n(q)$ *with* $\alpha(P) < (1+q^{-1})^M$ *is greater than* $(1-\epsilon)|\mathcal{U}_n(q)|$.
(3) *If* n *is even, the number of polynomials* $P \in \mathcal{O}_n(q)$ *with* $\alpha(P) < (1+q^{-1})^M$ *is greater than* $(1-\epsilon)|\mathcal{O}_n(q)|$.

Proof. As there exists C such that $(1-q^{-1})^{-1}\prod_{i\geq 1}(1+q^{-i}) < (1+q^{-1})^C$ for all $q \geq 2$, it suffices to prove that there exists $e \geq 2$ such that the fraction of polynomials P in $\mathcal{L}_n(q)$ (resp. $\mathcal{U}_n(q)$ or $\mathcal{O}_n(q)$) divisible by e different irreducible polynomials of the same degree is less than ϵ. The number of monic irreducible polynomials of degree k in $\mathbb{F}_q[x]$ is less than q^k/k, so the number of sets $\{Q_1, \ldots, Q_k\}$ of e such polynomials is at most $k^{-e}q^{ek}/e!$. For each possibility, there are q^{n-ek-1} choices for the remaining factor $P/\prod_i Q_i$, so there are at most $(k^{-e}/e!)q^{n-1}$ elements of $\mathcal{L}_n(q)$ with e distinct irreducible degree k factors. Summing over k, we get an upper bound of $\zeta(2)q^{n-1}/e!$, and $\zeta(2)/e!$ goes to 0 as e goes to ∞.

For statements (2) and (3) we consider factors of degree k which are either of the form Q, where $Q = Q^*$ is irreducible (in $\mathbb{F}_{q^2}[x]$ or $\mathbb{F}_q[x]$ respectively) or which are of the form QQ^*, where Q is of degree $k/2$ and $Q \neq Q^*$. As in Lemma 4.2, the two cases together contribute less than $2q^k/k$ possibilities. The number of e-element sets of such polynomials is therefore less than $(2k)^{-e}q^{ek}/e!$, and the argument goes through as before. □

Lemma 4.5. *Let* $n \geq 2$ *be an integer and* q *a prime power. The number of elements* $P \in \mathcal{L}_n(q)$ *such that*

$$P(\zeta x) \equiv P(x)$$

for some $\zeta \in \mathbb{F}_q \setminus \{1\}$ *is less than* $2q^{n/2-1}$. *Likewise, the number of elements* $P \in \mathcal{U}_n(q)$ *such that*

$$P(\zeta x) \equiv P(x)$$

for some $\zeta \in \mathbb{F}_{q^2} \setminus \{1\}$ *is less than* $2q^{n/2-1}$.

Proof. In both cases, if $P(\zeta x) \equiv P(x)$ for some $\zeta \neq 1$, then by comparing coefficients, the order $d > 1$ of ζ divides n, and $P(x) = P'(x^d)$ for some element $P' \in \mathcal{L}_{n/d,(-1)^n}(q)$ (resp. $\mathcal{U}_{n/d,(-1)^n}(q)$), for which there are $q^{n/d-1}$ possibilities. So the number of $P \in \mathcal{L}_n(q)$ (resp. $\mathcal{U}_n(q)$) with $P(\zeta x) \equiv P(x)$ for some $\zeta \in \mathbb{F}_q \setminus \{1\}$ (resp. $\mathbb{F}_{q^2} \setminus \{1\}$) is at most

$$\sum_{2 \leq i \leq n/2} q^{n/i-1} < 2q^{n/2-1}.$$

□

5. Classical groups

Finite simple groups G of rank $r > 8$ must be of type A_r, ${}^2A_r$, B_r, C_r, D_r, or ${}^2D_r$. In each case, G is closely related to a *classical group* G',

which we define below. We also define the sets A, $\tilde{A}$, B, $\tilde{B}$, and $\mathcal{P}$ used in Proposition 2.1.

In every case, A denotes the set of conjugacy classes of G and $\tilde{A}$, the set of conjugacy classes of the universal central extension $\tilde{G}$ of G. We denote by Z the center of $\tilde{G}$, so that we can think of $|Z|$ as the "generic" size of the fibers of the map ϕ obtained from the covering homomorphism $\tilde{G} \to G$ by taking conjugacy classes. The map f takes a conjugacy class of $\tilde{G}$ to its characteristic polynomial, with a slight modification when G is of type B.

We can regard G as the commutator group $[\underline{G}_{\mathrm{ad}}(\mathbb{F}_q), \underline{G}_{\mathrm{ad}}(\mathbb{F}_q)]$, where $\underline{G}_{\mathrm{ad}}$ is an adjoint simple algebraic group defined over $\mathbb{F}_q$. We define $B := \mathrm{Irr}(G)$, while $\tilde{B}$ denotes the set of pairs $(\chi, \chi_{\mathrm{ad}}) \in \mathrm{Irr}(G) \times \mathrm{Irr}(\underline{G}_{\mathrm{ad}}(\mathbb{F}_q))$ such that $\langle \chi, \mathrm{Res}_G \chi_{\mathrm{ad}} \rangle_G \geq 1$. We define $\psi(\chi, \chi_{\mathrm{ad}}) := \chi$. The Lusztig classification (see §8 below) assigns to each character χ_{ad} a semisimple conjugacy class in the $\mathbb{F}_q$-points of the dual group to $\underline{G}_{\mathrm{ad}}$. This is a simply connected simple algebraic group of classical type, so it has a natural representation, and we define $g((\chi, \chi_{\mathrm{ad}}))$ to be the characteristic polynomial of this semisimple class in this natural representation, with a slight modification in the case that G is of type C.

We divide into cases. A reference for dual groups for the various groups of classical types is [1, §2].

Case A. In this case, G must be of the form $\mathrm{PSL}_n(\mathbb{F}_q)$ or $\mathrm{PSU}_n(\mathbb{F}_q)$, where $n = r + 1$. We define G' to be $\mathrm{SL}_n(\mathbb{F}_q)$ or $\mathrm{SU}_n(\mathbb{F}_q)$ respectively. As $\underline{G}_{\mathrm{ad}}$ is PGL_n or PGU_n respectively, the dual group $(\underline{G}_{\mathrm{ad}})^*$ is SL_n or SU_n respectively, and $\mathcal{P} = \mathcal{L}_n(q)$. We have $|Z| \leq n$.

Case B. In this case, G is of the form $\Omega_n(\mathbb{F}_q)$, where $n = 2r + 1$, and we define G' to be $\mathrm{SO}_n(\mathbb{F}_q)$. In this case, G' is a subgroup of G of index ≤ 2. As $\underline{G}_{\mathrm{ad}} = \mathrm{SO}_n$, the dual group $(\underline{G}_{\mathrm{ad}})^*$ is Sp_{2r}. The characteristic polynomial of every element of $\mathrm{Sp}_{2r}(\mathbb{F}_q)$ lies in $\mathcal{P} := \mathcal{O}_{2r}(q)$. The characteristic polynomial of every element of $\mathrm{SO}_n(\mathbb{F}_q)$ is $(x - 1)$ times an element of $\mathcal{O}_{2r}(q)$, and we define f as the composition of $\tilde{G} \to G$, $G \to \mathrm{GL}_n(\mathbb{F}_q)$, the characteristic polynomial map, and division by $(x - 1)$. We have $|Z| \leq 2$.

