UNIFORM CHARACTER BOUNDS FOR FINITE CLASSICAL GROUPS

MICHAEL LARSEN AND PHAM HUU TIEP

Abstract. For every finite quasisimple group of Lie type G, every irreducible character χ of G, and every element g of G, we give an exponential upper bound for the character ratio $|\chi(g)|/\chi(1)$ with exponent linear in $\log_{|G|}|g^G|$, or, equivalently, in the ratio of the support of g to the rank of G. We give several applications, including a proof of Thompson's conjecture for all sufficiently large simple symplectic groups, orthogonal groups in characteristic 2, and some other infinite families of orthogonal and unitary groups.

Contents

1. Introduction

Let G be a finite group, g an element of G, and χ an irreducible character of G. As $\chi(g)$ is a sum of $\chi(1)$ roots of unity, $|\chi(g)| \leq \chi(1)$, and when g lies in the center of G, no better upper bound is possible. The goal of this paper is to provide a good bound for $|\chi(g)|$ in terms of $\chi(1)$ and $|g^G|$ over the whole range of character degrees and conjugacy class sizes, which applies to all finite quasisimple groups G of Lie type, (i.e. $G = [G, G]$ and $G/\mathbf{Z}(G)$ is a finite simple group of Lie type). Our main result is the following:

The first author was partially supported by the NSF grant DMS-2001349. The second author gratefully acknowledges the support of the NSF (grants DMS-1840702 and DMS-2200850), the Joshua Barlaz Chair in Mathematics, and the Charles Simonyi Endowment at the Institute for Advanced Study (Princeton).

The authors are grateful to Martin Liebeck and Persi Diaconis for helpful comments on the paper.

The authors are grateful to the referee for careful reading and many comments and suggestions that helped greatly improve the exposition of the paper.

Theorem A. *There exists an absolute constant $c > 0$ such that for all finite quasisimple groups G of Lie type, irreducible characters χ of G, and elements $g \in G$, we have*

$$|\chi(g)| \le \chi(1)^{1-c\frac{\log|g^G|}{\log|G|}}. \tag{1.1}$$

There are already many bounds for irreducible character values in the literature. For groups of Lie type, Gluck [Gl] bounded the character ratio $|\chi(g)|/|\chi(1)|$ away from 1 for all non-central g. For classical groups of Lie type, one can say more for almost all elements. We define the *support* $\mathsf{supp}(g)$ of an element $g \in \mathrm{GL}_n(\overline{\mathbb{F}}_q)$ to be the codimension of the eigenspace of g of maximal dimension. This leads naturally to a definition for the support of an element g of a classical finite group of Lie type; namely, we lift g to an element of its central extension which lies in GL_n. In [LaST1], the character ratio is shown to go to 0 as $\mathsf{supp}(g) \to \infty$. The papers [GLT1, GLT2] give *exponential character bounds*, i.e., upper bounds of the form $\chi(1)^\alpha$ as long as $\frac{\log|g^G|}{\log|G|}$ is close enough to 1. The exponents in these bounds go to 0 as $\frac{\log|g^G|}{\log|G|} \to 1$, so in this regime, the bounds are better than those of Theorem A. A bound of type (1.1) is given in [BLST] for many classes of elements, and this has been further extended in [TT], yielding in particular optimal bounds for semisimple elements, whose centralizer is a proper Levi subgroup. Furthermore, good character bounds for the exceptional groups of Lie type, which all have bounded rank, are provided in [LiT].

The strength of our paper is that it gives an exponential bound covering *all* elements and all characters. This is particularly valuable for applications involving the Frobenius formula, where the most difficult cases cannot be excluded. We also note that, up to a multiplicative constant, the exponent in the bound $|\chi(g)/\chi(1)| \le \chi(1)^{-c\log_{|G|}|g^G|}$ in Theorem A is optimal; see Examples 5.7, 6.8, and Lemma 5.8. Furthermore, the constant c is made explicit in the proof.

We remark that there has been a parallel effort to obtain exponential bounds for irreducible character values of symmetric (and alternating) groups; see, for instance, [FL, Ro, MS, RŚ, LaSh1, LifM].

Previous character bounds have seen a wide variety of interesting applications. They play an important role in the proof of Ore's conjecture [LOST1], versions of Waring's problem for finite simple groups [LaST1, LaST2], covering number computations for conjugacy classes [LiSh2], and estimates for the number of points of representation varieties over finite fields [LiSh4]. Additional applications are described in Liebeck's survey article [Li].

We present several applications illustrating the power of the new bounds. Thompson's conjecture [AH] asserts that for every finite simple group G, there exists a conjugacy class S such that $S^2 = G$. Ellers and Gordeev [EG] made substantial progress on this conjecture, leaving open the case of groups of Lie type with $q \le 8$; also, they completely settled the case of groups of type A_r. In this paper, we give an asymptotic treatment of the case C_r. Likewise, we treat D_r and ${}^2D_r$ either in characteristic 2 or in odd characteristic, where q satisfies a suitable condition (mod 4). That is, we show that Thompson's conjecture holds for all but finitely many such groups; see Theorem 7.7. With finitely many exceptions, all that now remains are certain unitary groups with $q \le 7$ as well as odd-dimensional orthogonal groups and certain even-dimensional orthogonal groups over $\mathbb{F}_3$ and $\mathbb{F}_5$. We also prove that various regular semisimple conjugacy classes S in $G = \mathrm{SL}_n(q)$ or $\mathrm{SU}_n(q)$, including all classes with irreducible characteristic polynomial, have the property that S^2 includes all elements of G whose support is larger than an absolute constant.

The mixing time for a random walk on a Cayley graph given by a conjugacy class S has been an object of study since the celebrated work of Diaconis and Shahshani [DS]. For finite simple groups of Lie type, Liebeck and Shalev [LiSh2, Corollary 1.14] gave the upper bound $O\big(\frac{\log^3|G|}{\log^2|S|}\big)$. In Theorem

8.1, we improve this to the optimal asymptotic, $O\big(\frac{\log|G|}{\log|S|}\big)$, settling conjectures of Lubotzky [Lu, p.179] and of Shalev [Sh, 4.3] in the affirmative.

Each non-trivial character χ of a finite group G determines a McKay graph on the vertices $\mathrm{Irr}(G)$. Liebeck, Shalev, and Tiep [LiST1, Conjecture 1] conjectured that the diameter of this graph is $O\big(\frac{\log|G|}{\log\chi(1)}\big)$ for all finite simple groups. We prove this conjecture, as well as a related conjecture of Gill [Gi] concerning products of irreducible complex characters, for all finite simple groups of Lie type, see Theorems 8.3 and 8.5. We also extend results of Fulman [Fu] to determine the asymptotic of the convergence rate (to the stationary distribution) for random walks on McKay graphs for any simple group of Lie type, see Theorem 8.4.

The non-commutative Waring problem has received considerable attention recently, see e.g. [LaSh2, LaST1, GLOST, LaST2]. In particular, [GLOST, Theorem 4] states that there is a function $f:\mathbb{Z}_{\geq 1}\to\mathbb{Z}_{\geq 1}$ such that if $N\geq 1$ is an integer with at most k prime factors, the power word map $(x,y)\mapsto x^Ny^N$ is surjective on any alternating group A_n with $n\geq f(k)$, and on any simple group of Lie type of rank $n\geq f(k)$, excluding types A and ${}^2A$. In [GLOST], it is asked whether the theorem extends to the excluded cases. In Theorem 8.10, we prove that it does.

If $\underline{G}$ is a simple algebraic group over any algebraically closed field K and $\underline{S}_1,\dots,\underline{S}_k$ are conjugacy classes of $\underline{G}$, then multiplication defines a morphism of varieties $\underline{X}:=\underline{S}_1\times\cdots\times\underline{S}_k\to\underline{G}$. We prove that if $\dim\underline{X}$ is at least an absolute constant multiple of $\dim\underline{G}$, then this morphism is flat, meaning, in this situation, that the fibers of the morphism all have the same dimension, $\dim\underline{X}-\dim\underline{G}$, see Theorem 8.11.

Our strategy for proving the main theorem reverses the usual order of things. Instead of using character estimates to prove mixing theorems, we use mixing theorems to prove character estimates. More precisely, we use probability-theoretic methods to show that if U_S is the uniform distribution on a very small conjugacy class S, the probability that a sample from the iterated convolution U_S^{*b} lands in a small conjugacy class is very low. We do this in two stages, first to obtain (with probability close to one), an element whose support is larger than a constant multiple of the dimension n of the natural representation of G, and then to obtain an element whose conjugacy class is large enough that the estimates of [GLT1, GLT2] apply.

The paper is organized as follows. In section 2, we prove basic combinatorial estimates. In section 3, we translate these into the probability-theoretic results necessary to bootstrap from elements of large support (satisfying a linear lower bound in $\mathrm{rank}(G)$) to elements of small centralizer (satisfying an exponential upper bound in $|G|$ which can be taken as small as we wish). The bootstrapping argument is carried out in sections 4 and 5 and produces a uniform exponential character bound in terms of the support, Theorem 5.5. In section 6, we compare two notions of smallness for a conjugacy class given by support and by class size, and this allows us to deduce Theorem A from Theorem 5.5. The applications to squares of conjugacy classes are given in section 7, and we conclude, in section 8, with the applications to mixing time, McKay graph diameter and products of irreducible complex characters, power word maps on simple groups, and flatness of product morphisms.

2. Counting lemmas

The key result in this section is Proposition 2.6, which given a classical group G acting on a vector space V, a subspace $U\subset V$, a fixed element of G, a fixed integer b, and a fixed polynomial $P(x)\in\mathbb{F}_q[x]$, bounds above the number of different ways it can happen that P evaluated at a product of b conjugates $g^{x_1},\dots,g^{x_b}$ of g annihilates U. When this occurs, for each basis vector u_i of U, we can track all the vectors appearing along the way in computing $P(g^{x_b}\cdots g^{x_1})u_i$ and count tuples encoding all that intermediate information. We use this to estimate the size of the

projection to $(x_1, \dots, x_b)$. To accomplish this, we need various estimates for orbit sizes for classical group actions.

Let q be a power of a prime p, $n \in \mathbb{Z}_{\geq 3}$, and $V = \mathbb{F}_q^n$. In what follows, by a *classical group* $G = \mathrm{Cl}_n(q) = \mathrm{Cl}(V)$ *on* V and its *dimension* D we specifically mean one of the following:

- $G = \mathrm{SL}(V)$ and $D = n^2 - 1$;
- $\mathrm{Sp}(V)$ and $D = n(n+1)/2$, if $2|n$ and V is endowed with a non-degenerate alternating bilinear form $(\cdot|\cdot)$;
- $\mathrm{SO}(V)$ and $D = n(n-1)/2$, if $p > 2$ and V is endowed with a non-degenerate symmetric bilinear form $(\cdot|\cdot)$;
- $\Omega(V)$ and $D = n(n-1)/2$, if $p = 2|n$ and V is endowed with a quadratic form Q, associated with a non-degenerate alternating bilinear form $(\cdot|\cdot)$;
- $\mathrm{SU}(V)$ and $D = (n^2-1)/2$, if $q = q_0^2$ is a square and V is endowed with a non-degenerate ($\mathbb{F}_{q_0}$-bilinear) Hermitian form $(\cdot|\cdot)$ so that $\mathrm{SU}(V) \cong \mathrm{SU}_n(q_0)$.

(See e.g. [KlL, Chapter 2] for definitions and basic facts on the associated forms for finite classical groups.) This convention ensures that $q^D > |G| > q^D/2$ (cf. [LMT, Lemma 4.1(ii)]). We remark that for unitary groups, we do not always denote the two relevant prime powers q_0 and $q = q_0^2$, sometimes preferring q and q^2, depending on whether the emphasis is on the field of definition of the algebraic group or on the field of definition of the natural representation. Note also that $\mathrm{SU}_n(q_0)$ and $\mathrm{SU}(\mathbb{F}_q^n)$ (and sometimes $\mathrm{Cl}_n(q)$ with specifying $\mathrm{Cl} = \mathrm{SU}$) are different names for the same group, and the same can be said for $\mathrm{SU}_n(q)$ and $\mathrm{SU}(\mathbb{F}_{q^2}^n)$ (and $\mathrm{Cl}_n(q^2)$, with specifying $\mathrm{Cl} = \mathrm{SU}$).

If $V_1, \dots, V_k$ are vector spaces over a finite field $\mathbb{F}$, and $g_1 \in \mathrm{GL}(V_1), \dots, g_k \in \mathrm{GL}(V_k)$, we denote by $\mathrm{diag}(g_1, \dots, g_k)$ the image of $(g_1, \dots, g_k)$ under the homomorphism

$$\mathrm{GL}(V_1) \times \cdots \times \mathrm{GL}(V_k) \to \mathrm{GL}(V_1 \oplus \cdots \oplus V_k).$$

We use the same notation for classical groups; for instance, if $g_i \in \mathrm{Sp}(V_i)$, we understand $\mathrm{diag}(g_1, \dots, g_k)$ to be an element of $\mathrm{Sp}(V_1 \oplus \cdots \oplus V_k)$.

Lemma 2.1. *If k and n are positive integers and $r \leq k$ is a non-negative integer, $V = \mathbb{F}_q^n$, and $w_1, \dots, w_k$ are linearly independent vectors in V, then the number of sequences of vectors $v_1, \dots, v_k \in V$ such that*

$$\dim \mathrm{Span}(v_1, \dots, v_k, w_1, \dots, w_k) = k + r$$

is less than

$$\binom{k}{r} q^{rn + k^2 - r^2}.$$

Proof. Any such sequence $(v_1, \dots, v_k)$, determines an r-subset $S \subseteq \{1, \dots, k\}$ such that $s \in S$ if and only if

$$v_s \notin \mathrm{Span}(v_1, \dots, v_{s-1}, w_1, \dots, w_k).$$

We will bound the number of such sequences by first fixing S, for which we have $\binom{k}{r}$ possibilities. Given S, there are less than q^n possibilities for v_s when $s \in S$ and q^{k+r} possibilities for v_s for each of the $k - r$ indices $s \notin S$. □

Lemma 2.2. *Let U be a subspace of $V = \mathbb{F}_q^n$ of dimension $d \leq (n-3)/2$, and let H denote the subgroup of all elements in $G = \mathrm{Cl}(V)$ that act trivially on U. Then $|H| < q^{D-dn}$ if $\mathrm{Cl} = \mathrm{SL}$ and $|H| \leq q^{D-dn+d(d+1)/2}$ otherwise.*