Case C. In this case, G is of the form $\mathrm{PSp}_n(\mathbb{F}_q)$, where $n = 2r$, and we define G' to be $\mathrm{Sp}_n(\mathbb{F}_q)$, so G is the quotient of G by a normal subgroup of order ≤ 2, and f is defined via the usual map $\mathrm{Sp}_n(\mathbb{F}_q) \to \mathcal{O}_n(\mathbb{F}_q)$. As $\underline{G}_{\mathrm{ad}} = \mathrm{PGSp}_n$, the dual group $(\underline{G}_{\mathrm{ad}})^*$ is Spin_{2r+1}. We define the map g by composing the maps $\mathrm{Spin}_{2r+1}(\mathbb{F}_q) \to \mathrm{SO}_{2r+1}(\mathbb{F}_q)$, $\mathrm{SO}_{2r+1}(\mathbb{F}_q) \to \mathrm{GL}_{2r+1}(\mathbb{F}_q)$, the characteristic polynomial map, and division by $(x - 1)$. We have $|Z| \leq 2$.

Case D. In this case, G is of the form $P\Omega_n^{\pm}(\mathbb{F}_q)$, where $n = 2r$, and we define G' to be $\mathrm{SO}_n^{\pm}(\mathbb{F}_q)$, so G is the quotient of a subgroup $\Omega_n^{\pm}(\mathbb{F}_q)$ of index ≤ 2 in G' by a normal subgroup of order ≤ 2. As $\underline{G}_{\mathrm{ad}} = \mathrm{PO}_n^{\pm}$, the dual group $(\underline{G}_{\mathrm{ad}})^*$ is $\mathrm{Spin}_n^{\pm}$. Both f and g are defined by composing $\mathrm{Spin}_n^{\pm}(\mathbb{F}_q) \to \mathrm{SO}_n^{\pm}(\mathbb{F}_q)$, $\mathrm{SO}_n^{\pm}(\mathbb{F}_q) \to \mathrm{GL}_n(\mathbb{F}_q)$, and the characteristic polynomial map, which sends

orthogonal $n \times n$ matrices to elements of $\mathcal{O}_n(q)$. Note that in this case f and g are not surjective. We have $|Z| \leq 4$.

We summarize all this information in the following table.

G	G'	$\tilde{G}$	$\underline{G}_{\mathrm{ad}}$
$\mathrm{PSL}_{r+1}(\mathbb{F}_q)$	$\mathrm{SL}_{r+1}(\mathbb{F}_q)$	$\mathrm{SL}_{r+1}(\mathbb{F}_q)$	PGL_{r+1}
$\mathrm{PSU}_{r+1}(\mathbb{F}_q)$	$\mathrm{SU}_{r+1}(\mathbb{F}_q)$	$\mathrm{SU}_{r+1}(\mathbb{F}_q)$	PGU_{r+1}
$\Omega_{2r+1}(\mathbb{F}_q)$	$\mathrm{SO}_{2r+1}(\mathbb{F}_q)$	$\mathrm{Spin}_{2r+1}(\mathbb{F}_q)$	SO_{2r+1}
$\mathrm{PSp}_{2r}(\mathbb{F}_q)$	$\mathrm{Sp}_{2r}(\mathbb{F}_q)$	$\mathrm{Sp}_{2r}(\mathbb{F}_q)$	PGSp_{2r}
$P\Omega^+_{2r}(\mathbb{F}_q)$	$\mathrm{SO}^+_{2r}(\mathbb{F}_q)$	$\mathrm{Spin}^+_{2r}(\mathbb{F}_q)$	PO^+_{2r}
$P\Omega^-_{2r}(\mathbb{F}_q)$	$\mathrm{SO}^-_{2r}(\mathbb{F}_q)$	$\mathrm{Spin}^-_{2r}(\mathbb{F}_q)$	PO^-_{2r}

Lemma 5.1. *In all four cases, conditions (7) and (8) of Proposition 2.1 hold if $N > 2$.*

Proof. By [4, Theorem 1.1], $k(\tilde{G}) \geq q^r$. By Lemma 4.1,

$$|\tilde{A}| = k(\tilde{G}) \geq q^r = |\mathcal{P}|.$$

This implies condition (7). As the projection map from $\tilde{B}$ to $\mathrm{Irr}(\underline{G}_{\mathrm{ad}}(\mathbb{F}_q))$ is surjective,

$$|\tilde{B}| \geq \mathrm{Irr}(\underline{G}_{\mathrm{ad}}(\mathbb{F}_q)) = k(\underline{G}_{\mathrm{ad}}(\mathbb{F}_q)) \geq q^r = |\mathcal{P}|,$$

again by [4, Theorem 1.1].

□

Proposition 5.2. *Let $G' \subset \mathrm{GL}_n(\mathbb{F}_{q^2})$ be a classical group. The characteristic polynomial of every element of g belongs to $\mathcal{L}_n(q)$, $\mathcal{U}_n(q)$, $(x-1)\mathcal{O}_{n-1}(q)$, $\mathcal{O}_n(q)$, $\mathcal{O}_n(q)$, or $\mathcal{O}_n(q)$ if G' is of type A, ${}^2A$, B, C, D, or ${}^2D$ respectively. Moreover, for each such element, there exist at most 4 semisimple conjugacy classes in G' whose elements have this characteristic polynomial.*

Proof. The first part is well-known; see, e.g., [10]. The second part follows from the following two claims. First, we assert the map from the variety of semisimple conjugacy classes of the underlying linear, unitary, symplectic, or orthogonal algebraic group to the variety of conjugacy classes of GL_n is at most 2 to 1. Second, we assert that the elements of G' in any semisimple conjugacy class of the underlying algebraic group $\underline{G}$ split into at most 2 G'-conjugacy classes.

For the first assertion, we may work over $\mathbb{F}_q$ and fix a maximal torus $\underline{T}$ of $\underline{G}$ which lies in the maximal torus D of diagonal elements in GL_n. Let W denote the Weyl group of $\underline{G}$ with respect to $\underline{T}$ and consider the map $T/W \to D/S_n$. We claim that for any $t \in \underline{T}$, there are at most 2 different W-orbits in $\underline{T} \cap t^{S_n}$. This is obvious for type A. If $n = 2r$, two n-tuples of the form

$$(x_1, x_1^{-1}, \ldots, x_r, x_r^{-1})$$

are the same up to rearrangement if and only if the multisets

$$\{\{x_1, x_1^{-1}\}, \ldots, \{x_r, x_r^{-1}\}\}$$

are the same, and this implies that the n-tuples lie in the same $(\mathbb{Z}/2\mathbb{Z})^r \rtimes S_r$-orbit. This shows that the map $T/W \to D/S_n$ is one-to-one in case C and at most 2 to 1 in case D. If $n = 2r+1$, then two n-tuples

$$(x_1, x_1^{-1}, \dots, x_r, x_r^{-1}, 1)$$

are the same up to rearrangement if and only if the n-tuples lie in the same $(\mathbb{Z}/2\mathbb{Z})^r \rtimes S_r$-orbit, so again the map is one-to-one.

For the second assertion, we use the fact that the map from the universal cover of $\underline{G}$ to $\underline{G}$ is at most 2 to 1. From Steinberg's theorem [17, Theorem 9.1] it follows if $\underline{Z}_s$ is the centralizer of a semisimple element s in $\underline{G}$, then $\underline{Z}_s/\underline{Z}_s^\circ$ is of order 1 or 2. By Lang's theorem, it follows that there are at most two G'-conjugacy classes of elements in G' conjugate to s under $\underline{G}$.

□

6. Unipotent conjugacy classes

Lemma 6.1. *The sequence whose rth term is maximum number of unipotent conjugacy classes in any classical group of rank r over any field $\mathbb{F}_q$ has subexponential growth.*

Proof. By [8, Prop. 2.1], the number of unipotent conjugacy classes in $\mathrm{SL}_n(\mathbb{F}_q)$ is $\leq np(n)$. By [8, Prop. 2.2], the same bound applies for $\mathrm{SU}_n(\mathbb{F}_q)$. By [8, Prop. 2.3], for a symplectic group of rank r, the number of unipotent conjugacy classes is the sum of 2^{a_λ} over partitions λ of $2r$, where a_λ denotes the number of distinct even parts. Since the sum of a_λ distinct positive even integers is at least $a_\lambda^2 + a_\lambda \leq 2r$, it follows that the maximum of 2^{a_λ} is subexponential in r, as is $p(2r)$. By [8, Prop. 2.4], for any orthogonal group of rank r, the number of unipotent conjugacy classes is the sum of 2^{a_λ} over partitions λ of $2r$, where a_λ is one less than the number of odd parts in λ, with the exception that if λ has no odd parts, the summand is either 0 or 1, depending on whether G is of the form SO^- or SO^+.

For G either orthogonal or symplectic and q even, [8, Prop. 3.1] gives a more complicated classification of unipotent conjugacy classes, but the number of representations is certainly bounded above by ordered quadruples of partitions summing to r, which is the z^r coefficient of $\prod_{i=1}^\infty (1-z^i)^{-4}$ and therefore subexponential in r.

□

Proposition 6.2. *For all $\epsilon > 0$ there exists N with the following property. For any finite field $\mathbb{F}_q$, any $n > N$, and any semisimple element s in a classical subgroup $G' = \underline{G}'(\mathbb{F}_q)$ of $\mathrm{GL}_n(\mathbb{F}_q)$, let $\underline{H}$ be the centralizer of s in $\underline{G}'$, $\underline{H}^\circ$ the identity component of $\underline{H}$, $\underline{S}$ the derived group of $\underline{H}^\circ$, and r the absolute rank of $\underline{S}$. Then the number of $\underline{H}(\mathbb{F}_q)$-conjugacy classes of unipotent elements in $\underline{H}^\circ(\mathbb{F}_q)$ is less than $q^{\epsilon r}$. The analogous statement is also true when $\underline{H}$ is the centralizer of a semisimple element s in $G' = \mathrm{SU}_n(\mathbb{F}_q)$.*

Proof. It suffices to prove that the number of conjugacy classes of unipotent elements in $\underline{H}^\circ(\mathbb{F}_q)$ is subexponential. As $\underline{H}^\circ/\underline{S}$ is diagonal, every unipotent

element of $\underline{H}^\circ(\mathbb{F}_q)$ lies in $\underline{S}(\mathbb{F}_q)$. Thus it suffices to prove a subexponential bound for the unipotent conjugacy classes of $\underline{S}(\mathbb{F}_q)$.

We decompose the natural representation space of $\mathbb{F}_q^n$ of $\mathrm{GL}_n(\mathbb{F}_q)$ by s into s-isotypic factors $V_Q \cong W_Q^{a_Q}$ indexed by monic irreducible polynomials $Q(x) \in \mathbb{F}_q[x]$ and denote by b_Q the dimension $\dim W_Q = \deg Q$. If $G' = \mathrm{SL}_n(\mathbb{F}_q)$, then

$$\underline{S} = \prod_Q \mathrm{Res}_{\mathbb{F}_{q^{b_Q}}/\mathbb{F}_q} \mathrm{SL}_{a_Q,\mathbb{F}_q},$$

where Res denotes restriction of scalars. Each factor is of rank $b_Q(a_Q - 1)$ over $\mathbb{F}_q$, so the rank of $\underline{S}$ is $\rho(P)$, where P is the characteristic polynomial of s.

For orthogonal groups G', let Π denote the set of orbits for the involution $Q \mapsto Q^*$ defined in (4.1). For $\pi \in \Pi$, we denote by V_π, W_π, a_π, and b_π the sum $\bigoplus_{Q\in\pi} V_Q$, $\bigoplus_{Q\in\pi} W_Q$, $a_Q = a_{Q^*}$, and $\dim W_\pi$ respectively. As s preserves the inner product $\langle\,,\,\rangle$, we have $V_Q \perp V_R$ unless Q and R belong to the same orbit, so the centralizer of s in G' is

$$\prod_{\pi\in\Pi} \mathrm{Aut}_{\mathbb{F}_{q^{b_\pi}}}(V_\pi, \langle\,,\,\rangle). \tag{6.1}$$

The derived group of the identity component is therefore a product of simple algebraic groups $\underline{S}_\pi$ indexed by $\pi \in \Pi$. If $\pi = \{x-1\}$ or $\pi = \{x+1\}$, then $\underline{S}_\pi$ is of absolute rank $\lfloor a_x/2 \rfloor$ and of type D or B as a_x is even or odd. Otherwise, it is of type D or A, depending on whether π has one element or two and of absolute rank $b_\pi(a_\pi - 1)$ in either case. For symplectic groups, we proceed in the same way, with the difference that polynomials $Q = Q^*$ give rise to factors of type C.

For unitary groups, G' acts on an n-dimensional vector space over $\mathbb{F}_{q^2}$. We decompose $\mathbb{F}_{q^2}^n$ into isotypical spaces $V_Q \cong W_Q^{a_Q}$ for the action of s, where Q ranges over monic irreducible polynomials in $\mathbb{F}_{q^2}[x]$. Let Π denote the set of orbits of $\{Q \mid a_Q > 0\}$ under $Q \mapsto Q^*$. Let $W_\pi = \bigoplus_{Q\in\pi} W_Q$ and $V_\pi = \bigoplus_{Q\in\pi} V_Q = W_\pi^{a_\pi}$. Let $\langle\,,\,\rangle$ denote the sesquilinear form which G' respects. The different V_π are mutually orthogonal with respect to this form, and the centralizer of s in G' is again given by (6.1). The derived group is therefore a product of simple algebraic groups indexed by Q, and each is of type A and absolute rank $b_\pi(a_\pi - 1)$, where $b_\pi = \dim W_\pi$.