Proof. If $G = \mathrm{SL}_n(q)$, then

$$|H| = q^{d(n-d)} |\mathrm{SL}_{n-d}(q)| < q^{d(n-d)+(n-d)^2-1} = q^{D-dn}.$$

We will now consider the case $\mathrm{Cl} \neq \mathrm{SL}$ and so V is endowed with G-invariant (bilinear or Hermitian) form $(\cdot|\cdot)$ (and quadratic form Q when $p = 2$ and $\mathrm{Cl} = \Omega$). Let $\kappa := -1$ if $p > 2$ and $\mathrm{Cl} = \mathrm{Sp}$, and $\kappa := 1$ otherwise, and set

$$W := U \cap U^\perp,\ a := \dim W,\ b := d - a.$$

Consider the H-invariant (partial) flag

$$\{0\} \subseteq W \subseteq U \subseteq W^\perp \subseteq V.$$

Note that $W^\perp = U + U^\perp$, and $(\cdot|\cdot)$ induces a non-degenerate bilinear form on $W^\perp/W$ (of the same kind). With respect to this induced form, U/W is a non-degenerate subspace with orthogonal complement $U^\perp/W$. So we can find a basis

$$(e_1, \dots, e_a, g_1, \dots, g_b, h_1, \dots, h_{n-2a-b})$$

of $W^\perp$, such that

$$U = \mathrm{Span}(e_1, \dots, e_a, g_1, \dots, g_b),\ U^\perp = \mathrm{Span}(e_1, \dots, e_a, h_1, \dots, h_{n-2a-b}).$$

and moreover the Gram matrix of the form induced by $(\cdot|\cdot)$ on $W^\perp$ in this basis is $\begin{pmatrix} 0 & 0 & 0 \\ 0 & B & 0 \\ 0 & 0 & C \end{pmatrix}$ with $\det(B)\det(C) \neq 0$. In particular, $S := \mathrm{Span}(g_1, \dots, g_b, h_1, \dots, h_{n-2a-b})$ is a non-degenerate subspace of V. So $S^\perp$ is also a non-degenerate subspace of V of dimension $2a$, which contains W as a maximal totally singular subspace. Hence we extend $(e_1, \dots, e_a)$ to a basis $(e_1, \dots, e_a, f_1, \dots, f_a)$ of $S^\perp$ in which $(\cdot|\cdot)$ has the Gram matrix $\begin{pmatrix} 0 & I_a \\ \kappa I_a & 0 \end{pmatrix}$. Thus the Gram matrix of $(\cdot|\cdot)$ in the basis

$$(e_1, \dots, e_a, g_1, \dots, g_b, h_1, \dots, h_{n-2a-b}, f_1, \dots, f_a)$$

of V is

$$\begin{pmatrix} 0 & 0 & 0 & I_a \\ 0 & B & 0 & 0 \\ 0 & 0 & C & 0 \\ \kappa I_a & 0 & 0 & 0 \end{pmatrix}. \tag{2.1}$$

Consider any element $h \in H$. Then h acts trivially on U and on $V/W^\perp \cong W^*$, and preserves the orthogonal complement $U^\perp/W$ to U/W in $W^\perp/W$, whence we get a homomorphism

$$\varphi : H \to \mathrm{Cl}(U^\perp/W) \cong \mathrm{Cl}_{n-2a-b}(q).$$

We will bound $|\varphi(H)|$ and $|\mathrm{Ker}(\varphi)|$, representing each $x \in \mathrm{Ker}(\varphi)$ by the matrix

$$\begin{pmatrix} I_a & 0 & X & Y \\ 0 & I_b & 0 & Z \\ 0 & 0 & I_{n-2a-b} & T \\ 0 & 0 & 0 & I_a \end{pmatrix}$$

in the chosen basis, where the matrices X, Y, Z, T over $\mathbb{F}_q$ satisfy the conditions

$$Z = 0,\ \kappa X + {}^tT^*C = 0,\ \kappa Y + {}^tY^* + {}^tT^*CT = 0 \tag{2.2}$$

which are obtained using the fact that x preserves $(\cdot|\cdot)$ with Gram matrix (2.1). For instance, $Z = 0$ because, for any $v \in V$ and $u \in U$,

$$(x(v) - v|u) = (x(v)|u) - (v|u) = (x(v)|x(u)) - (v|u) = 0, \tag{2.3}$$

i.e. $x(v)-v \in U^\perp$. Here, for a matrix $A = (a_{ij})$ over $\mathbb{F}_q$, A^* is interpreted as A in the case Cl = Sp, SO, or Ω and as $A^{(q_0)} = (a_{ij}^{q_0})$ in the case Cl = SU.

(a) Suppose Cl = Sp. Then $2|b$ and $2|n$, and writing $b = 2c$ and $n = 2m$ we have

$$|\varphi(H)| \le |\mathrm{Sp}_{2m-2a-2c}(q)| < q^{(m-a-c)(2(m-a-c)+1)}.$$

For $x \in \mathrm{Ker}(\varphi)$, there are $q^{2a(m-a-c)}$ choices for T, and, by (2.2), for each choice of T, X is uniquely determined and there are $q^{a(a+1)/2}$ choices for Y. Thus $|H| < q^E$, with

$$E := (m-a-c)(2(m-a-c)+1) + 2a(m-a-c) + a(a+1)/2 = D - 2dm + d(d-1)/2,$$

since $D = m(2m+1)$ and $d = a+2c$.

(b) Suppose Cl = SU. Then

$$|\varphi(H)| \le |\mathrm{SU}_{n-2a-b}(q_0)| < q_0^{(n-2a-b)^2-1)} = q^{((n-2a-b)^2-1)/2}.$$

For $x \in \mathrm{Ker}(\varphi)$, there are $q^{a(n-2a-b)}$ choices for T, and, by (2.2), for each choice of T, X is uniquely determined and there are $q_0^{a^2} = q^{a^2/2}$ choices for Y. Thus $|H| < q^E$, with

$$2E := (n-2a-b)^2 - 1 + 2a(n-2a-b) + a^2 = 2D - 2kn + d^2,$$

since $D = (n^2-1)/2$ and $d = a+b$.

(c) Suppose Cl = SO or Ω. Then $n - 3 \ge 2d = 2a + 2b$, whence $n - 2a - b \ge 3$, and

$$|\varphi(H)| \le |\mathrm{SO}_{n-2a-b}(q)| < q^{(n-2a-b)(n-2a-b-1)/2}.$$

For $x \in \mathrm{Ker}(\varphi)$, there are $q^{a(n-2a-b)}$ choices for T, and, by (2.2), for each choice of T, X is uniquely determined and, if $p > 2$ then there are at most $q^{a(a-1)/2}$ choices for Y, so

$$|\mathrm{Ker}(\varphi)| \le q^{a(n-2a-b)+a(a-1)/2}. \tag{2.4}$$

We want to show that (2.4) also holds when $p = 2$. Indeed, suppose $p = 2$. Then the number of elements in $\mathrm{Ker}(\varphi)$ that correspond to the same T is the number of elements in $\mathrm{Ker}(\varphi)$ that have $T = 0$. In addition to (2.2) which gives ${}^tY + Y = 0$, i.e. $Y = (y_{ij})$ is symmetric, any such element must satisfy

$$\mathsf{Q}(f_j) = \mathsf{Q}(x(f_j)) = \mathsf{Q}(f_j + \sum_i y_{ij}e_i) = \mathsf{Q}(f_j) + y_{jj} + \mathsf{Q}(\sum_i y_{ij}e_i). \tag{2.5}$$

Since $p = 2$, every scalar $z \in \mathbb{F}_q$ has a unique square root in $\mathbb{F}_q$, and hence the map

$$\sqrt{\mathsf{Q}} : V \to \mathbb{F}_q,\ v \mapsto \sqrt{\mathsf{Q}(v)}$$

is well-defined. Furthermore, $\sqrt{\mathsf{Q}}$ is $\mathbb{F}_q$-linear on $\mathrm{Span}(e_1, \dots, e_a)$, so we may assume that $\mathsf{Q}(e_1) = \dots = \mathsf{Q}(e_{a-1}) = 0$, and $\mathsf{Q}(e_a) = 0$ or $\mathsf{Q}(e_a) = 1$. In the former case, (2.5) yields $y_{jj} = 0$, whence Y has zero main diagonal and so the number of such Y is $q^{a(a-1)/2}$, and thus (2.4) holds. In the latter case, (2.5) yields $y_{jj} = y_{aj}^2$ when $j < a$, and $y_{aa} + y_{aa}^2 = 0$, i.e. $y_{aa} = 0$ or 1. Thus, when T is fixed, there are (at most) $2q^{a(a-1)/2}$ choices for $x \in \mathrm{Ker}(\varphi)$. Next, writing $n - 2a - b =: 2c$, we can choose $(h_1, \dots, h_{2c})$ so that the Gram matrix C is $\begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & \dots & 1 & 0 \\ & & \dots & & \\ 1 & 0 & \dots & 0 & 0 \end{pmatrix}$. Then

$$\mathsf{Q}(h_j) = \mathsf{Q}(x(h_j)) = \mathsf{Q}(h_j + \sum_i x_{ij}e_i) = \mathsf{Q}(h_j) + \mathsf{Q}(\sum_i x_{ij}e_i) = \mathsf{Q}(h_j) + x_{aj}^2,$$

and so $x_{aj} = 0$. On the other hand, $X = {}^tTC$ by (2.2), hence

$$0 = x_{aj} = ({}^tTC)_{aj} = t_{2c+1-j,a}$$

for $1 \le j \le 2c$. These relations show that there are at most $q^{(a-1)(n-2a-b)}$ choices for T, and, for each choice of T, X is uniquely determined and there are at most $2q^{a(a-1)/2}$ choices for Y. Since $q^{n-2a-b} \ge 2$, (2.4) holds in this case as well.

Thus we always have $|H| \le q^E$, with

$$2E := (n-2a-b)(n-2a-b-1) + 2a(n-2a-b) + a(a-1) = 2D - 2kn + d(d+1),$$

since $D = n(n-1)/2$ and $d = a+b$. □

Lemma 2.3. *Let $k \in \mathbb{Z}_{\ge 1}$ and let q be any prime power. Suppose that either $K = \mathbb{F}_q^k$ is endowed with a nonzero alternating bilinear form $(\cdot|\cdot)$, or a quadratic form Q associated to a nonzero symmetric bilinear form $(\cdot|\cdot)$, or q is a square and $K = \mathbb{F}_q^k$ is endowed with a nonzero Hermitian form $(\cdot|\cdot)$. Let $K^\perp$ denote the radical of $(\cdot|\cdot)$, and let $v \in K \smallsetminus K^\perp$. Then the set $\Omega(v)$ of the vectors $u \in K \smallsetminus K^\perp$ with $(v|v) = (u|u)$, respectively, $\mathsf{Q}(v) = \mathsf{Q}(u)$, $(v|v) = (u|u)$, has cardinality $\ge q^{k-2}$.*

Proof. (a) First we consider the case $(\cdot|\cdot)$ is non-degenerate, i.e. $K^\perp = 0$. The bound on $|\Omega(v)|$ is obvious if $k \le 2$, so we may assume $k \ge 3$. Let $\tilde{G}$ denote the full isometry group of $(\cdot|\cdot)$, respectively of Q, $(\cdot|\cdot)$. By Witt's lemma [KlL, Proposition 2.1.6], $\Omega(v)$ is just the orbit $v^{\tilde{G}}$ of v. In the symplectic case, we have

$$|v^{\tilde{G}}| = |K \smallsetminus \{0\}| = q^k - 1 > q^{k-1}.$$

In the odd-dimensional orthogonal case, we have $2 \nmid q$ and $k = 2m+1$ for some $m \ge 1$. Then $\tilde{G} = \mathrm{GO}_{2m+1}(q)$ has one orbit of isotropic vectors of length $q^{2m}-1$, $(q-1)/2$ orbits of anisotropic vectors of length $q^m(q^m-1)$ each, and $(q-1)/2$ orbits of anisotropic vectors of length $q^m(q^m+1)$ each, see e.g. [KlL, §4.1], and any of these lengths is at least q^{2m-1}.

In the even-dimensional orthogonal case, we have $k = 2m$ with $m \ge 2$. Then $\tilde{G} = \mathrm{GO}^\varepsilon_{2m}(q)$ for some $\varepsilon = \pm$. If $2 \nmid q$, then $\tilde{G}$ has one orbit of isotropic vectors of length $(q^m - \varepsilon)(q^{m-1} + \varepsilon)$, $(q-1)/2$ orbits of anisotropic vectors of length $(q^m - \varepsilon)(q^{m-1}+1)$ each, and $(q-1)/2$ orbits of anisotropic vectors of length $(q^m - \varepsilon)(q^{m-1}+1)$ each, again see e.g. [KlL, §4.1], and any of these lengths is larger than q^{2m-2}. If $2|q$, then $\tilde{G}$ has one orbit of isotropic vectors of length $(q^m - \varepsilon)(q^{m-1} + \varepsilon)$, and $q-1$ orbits of anisotropic vectors of length $q^{m-1}(q^m - \varepsilon)$ each, and any of these lengths is larger than q^{2m-2}.

In the unitary case, we have $q = q_0^2$. With $\varepsilon := -1$, $\tilde{G} = \mathrm{GU}_k(q_0)$ has one orbit of isotropic vectors of length $(q_0^k - \varepsilon^k)(q_0^{k-1} + \varepsilon^k)$, and $q_0 - 1$ orbits of anisotropic vectors of length $q_0^{k-1}(q_0^k - \varepsilon^k)$ each, again see e.g. [KlL, §4.1], and any of these lengths is larger than $q_0^{2k-2} = q^{k-1}$.

(b) Now we consider the case the radical $K^\perp$ of $(\cdot|\cdot)$ has dimension $a \ge 1$ over $\mathbb{F}_q$. Then $(\cdot|\cdot)$ induces a non-degenerate form on $K/K^\perp$ of dimension $k - a \ge 1$. If we are in the orthogonal case with $2|q$, assume in addition that Q is identically zero on $K^\perp$. Then note that all the q^a vectors in the coset $v + K^\perp$ belongs to $\Omega(v)$. Applying (a) to $K/K^\perp$, we see that $|\Omega(v)| \ge q^{k-a-2}q^a = q^{k-2}$.

Assume now that we are in the orthogonal case with $2|q$ but Q is not identically zero on $V^\perp$. As mentioned in the proof of Lemma 2.2, $\sqrt{\mathsf{Q}} : V^\perp \to \mathbb{F}_q$ is $\mathbb{F}_q$-linear and nonzero, hence surjective. Fixing $w \in V^\perp$ with $\mathsf{Q}(w) = 1$, we see that each coset $u + \langle w \rangle_{\mathbb{F}_q}$ with $u \in K \smallsetminus K^\perp$ contains a unique point in $\Omega(v)$. It follows that $|\Omega(v)| = (q^k - q^a)/q \ge q^{k-2}$. □

Lemma 2.4. *Let U be a subspace of $V = \mathbb{F}_q^n$ of dimension $d \le (n-3)/2$, and let H denote the subgroup of all elements in $G = \mathrm{Cl}(V)$ that act trivially on U. For any $v \in V \smallsetminus U$, the H-orbit v^H has length $|v^H| = q^n - q^d > q^n/2$ if $\mathrm{Cl} = \mathrm{SL}$ and $|v^H| \ge q^{n-d-2}$ otherwise.*

Proof. By assumption, $\operatorname{codim} U \ge (n+3)/2 \ge 2$. Hence, in the case $\mathrm{Cl} = \mathrm{SL}$, H acts transitively on $V \smallsetminus U$, which has cardinality $q^n - |U| \ge q^n/2$.