In every case, therefore, $\underline{S}(\mathbb{F}_q)$ is a product of classical groups of total rank $r \le \rho(P)$. The number of unipotent conjugacy classes is therefore $\le \prod_Q c_{b_Q}$, where $(c_i)_{i=1,2,\dots}$ is the subexponential sequence given by Lemma 6.1. By Lemma 3.2, for any fixed q, the number of conjugacy classes is $O(q^{\epsilon r/2})$ and therefore less than $q^{\epsilon r}$ if r is sufficiently large. On the other hand, there exists α such that $c_i < \alpha^i$ for all i. If $q > \alpha^{1/\epsilon}$, then the number of conjugacy classes is less than or equal to $\alpha^r \le q^{\epsilon r}$.

□

7. Unipotent characters

Let $\underline{G}$ be a connected reductive group over $\mathbb{F}_q$. Following Lusztig [13], we say that an irreducible character of $\underline{G}(\mathbb{F}_q)$ is *unipotent* if it appears with nonzero multiplicity in the Deligne-Lusztig character $R_{\underline{T}}^{\underline{G}}(1)$ associated to the trivial character on maximal torus $\underline{T}(\mathbb{F}_q)$. In particular, the trivial character is unipotent. The classication of unipotent characters depends only on the adjoint quotient of $\underline{G}$ (see [14, Remark]), therefore only on the root system of $\underline{G}$ together with Frobenius action.

Assuming $\underline{G}$ has connected center, Lusztig gave [13, p. x] a "Jordan decomposition" of irreducible characters χ of $\underline{G}(\mathbb{F}_q)$. We briefly recall the setup, referring the reader to [13] for details. Each such character has nonzero multiplicity in some Deligne-Lusztig character $R_{\underline{G}}^{\underline{T}}(\theta)$, and θ determines a semisimple element t of the dual group $\underline{G}^*(\mathbb{F}_q)$, where $\underline{G}^*$ is the connected reductive algebraic group over $\mathbb{F}_q$ whose root datum is dual to that of $\underline{G}$, with corresponding Frobenius action. The element t is well-defined up to conjugacy class by χ. As $\underline{G}$ has connected center, the derived group of $\underline{G}^*$ is simply connected, so choosing a representative t, the centralizer $\underline{H}^*$ of t in $\underline{G}^*$ is a connected reductive group. If $\underline{H}$ denotes the dual group of $\underline{H}^*$, there is a bijective correspondence $\pi \mapsto \chi_\pi$ between the set of unipotent characters π of $\underline{H}(\mathbb{F}_q)$ and the set $\mathcal{E}(t)$ of irreducible characters χ_π of $\underline{G}(\mathbb{F}_q)$ associated to the class of t. For us, the most important point is that

$$\chi_\pi(1) = \frac{|\underline{G}(\mathbb{F}_q)|'}{|\underline{H}(\mathbb{F}_q)|'}\pi(1), \tag{7.1}$$

where m' denotes the largest divisor of m prime to q.

We record the following consequence.

Lemma 7.1. *If χ_{ad} is a character of $\underline{G}_{\mathrm{ad}}(\mathbb{F}_q)$ associated to the class of a semisimple element $t \in (\underline{G}_{\mathrm{ad}})^*(\mathbb{F}_q)$, and if the order of the centralizer of t is not divisible by a prime $\ell \nmid q$, then*

$$\mathrm{ord}_\ell \chi_{\mathrm{ad}}(1) = \mathrm{ord}_\ell |\underline{G}_{\mathrm{ad}}(\mathbb{F}_q)|.$$

Proof. As $\ell \nmid q$, we have $\mathrm{ord}_\ell |\underline{G}_{\mathrm{ad}}(\mathbb{F}_q)| = \mathrm{ord}_\ell |\underline{G}_{\mathrm{ad}}(\mathbb{F}_q)|'$. Defining π so that $\chi_{\mathrm{ad}} = \chi_\pi$, by (7.1),

$$\mathrm{ord}_\ell \chi_{\mathrm{ad}}(1) = \mathrm{ord}_\ell |\underline{G}_{\mathrm{ad}}(\mathbb{F}_q)| \pi(1) \geq \mathrm{ord}_\ell |\underline{G}_{\mathrm{ad}}(\mathbb{F}_q)|.$$

The opposite inequality follows from the fact that $\chi_{\mathrm{ad}}(1)$ divides $|\underline{G}_{\mathrm{ad}}(\mathbb{F}_q)|$. □

Proposition 7.2. *For all $\epsilon > 0$ there exists N with the following property. For any finite field $\mathbb{F}_q$, any $r > N$, any adjoint simple group $\underline{G}$ over $\mathbb{F}_q$ of type A, B, C, or D, and any semisimple element $t \in \underline{G}^*(\mathbb{F}_q)$, such that the centralizer of t in $\underline{G}^*$ has absolute semisimple rank r, the number of elements in $\mathcal{E}(t)$ is less than $q^{\epsilon r}$.*

Proof. The proof is essentially the same as that of Proposition 6.2. The only difference is that instead of Lemma 6.1, we use a subexponential estimate for the number of unipotent characters of a classical simple group of rank r. The number of unipotent characters is independent of q. For special linear and unitary groups, it is given by the partition function $p(r)$ [13, p. 358]. For orthogonal and symplectic groups, there are at most two different unipotent characters associated to a Lusztig symbol of rank r [13, p. 359]. The number of such symbols grows subexponentially by [12, Prop. 3.4] and Proposition 3.1. □

The irreducible characters of the finite simple group G can be regarded as the Z-trivial characters of $\tilde{G}$, where Z is the center of $\tilde{G} = \underline{G}_{\mathrm{sc}}(\mathbb{F}_q)$. By [14, Prop. 5.1], $\mathrm{Irr}(\tilde{G})$ can be decomposed into rational Lusztig series $\mathcal{E}(s)$ indexed by semisimple conjugacy classes in $(\underline{G}_{\mathrm{sc}})^*(\mathbb{F}_q)$. Moreover, the conjugation action of $\underline{G}_{\mathrm{ad}}(\mathbb{F}_q)/G$ on $\mathrm{Irr}(G)$ preserves this decomposition, and the orbits corresponding to elements of $t \in (\underline{G}_{\mathrm{sc}})^*(\mathbb{F}_q)$ with connected centralizer are singletons. For such s, therefore, each character of G extends to $|Z|$ different characters of $\underline{G}_{\mathrm{ad}}(\mathbb{F}_q)$, obtained from one another by tensor product by 1-dimensional characters of $\underline{G}_{\mathrm{ad}}(\mathbb{F}_q)/G$ (which are necessarily trivial on G). Thus the correspondence between $\mathrm{Irr}(\underline{G}_{\mathrm{ad}}(\mathbb{F}_q))$ and $\mathrm{Irr}(G)$ is given by a function (namely, restriction) on the complement of the set of characters of $\mathrm{Irr}(G)$ corresponding to t with disconnected centralizer. If $\tilde{t} \in (\underline{G}_{\mathrm{ad}})^*(\mathbb{F}_q)$ is a lift of t to an element on the universal cover, then t fails to have connected centralizer only if the multiple of $\tilde{t}$ by some non-trivial central element is conjugate to $\tilde{t}$ and therefore only if the characteristic polynomial of $\tilde{t}$ is a polynomial $P(x)$ satisfying $P(\zeta x) \equiv P(x)$ for some $\zeta \neq 1$.