We will now consider the case $\mathrm{Cl} \ne \mathrm{SL}$ and so V is endowed with a non-degenerate G-invariant (bilinear or Hermitian) form $(\cdot|\cdot)$ (and quadratic form Q when $p = 2$ and $\mathrm{Cl} = \Omega$). In particular, we consider the orthogonal complement $U^\perp$ of dimension $n-d$ and fix a basis $(u_1, \dots, u_d)$ of U. We claim that $|v^H|$ is the number N of vectors $v' = v + u \in V$ such that

$$u \in U^\perp,\ v + u \notin U, \text{ and the subspaces } \langle U, v\rangle_{\mathbb{F}_q}, \langle U, v'\rangle_{\mathbb{F}_q} \text{ are isometric.} \tag{2.6}$$

Indeed, if $v' = h(v)$ for some $h \in H$, then $u := v' - v \in U^\perp$ by (2.3), $v' \notin U$, and h induces an isometry between $\langle U, v\rangle_{\mathbb{F}_q}$ and $\langle U, v'\rangle_{\mathbb{F}_q}$. Conversely, suppose $v' = v + u$ satisfies (2.6), and let $\tilde{G}$ denote the full isometry group of V. By Witt's lemma, there exists $g \in \tilde{G}$ that maps $u_i \mapsto u_i$ and $v \mapsto v'$. We also note that the proof of Lemma 2.1 shows that we can put U in a non-degenerate (with respect to $(\cdot|\cdot)$) subspace W of V dimension $\le 2d$. (Indeed, in the notation introduced prior to (2.1) we can take $W = \langle U, f_1, \dots, f_a\rangle_{\mathbb{F}_q}$ of dimension $d + a \le 2d$.) The same claim applied to $\langle U, v\rangle_{\mathbb{F}_q}$ allows us to put this subspace in a non-degenerate subspace W of dimension $\le 2(d+1) \le n-1$. In particular, $\dim W^\perp \ge 1$. In fact, in the cases where $\mathrm{Cl} = \mathrm{Sp}$, or $2|q$ and $\mathrm{Cl} = \Omega$, we have $2|n$ and so $2(d+1) \le n-2$, whence $\dim W^\perp \ge 2$. This condition on $\dim W^\perp$ ensures that $\tilde{G} = G\tilde{G}_W$, where $\tilde{G}_W$ consists of the elements of $\tilde{G}$ that act trivially on W (and so is isomorphic to the full isometry group of $W^\perp$). Hence we can write $g = hy$ with $h \in G$ and $y \in \tilde{G}_W$, and observe that $h \in G$ still maps $u_i \mapsto u_i$, $v \mapsto v'$. Thus $h \in H$, and $v' = h(v) \in v^H$.

Next we consider the case

$$v \in U + U^\perp,$$

so that $v = v_0 + v_1$ with $v_0 \in U$ and $v_1 \in U^\perp \smallsetminus U = K \smallsetminus K^\perp$, where $K := U^\perp$ and $K^\perp = U \cap U^\perp$ is the radical of the restriction of $(\cdot|\cdot)$ to K. Then

$$|v^H| = |\Omega(v_1)|$$

with $\Omega(v_1)$ defined in Lemma 2.3. Indeed, for any $u \in U^\perp$, we have $v + u \notin U$ if and only if $v_1 + u \in K \smallsetminus K^\perp$, furthermore,

$$(v'|v') - (v|v) = (v_0 + v_1 + u|v_0 + v_1 + u) - (v_0 + v_1|v_0 + v_1) = (v_1 + u|v_1 + u) - (v_1|v_1),$$

and, in the presence of Q,

$$\mathsf{Q}(v') - \mathsf{Q}(v) = \mathsf{Q}(v_0 + v_1 + u) - \mathsf{Q}(v_0 + v_1) = \mathsf{Q}(v_0) + \mathsf{Q}(v_1 + u) - \mathsf{Q}(v_0) - \mathsf{Q}(v_1) = \mathsf{Q}(v_1 + u) - \mathsf{Q}(v_1).$$

Thus the map $u \mapsto v_1 + u$ is a bijection between the set of vectors u satisfying (2.6) and $\Omega(v_1)$. Hence $|v^H| = |\Omega(v_1)| \ge q^{n-d-2}$ by Lemma 2.3, and we are done in this case.

From now on, we may assume that

$$v \notin U + U^\perp,$$

in which case $v + u \notin U$ for any $u \in U^\perp$. So $|v^H|$ is just the number N of vectors u such that

$$u \in U^\perp \text{ and the subspaces } \langle U, v\rangle_{\mathbb{F}_q}, \langle U, v'\rangle_{\mathbb{F}_q} \text{ are isometric.} \tag{2.7}$$

(a) Let $\mathrm{Cl} = \mathrm{Sp}$. Then (2.7) is equivalent to $u \in U^\perp$. It follows that $|v^H| = |U^\perp| = q^{n-d}$.

(b) Assume Cl = SU. Then (2.7) is equivalent to $u \in U^\perp$ and $(v|v) = (v+u|v+u)$, i.e.

$$(v|u) + (u|v) + (u|u) = 0. \tag{2.8}$$

Thus we need to count the number N of solutions $u \in U^\perp$ for (2.8).

By Witt's lemma, we can find a basis $(e_1, \dots, e_m, g_1, \dots, g_k)$ of $U^\perp$, with $k, m \geq 0$ and $k+m = n-d$, such that the Gram matrix of $(\cdot|\cdot)$ on $U^\perp$ in this basis is $\begin{pmatrix} 0 & 0 \\ 0 & I_k \end{pmatrix}$. Let $a_i := (e_i|v)$ and $b_j := (g_j|v)$. Since $v \notin U = (U^\perp)^\perp$,

$$(a_1, \dots, a_m, b_1, \dots, b_k) \neq (0, 0, \dots, 0). \tag{2.9}$$

Writing $u = \sum_i x_i e_i + \sum_j y_j g_j$ with $x_i, y_j \in \mathbb{F}_q$, (2.8) amounts to

$$0 = \sum_j y_j^{q_0+1} + \sum_i \big(x_i a_i + (x_i a_i)^{q_0}\big) + \sum_j \big(y_j b_j + (y_j b_j)^{q_0}\big). \tag{2.10}$$

Note that, for any $c \in \mathbb{F}_{q_0}$, the equation $x^{q_0+1} = c$ has at least one solution in $\mathbb{F}_q$. Hence, if $k \geq 1$, for any choice of $(x_1, \dots, x_m, y_2, \dots, y_k)$ we have at least one choice of y_1 to fulfill (2.10). It follows that $N \geq q^{m+k-1} = q^{n-d-1}$. Assume $k = 0$. Then we may assume by (2.9) that $a_1 \neq 0$. Then, for any $c \in \mathbb{F}_{q_0}$, the equation $x_1 a_1 + (x_1 a_1)^{q_0} = c$ has q_0 solutions in $\mathbb{F}_q$. Hence, for any choice of $(x_2, \dots, x_m)$ we have at least one choice of x_1 to fulfill (2.10), and thus $N \geq q^{m-1} = q^{n-d-1}$.

(c) Consider the case Cl = SO and $p > 2$. Then (2.7) is equivalent to $u \in U^\perp$ and $(v|v) = (v+u|v+u)$, i.e.

$$\mathsf{Q}(u) + (u|v) = 0, \tag{2.11}$$

where $\mathsf{Q}(u) := (u|u)/2$. Thus we need to count the number N of solutions $u \in U^\perp$ for (2.11).

By Witt's lemma, we can find a basis $(e_1, \dots, e_m, g_1, \dots, g_k)$ of $U^\perp$, with $k, m \geq 0$ and $k+m = n-d$, such that the Gram matrix of $(\cdot|\cdot)$ on $U^\perp$ in this basis is $\begin{pmatrix} 0 & 0 \\ 0 & E \end{pmatrix}$; moreover, if $k \geq 3$, or if $k = 2$ and $\mathrm{Span}(g_1, g_2)$ is of type $+$, then we can choose to have

$$E = \mathrm{diag}\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \mathrm{diag}(\varepsilon_3, \dots, \varepsilon_k)\right)$$

for some $\varepsilon_j \in \mathbb{F}_q^\times$. Let $a_i := (e_i|v)$ and $b_j := (g_j|v)$. Since $v \notin U = (U^\perp)^\perp$, (2.9) holds; also write $u = \sum_i x_i e_i + \sum_j y_j g_j$ with $x_i, y_j \in \mathbb{F}_q$ and $w := \sum_j e_j$.

Now, if $m \geq 1$ and, say $a_1 \neq 0$, then (2.11) amounts to

$$a_1 x_1 + \sum_{i \geq 2} a_i x_i + \mathsf{Q}(w) + (w|v) = 0.$$

For every choice of $(x_2, \dots, x_m, y_1, \dots, y_k)$ we have a unique choice of x_1 to fulfill this equation, and so $N = q^{m+k-1} = q^{n-d-1}$. Assume now that $a_1 = \dots = a_m = 0$; hence $k \geq 1$ by (2.9). If $k \geq 3$, or $k = 2$ but $\mathrm{Span}(g_1, g_2)$ is of type $+$, then our choice of E transforms (2.11) into

$$0 = y_1 y_2 + \sum_{j \geq 3} y_j \varepsilon_j^2 + \sum_j y_j b_j.$$

Note that, for any $c \in \mathbb{F}_q$, the equation $y_1 y_2 + b_1 y_1 + b_2 y_2 = c$, which is equivalent to

$$(y_1 + b_2)(y_2 + b_1) = c + b_1 b_2,$$

has at least $q-1$ solutions in $\mathbb{F}_q$ (one for each choice of $y_2 \neq -b_1$), whence $N \geq (q-1)q^{m+k-2} = (q-1)q^{n-d-2}$. If $k \leq 2$, then we can choose $y_1 = \dots = y_k = 0$ and x_i arbitrarily, yielding

$N \geq q^m \geq q^{n-d-2}$. (A more careful analysis shows that $N = (q-1)q^m$ if $k = 1$, and $N = (q+1)q^m$ if $k = 2$, using the transitivity of $\mathrm{GO}_2^-(q)$ on vectors $y \in \mathrm{Span}(g_1, g_2)$ of given $\mathsf{Q}(y) \in \mathbb{F}_q^\times$.)

(d) Finally, let $\mathrm{Cl} = \Omega$ and $p = 2$. Then (2.7) is equivalent to $u \in U^\perp$ and $\mathsf{Q}(v) = \mathsf{Q}(v+u)$, i.e. $u \in U^\perp$ satisfies (2.11). Thus we need to count the number N of solutions $u \in U^\perp$ for (2.11).

By Witt's lemma, we can find a basis $(e_1, \dots, e_m, g_1, \dots, g_{2k})$ of $U^\perp$, with $k, m \geq 0$, and $2k+m = n-d$, such that the Gram matrix of $(\cdot|\cdot)$ on $U^\perp$ in this basis is $\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & I_k \\ 0 & I_k & 0 \end{pmatrix}$. Let

$$a_i := (e_i|v),\ b_j := (g_j|v),\ c_i := \mathsf{Q}(e_i),\ d_j := \mathsf{Q}(g_j).$$

Since $v \notin U = (U^\perp)^\perp$, (2.9) holds; also write $u = \sum_i x_i e_i + \sum_j y_j g_j$, $x_i, y_j \in \mathbb{F}_q$, and $w := \sum_j y_j g_j$. Then (2.11) amounts to

$$\sum_i \left(a_i x_i + c_i x_i^2\right) + \mathsf{Q}(w) + (w|v) = 0.$$

(d1) Suppose $k \geq 2$, or $k = 1$ but $\mathrm{Span}(g_1, g_2)$ is of type $+$. Then we can choose $(g_1, \dots, g_{2k})$ so that $d_1 = \mathsf{Q}(g_1) = 0$. Then, for any $c \in \mathbb{F}_q$, the equation $y_1 y_{k+1} + b_1 y_1 + b_{k+1} y_{k+1} + d_{k+1} y_{k+1}^2 = c$ has at least $q-1$ solutions in $\mathbb{F}_q$ (one for each choice of $y_{k+1} \neq b_1$). In this case, for every choice of $(x_1, \dots, x_m, y_j \mid j \neq 1, k+1)$ we have at least $q-1$ choices of (y_1, y_{k+1}) to fulfill (2.11), and so $N \geq (q-1)q^{m+2k-2} \geq q^{n-d-2}$.

(d2) If, for instance, $a_1 = 0$ but $c_1 \neq 0$, or $a_1 \neq 0$ but $c_1 = 0$, then for any $c \in \mathbb{F}_q$ the equation $c_1 x_1^2 + a_1 x_1 = c$ has a unique solution in $\mathbb{F}_q$. In this case, for every choice of $(x_2, \dots, x_m, y_1, \dots, y_{2k})$ we have at a unique choice of x_1 to fulfill (2.11), and so $N = q^{m+2k-1} = q^{n-d-1}$.

(d3) Suppose $k = 1$ but $\mathrm{Span}(g_1, g_2)$ is of type $-$. If, say, $c_1 = \mathsf{Q}(e_1) \neq 0$, then, replacing g_1 by $g_1 + e_1/\sqrt{c_1}$ we get $\mathsf{Q}(g_1) = 0$, and so $\mathrm{Span}(g_1, g_2)$ is now of type $+$ and we can finish as in (d1). Otherwise we have $c_i = 0$ for all i. Now, if, say $a_1 \neq 0$, then we can argue as in (d2). If $a_i = 0$ for all i, then by choosing $y_1 = y_2 = 0$ but $x_1, \dots, x_m$ arbitrarily, we get $N \geq q^m = q^{n-d-2}$.

(d4) It remains to consider the case $k = 0$. Then $\sqrt{\mathsf{Q}}$ is $\mathbb{F}_q$-linear on $U^\perp = \mathrm{Span}(e_1, \dots, e_m)$, so we can choose $(e_1, \dots, e_m)$ such that $c_1 = \dots = c_{m-1} = 0$. Now, if $a_i \neq 0$ for some $1 \leq i \leq m-1$, then we can argue as in (d2). Otherwise we have $a_1 = \dots = a_{m-1} = 0$. Choosing $x_m = 0$ but $x_1, \dots, x_{m-1}$ arbitrarily, we get $N \geq q^{m-1} = q^{n-d-1}$. □

Proposition 2.5. *Let $n \geq 5$, $m < n$, and $k \leq (n-1)/4$ be positive integers and r a non-negative integer. Let $V = \mathbb{F}_q^n$, $G = \mathrm{GL}(V)$ or $\mathrm{Cl}(V)$, and let g be an element of G with $\mathsf{supp}(g) \geq n - m$. Let*

$$\mathbf{v} = (v_1, \dots, v_k) \text{ and } \mathbf{w} = (w_1, \dots, w_k)$$

denote two sequences of linearly independent vectors of V, and suppose

$$r = \dim \mathrm{Span}(v_1, \dots, v_k, w_1, \dots, w_k) - k.$$

Let

$$G_{\mathbf{v},\mathbf{w}} := \left\{x \in G \mid x^{-1} g x(w_i) = v_i,\ 1 \leq i \leq k\right\}.$$

Then the number of elements in $G_{\mathbf{v},\mathbf{w}}$ is at most

$$2^r q^{n^2 - k(n-m) - rm}$$

if $G = \mathrm{GL}(V)$ or $\mathrm{SL}(V)$, and at most

$$q^{D - k(n-m) + r(k-m+1) + k(k+1)/2}$$

if $G = \mathrm{Cl}(V)$ with $\mathrm{Cl} = \mathrm{SU}, \mathrm{Sp}, \mathrm{SO}$, or Ω.

Proof. (i) Suppose first that $r = 0$, so $v_1, \dots, v_k$ and $w_1, \dots, w_k$ span the same subspace W of V. Let T denote the linear transformation on W defined by $w_i \mapsto v_i$. We consider $\overline{V} := V \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q$ and $\overline{W} := W \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q$ as $\mathbb{F}_q[t]$-modules, where t acts by $g \otimes 1$ and $T \otimes 1$ on these spaces respectively. The condition $x^{-1}gxw_i = v_i$ implies that $x \otimes 1$ induces a $\overline{\mathbb{F}}_q[t]$-linear map from $\overline{W}$ to $\overline{V}$.

For $\lambda \in \overline{\mathbb{F}}_q$, let $\overline{V}_\lambda$ and $\overline{W}_\lambda$ be the corresponding generalized eigenspaces, i.e. $\mathrm{Ker}((t-\lambda)^n)$ on $\overline{V}$ and $\overline{W}$. Then

$$\mathrm{Hom}_{\overline{\mathbb{F}}_q[t]}(\overline{W}, \overline{V}) = \prod_\lambda \mathrm{Hom}_{\overline{\mathbb{F}}_q}(\overline{W}_\lambda, \overline{V}_\lambda).$$

For each λ, we choose decompositions

$$\overline{V}_\lambda = \bigoplus_i \overline{V}_{\lambda,i}, \ \overline{W}_\lambda = \bigoplus_i \overline{W}_{\lambda,i},$$

where

$$\overline{V}_{\lambda,i} \cong (\overline{\mathbb{F}}_q[t]/(t-\lambda)^i\overline{\mathbb{F}}_q[t])^{a_{\lambda,i}}, \ \overline{W}_{\lambda,i} \cong (\overline{\mathbb{F}}_q[t]/(t-\lambda)^i\overline{\mathbb{F}}_q[t])^{b_{\lambda,i}}.$$

Thus,

$$\dim_{\overline{\mathbb{F}}_q} \mathrm{Hom}_{\overline{\mathbb{F}}_q[t]}(\overline{W}, \overline{V}) = \sum_\lambda \sum_{i,j} \min(i,j) a_{\lambda,i} b_{\lambda,j}.$$

As $\dim \mathrm{Ker}(g-\lambda) = \sum_i a_{\lambda,i} \le m$ for all λ, for each $j \ge 1$, we have

$$\sum_i \min(i,j) a_{\lambda,i} \le j \sum_i a_{\lambda,i} = jm.$$

Furthermore, $\sum_{j,\lambda} j b_{\lambda,j} = k$, hence

$$\dim_{\overline{\mathbb{F}}_q} \mathrm{Hom}_{\overline{\mathbb{F}}_q[t]}(\overline{W}, \overline{V}) \le \sum_\lambda \sum_j jmb_{\lambda,j} = mk.$$

Thus, for any $x \in \mathrm{End}_{\mathbb{F}_q} V$ such that $(x \otimes 1)|_{\overline{W}} \in \mathrm{Hom}_{\overline{\mathbb{F}}_q[t]}(\overline{W}, \overline{V})$, there are at most q^{mk} possibilities for the restriction of x to W. If $G = \mathrm{GL}(V)$ or $\mathrm{SL}(V)$, then there are at most $q^{(n-k)n}$ possibilities for the restriction of x to a complement to W in V. Therefore,

$$|G_{\mathbf{v},\mathbf{w}}| \le |\{x \in \mathrm{End}_{\mathbb{F}_q} V : (x \otimes 1)|_{\overline{W}} \in \mathrm{Hom}_{\overline{\mathbb{F}}_q[t]}(\overline{W}, \overline{V})\}| \le q^{n^2 - k(n-m)},$$

which implies the proposition in the case $r = 0$ and $G = \mathrm{GL}(V), \mathrm{SL}(V)$.

Suppose $G = \mathrm{Cl}(V) \ne \mathrm{SL}(V)$. Note that $\dim W = k \le (n-1)/4 \le (n-3)/2$. The number of elements $x \in G_{\mathbf{v},\mathbf{w}}$ with a fixed action on W is at most the order of the pointwise stabilizer H of W in G, which is bounded by $q^{D-kn+k(k+1)/2}$ by Lemma 2.2. Hence,

$$|G_{\mathbf{v},\mathbf{w}}| \le q^{D-k(n-m)+k(k+1)/2},$$

completing the proof of the statement in the case $r = 0$.

(ii) For the general statement, we use induction on k, with the obvious induction base $k = 0$. Suppose the proposition holds for $k-1 \ge 0$. Using the case $r = 0$ established in (i), we may assume without loss of generality that $v_k \notin \mathrm{Span}(w_1, \dots, w_k)$. Hence we can find $v^* \in V^*$, a dual vector of V, such that $v^*(w_i) = 0$ for $1 \le i \le k$ and $v^*(v_k) = 1$. For $1 \le i < k$, we denote $c_i := v^*(v_i)$, and observe that replacing v_i by $v_i - c_i v_k$ and w_i by $w_i - c_i w_k$ for $1 \le i \le k-1$ does not affect the set $G_{\mathbf{v},\mathbf{w}}$. After this replacement, we now have $v^*(v_i) = 0$ for $1 \le i \le k-1$, $v^*(v_k) = 1$, and $v^*(w_i) = 0$ for $1 \le i \le k$. Hence

$$v_k \notin U := \mathrm{Span}(v_1, \dots, v_{k-1}, w_1, \dots, w_k). \tag{2.12}$$

Let $\Omega := V \smallsetminus U$, and let

$$\mathbf{v}' := (v_1, \dots, v_{k-1}),\ \mathbf{w}' := (w_1, \dots, w_{k-1}),$$
$$H := \{x \in G \mid x(v_i) = v_i,\ 1 \le i \le k-1,\ x(w_j) = w_j,\ 1 \le j \le k\}.$$

We also note that $\dim U \le 2k-1 \le (n-3)/2$. Next, for all $h \in G$ we have that

$$|G_{h(\mathbf{v}),h(\mathbf{w})}| = |G_{\mathbf{v},\mathbf{w}}|.$$

Taking $h \in H$, we have $h(v_k) \in \Omega$ by (2.12). Moreover, if $h, h' \in H$ and $h(v_k) \ne h'(v_k)$, then $G_{h(\mathbf{v}),h(\mathbf{w})}$ and $G_{h'(\mathbf{v}),h'(\mathbf{w})}$ are disjoint subsets of $G_{\mathbf{v}',\mathbf{w}'}$ of the same size. It follows that

$$|G_{\mathbf{v},\mathbf{w}}| \le \frac{|G_{\mathbf{v}',\mathbf{w}'}|}{|v^H|}. \tag{2.13}$$

Also set

$$r' := \dim \mathrm{Span}(v_1, \dots, v_{k-1}, w_1, \dots, w_{k-1}) - (k-1).$$

Then (2.12) implies that $r' \le r \le r' + 1$.

(a) Here we consider the case $G = \mathrm{GL}(V)$ or $\mathrm{SL}(V)$. Then H acts transitively on Ω which has cardinality at least $q^n/2$. Therefore, (2.13) implies that

$$|G_{\mathbf{v},\mathbf{w}}| \le \frac{|G_{\mathbf{v}',\mathbf{w}'}|}{|\Omega|} \le \frac{2|G_{\mathbf{v}',\mathbf{w}'}|}{q^n}. \tag{2.14}$$

The proposition now follows by induction. Indeed, by induction hypothesis and (2.14),

$$\begin{aligned} |G_{\mathbf{v},\mathbf{w}}| &\le 2^{r'+1} q^{n^2-(k-1)(n-m)-r'm-n} \\ &= 2^{r'+1} q^{n^2-k(n-m)-(r'+1)m} \\ &\le 2^r q^{n^2-k(n-m)-rm} \end{aligned}$$

since $q^m \ge 2$.

(b) Now consider the case $G = \mathrm{Cl}(V) \ne \mathrm{SL}(V)$. Then the induction hypothesis for $k-1$ implies

$$|G_{\mathbf{v}',\mathbf{w}'}| \le q^{D-(k-1)(n-m)+r'(k-m)+k(k-1)/2}.$$

On the other hand, (2.12) implies that $\dim U = k + r - 1$, and so Lemma 2.4 yields

$$|v^H| \ge q^{n-\dim U-2} = q^{n-k-r-1}.$$

It follows from (2.13) that $|G_{\mathbf{v},\mathbf{w}}| \le q^E$, where

$$\begin{aligned} E &= D - (k-1)(n-m) + r'(k-m) + k(k-1)/2 - (n-k-r-1) \\ &= D - k(n-m) + k(k+1)/2 + r'(k-m) + r - m + 1. \end{aligned}$$

If $r = r'$, then

$$\begin{aligned} E &= D - k(n-m) + r(k-m+1) + k(k+1)/2 + 1 - m \\ &\le D - k(n-m) + r(k-m+1) + k(k+1)/2 \end{aligned}$$

since $m \ge 1$. If $r = r' + 1$, then

$$\begin{aligned} E &= D - k(n-m) + r(k-m+1) + k(k+1)/2 + 1 - k \\ &\le D - k(n-m) + r(k-m+1) + k(k+1)/2 \end{aligned}$$

since $k \ge 1$, and the induction step is completed. □

We denote $x^{-1}gx$ by g^x.

Proposition 2.6. *Let $n \geq 5$ be an integer, $V := \mathbb{F}_q^n$, and $G := \mathrm{GL}(V)$ or $\mathrm{Cl}(V)$. Let $m < n$ be a positive integer and let $g \in G$ be an element with $\mathsf{supp}(g) \geq n - m$. Let a, b and d be integers such that $k := ad \leq (n-1)/4$ and $b \geq \frac{n}{n-m}$. Let $P(x) = \sum_h p_h x^h \in \mathbb{F}_q[x]$ be a monic polynomial of degree $\leq d-1$. Let $u_1, \ldots, u_a \in V$ be linearly independent. Then the number of b-tuples $(x_1, \ldots, x_b) \in G^b$ such that $P(g^{x_b} \cdots g^{x_1})u_i = 0$ for $1 \leq i \leq a$ is bounded above by*

$$q^{bn^2+(b-1)k^2+2bk-an+1}$$

if $G = \mathrm{GL}(V)$ or $\mathrm{SL}(V)$, and by

$$q^{bD+(\frac{5}{2}b-1)k^2+\frac{7}{2}bk-an}$$

if $G = \mathrm{Cl}(V) \neq \mathrm{SL}(V)$.

Proof. (i) For $0 \leq j \leq b-1$, $1 \leq i \leq a$, and $0 \leq h \leq d-1$, consider all choices $(\mathbf{w}, \mathbf{v})$ of vectors $v_{i,j}^h, w_{i,j}^h \in V$ satisfying the following conditions:

(a) For $1 \leq i \leq a$, $w_{i,0}^0 = u_i$.
(b) For $0 \leq j \leq b-2$, $w_{i,j+1}^h = v_{i,j}^h$.
(c) For $0 \leq h \leq d-2$, $w_{i,0}^{h+1} = v_{i,b-1}^h$.
(d) For $1 \leq i \leq a$, $\sum_h p_h v_{i,b-1}^h = 0$.
(e) For each j, the $k = ad$ vectors of the form $w_{i,j}^h$ are linearly independent.

Given such choices, we define

$$r_{\mathbf{w},\mathbf{v},j} := \dim \mathrm{Span} \bigcup_{h,i} \{v_{i,j}^h, w_{i,j}^h\} - k.$$

For each b-tuple $(r_0, r_1, \ldots, r_{b-1})$, we would like to bound above the number of pairs $(\mathbf{w}, \mathbf{v})$ with $r_{\mathbf{w},\mathbf{v},j} = r_j$ for $j = 0, 1, \ldots, b-1$. To do this, we choose $0 \leq t \leq b-1$ such that $r_t = \max(r_0, \ldots, r_{b-1})$. We first choose all the $w_{i,0}^h$. By condition (a), the values for $h = 0$ are determined, so there are less than $q^{(k-a)n}$ possibilities. By conditions (c) and (d), these choices determine $v_{i,b-1}^h$ for all h and i.

Next, iteratively, for $0 \leq j < t$, we choose $w_{i,j+1}^h = v_{i,j}^h$ for $0 \leq h \leq d-1$ and $1 \leq i \leq a$, subject to the condition $r_{\mathbf{w},\mathbf{v},j} = r_j$. By Lemma 2.1, there are at most $\binom{k}{r_j} q^{r_j n + k^2}$ choices at each step. For the remaining values of j, we work backward for $t < j < b$, choosing $w_{i,j}^h$ for $0 \leq h \leq d-1$ and $1 \leq i \leq a$, subject to the condition that $r_{\mathbf{w},\mathbf{v},j} = r_j$. Again, there are at most $\binom{k}{r_j} q^{r_j n + k^2}$ choices at each step. Therefore, the total number of choices is at most

$$q^{(k-a)n} \prod_{j \neq t} \binom{k}{r_j} q^{r_j n + k^2} \leq q^{(k-a)n + \frac{(b-1)rn}{b} + (b-1)k^2} \prod_{j \neq t} \binom{k}{r_j},$$

where $r := r_0 + \cdots + r_{b-1}$. Since

$$\sum_{r_0 + \ldots + r_{b-1} = r} \prod_j \binom{k}{r_j} \leq \prod_{j=0}^{b-1} \Big(\sum_{r_j = 0}^{k} \binom{k}{r_j} \Big) = 2^{bk},$$

the number N_1 of pairs $(\mathbf{w}, \mathbf{v})$ with $\sum_j r_{\mathbf{w},\mathbf{v},j} = r$ is less than

$$2^{bk} q^{(k-a)n + \frac{(b-1)rn}{b} + (b-1)k^2}.$$

For given $(\mathbf{w}, \mathbf{v})$ we consider the number N_2 of $(x_0, \ldots, x_{b-1}) \in G^b$ such that

$$g^{x_j} w_{i,j}^h = v_{i,j}^h \ \forall h, i, j. \tag{2.15}$$

(ii) Consider the case $G = \mathrm{GL}(V)$ or $\mathrm{SL}(V)$. By Proposition 2.5,

$$N_2 \le \prod_{j=0}^{b-1} 2^{r_{\mathbf{w},\mathbf{v},j}} q^{n^2-k(n-m)-r_{\mathbf{w},\mathbf{v},j}m} = 2^r q^{bn^2-bk(n-m)-rm}.$$

Therefore, the number N of tuples $(\mathbf{w}, \mathbf{v}, x_1, \dots, x_b)$ satisfying (2.15) is at most

$$2^{2bk+1} \max_{0\le r\le bk} q^{bn^2+(b-1)k^2-(bk-r)(\frac{b-1}{b}n-m)-an}.$$

As $b \le \frac{n}{n-m}$, this is bounded above by $q^{bn^2+(b-1)k^2+2bk-an+1}$. The projection onto G^b of the set of tuples $(\mathbf{w}, \mathbf{v}, x_1, \dots, x_b)$ satisfying (2.15) therefore has order at most $q^{bn^2+(b-1)k^2+2bk-an+1}$, which proves the proposition in this case.

(iii) Now let $G = \mathrm{Cl}(V) \ne \mathrm{SL}(V)$. By Proposition 2.5,

$$N_2 \le \prod_{j=0}^{b-1} q^{D-k(n-m)+k(k+1)/2+r_{\mathbf{w},\mathbf{v},j}(k-m+1)} = q^{bD-bk(n-m)+bk(k+1)/2+r(k-m+1)}.$$

Therefore, the number N of tuples $(\mathbf{w}, \mathbf{v}, x_1, \dots, x_b)$ satisfying (2.15) is at most

$$2^{2bk} \max_{0\le r\le bk} q^{bD-bk(n-m)+bk(k+1)/2+r(k-m+1)+(k-a)n+(b-1)k^2+(b-1)rn/b}.$$

As $b \le \frac{n}{n-m}$, this is bounded above by $q^{bD+(\frac{5}{2}b-1)k^2+\frac{7}{2}bk-an}$. Again projecting onto G^b, we obtain the proposition in this case. □

3. Probabilistic lemmas

The probability theory terminology used in this section and beyond can be found in a standard text such as [Du]. Given a specified finite group G, we denote by $\mathsf{X}_1, \mathsf{X}_2, \dots$ a sequence of independent uniformly distributed random variables on G. Thus, for $g \in G$, g^{X_i} are independent uniformly distributed random elements of the conjugacy class of g in G. We use the counting results of the previous section to prove, roughly, that for finite classical groups the maximum eigenspace dimension of $g^{\mathsf{X}_1} \cdots g^{\mathsf{X}_b}$ almost always grows sublinearly in n, provided that $\mathsf{supp}(g)$ is sufficiently large and $b\,\mathsf{supp}(g) \ge n$. We will be particularly interested in the case that $\mathsf{supp}(g)$ is bounded below by a constant multiple of n as $n \to \infty$; in this regime, it is important that the probability that a large eigenspace exists goes to zero exponentially in n^2.