8. Zsigmondy primes

We recall that given q and m, a *Zsigmondy prime for the pair* (q, m) is a prime ℓ such that q has order exactly m in $\mathbb{F}_\ell^\times$. Zsigmondy's theorem asserts that such a prime always exists if $m > 6$.

Lemma 8.1. *If ℓ is a Zsigmondy prime for (q, m), then ℓ divides $q^k - 1$ if and only if m divides k, and ℓ divides $q^k + 1$ if and only if $2 \mid m$ and k is an odd multiple of $m/2$.*

Proof. The condition that ℓ divides $q^k - 1$ is equivalent to the condition that the kth power of q in $\mathbb{F}_\ell^\times$ is 1, i.e., that m divides k. The condition that ℓ divides $q^k + 1$ is equivalent to the condition that m divides $2k$ but not k, i.e., $dm = 2k$ for some odd integer d. Equivalently k is an odd multiple of $m/2$. □

Lemma 8.2. *If a semisimple element $s \in \mathrm{SL}_n(\mathbb{F}_q)$ has characteristic polynomial P, $m > 2\rho(P)$, and no irreducible factor of P has degree a multiple of m, then any Zsigmondy prime ℓ for (q, m) is relatively prime to the order*

of the centralizer of s in $\mathrm{SL}_n(\mathbb{F}_q)$. Likewise, if $m > 4\rho(P)$, $s \in \mathrm{SU}_n(\mathbb{F}_q)$, and no irreducible $\mathbb{F}_{q^2}[x]$ factor of P has degree an integer multiple of $m/2$, then any Zsigmondy prime ℓ for (q,m) is relatively prime to the order of the centralizer of s in $\mathrm{SU}_n(\mathbb{F}_q)$.

Proof. For $\mathrm{SL}_n(\mathbb{F}_q)$, it suffices to prove that ℓ does not divide the order of the centralizer of s in $\mathrm{GL}_n(\mathbb{F}_q)$. Factoring

$$P = \prod_{i=1}^{j} Q_i^{a_i},$$

with $\deg Q_i = b_i$, the centralizer of s can be written

$$\prod_{i=1}^{j} \mathrm{GL}_{a_i}(\mathbb{F}_{q^{b_i}}).$$

For each i, $b_i(a_i - 1) \le \rho(P)$, so if $a_i \ge 2$, we have $a_i b_i \le 2\rho(P) < m$, so

$$|\mathrm{GL}_{a_i}(\mathbb{F}_{q^{b_i}})| = \prod_{k=0}^{a_i-1} q^{b_i k}(q^{b_i(a_i-k)} - 1)$$

is prime to ℓ. If $a_i = 1$, then $\mathrm{GL}_1(\mathbb{F}_{q^{b_i}})$ has order $q^{b_i} - 1$ which is again prime to ℓ.

For $\mathrm{SU}_n(\mathbb{F}_q)$, we proceed as before, computing the centralizer of s in $U_n(\mathbb{F}_q)$ as in Proposition 6.2. In this case, the centralizer factors are of the form $U_{a_i}(\mathbb{F}_{q^{b_i}})$ or $\mathrm{GL}_{a_i}(\mathbb{F}_q^{2b_i})$ depending on whether $Q_i = Q_i^*$. As $a_i \ge 2$ implies $2a_ib_i \le 4\rho(P) < m$, it follows that no Zsigmondy prime for (q,m) can divide the order of a factor of either kind, so we may assume $a_i = 1$. As b_i is not a multiple of $m/2$, ℓ divides neither the order of $\mathrm{GL}_1(\mathbb{F}_q^{2b_i})$ nor $U_1(\mathbb{F}_q^{b_i})$.

□

We remark that if ℓ is a Zsigmondy prime for (q,m), then m divides $\ell - 1$.

9. Weak regularity conditions

Let $k \ge 1$ and $m \ge 0$ be integers. We say a polynomial $P(x) \in \bar{\mathbb{F}}_q[x]$ is *m-regular* if the following two conditions hold:

(1) $\rho(P) \le m$.
(2) $P(x)$ is not identical to $P(\zeta x)$ for any $\zeta \ne 1$.

If the characteristic polynomial of an element in $\mathrm{GL}_n(\bar{\mathbb{F}}_q)$ is m-regular, we say that this element is m-regular. This depends only on the semisimple part s in the Jordan decomposition of the element. Likewise, we say an irreducible character of $\underline{G}_{\mathrm{ad}}(\mathbb{F}_q)$ is m-regular if and only if it belongs to $\mathcal{E}(s)$, where the characteristic polynomial of the image of s under the natural representation of $(\underline{G}_{\mathrm{ad}})^*(\mathbb{F}_q)$ is m-regular.

Let G be a classical finite simple group. We define G', A, $\tilde{A}$, B, $\tilde{B}$, $\mathcal{P}$ as in §5. Given a fixed choice of m, we define $\mathcal{P}^\circ$ to be the subset of m-regular polynomials in $\mathcal{P}$, $\tilde{A}^\circ := f^{-1}(\mathcal{P}^\circ)$, $A^\circ := \phi(\tilde{A}^\circ)$, $\tilde{B}^\circ := g^{-1}(\mathcal{P}^\circ)$, $B^\circ := \psi(\tilde{B}^\circ)$. Note that $\phi^{-1}(A^\circ) = \tilde{A}^\circ$ since $\rho(P(x)) = \rho(\omega^{-\deg P} P(\omega x))$ for all scalars $\omega \neq 0$. Likewise, $\psi^{-1}(B^\circ) = \tilde{B}^\circ$, since if $(\chi, \chi_{\mathrm{ad}})$ and $(\chi, \chi'_{\mathrm{ad}})$ both lie in $\tilde{B}$, and $s \in \tilde{G}$ lies in the semisimple class associated to χ_{ad}, then there exists $z \in Z$ such that zs lies in the semisimple class associated to χ'_{ad}.

By definition, the image of any element of $\tilde{A}^\circ$ in G' is m-regular. Part (2) of the definition of m-regularity guarantees that the fibers of ϕ over A° and of ψ over B° all have exactly $|Z|$ elements, where Z is the center of $\tilde{G}$. Since $\tilde{G} \to G$ is $|Z|$ to 1 and G is of index $|Z|$ in $\underline{G}_{\mathrm{ad}}(\mathbb{F}_q)$, all fibers of ϕ and ψ have cardinality $\leq |Z|$. This gives conditions (3) and (4) of Proposition 2.1.

If $s \in G'$ is semisimple and m-regular, its centralizer in G' is the group of $\mathbb{F}_q$-points of a reductive algebraic group $\underline{H}$ over $\mathbb{F}_q$. We have seen that $\underline{H}$ has at most 2 components, so if q is odd, every unipotent element $u \in G'$ which commutes with s lies in $\underline{H}^\circ(\mathbb{F}_q)$. If q is even, we can regard G' as the group of $\mathbb{F}_q$-points of a simply connected semisimple group, so the centralizer of s is connected, and again $u \in \underline{H}^\circ(\mathbb{F}_q)$. To bound the number of G'-conjugacy classes of elements in G' with semisimple part conjugate to s, it suffices to bound the $\underline{H}^\circ(\mathbb{F}_q)$-conjugacy classes of unipotent elements in $\underline{H}^\circ(\mathbb{F}_q)$. By Proposition 6.2, we have a subexponential bound for this quantity. As the homomorphism $\tilde{G} \to G'$ is at most 2 to 1, we have a subexponential bound in m for the number of elements of $\tilde{A}^\circ$ mapping to any element of $\mathcal{P}^\circ$, the set of m-regular polynomials in $\mathcal{P}$. Likewise, by Proposition 7.2, we have a subexponential bound for the number of elements of $\tilde{B}^\circ$ mapping to any element of $\mathcal{P}^\circ$.

By Lemma 4.3, the fraction of elements P of $\mathcal{P}$ with $\rho(P) \geq m$ is less than or equal to $4 \cdot 2^{-m/4}$. There exists a subexponential sequence $\sigma_1, \sigma_2, \ldots$ such that

$$|f^{-1}(P)|,\ |g^{-1}(P)| \leq \sigma_m$$

if $\rho(P) \leq m$, so there exists N for which conditions (5) and (6) of Proposition 2.1 hold. Each element in $\tilde{A} \setminus \tilde{A}^\circ$ either has ρ-invariant greater than m or has invariant $\leq m$ but satisfies $P(x) \equiv P(\zeta x)$ for some $\zeta \neq 1$. If m is sufficiently large in absolute terms, we may assume that the contribution of all elements with ρ-invariant greater than m to either $\tilde{A}$ or $\tilde{B}$ represents less than a $\delta/2$ fraction of the total elements of $\tilde{A}$ or $\tilde{B}$ respectively. Once m is fixed, we have an upper bound for the size of fibers of f or g, so if q^n is sufficiently large, Lemma 4.5 implies that the contribution of all fibers of all elements of P with $P(x) \equiv P(\zeta x)$, as ζ ranges over all elements other than 1, is again less than a $\delta/2$ fraction of the elements of $\tilde{A}$ or $\tilde{B}$. To summarize, we have proven the following.

Proposition 9.1. *If G is sufficiently large, for all $\delta > 0$ if m is chosen to be sufficiently large, conditions (1)–(6) of Proposition 2.1 hold for $\mathcal{P}^\circ$ defined by m-regularity.*

10. End of the proof

Proposition 10.1. *For all $\epsilon > 0$, there exists C such that if G is a classical finite simple group of rank r, the fraction of elements $P \in \mathcal{P}$ such that some element of $f^{-1}(P)$ has centralizer order greater than Cq^r in $\tilde{G}$ is less than ϵ.*

Proof. By Lemma 4.3, if $q > 8/\epsilon$, the fraction of elements $P \in \mathcal{P}$ for which $\rho(P) > 0$ is less than $\epsilon/2$. When $\rho(P) = 0$, the centralizer of every element of $f^{-1}(P)$ is the group of $\mathbb{F}_q$-points of a maximal torus. We claim that this group has order $\leq \alpha(P)q^r$. For semisimple $s \in \mathrm{SL}_{r+1}(\mathbb{F}_q)$ with characteristic polynomial $Q_1 \cdots Q_j$, Q_i irreducible, the order of the centralizer of s is

$$\frac{\prod_{i=1}^j (q^{\deg Q_i} - 1)}{q-1} \leq (1 - q^{-1})^{-1} q^r \leq \alpha(P) q^r.$$

For semisimple $s \in \mathrm{SU}_{r+1}(\mathbb{F}_q)$ with characteristic polynomial $Q_1 \cdots Q_j$, the order of the centralizer is

$$\frac{\prod_{i=1}^j (q^{\deg Q_i} - (-1)^{\deg Q_i})}{q+1} \leq \alpha(P) q^r.$$

For $\mathrm{SO}_{2r+1}(\mathbb{F}_q)$, $\mathrm{Sp}_{2r}(\mathbb{F}_q)$ or $\mathrm{SO}^{\pm}_{2r}(\mathbb{F}_q)$ every irreducible $Q_i = Q_i^*$ of degree ≥ 2 contributes a factor of $q^{\deg Q_i/2} - 1$, while every pair $\{Q_i, Q_j\}$ with $Q_j = Q_i^*$ contributes a factor of $q^{\deg Q_i} + 1 = q^{\deg Q_j} + 1$, so the centralizer order is less than $\alpha(P)q^r$.

By Lemma 4.4, if q is sufficiently large, we may assume $\alpha(P) < 2$ for all but an $\epsilon/2$ fraction of elements of $\mathcal{P}$, and the lemma follows. It therefore suffices to prove the lemma when q is fixed. By Lemma 4.3, we may additionally assume $\rho(P)$ is bounded. We can therefore factor P as a product of two polynomials, a square-free factor Q and a factor R relatively prime to Q and of bounded degree. The centralizer of s is therefore a product of a torus with $\leq \alpha(Q)q^{r-r_0}$ elements, and a connected reductive group of rank r_0, with a bounded number of elements. This gives the desired bound. □

The following theorem is not needed for the main result but may be of interest in its own right.

Theorem 10.2. *For all $\epsilon > 0$ there exists $\delta > 0$ such that if G is a finite simple group of Lie type, and S is a normal subset of G with less than $\delta|G|$ elements, then S consists of less than $\epsilon k(G)$ conjugacy classes.*

Proof. First we assume that G is of type A–D and of sufficiently high rank, so we are in the setting of Proposition 2.1. Let $T \subset A$ denote the set of conjugacy classes in G corresponding to elements of S. By construction, the

cardinality of any fiber of $\phi\colon \tilde{A} \to A$ over A° is $|Z|$. By Proposition 9.1, hypotheses (1) and (3) of Proposition 2.1 hold when $\tilde{A} = \tilde{G}^{\tilde{G}}$ and $A = G^G$. Choosing the parameter δ of this proposition sufficiently small, we may assume that $|\phi^{-1}(T)| > |Z||T|/2$.