Proposition 3.1. *Let $0 < \varepsilon < 1$, $d \in \mathbb{Z}_{\ge 2}$, $n \in \mathbb{Z}_{\ge 1}$, $G = \mathrm{Cl}(V)$, or $G = \Omega(V)$ when $2 \nmid q$. Suppose $s \in \mathbb{Z}_{\ge 1}$ is such that $n > s \ge 8d^2/\varepsilon$ if $G = \mathrm{SL}(V)$ and $n > s \ge 23d^2/\varepsilon$ if $G \ne \mathrm{SL}(V)$. Then, with*

$$b := \lceil n/s \rceil,$$

the following statement holds for any element $g \in G$ with $\mathsf{supp}(g) \ge s$. The probability that there exists a non-zero polynomial $P(x) \in \mathbb{F}_q[x]$ of degree $< d$ such that

$$\dim \mathrm{Ker} P(g^{\mathsf{X}_1} \cdots g^{\mathsf{X}_b}) \ge \varepsilon n$$

is less than

$$q^{3+d-\frac{\varepsilon^2 ns}{18d^2}}$$

if $G = \mathrm{SL}(V)$, and less than

$$q^{2+d-\frac{\varepsilon^2 ns}{31d^2}}$$

if $G \ne \mathrm{SL}(V)$.

Proof. Since the number of non-zero polynomials in $\mathbb{F}_q[x]$ of degree $< d$ is $q^d - 1$, it suffices to prove that for each P,

$$\mathbf{P}[\dim \mathrm{Ker} P(g^{\mathsf{X}_1} \cdots g^{\mathsf{X}_b}) \geq \varepsilon n] \leq \begin{cases} q^{3-\frac{\varepsilon^2 ns}{18d^2}}, & G = \mathrm{SL}(V), \\ q^{2-\frac{\varepsilon^2 ns}{31d^2}}, & G \neq \mathrm{SL}(V). \end{cases}$$

We fix P and, with a chosen below, let $(\mathsf{U}_1, \ldots, \mathsf{U}_a)$ denote a random ordered a-tuple of linearly independent vectors in V, uniformly distributed among all such a-tuples and independent of the X_i.

(i) First consider the case $G = \mathrm{SL}(V)$. Since $n > s \geq 8d^2/\varepsilon$, we have $2 \leq b < n\varepsilon/8d^2 + 1 \leq n\varepsilon/7d^2$. In particular,

$$2bd + 2(b-1)d^2 < 3bd^2 < 3n\varepsilon/7 < n\varepsilon/2, \text{ and } 2bd \leq bd^2 \leq n\varepsilon/7. \tag{3.1}$$

We also choose

$$a := \lfloor \alpha \rfloor, \text{ where } \alpha := \frac{\varepsilon n - 2bd}{2(b-1)d^2}. \tag{3.2}$$

Note from (3.1) that $\alpha > 2$. Furthermore, $ad \leq \alpha d < \varepsilon n/4 < n/4$, and so $ad \leq (n-1)/4$. Hence by Proposition 2.6 we have

$$\mathbf{P}[P(g^{\mathsf{X}_1} \cdots g^{\mathsf{X}_b})\mathsf{U}_i = 0, \ \forall\, i \leq a] \leq \frac{q^{bn^2 + (b-1)a^2d^2 + 2abd - an + 1}}{|G|^b}.$$

The number of b-tuples in G is greater than $\frac{q^{bn^2}}{(4q)^b} \geq q^{bn^2 - 3b}$, so

$$\mathbf{P}[P(g^{\mathsf{X}_1} \cdots g^{\mathsf{X}_b})\mathsf{U}_i = 0, \ \forall\, i \leq a] \leq q^{3b + (b-1)a^2d^2 + 2abd - an + 1}.$$

If W is a subspace of V of dimension $\geq \varepsilon n$, then

$$\mathbf{P}[\mathsf{U}_1, \ldots, \mathsf{U}_a \in W] \geq \frac{(q^{\varepsilon n} - 1) \cdots (q^{\varepsilon n} - q^{a-1})}{(q^n - 1) \cdots (q^n - q^{a-1})} \geq \frac{q^{a\varepsilon n}}{4q^{an}} \geq q^{\varepsilon an - an - 2}. \tag{3.3}$$

Thus,

$$\begin{aligned} q^{3b + (b-1)a^2d^2 + 2abd - an + 1} & \\ &\geq \mathbf{P}[\mathsf{U}_1, \ldots, \mathsf{U}_a \in \mathrm{Ker} P(g^{\mathsf{X}_1} \cdots g^{\mathsf{X}_b})] \\ &\geq \sum_{\{W \mid \dim W \geq \varepsilon n\}} \mathbf{P}[\mathrm{Ker} P(g^{\mathsf{X}_1} \cdots g^{\mathsf{X}_b}) = W]\, \mathbf{P}[\mathsf{U}_1, \ldots, \mathsf{U}_a \in W] \\ &\geq q^{\varepsilon an - an - 2} \sum_{\dim W \geq \varepsilon n} \mathbf{P}[\mathrm{Ker} P(g^{\mathsf{X}_1} \cdots g^{\mathsf{X}_b}) = W] \\ &= q^{\varepsilon an - an - 2} \mathbf{P}[\dim \mathrm{Ker} P(g^{\mathsf{X}_1} \cdots g^{\mathsf{X}_b}) \geq \varepsilon n]. \end{aligned}$$

We deduce that

$$\mathbf{P}[\dim \mathrm{Ker} P(g^{\mathsf{X}_1} \cdots g^{\mathsf{X}_b}) \geq \varepsilon n] \leq q^{3 + 3b + (b-1)a^2d^2 + 2abd - \varepsilon an}. \tag{3.4}$$

By (3.1) and (3.2), the exponent in (3.4) is bounded above by

$$\begin{aligned}3+3b+(b-1)d^2\alpha^2+(2bd-\varepsilon n)(\alpha-1) &= 3+3b-\frac{(\varepsilon n-2bd)^2}{4(b-1)d^2}+(\varepsilon n-2bd)\\ &< 3-\frac{(\varepsilon n-2bd)^2}{4(b-1)d^2}+\varepsilon n < 3-\frac{(\varepsilon n-2bd)^2}{4d^2n/s}+\varepsilon n\\ &< 3-\frac{(6\varepsilon n/7)^2}{4d^2n/s}+\varepsilon n = 3-\frac{9\varepsilon^2 ns}{49d^2}+\varepsilon n < 3-\frac{\varepsilon^2 ns}{18d^2},\end{aligned}$$

since $s \geq 8d^2/\varepsilon$.

(ii) Now let $G \neq \mathrm{SL}(V)$. Since $n > s \geq 23d^2/\varepsilon$, we have $2 \leq b < n\varepsilon/23d^2 + 1 \leq n\varepsilon/22d^2$. In particular,

$$\frac{7}{2}bd + 2(10b-4)d^2 < 22bd^2 < n\varepsilon, \text{ and } \frac{7}{2}bd \leq \frac{7}{4}bd^2 \leq \frac{n\varepsilon}{22\cdot 4/7} < \frac{n\varepsilon}{12}. \tag{3.5}$$

We also choose

$$a := \lfloor \alpha \rfloor, \text{ where } \alpha := \frac{\varepsilon n - \frac{7}{2}bd}{(10b-4)d^2}. \tag{3.6}$$

Note from (3.5) that $\alpha > 2$. Furthermore, $ad \leq \alpha d < \varepsilon n/12 < n/4$, and so $ad \leq (n-1)/4$. Hence by Proposition 2.6 we have

$$\mathbf{P}[P(g^{\mathsf{X}_1}\cdots g^{\mathsf{X}_b})\mathsf{U}_i = 0,\ 1 \leq i \leq a] \leq \frac{q^{bD+(\frac{5}{2}b-1)a^2d^2+\frac{7}{2}abd-an}}{|G|^b}.$$

The number of b-tuples in G is greater than $\frac{q^{bD}}{4^b} \geq q^{bD-2b}$, where we use the bound

$$|\Omega(V)| = |\mathrm{SO}(V)|/2 > q^D/4$$

when $2 \nmid q$. Therefore,

$$\mathbf{P}[P(g^{\mathsf{X}_1}\cdots g^{\mathsf{X}_b})\mathsf{U}_i = 0,\ 1 \leq i \leq a] \leq q^{2b+(\frac{5}{2}b-1)a^2d^2+\frac{7}{2}abd-an}.$$

Again using (3.3) as above, we deduce that

$$q^{2b+(\frac{5}{2}b-1)a^2d^2+\frac{7}{2}abd-an} \geq q^{\varepsilon an-an-2}\mathbf{P}[\dim \mathrm{Ker}P(g^{\mathsf{X}_1}\cdots g^{\mathsf{X}_b}) \geq \varepsilon n],$$

and so

$$\mathbf{P}[\dim \mathrm{Ker}P(g^{\mathsf{X}_1}\cdots g^{\mathsf{X}_b}) \geq \varepsilon n] \leq q^{2+2b+(\frac{5}{2}b-1)a^2d^2+\frac{7}{2}abd-\varepsilon an}. \tag{3.7}$$

Note that $16 \leq 10b-4 < 10n/s+6 < 11n/s$. Hence, by (3.5) and (3.6), the exponent in (3.7) is bounded above by

$$\begin{aligned}2+2b+(\frac{5}{2}b-1)d^2\alpha^2+(\frac{7}{2}bd-\varepsilon n)(\alpha-1) &= 2+2b-\frac{(\varepsilon n-\frac{7}{2}bd)^2}{(10b-4)d^2}+(\varepsilon n-\frac{7}{2}bd)\\ &< 2-\frac{(\varepsilon n-\frac{7}{2}bd)^2}{(10b-4)d^2}+\varepsilon n < 2-\frac{(\varepsilon n-\frac{7}{2}bd)^2}{11d^2n/s}+\varepsilon n\\ &< 2-\frac{(11\varepsilon n/12)^2}{11d^2n/s}+\varepsilon n = 2-\frac{11\varepsilon^2 ns}{144d^2}+\varepsilon n < 2-\frac{\varepsilon^2 ns}{31d^2},\end{aligned}$$

since $s \geq 23d^2/\varepsilon$. □

Recall that $\mathbf{E}(\mathsf{X})$ denotes the expected value of the random variable X.

Lemma 3.2. *For any finite group G, any element $g \in G$, any irreducible character χ of G, and any positive integer b,*

$$\mathbf{E}[\chi(g^{\mathsf{X}_1} \cdots g^{\mathsf{X}_b})] = \frac{\chi(g)^b}{\chi(1)^{b-1}}.$$

Proof. For any $h \in G$, the probability $\mathbf{P}[g^{\mathsf{X}_1} \cdots g^{\mathsf{X}_b} = h]$ is given by the Frobenius formula

$$\frac{1}{|G|} \sum_{\varphi \in \mathrm{Irr}(G)} \frac{\varphi(g)^b \overline{\varphi}(h)}{\varphi(1)^{b-1}}.$$

Therefore,

$$\begin{aligned}\mathbf{E}[\chi(g^{\mathsf{X}_1} \cdots g^{\mathsf{X}_b})] &= \sum_{h \in G} \chi(h) \frac{1}{|G|} \sum_{\varphi \in \mathrm{Irr}(G)} \frac{\varphi(g)^b \overline{\varphi}(h)}{\varphi(1)^{b-1}} \\ &= \sum_{\varphi \in \mathrm{Irr}(G)} \frac{\varphi(g)^b}{\varphi(1)^{b-1}} \frac{1}{|G|} \sum_{h \in G} \chi(h) \overline{\varphi}(h) = \frac{\chi(g)^b}{\chi(1)^{b-1}}\end{aligned}$$

by the orthonormality of irreducible characters. □

4. Character bounds for elements with large support

The main result in this section is Theorem 4.4, which gives an exponential character bound at $g \in G$ whenever $\mathsf{supp}(g)$ is bounded below by a fixed positive multiple of n. We use the results of the previous section to show that, assuming n is large, a random walk on the Cayley graph of G with respect to g^G almost always leads in a bounded number of steps to an element whose centralizer order is smaller than any desired power of $|G|$. Using known character bounds for such elements, we can estimate the expectation of χ on such elements, and deduce an exponential upper bound for $|\chi(g)|$.

Lemma 4.1. *For any $0 < \nu < 1$, there exists $0 < \alpha < 1$ such that, for any $n \in \mathbb{Z}_{\geq 2}$ and any prime power q, if $V = \mathbb{F}_q^n$, $g \in \mathrm{GL}(V)$, and*

$$\dim \mathbf{C}_{\mathrm{End}(V)}(g) \geq \alpha n^2, \tag{4.1}$$

then $|\mathbf{C}_{\mathrm{SL}(V)}(g)| > |\mathrm{SL}(V)|^{1-\nu}$.

Proof. We can take $\alpha = 1 - \nu^2/4$. If d denotes $\dim \mathbf{C}_{\mathrm{End}(V)}(g)$, then d is the dimension of the centralizer $\underline{C}(g)$ of g in the algebraic group GL_n. The finite group $\underline{C}(g)(\mathbb{F}_q) = \mathbf{C}_{\mathrm{GL}(V)}(g)$ has a normal series, whose factors X_i are unipotent groups of order q^{d_i}, or $\mathrm{GL}_{m_i}(q^{a_i})$ with $d_i := m_i^2 a_i$, and $\sum_i d_i = d$. Note that since $q^{a_i j} - 1 \geq (q-1)^{a_i} q^{a_i j - a_i}$ for $1 \leq j \leq m_i$,

$$q^{d_i} \geq |\mathrm{GL}_{m_i}(q^{a_i})| = q^{a_i m_i (m_i - 1)/2} \cdot \prod_{j=1}^{m_i} (q^{a_i j} - 1) \geq (q-1)^{m_i a_i} q^{d_i - m_i a_i},$$

and $\mathrm{GL}_{m_i}(q^{a_i})$ has $\mathbb{F}_q$-rank $m_i a_i$. Since the rank of $\underline{C}(g)$ is at most n, it follows that

$$q^d \geq |\mathbf{C}_{\mathrm{GL}(V)}(g)| \geq (q-1)^n q^{d-n}, \tag{4.2}$$

and so

$$|\mathbf{C}_{\mathrm{SL}(V)}(g)| \geq (q-1)^{n-1} q^{d-n}. \tag{4.3}$$

Now, if $n \geq 2/\nu$, then, since $\alpha = 1 - \nu^2/4 > 1 - \nu/2$, we have

$$|\mathbf{C}_{\mathrm{SL}(V)}(g)| \geq q^{d-n} \geq q^{(\alpha - 1/n)n^2} > q^{(1-\nu/2-\nu/2)n^2} > |G|^{1-\nu}.$$

If $n < 2/\nu$, then $\alpha = 1 - \nu^2/4 > 1 - 1/n^2$, whence (4.1) implies that g is a scalar matrix and therefore that $\mathbf{C}_{\mathrm{SL}(V)}(g) = \mathrm{SL}(V)$. □

Proposition 4.2. *Let $n \geq 2$, $V = \mathbb{F}_q^n$, and let $g \in \mathrm{GL}(V)$ have support $s := \mathsf{supp}(g)$. Then*

(a) $(n-s)^2 \leq \dim \mathbf{C}_{\mathrm{GL}(V\otimes_{\mathbb{F}_q}\overline{\mathbb{F}}_q)}(g) \leq n(n-s)$,

(b) $|\mathbf{C}_{\mathrm{GL}(V)}(g)| \leq q^{n(n-s)}$, *and*

(c) $q^{ns-2} \leq |g^{\mathrm{SL}(V)}| \leq q^{2ns+n-s^2-1}$. *If particular,* $|\mathrm{SL}(V)|^{s/3n} \leq |g^{\mathrm{SL}(V)}| \leq |\mathrm{SL}(V)|^{3s/n}$; *in fact,* $|\mathrm{SL}(V)|^{s/2n} \leq |g^{\mathrm{SL}(V)}| \leq |\mathrm{SL}(V)|^{2.5s/n}$ *if* $(n,q) \neq (2,2), (2,3)$.