Let $\tilde{S}$ denote the inverse image of S in $\tilde{G}$, so $|\tilde{S}|/|\tilde{G}| = |S|/|G|$. Let $\tilde{T} \subset \tilde{A}$ denote the set of conjugacy classes in $\tilde{G}$ corresponding to elements of $\tilde{S}$. Then $\tilde{T} = \phi^{-1}(T)$, so

$$\frac{|\tilde{T}|}{|\tilde{A}|} > \frac{|Z||T|}{2|\tilde{A}|} \geq \frac{|T|}{2|A|}.$$

It therefore suffices to prove that for all $\epsilon > 0$ there exists $\delta > 0$ such that for all normal subsets $\tilde{S}$ of $\tilde{G}$ with $|\tilde{S}| \leq \delta|\tilde{G}|$ elements, the number $|\tilde{T}|$ of conjugacy classes in $\tilde{S}$ is $\leq \epsilon|\tilde{A}| = \epsilon k(\tilde{G})$.

By Proposition 10.1, fixing C sufficiently large, the fraction of elements in $\mathcal{P}$ whose fibers have elements with centralizer order greater than Cq^r is as small as desired. By inequality (2.3) and condition (7), the fraction of elements in $\tilde{G}$ with centralizer order greater than Cq^r is likewise as small as desired. Therefore, we may assume that in any normal subset $\tilde{S}$ of $\tilde{G}$ containing $\epsilon k(\tilde{G})$ conjugacy classes, at least $\epsilon k(\tilde{G})/2$ have centralizer order $\leq Cq^r$. These account for at least

$$\frac{\epsilon k(\tilde{G})|\tilde{G}|}{2Cq^r}$$

elements in $\tilde{S}$. By [4, Theorem 1.1], $k(\tilde{G}) \geq q^r$, so we may take $\delta := \epsilon/2C$. This leaves the bounded rank case.

In the limit as $q \to \infty$, the fraction of elements of $\tilde{G}$ which are regular semisimple goes to 1. The centralizers of any semisimple element is connected reductive, and for regular semisimple elements, the centralizer is a torus and therefore has at most $(q+1)^r$ elements. As r is fixed, this gives an upper bound of the form Cq^r. Thus, the above claim for $\tilde{S}$ holds as in the high rank classical case.

In the large q limit, the fraction of elements g of $\tilde{G}$ which are conjugate to gz for some non-trivial central element $z \in Z$ goes to 0, essentially by the uniform version of the Lang-Weil estimate. The precise statement we want is that if $\mathcal{G}$ is a split, simply connected, semisimple group scheme over $\operatorname{Spec}\mathbb{Z}$, $\mathcal{H}$ is a closed subscheme of $\mathcal{G}$, p is a rational prime such that $\mathcal{H}(\bar{\mathbb{F}}_p)$ is a proper subset of $\mathcal{G}(\bar{\mathbb{F}}_p)$, and F is a generalized Frobenius map (possibly of Suzuki-Ree type), then the fraction of elements of $\mathcal{G}(\bar{\mathbb{F}}_p)^F$ which lie in $\mathcal{H}(\bar{\mathbb{F}}_p)$ goes to zero as the degree of F goes to ∞, independently of the value of p. A proof of this statement is given in [9, Prop. 3.4]. The proposition is proved in the setting that $\mathcal{G}$ is a power of a simple group scheme and $\mathcal{H}$ is the fiber of a word map, but the proof makes no use of these assumptions. In the complement of the set of elements g which are conjugate to gz, the map from conjugacy classes of $\tilde{G}$ to conjugacy classes of G is $|Z|$ to 1. Thus,

the theorem for S again reduces to the claim for $\tilde{S}$, just as in the classical case.

For Suzuki and Ree groups, the proof of [9, Prop. 3.4] uses deep algebraic geometry, and we are grateful to the referee for pointing out the following direct proof. For G of type ${}^2B_2(q^2)$, ${}^2G_2(q^2)$, and ${}^2F_4(q^2)$ respectively, by [11], the number of conjugacy classes (regular semisimple conjugacy classes) is q^2+3 (q^2-1), q^2+8 (q^2-2), and q^4+2q^2+17 (q^4-2q^2+1) respectively. Therefore, if q is sufficiently large, the number of conjugacy classes in S which are not regular semisimple is less than $\delta k(G)$. Again, if q is sufficiently large, the number N of regular semisimple conjugacy classes in S satisfies

$$\frac{N|G|}{q^r} \leq 1.5|S| < 1.5\delta|G|,$$

so $N < 1.5\delta q^r < 2\delta k(G)$. Choosing $\delta < \epsilon/3$ small enough that q must be sufficiently large, we conclude that together the number of conjugacy classes in S is less than $3\delta k(G) < \epsilon k(G)$. □

We now prove Theorem 1.1.

Proof. We need only prove that given $\epsilon > 0$, if $|G|$ is sufficiently large, we can choose $\delta > 0$ and then m so that for $\mathcal{P}^\circ$ defined by m-regularity, condition (9) of Proposition 2.1 holds.

For all $k > 0$ there exists N such if $n \geq 2$ and q is a prime power, then the fraction of elements of $\mathcal{L}_n(q), \mathcal{U}_n(q)$, or $\mathcal{O}_n(q)$ with more than $N \log n$ factors is less than n^{-k} [10, Prop. 2.4–2.6]. Therefore, for every k, for sufficiently large n, in any of these groups, the fraction of elements with no irreducible factor of degree $> 2\sqrt{n}$ is less than n^{-k}, which can be taken as small as we wish. In the case that G is of linear or unitary type, by Lemma 4.2, we may further assume that no prime factor of n is $\equiv 1$ modulo the degree of an irreducible factor with degree $> 2\sqrt{n}$. Assuming $P_1 \in \mathcal{P}^\circ$ has an irreducible factor Q of degree $> 2\sqrt{n}$, then by Lemma 4.2, the fraction of elements $P_2 \in \mathcal{P}^\circ$ such that P_2 has an irreducible factor whose degree is an integer multiple of $\deg Q/2$ goes to 0 as $n \to \infty$. By Lemma 8.2, if $\epsilon_1 > 0$ and n is sufficiently large, at least a $1 - \epsilon_1$ fraction of pairs $(P_1, P_2) \in \mathcal{P}^2$ have the property that if $s_i \in \tilde{G}$ is semisimple and maps to P_i for $i = 1$ and $i = 2$, then there exists a prime ℓ such that

$$\ell \mid |Z_{\tilde{G}}(s_1)|,\ \ell \nmid |Z_{\tilde{G}}(s_2)|. \tag{10.1}$$

By construction, ℓ does not divide n.

To prove condition (9), we may partition the set

$$\{(P_1, P_2) \in \mathcal{P}^\circ \times \mathcal{P}^\circ \mid (P_1, P_2) \in (f, g)((\phi, \psi)^{-1}(X))\}$$

into two subsets, one consisting of pairs satisfying (10.1) and one consisting of pairs which do not satisfy it. We have already bounded the latter set, and it suffices to prove that for $\epsilon_2 > 0$, if n is sufficiently large, the first set has less than $\epsilon_2|\mathcal{P}|^2$ elements. Suppose that this is not the case.