Proof. (a) In the case g is unipotent, the estimates were already proved in [LiSh1, pp. 509–510]. In the general case, we can replace V by $V \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q$, and let $\lambda_1, \dots, \lambda_m \in \overline{\mathbb{F}}_q^\times$ be all the distinct eigenvalues of the semisimple part t of $g = tu$ on V, with multiplicities $n_1, \dots, n_m$. If $V_i = \overline{\mathbb{F}}_q^{n_i}$ denotes the corresponding t-eigenspace on V and if the unipotent part u of g acts on V_i as u_i, then

$$\mathbf{C}_{\mathrm{GL}(V)}(g) = \prod_{i=1}^m \mathbf{C}_{\mathrm{GL}(V_i)}(u_i).$$

For $s_i := \mathsf{supp}(u_i)$, the largest g-eigenspace on V_i has dimension $n_i - s_i$, and we may assume that

$$n_i - s_i \leq n - s = n_1 - s_1.$$

By the unipotent case, $(n_i - s_i)^2 \leq \dim \mathbf{C}_{\mathrm{GL}(V_i)}(u_i) \leq n_i(n_i - s_i)$. Hence

$$(n-s)^2 = (n_1-s_1)^2 \leq \sum_i (n_i-s_i)^2 \leq \dim \mathbf{C}_{\mathrm{GL}(V)}(g) \leq \sum_i n_i(n_i-s_i) \leq (n_1-s_1)\sum_i n_i = n(n-s).$$

(b) follows from (a) by (4.2).

(c) By [LMT, Lemma 4.1(ii)], $q^{n^2-2} < |\mathrm{SL}_n(q)| < q^{n^2-1}$. On the other hand, setting $d := \dim \mathbf{C}_{\mathrm{GL}(V)}(g)$, we have $q^{d-n} \leq |\mathbf{C}_{\mathrm{SL}_n(q)}(g)| \leq q^d$ by (4.2)–(4.3), and $(n-s)^2 \leq d \leq n(n-s)$ by (a). It follows that $q^{ns-2} \leq |g^{\mathrm{SL}_n(q)}| \leq q^{2ns+n-s^2-1}$, yielding the first statement.

The second statement is obvious when $s = 0$, and can be checked directly when $n = 2$. When $n \geq 3$, $2ns + n - s^2 - 1 \leq (n^2-2)(3s/n)$ and $ns - 2 \geq (n^2-1)(s/3n)$.

The third statement is obvious when $s = 0$, and can be checked directly when $n = 2$ or $s = 1$. When $n \geq 3$ and $s \geq 2$, $2ns + n - s^2 - 1 \leq (n^2-2)(2.5s/n)$ and $ns - 2 \geq (n^2-1)(s/2n)$. □

Lemma 4.3. *For $1 \geq \varepsilon > 0$ and $n \in \mathbb{Z}_{\geq 1}$, if $V = \mathbb{F}_q^n$, $g \in \mathrm{GL}(V)$, and $\dim \mathrm{Ker} P(g) \leq \varepsilon n$ for all polynomials $P(x) \in \mathbb{F}_q[x]$ of degree $< d := \lceil 1/\varepsilon \rceil$, then*

$$|\mathbf{C}_{\mathrm{GL}(V)}(g)| \leq q^{n^2\varepsilon}.$$

Proof. Let $s := \mathsf{supp}(g)$ and suppose that $s < n - \varepsilon n$. Then $n - s = \dim \mathrm{Ker}(g - \lambda)$ for some eigenvalue λ of g on $V \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q$. Since any Galois conjugate of λ over $\mathbb{F}_q$ is also an eigenvalue for g with eigenspace of the same dimension $n-s$, the Galois orbit of λ has length $e \leq n/(n-s) < 1/\varepsilon \leq d$. Thus λ is a root of some polynomial $P \in \mathbb{F}_q[x]$ of degree $e < d$. Hence, by hypothesis,

$$n - s = \dim \mathrm{Ker}(g - \lambda) \leq \varepsilon n,$$

and so $s \geq n - \varepsilon n$, a contradiction. We have shown that $s \geq n - \varepsilon n$. By Proposition 4.2(b), this implies that $|\mathbf{C}_{\mathrm{GL}(V)}(g)| \leq q^{n^2\varepsilon}$. □

Now we can prove character bounds for elements with large support.

Theorem 4.4. *There exist explicit constants $\gamma > 0$ and $C \geq 4$ such that the following statement holds for any positive integer n, any $0 < \beta < 1$, any $V = \mathbb{F}_q^n$ for any prime power q, any $G := \mathrm{SL}(V)$, $\mathrm{SU}(V)$, $\mathrm{Sp}(V)$, or $\Omega(V)$ (or $\mathrm{SO}(V)$ or $\mathrm{Spin}(V)$ if q is odd), any element $g \in G$, and any irreducible character $\chi \in \mathrm{Irr}(G)$. If $s := \mathsf{supp}(g) \geq \max(C, \beta n)$, then*

$$\frac{|\chi(g)|}{\chi(1)} \leq \chi(1)^{-\frac{\gamma s}{n \cdot \lceil 1/\beta \rceil}}.$$

Proof. As $n \geq C$, by taking C sufficiently large, we can guarantee that n is as large as we wish; also we may assume that $\chi(1) > 1$. Let $b := \lceil n/s \rceil$. Also set

$$\varepsilon_0 = \frac{1}{12},\ \delta_0 = \frac{8}{9}$$

if $G = \mathrm{SL}(V)$ or $\mathrm{SU}(V)$, and

$$\varepsilon_0 = 0.0011,\ \delta_0 = 0.992$$

otherwise. By Lemma 4.3, there exist $d \in \mathbb{Z}_{\geq 3}$ and $0 < \varepsilon < 1$ such that for $h \in G$, if $\dim \mathrm{Ker} P(h) \leq \varepsilon n$ for all non-constant $P(x) \in \mathbb{F}_q[x]$ of degree $< d$, then

$$\begin{aligned}
|\mathbf{C}_{\mathrm{GL}(V)}(h)| &\leq q^{n^2/12}, \text{ if } G = \mathrm{SL}(V) \cong \mathrm{SL}_n(q),\\
|\mathbf{C}_{\mathrm{GL}(V)}(h)| &\leq q_0^{n^2/12}, \text{ if } G = \mathrm{SU}(V) \cong \mathrm{SU}_n(q_0),\\
|\mathbf{C}_{\mathrm{GL}(V)}(h)| &\leq q^{(n/2-1)^2\varepsilon_0}, \text{ if } G = \mathrm{Sp}(V),\ \mathrm{SO}(V),\ \Omega(V),\\
|\mathbf{C}_{\mathrm{GL}(V)}(\bar{h})| &\leq q^{(n/2-1)^2\varepsilon_0}/2, \text{ if } 2 \nmid q \text{ and } G = \mathrm{Spin}(V),
\end{aligned} \tag{4.4}$$

(with the convention that in the spin case, $\bar{h}$ is the image of h in $\Omega(V)$ and $P(h)$ is replaced by $P(\bar{h})$; this ensures $|\mathbf{C}_G(h)| \leq q^{(n/2-1)^2\varepsilon_0}$ in the spin case). Indeed, we can take

$$\varepsilon = 1/4000,\ d = \lceil \varepsilon^{-1} \rceil = 4000,\ C \geq 224,$$

and have

$$q^{(n/2-1)^2\varepsilon_0}/2 \geq q^{(n/2-1)^2\varepsilon_0 - 1} > q^{n^2\varepsilon}.$$

The centralizer bound (4.4) implies by [GLT1, Theorem 1.5] and [GLT2, Theorem 1.4] that

$$|\chi(h)| \leq \chi(1)^{\delta_0}. \tag{4.5}$$

If $G = \mathrm{SL}(V)$, by Proposition 3.1, choosing $C \geq 8d^2/\varepsilon$ and $\gamma > 0$ sufficiently small so that

$$3 + d - \frac{\varepsilon^2 ns}{18d^2} < -\gamma ns, \tag{4.6}$$

we then have

$$\mathbf{P}\big[|\mathbf{C}_{\mathrm{GL}_n(q)}(g^{\mathsf{X}_1} \cdots g^{\mathsf{X}_b})| \geq q^{n^2/12}\big] < q^{-\gamma ns}.$$

If $G \neq \mathrm{SL}(V)$, by Proposition 3.1, choosing $C \geq 23d^2/\varepsilon$ and $\gamma > 0$ sufficiently small so that

$$2 + d - \frac{\varepsilon^2 ns}{31d^2} < -\gamma ns, \tag{4.7}$$

we then have

$$\mathbf{P}\big[|\mathbf{C}_{\mathrm{GL}(V)}(g^{\mathsf{X}_1} \cdots g^{\mathsf{X}_b})| \geq q_0^{n^2/12}\big] < q^{-\gamma ns}$$

when $G = \mathrm{SU}(V)$,

$$\mathbf{P}\big[|\mathbf{C}_{\mathrm{GL}(V)}(g^{\mathsf{X}_1} \cdots g^{\mathsf{X}_b})| \geq q^{(n/2-1)^2\varepsilon_0}\big] < q^{-\gamma ns}$$

when $G = \mathrm{Sp}(V)$, $\mathrm{SO}(V)$, or $\Omega(V)$, and

$$\mathbf{P}\big[|\mathbf{C}_{\mathrm{GL}(V)}(\bar{g}^{\mathsf{X}_1} \cdots \bar{g}^{\mathsf{X}_b})| \geq q^{(n/2-1)^2\varepsilon_0}/2\big] < q^{-\gamma ns}$$

when $2 \nmid q$ and $G = \mathrm{Spin}(V)$. Indeed, by taking $C \geq 23d^2/\varepsilon$ and $0 < \gamma \leq \varepsilon^2/32d^2$, we have

$$\frac{\varepsilon^2 ns}{31d^2} - \gamma ns \geq \frac{\varepsilon^2 ns}{992d^2} \geq \frac{C^2\varepsilon^2}{992d^2} = \frac{529d^2}{992} \geq d+3$$

when $d \geq 3$, ensuring (4.6) and (4.7).

By (4.5) applied to $h = g^{\mathsf{X}_1} \cdots g^{\mathsf{X}_b}$, this implies that

$$\mathbf{P}\big[|\chi(g^{\mathsf{X}_1} \cdots g^{\mathsf{X}_b})| \geq \chi(1)^{\delta_0}\big] < q^{-\gamma ns}.$$

Thus,

$$\big|\mathbf{E}[\chi(g^{\mathsf{X}_1} \cdots g^{\mathsf{X}_b})]\big| \leq \mathbf{E}\big[|\chi(g^{\mathsf{X}_1} \cdots g^{\mathsf{X}_b})|\big] \leq \chi(1)^{\delta_0} + \chi(1)q^{-\gamma ns}. \tag{4.8}$$

On the other hand,

$$\mathbf{E}[\chi(g^{\mathsf{X}_1} \cdots g^{\mathsf{X}_b})] = \chi(g)^b/\chi(1)^{b-1} \tag{4.9}$$

by Lemma 3.2.

Now assume that $s = \mathsf{supp}(g) \geq \beta n$. Then

$$b = \lceil n/s \rceil \leq \lceil 1/\beta \rceil.$$

As $\chi(1) < |G|^{1/2} < q^{n^2/2}$, we have $q^{-\gamma ns} \leq \chi(1)^{-2\gamma s/n}$. Without loss of generality, we may assume $\gamma \leq (1-\delta_0)/2 = 0.004$, so

$$\chi(1)^{\delta_0} \leq \chi(1)^{1-\frac{2\gamma s}{n}}.$$

For $n \geq 9$, the minimal degree for a non-trivial character of G is at least $2^{n/2}$ [LaSe], so we have $\chi(1)^{-\gamma s/n} \leq 2^{-\gamma s/2}$. If C is sufficiently large (say $C \geq 2/\gamma$), this is at most $1/2$, so when $\chi(1) > 1$,

$$2\chi(1)^{1-\frac{2\gamma s}{n}} \leq \chi(1)^{1-\frac{\gamma s}{n}}.$$

It now follows from (4.8) and (4.9) that

$$|\chi(g)| \leq \chi(1)^{1-\frac{\gamma s}{nb}} \leq \chi(1)^{1-\frac{\gamma s}{n\lceil 1/\beta \rceil}},$$

as stated. Moreover, our proof shows that one can take

$$\gamma = \frac{\varepsilon^2}{32d^2} = \frac{1}{2^{13} \cdot 10^{12}},\ C = \frac{64d^2}{\varepsilon^2} = 2^{14} \cdot 10^{12},$$

although this choice is not optimal. □

[GLT1, Theorem 1.5] and [GLT2, Theorem 1.3] produced the character bound $|\chi(1)|^\delta$ for any element g in a classical group G with $|\mathbf{C}_G(g)| \leq |G|^\varepsilon$, but only *for certain positive constants* $\varepsilon < 1$. Our next result generalizes this to *arbitrary constants* $0 < \varepsilon < 1$:

Theorem 4.5. *For any $0 < \varepsilon < 1$, there exists a constant $0 < \delta < 1$ such that the following statement holds. For any $n \in \mathbb{Z}_{\geq 2}$, any prime power q, any quasisimple classical group*

$$G = \mathrm{SL}_n(q),\ \mathrm{SU}_n(q),\ \mathrm{Sp}_{2n}(q),\ \Omega_n^\pm(q),\ \mathrm{Spin}_n^\pm(q)$$

any element $g \in G$, and any irreducible character $\chi \in \mathrm{Irr}(G)$, if $|\mathbf{C}_G(g)| \leq |G|^\varepsilon$ we have

$$|\chi(g)| \leq \chi(1)^\delta.$$

Proof. (a) First suppose that $|\mathbf{C}_H(h)| \leq |H|^\varepsilon$ for some element h of $H := \mathrm{SU}(V)$, $\mathrm{Sp}(V)$, $\mathrm{SO}(V)$, or $\Omega(V)$. Here V is $\mathbb{F}_{q^2}^n$, $\mathbb{F}_q^{2n}$, $\mathbb{F}_q^n$, and $\mathbb{F}_q^n$ respectively for $\mathrm{SU}_n(q)$, $\mathrm{Sp}_{2n}(q)$, $\mathrm{SO}_n(q)$, and $\Omega_n(q)$ respectively. Then $H \leq L := \mathrm{SL}(V)$ and $|H| > |L|^{1/3}$. Since

$$|L| \geq |H\mathbf{C}_L(h)| = \frac{|H| \cdot |\mathbf{C}_L(h)|}{|\mathbf{C}_H(h)|},$$

we have

$$|\mathbf{C}_L(h)| \leq \frac{|L|}{|H|/|\mathbf{C}_H(h)|} \leq \frac{|L|}{|H|^{1-\varepsilon}} \leq |L|^{(2+\varepsilon)/3}.$$

Next, suppose that $2 \nmid q$ and $|\mathbf{C}_H(h)| \leq |H|^\varepsilon$ for some element h of $H = \mathrm{Spin}(V)$. Then H projects onto $\bar{H} := \Omega(V) \leq L = \mathrm{SL}(V)$, sending h to $\bar{h}$, and $|\mathbf{C}_{\bar{H}}(\bar{h})| \leq |\mathbf{C}_H(h)| \leq |H|^\varepsilon$. As above, we still have $|H| > |L|^{1/3}$. Hence the above argument yields $|\mathbf{C}_L(\bar{h})| \leq |L|^{(2+\varepsilon)/3}$.

(b) Now set $\nu := 1 - \varepsilon$ if $G = \mathrm{SL}(V)$, and $\nu := (1-\varepsilon)/3$ otherwise. By the observations in (a), we have $|\mathbf{C}_{\mathrm{SL}(V)}(g)| \leq |\mathrm{SL}(V)|^{1-\nu}$, with the convention that g is replaced by its image in $\Omega(V)$ in the case $G = \mathrm{Spin}(V)$. By Lemma 4.1, there exists some $0 < \alpha < 1$ such that

$$\dim_{\mathbb{F}_q} \mathbf{C}_{\mathrm{End}(V)}(g) \leq \alpha n^2.$$

On the other hand, g has an eigenspace of dimension $n - s$ on $\overline{V} = V \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q$ for $s := \mathsf{supp}(g)$, hence

$$\dim_{\mathbb{F}_q} \mathbf{C}_{\mathrm{End}(V)}(g) = \dim_{\overline{\mathbb{F}}_q} \mathbf{C}_{\mathrm{End}(\overline{V})}(g) \geq (n-s)^2.$$

It follows that $s \geq n(1 - \sqrt{\alpha})$. Now we can apply Theorem 4.4(i), with $\beta := 1 - \sqrt{\alpha}$, and take $\delta \geq \gamma\beta/\lceil 1/\beta \rceil$ when $s \geq C$. If $s < C$, then n is bounded, and the result of Gluck [Gl] implies the statement in this case. □

5. Further bootstrapping and uniform character bounds

In this section, we prove Theorem 5.5, an exponential upper bound for $|\chi(g)|$ with exponent linear in $\frac{\mathsf{supp}(g)}{n}$, with an explicit, though very small, coefficient. If $\mathsf{supp}(g)$ is greater than any given positive constant multiple of n, we already have this by the results of section 4, so what is needed is a second bootstrapping argument to go from elements of small support to elements whose support satisfies a linear lower bound. It may be useful for the reader to keep in mind the case that g is a transvection. Here we want that the support of the product of b random transvections, with probability very close to 1, grows linearly with b for $b < n$; this is given by Proposition 5.4.

Lemma 5.1. *Let V be a finite dimensional vector space over a field $\mathbb{F}$, $g, h \in \mathrm{End}(V)$, and let $\lambda, \mu \in \overline{\mathbb{F}}$. Then the following statements hold.*

(i) $\mathrm{codim}\,\mathrm{Ker}(gh - \lambda\mu) \leq \mathrm{codim}\,\mathrm{Ker}(g - \lambda) + \mathrm{codim}\,\mathrm{Ker}(h - \mu)$.
(ii) $\mathsf{supp}(gh) \leq \mathsf{supp}(g) + \mathsf{supp}(h)$.

Proof. (i) Let $A := \mathrm{Ker}(g - \lambda)$ and $B := \mathrm{Ker}(h - \mu)$. As $A + B \subseteq V$, we have

$$\dim(A \cap B) \geq \dim(A) + \dim(B) - \dim(V) = \dim(V) - \mathrm{codim}(A) - \mathrm{codim}(B).$$

Since $A \cap B \subseteq \mathrm{Ker}(gh - \lambda\mu)$, the statement follows.

(ii) Now choose λ, μ so that $\mathrm{codim}\,\mathrm{Ker}(g - \lambda) = \mathsf{supp}(g)$ and $\mathrm{codim}\,\mathrm{Ker}(h - \mu) = \mathsf{supp}(h)$. Since $\mathsf{supp}(gh) \leq \mathrm{codim}\,\mathrm{Ker}(gh - \lambda\mu)$, the statement follows from (i). □

In the next statement, we identify $V^* \otimes V$ with $\mathrm{End}(V)$ for any finite dimensional vector space over a field $\mathbb{F}$, and $\lambda \in \mathbb{F}$ with $\lambda \cdot \mathrm{Id}_V$.

Proposition 5.2. *Let V be an n-dimensional vector space over a field $\mathbb{F}$ and b and k positive integers. Let $x_1, \ldots, x_b$ be elements of $\mathrm{GL}(V)$ and $v_1, \ldots, v_k \in V$ and $\phi_1, \ldots, \phi_k$ linearly independent vectors in V and V^* respectively. Let $0 \neq \lambda \in \mathbb{F}$ be a scalar and let*

$$T := \lambda + \sum_{j=1}^{k} \phi_j \otimes v_j$$

be regarded as an element of $\mathrm{End}(V)$. *For* $1 \le i \le b$ *and* $1 \le j \le k$, *let* $w_{i,j} := x_i^{-1}(v_j)$ *and* $\psi_{i,j} := x_i^{-1}(\phi_j)$. *For* $1 \le s \le b$, *let*

$$A_s := \dim \mathrm{Span}(w_{i,j} \mid 1 \le i \le s, 1 \le j \le k),\ B_s := \dim \mathrm{Span}(\psi_{i,j} \mid s \le i \le b, 1 \le j \le k).$$

Then the rank of $T^{x_1} \cdots T^{x_b} - \lambda^b$ *is at least*

$$\sum_{s=1}^{b} \max(0, A_s - A_{s-1} + B_s - B_{s+1} - k).$$

Proof. It suffices to find vectors $u_{s,t} \in V$ and $\omega_{s,t} \in V^*$ indexed by

$$1 \le s \le b,\ 1 \le t \le \max(0, A_s - A_{s-1} + B_s - B_{s+1} - k)$$

such that

$$\omega_{s',t'}\big((T^{x_1} \cdots T^{x_b} - \lambda^b)(u_{s,t})\big) = \begin{cases} \lambda^{b-1}, & \text{if } (s',t') = (s,t), \\ 0, & \text{if } s' \ge s \text{ and } (s',t') \ne (s,t). \end{cases} \tag{5.1}$$

Indeed, this guarantees that, with respect to the lexicographic ordering on the two bases, the pairing $\langle \omega | v \rangle := \omega((T^{x_1} \cdots T^{x_b} - \lambda^b)(v))$ induced by (5.1) between the span of the $\omega_{s',t'}$ and the span of the $\lambda^{1-b} u_{s,t}$ is unitriangular in terms of these bases, hence perfect.

To achieve this, we construct vectors $u_{s,t} \in V$ and $\omega_{s,t} \in V^*$ with the following properties:

(a) For $s < i$, $\psi_{i,j}(u_{s,t}) = 0$.
(b) For $s > i$, $\omega_{s,t}(w_{i,j}) = 0$.
(c) For all s, t, and t', $\omega_{s,t}((T^{x_s} - \lambda)(u_{s,t'})) = \delta_{t,t'}$.

To accomplish this goal, for each s, let

$$W_s := \mathrm{Span}(w_{s,1}, \ldots, w_{s,k}),\ \Psi_s := \mathrm{Span}(\psi_{s,1}, \ldots, \psi_{s,k}).$$

For $1 \le s, s' \le b$, we define

$$W_{[s,s']} := W_s + W_{s+1} + \cdots + W_{s'},\ \Psi_{[s,s']} := \Psi_s + \Psi_{s+1} + \cdots + \Psi_{s'},$$

with the convention that, if $s > s'$ we have $W_{[s,s']} = \Psi_{[s,s']} = \{0\}$.

As

$$\dim \Psi_s / (\Psi_s \cap \Psi_{[s+1,b]}) = \dim \Psi_{[s,b]} / \Psi_{[s+1,b]} = B_s - B_{s+1},$$

there exists a $(B_s - B_{s+1})$-dimensional subspace $U_s \subseteq V$ such that $\psi_{i,j}(U_s) = 0$ whenever $i > s$ but for $u \in U_s$, $\psi_{s,j}(u) = 0$ for all j implies $u = 0$. Thus the operator

$$T^{x_s} - \lambda = \sum_{j=1}^{k} x_s^{-1}(\phi_j) \otimes x_s^{-1}(v_j) = \sum_{j=1}^{k} \psi_{s,j} \otimes w_{s,j}$$

annihilates every element of V killed by Ψ_s, maps V to W_s, and maps U_s injectively to W_s, and so

$$\mathrm{Ker}(T^{x_s} - \lambda) \cap U_s = \{0\}. \tag{5.2}$$

Let $W_s' \subseteq W_s$ denote a subspace (of dimension $A_s - A_{s-1}$) complementary in W_s to $W_{[1,s-1]} \cap W_s$, and let

$$U_s' := \{u \in U_s \mid (T^{x_s} - \lambda)(u) \in W_s'\}.$$

Then the dimension c_s of U_s' satisfies

$$c_s \ge \dim U_s + \dim W_s' - \dim W_s = B_s - B_{s+1} + A_s - A_{s-1} - k.$$

Let $(u_{s,1}, \ldots, u_{s,c_s})$ denote any basis of U_s'. Condition (a) holds for all vectors in U_s and therefore for the $u_{s,t}$.

Next, for each s we choose $\omega_{s,1},\dots,\omega_{s,c_s}$ satisfying condition (c) and annihilating $W_{[1,s-1]}$ (guaranteeing condition (b)). We can do this because the conditions on $\omega_{s,t}$ are that $\omega_{s,t}((T^{x_s}-\lambda)(u_{s,t}))=1$ and $\omega_{s,t}$ annihilates

$$(T^{x_s}-\lambda)(\mathrm{Span}(u_{s,1},\dots,u_{s,t-1},u_{s,t+1},\dots,u_{s,c_s}))+W_{[1,s-1]}. \tag{5.3}$$

Thus, it suffices to show that $(T^{x_s}-\lambda)(u_{s,t})$ does not belong to the vector space (5.3). As the vectors $u_{s,1},\dots,u_{s,c_s}$ form a basis of U'_s, by (5.2), the latter condition holds since $(T^{x_s}-\lambda)(U'_s)\subseteq W'_s$ meets $W_{[1,s-1]}$ in $\{0\}$ by definition of W'_s.

We claim that for $s+1\le s'\le b+1$, we have

$$T^{x_{s'}}\cdots T^{x_b}(u_{s,t})=\lambda^{b+1-s'}u_{s,t}, \tag{5.4}$$

by descending induction on s'. The statement is trivially true for $s'=b+1$ (since $T^{x_{s'}}\cdots T^{x_b}$ means Id_V). If (5.4) holds for $s'+1$, then

$$T^{x_{s'}}\cdots T^{x_b}(u_{s,t})=T^{x_{s'}}(\lambda^{b-s'}u_{s,t})=\lambda^{b+1-s'}u_{s,t}+\lambda^{b-s'}\sum_{j=1}^{k}\psi_{s',j}(u_{s,t})w_{s,j}=\lambda^{b+1-s'}u_{s,t},$$

where the last equality follows from condition (a).

Applying T^{x_s} to both sides of (5.4) with $s'=s+1$, we obtain

$$T^{x_s}T^{x_{s+1}}\cdots T^{x_b}(u_{s,t})=\lambda^{b-s}T^{x_s}(u_{s,t}). \tag{5.5}$$

Next, we claim that for $1\le i\le s$, we have

$$T^{x_i}T^{x_{i+1}}\cdots T^{x_s}(u_{s,t})\in\lambda^{s-i}T^{x_s}(u_{s,t})+W_{[i,s-1]}. \tag{5.6}$$

Indeed, this is trivial when $i=s$. If (5.6) holds for $i+1$, then there exists $w\in W_{[i+1,s-1]}$ so that

$$\begin{aligned}T^{x_i}T^{x_{i+1}}\cdots T^{x_s}(u_{s,t})&=T^{x_i}(\lambda^{s-i-1}T^{x_s}(u_{s,t})+w)\\&\in\lambda^{s-i}T^{x_s}(u_{s,t})+\lambda w+W_i\subset\lambda^{s-i}T^{x_s}(u_{s,t})+W_{[i,s-1]}.\end{aligned}$$

By (5.5) and the $i=1$ case of (5.6), we obtain

$$\begin{aligned}T^{x_1}\cdots T^{x_b}(u_{s,t})&=\lambda^{b-s}T^{x_1}\cdots T^{x_s}(u_{s,t})\in\lambda^{b-1}T^{x_s}(u_{s,t})+W_{[1,s-1]}\\&=\lambda^bT^{x_s}(u_{s,t})+\lambda^{b-1}(T^{x_s}-\lambda)(u_{s,t})+W_{[1,s-1]}.\end{aligned}$$

Subtracting $\lambda^bu_{s,t}$ and applying $\omega_{s',t'}$ to both sides with $s'\ge s$, condition (b) implies

$$\omega_{s',t'}((T^{x_1}\cdots T^{x_b}-\lambda^b)(u_{s,t}))=\lambda^{b-1}\omega_{s',t'}\big((T^{x_s}-\lambda)(u_{s,t})\big).$$

If $s'=s$, this is $\lambda^{b-1}\delta_{t,t'}$ by condition (c), and if $s'>s$, it is zero by condition (b), yielding (5.1) as desired. □

Proposition 5.3. *Let $V=\mathbb{F}_q^n$, $b\ge 2$ and k positive integers with $bk\le n/2$, and let $v_1,\dots,v_k$ be linearly independent vectors in V. Let $\mathsf{X}_1,\dots,\mathsf{X}_b$ be uniform independent random variables on $G=\mathrm{Cl}(V)$. Then we have*

$$\mathbf{P}\big[\dim\mathrm{Span}(\mathsf{X}_i(v_j)\mid 1\le i\le b,1\le j\le k)\le\frac{2bk}{3}\big]<\begin{cases}q^{bk(1-n/6)}, & \mathrm{Cl}=\mathrm{SL},\\ q^{bk(1-n/12)}, & \mathrm{Cl}\ne\mathrm{SL}.\end{cases}$$

Proof. Consider the bk-term sequence of random vectors

$$\mathsf{X}_1(v_1),\dots,\mathsf{X}_1(v_k),\mathsf{X}_2(v_1),\dots,\mathsf{X}_2(v_k),\dots,\mathsf{X}_b(v_1),\dots,\mathsf{X}_b(v_k).$$

First we bound from the above the probability $\mathbf{P}_{ij}$ that $\mathsf{X}_i(v_j)$ lies in the span

$$S_{ij}:=\mathrm{Span}(\mathsf{X}_{i'}(j'),1\le i'<i,1\le j'\le k,\ \mathsf{X}_i(v_l),1\le l\le j-1)$$

of the preceding vectors, conditioning on all the vectors preceding $\mathsf{X}_i(v_j)$ in the sequence. Since $v_1, \dots, v_k$ are linearly independent, this conditional probability is 0 if $i = 1$. Next, let $i \geq 2$, and let H denote the subgroup of all the elements in G that fix each of $v_1, \dots, v_{j-1}$ (in particular, $H = G$ if $j = 1$). By Lemma 2.4 applied to $d = j - 1$ (so that $d \leq k - 1 \leq n/4 - 1 \leq (n-3)/2$), H acts on

$$\Omega := V \smallsetminus \mathrm{Span}(v_1, \dots, v_{j-1})$$

with orbits $\Omega_1 = w_1^H, \dots, \Omega_s = w_s^H$, each of length at least

$$L := \begin{cases} q^n - q^{j-1}, & \mathrm{Cl} = \mathrm{SL}, \\ q^{n-d-2} = q^{n-j-1}, & \mathrm{Cl} \neq \mathrm{SL}. \end{cases}$$

We want to count the number of $g \in G$, with $g(v_1), \dots, g(v_{j-1})$ all fixed, and with $g(v_j) \in S_{ij}$. Fix such a g, and consider any such g'. Then $h := g^{-1}g' \in H$, and so it sends $v_j \in \Omega$ to some $w \in \Omega_t$ with $1 \leq t \leq s$. With w fixed, the number of possibilities for h is at most $|\mathrm{Stab}_H(w_t)|$. Hence, with t fixed, the number of possibilities for such g' is at most

$$|\Omega_t \cap S_{ij}| \cdot |\mathrm{Stab}_H(w_t)| = |H| \cdot |\Omega_t \cap S_{ij}|/|\Omega_t| \geq \frac{|H| \cdot |\Omega_t \cap S_{ij}|}{L}.$$

As we condition on all the vectors preceding $\mathsf{X}_i(v_j)$, it follows that

$$\mathbf{P}_{ij} \leq \frac{1}{|H|} \cdot \sum_{t=1}^{s} \frac{|H| \cdot |\Omega_t \cap S_{ij}|}{L} \leq \frac{|S_{ij}|}{L}.$$

Note that $\dim S_{ij} \leq k(i-1) + j - 1$. Hence, conditioning on the sequence of previous vectors, the probability $\mathbf{P}_{ij}$ that $\mathsf{X}_i(v_j)$ lies in their span S_{ij} is at most

$$\frac{q^{k(i-1)+j-1}}{q^n - q^{j-1}} < 2q^{k(i-1)+j-1-n} \leq q^{bk-n}$$

when $\mathrm{Cl} = \mathrm{SL}$, and at most

$$\frac{q^{k(i-1)+j-1}}{q^{n-j-1}} < q^{k(i-1)+2j-n} \leq q^{(b+1)k-n}$$

when $\mathrm{Cl} \neq \mathrm{SL}$, regardless of what the previous vectors are.