If (P_1, P_2) belongs to the subset satisfying (10.1), choose $\tilde{g}^{\tilde{G}} \in \tilde{A}$ lying over P_1 and $(\chi, \chi_{\mathrm{ad}})$ in $\tilde{B}$ lying over P_2 such that $\chi(g) \neq 0$, where $g^G = \phi(\tilde{g}^{\tilde{G}})$. We denote the semisimple conjugacy class of $\tilde{G} = (\underline{G}_{\mathrm{ad}})^*(\mathbb{F}_q)$ associated to χ_{ad} by $t^{\tilde{G}}$, so the image of t in its natural representation has characteristic polynomial P_2. By Lemma 8.1, there exists a Zsigmondy prime $\ell > \sqrt{n}$ which divides the order of the centralizer of g in G but not the order of the centralizer of t in $\tilde{G}$. Therefore,

$$\mathrm{ord}_\ell |g^G| < \mathrm{ord}_\ell |G| \ = \mathrm{ord}_\ell |\tilde{G}| = \mathrm{ord}_\ell \chi_{\mathrm{ad}}(1).$$

The fraction $\chi_{\mathrm{ad}}(1)/\chi(1)$ is an integer dividing the order of the center of $\tilde{G}$ and therefore not divisible by ℓ, so ℓ divides $d_{g^G,\chi}$. As the map ϕ is at most $|Z|$ to 1, we obtain at least $\epsilon_2 |\mathcal{P}|^2/|Z|$ such pairs (g^G, χ).

For any $\alpha \in \mathbb{Q}(\zeta_{|G|})$, let $T(\alpha)$ denote the normalized trace

$$\frac{1}{[\mathbb{Q}(\zeta_{|G|}) : \mathbb{Q}]} \mathrm{Tr}_{\mathbb{Q}(\zeta_{|G|})/\mathbb{Q}}(\alpha).$$

Note that $\mathrm{Gal}(\mathbb{Q}(\zeta_{|G|})/\mathbb{Q})$ is commutative, and complex conjugation is an element of the group, so if the $\mathrm{Aut}(\mathbb{C})$-orbit of a non-zero algebraic integer α is $\{\alpha_1, \ldots, \alpha_k\}$, then

$$T(|\alpha|^2) = T(\alpha\bar{\alpha}) = \frac{1}{k} \sum_{i=1}^{k} \alpha_i \bar{\alpha}_i \geq 1.$$

As $(g^G, \chi) \in X$, by definition $\chi(g) \neq 0$, so $T(|\chi(g)|^2) \geq n$. Therefore,

$$\sum_{h \in g^G} T(|\chi(h)|^2) \geq n |g^G|.$$

If n is sufficiently large, by Proposition 10.1, we may assume that at least $\epsilon_3 |\mathcal{P}|^2/|Z|$ pairs (g^G, χ) arising in this way satisfy $|g^G| > |G|/Cq^r$. Thus,

$$\begin{aligned} |G| \cdot \mathrm{Irr}(G) &= T(\sum_{h \in G} \sum_{\chi \in \mathrm{Irr}(G)} |\chi(h)|^2) \\ &= \sum_{h \in G} \sum_{\chi \in \mathrm{Irr}(G)} T(|\chi(h)|^2) \geq \frac{\epsilon_3 |\mathcal{P}|^2}{|Z|} \frac{n|G|}{Cq^r} \\ &= \frac{\epsilon_3 q^r n |G|}{|Z| C}. \end{aligned}$$

By [4, Th. 1.1], $|\mathrm{Irr}(G)| \leq 27.2 q^r$. For orthogonal and symplectic groups, $|Z| \leq 4$, so that $|\mathrm{Irr}(G)| < 109 q^r/|Z|$. By [4, Cor. 3.7], $|\mathrm{Irr}(G)| < 4q^r/|Z|$ for $G = \mathrm{PSL}_{r+1}(q)$, and by [4, Prop. 3.10], $|\mathrm{Irr}(G)| \leq 9q^r/|Z|$ for $G = \mathrm{PSL}_{r+1}(q)$. Putting these together, we deduce $109 > \epsilon_3 n/C$, which is impossible for large n.

□

References

1. R. W. Carter, Centralizers of semisimple elements in the finite classical groups. *Proc. London Math. Soc. (3)* **42** (1981), no. 1, 1–41.
2. P. Erdős and J. Lehner, The distribution of the number of summands in the partitions of a positive integer. *Duke Math. J.* **8** (1941), 335–345.
3. P. Erdős and P. Turán, On some problems of a statistical group-theory. I. *Z. Wahrscheinlichkeitstheorie und Verw. Gebiete* **4** (1965), 175–186.
4. J. Fulman and R. Guralnick, Bounds on the number and sizes of conjugacy classes in finite Chevalley groups with applications to derangements. *Trans. Amer. Math. Soc.* **364** (2012), 3023–3070.
5. J. Fulman and R. Guralnick, The number of regular semisimple conjugacy classes in the finite classical groups. *Linear Algebra Appl.* **439**, no. 2, (2013), 488–503.
6. P. X. Gallagher, Degrees, class sizes and divisors of character values. *J. Group Theory* **15** (2012), 455–467.
7. P. X. Gallagher, M. Larsen and A. R. Miller, Many zeros of many characters of $\mathrm{GL}(n, q)$, arXiv:1909.01111.
8. S. Gonshaw, M. W. Liebeck, and E. A. O'Brien, Unipotent class representatives for finite classical groups. *J. Group Theory* **20** (2017), no. 3, 505–525.
9. M. Larsen and A. Shalev, Fibers of word maps and some applications. *J. Algebra* **354** (2012), 36–48.
10. M. Larsen and A. Shalev, On the distribution of values of certain word maps. *Trans. Amer. Math. Soc.* **368** (2016), 1647–1661.
11. F. Lübeck, `http://www.math.rwth-aachen.de/?Frank.Luebeck/chev/nrclasses/nrclasses.html`
12. G. Lusztig, Irreducible representations of finite classical groups, *Invent. Math.* **43** (1977), no. 2, 125–175.
13. G. Lusztig, Characters of reductive groups over a finite field, Annals of Mathematics Studies, 107. Princeton University Press, Princeton, NJ, 1984.
14. G. Lusztig, On the representations of reductive groups with disconnected centre, Orbites unipotentes et représentations, I. Astérisque No. 168 (1988), 10, 157–166.
15. A. R. Miller, The probability that a character value is zero for the symmetric group, *Math. Z.* **277** (2014), 1011–1015.
16. A. R. Miller, On parity and characters of symmetric groups. *J. Combin. Theory Ser. A* **162** (2019), 231–240.
17. R. Steinberg, Endomorphisms of linear algebraic groups. Memoirs of the American Mathematical Society, No. 80 American Mathematical Society, Providence, R.I. 1968.

Department of Mathematics, Indiana University, Bloomington, IN, USA
E-mail address: `mjlarsen@indiana.edu`

Faculty of Mathematics, University of Vienna, Austria
E-mail address: `alexander.r.miller@univie.ac.at`