We also note that, since $b \geq 2$ and $bk \leq n/2$, $(b+1)k \leq 3bk/2 \leq 3n/4$. Therefore, the probability that there exist r terms $\mathsf{X}_i(v_j)$ in this sequence belonging to the span of previous terms is less than

$$\binom{bk}{r} q^{r(bk-n)} \leq \binom{bk}{r} q^{-rn/2}$$

when $\mathrm{Cl} = \mathrm{SL}$, and less than

$$\binom{bk}{r} q^{r((b+1)k-n)} \leq \binom{bk}{r} q^{-rn/4}$$

when $\mathrm{Cl} \neq \mathrm{SL}$. In particular, the probability that $r \geq bk/3$ is less than

$$\sum_{r=\lceil bk/3 \rceil}^{bk} \binom{bk}{r} q^{-rn/2\kappa} < 2^{bk} q^{-bkn/6\kappa} < q^{bk(1-n/6\kappa)}$$

with $\kappa = 1$ when $\mathrm{Cl} = \mathrm{SL}$ and $\kappa = 2$ when $\mathrm{Cl} \neq \mathrm{SL}$. □

Proposition 5.4. *If n is a sufficiently large positive integer, $V = \mathbb{F}_q^n$, $g \in G := \mathrm{Cl}(V)$, then there exists a positive integer b such that*

$$b \cdot \mathsf{supp}(g) \leq n,$$

and if $\mathsf{X}_1, \dots, \mathsf{X}_b$ *are i.i.d. uniform random variables on* G*, then*

$$\mathbf{P}[\mathsf{supp}(g^{\mathsf{X}_1} \cdots g^{\mathsf{X}_b}) < n/9] < \begin{cases} q^{-n^2/20}, & \mathrm{Cl} = \mathrm{SL} \\ q^{-n^2/40}, & \mathrm{Cl} \neq \mathrm{SL}. \end{cases}$$

Proof. If $\mathsf{supp}(g) \geq n/6$, we can take $b = 1$. Hence, without loss of generality, we may assume $k := \mathsf{supp}(g) < n/6$, and hence we may choose $b \in \mathbb{Z}_{\geq 2}$ so that $n/3 \leq bk < n/2$. Let λ be an eigenvalue of g such that $k = \operatorname{codim} \operatorname{Ker}(g - \lambda)$, and choose linearly independent vectors $v_1, \dots, v_k \in V$ and $v_1^*, \dots, v_k^* \in V^*$ such that

$$g = \lambda + \sum_{j=1}^{k} v_j^* \otimes v_j.$$

By Lemma 5.1(i), $\operatorname{codim} \operatorname{Ker}(g^{\mathsf{X}_1} \cdots g^{\mathsf{X}_b} - \lambda^b) \leq bk < n/2$. Thus $\operatorname{Ker}(g^{\mathsf{X}_1} \cdots g^{\mathsf{X}_b} - \lambda^b)$ is the largest eigenspace for $g^{\mathsf{X}_1} \cdots g^{\mathsf{X}_b}$, and so $\mathsf{supp}(g^{\mathsf{X}_1} \cdots g^{\mathsf{X}_b}) = \operatorname{codim} \operatorname{Ker}(g^{\mathsf{X}_1} \cdots g^{\mathsf{X}_b} - \lambda^b)$.

Again define $\kappa := 1$ if $G = \mathrm{SL}(V)$ and $\kappa := 2$ if $G \neq \mathrm{SL}(V)$. By Proposition 5.3, the probability that $\dim \operatorname{Span}(\mathsf{X}_i(v_j))$ or $\dim \operatorname{Span}(\mathsf{X}_i(v_j^*))$ is $\leq 2bk/3$ is at most

$$2q^{bk(1-n/6\kappa)} \leq 2q^{n(1-n/6\kappa)/3} \leq q^{-n^2/20\kappa}$$

if n is sufficiently large. On the other hand, by Proposition 5.2, if

$$\dim \operatorname{Span}(\mathsf{X}_i(v_j)),\ \dim \operatorname{Span}(\mathsf{X}_i(v_j^*)) > \frac{2bk}{3},$$

then

$$\begin{aligned} \operatorname{codim} \operatorname{Ker}(g^{\mathsf{X}_1} \cdots g^{\mathsf{X}_b} - \lambda^b) &\geq \sum_{s=1}^{b} \max(0, A_s - A_{s-1} + B_s - B_{s+1} - k) \\ &\geq \sum_{s=1}^{b} (A_s - A_{s-1} + B_s - B_{s+1} - k) \\ &= A_b - A_0 + B_1 - B_{b+1} - bk \\ &> \frac{2bk}{3} + \frac{2bk}{3} - bk \\ &= \frac{bk}{3} \geq \frac{n}{9}. \end{aligned}$$

Hence the proposition follows. □

Now we can prove one of the main results of the paper, giving a uniform exponential character bound in terms of the support.

Theorem 5.5. *There exists an explicit constant* $\sigma > 0$ *such that the following statement holds for any positive integer* $n \geq 3$*, any* $V = \mathbb{F}_q^n$ *for any prime power* q*, any* $G := \mathrm{SL}(V)$*,* $\mathrm{SU}(V)$*,* $\mathrm{Sp}(V)$*, or* $\Omega(V)$ *(or* $\mathrm{SO}(V)$ *or* $\mathrm{Spin}(V)$ *if* q *is odd), any* $g \in G$*, and any irreducible character* $\chi \in \operatorname{Irr}(G)$*:*

$$\frac{|\chi(g)|}{\chi(1)} \leq \chi(1)^{-\sigma \cdot \mathsf{supp}(g)/n}.$$

Proof. First we apply Theorem 4.4 to obtain the positive constants C and γ. By [LaST1, Theorem 1.2.1],

$$\frac{|\chi(g)|}{\chi(1)} \leq q^{-\sqrt{\mathsf{supp}(g)}/481}.$$

Therefore, by choosing $\sigma > 0$ small enough, say $\sigma \le 1/(241 \cdot (9C)^{3/2})$ we may ignore the cases where $n < 9C$ (or if $\chi(1) = 1$): if $s := \mathsf{supp}(g) \le n < 9C$, then $\chi(1) \le |G|^{1/2} \le q^{n^2/2}$, hence

$$\chi(1)^{\sigma s/n} \le q^{\sigma n s/2} < q^{\sqrt{s}/481}.$$

Henceforth we may assume that $n \ge \max(9C, 9)$ and $\chi(1) > 1$; in particular, $\chi(1) > 2^{n/3}$ by [LaSe].

Now, if $s := \mathsf{supp}(g) \ge n/9$, then $s \ge C$, and so we are done by Theorem 4.4, taking $\beta := 1/9$ and $\sigma \le \gamma/9$; in particular,

$$|\chi(g)| \le \chi(1)^{1-\gamma/81}. \tag{5.7}$$

Consider the case $1 \le s < n/9$ and apply Proposition 5.4 to get $2 \le b \le n/s$ and that

$$\mathbf{P}[\mathsf{supp}(g^{\mathsf{X}_1} \cdots g^{\mathsf{X}_b}) < n/9] < q^{-n^2/20\kappa},$$

with $\kappa = 1$ if $G = \mathrm{SL}(V)$ and $\kappa = 2$ if $G \ne \mathrm{SL}(V)$. By the previous bound (5.7) for elements with support $\ge n/9$, this implies that

$$\mathbf{P}\big[|\chi(g^{\mathsf{X}_1} \cdots g^{\mathsf{X}_b})| \ge \chi(1)^{1-\gamma/81}\big] < q^{-n^2/20\kappa} < \chi(1)^{-1/10\kappa}$$

since $\chi(1) \le |G|^{1/2} < q^{n^2/2}$. Thus,

$$\big|\mathbf{E}[\chi(g^{\mathsf{X}_1} \cdots g^{\mathsf{X}_b})]\big| \le \mathbf{E}\big[|\chi(g^{\mathsf{X}_1} \cdots g^{\mathsf{X}_b})|\big] \le \chi(1)^{1-\gamma/81} + \chi(1)^{1-1/10\kappa}.$$

Since $\chi(1) \ge q^{n/3} \ge 2^{3C}$ by [LaSe], by choosing $\sigma > 0$ small enough, we then have

$$\big|\mathbf{E}[\chi(g^{\mathsf{X}_1} \cdots g^{\mathsf{X}_b})]\big| \le \chi(1)^{1-\gamma/81} + \chi(1)^{1-1/10\kappa} \le \chi(1)^{1-\sigma}. \tag{5.8}$$

It now follows from (4.9) and (5.8) that

$$|\chi(g)| \le \chi(1)^{1-\frac{\sigma}{b}} \le \chi(1)^{1-\frac{\sigma s}{n}},$$

as stated. In fact, our proof shows that we can take

$$\sigma = \min\left(\frac{1}{241 \cdot (9C)^{3/2}}, \frac{\gamma}{82}\right),$$

which is $1/(6507 \cdot 2^{21} \cdot 10^{18}) > 7 \cdot 10^{-29}$ for our chosen C and γ. □

As a consequence of Theorem 5.5, we can prove the following linear refinement of [LaST1, Theorem 1.2.1]:

Corollary 5.6. *There exists an absolute constant $\gamma > 0$ such that the following statement holds. For any $n \in \mathbb{Z}_{\ge 2}$, any prime power q, any quasisimple classical group*

$$G = \mathrm{SL}_n(q),\ \mathrm{SU}_n(q),\ \mathrm{Sp}_{2n}(q),\ \Omega_n^{\pm}(q),\ \mathrm{Spin}_n^{\pm}(q),$$

any $g \in G$, and any $\chi \in \mathrm{Irr}(G)$ of degree $\chi(1) > 1$, we have

$$\frac{|\chi(g)|}{\chi(1)} \le q^{-\gamma \cdot \mathsf{supp}(g)}.$$

Proof. By [LaST1, Theorem 1.2.1],

$$|\chi(g)|/\chi(1) \le q^{-\sqrt{\mathsf{supp}(g)}/481}.$$

Hence, by choosing $\gamma \le 1/1443$ we may ignore the cases where $\mathsf{supp}(g) \le 9$, in particular if $n \le 9$. Assume now that $n \ge 10$, which implies $\chi(1) \ge q^{n/3}$ by [LaSe]. Hence Theorem 5.5 yields $|\chi(g)/\chi(1)| \le q^{-\sigma s/3}$, and we are done by taking

$$\gamma = \min(1/1443, \sigma/3),$$

which is $1/(19521 \cdot 2^{21} \cdot 10^{18}) > 2 \cdot 10^{-29}$ for our chosen σ. □

We conclude this section with the following examples, which show that the exponent $\sigma\cdot\mathsf{supp}(g)/n$ in Theorem 5.5, is optimal (up to the constant σ).

Example 5.7. Consider $G=\mathrm{SL}_n(2)$, $n\geq 3$, and the unique irreducible character τ of degree 2^n-2 of G, so that $2\cdot 1_G+\tau$ is the permutation character of G acting on the point set of $V=\mathbb{F}_2^n$. Suppose $2\leq s\leq n-1$. Choose $\xi\in\overline{\mathbb{F}}_2^\times$ of order 2^s-1 and $g\in\mathrm{SL}_n(2)$ that is conjugate to $\mathrm{diag}\big(1,\dots,1,\xi,\xi^2,\dots,\xi^{2^{s-1}}\big)$ over $\overline{\mathbb{F}}_2$. Then $\mathsf{supp}(g)=s$, $\tau(1)=2^n-2$, and $\tau(g)=2^{n-s}-2$, whence $|\tau(g)/\tau(1)|\approx\tau(1)^{-s/n}$. If $s=1$, we can choose g to be a transvection, for which we have $\mathsf{supp}(g)=1$, $\tau(g)=2^{n-1}-2$, and so again $|\tau(g)/\tau(1)|\approx\tau(1)^{-s/n}$.

More generally, we have

Lemma 5.8. *Let $G=\mathrm{Cl}_n(q)$ be a simple classical group with $n\geq 7$. If $|G|$ is large enough, and if $g\in G$ has support $s=\mathsf{supp}(g)\leq n-2$, then there is a non-trivial $\chi\in\mathrm{Irr}(G)$ such that $|\chi(g)/\chi(1)|\geq\chi(1)^{-6s/n}$.*

Proof. The statement is obvious for $s=0$, so we assume $1\leq s\leq n-2$. Choosing G of large enough order, we have $\sum_{1_G\neq\chi\in\mathrm{Irr}(G)}\chi(1)^{-0.55}<1$ by [LiSh3, Corollary 1.3]. Assume to the contrary that $|\chi(g)|\leq\chi(1)^{1-6s/n}$ for all $\chi\in\mathrm{Irr}(G)$. Choosing $k:=\lfloor(n-2)/s\rfloor$ we have $ks\leq n-2\leq(k+1)s-1$, and so

$$6ks-2.55n\geq 3.45ks-2.55s-2.55\geq 6.9s-2.55s-2.55>0$$

if $k\geq 2$. If $k=1$, then $s\geq(n-1)/2$, and so $6ks\geq 3n-3\geq 2.55n$ since $n\geq 7$. Hence, for any $x\in G$ we have

$$\sum_{1_G\neq\chi\in\mathrm{Irr}(G)}\frac{|\chi(g)^k\bar\chi(x)|}{\chi(1)^{k-1}}\leq\sum_{1_G\neq\chi\in\mathrm{Irr}(G)}\frac{|\chi(g)^k|}{\chi(1)^{k-2}}\leq\sum_{1_G\neq\chi\in\mathrm{Irr}(G)}\frac{1}{\chi(1)^{6ks/n-2}}\leq\sum_{1_G\neq\chi\in\mathrm{Irr}(G)}\chi(1)^{-0.55}<1,$$

and thus every element $x\in G$ is a product of k conjugates of g and so has $\mathsf{supp}(x)\leq ks\leq n-2$ by Lemma 5.1(ii). But this is a contradiction since G always contains elements of support $n-1$. □

6. Support vs. class size, and proof of Theorem A

In this section, we deduce Theorem A from Theorem 5.5. The main difficulty is to bound conjugacy class sizes $|g^G|$ in terms of the support $\mathsf{supp}(g)$ for all classical groups $G\leq\mathrm{GL}(V)$. To do this, we need an analogue of Proposition 4.2(c) for all classical groups. There are results of Liebeck-Shalev [LiSh1] and Liebeck-Schul-Shalev [LSS] which are very much in this spirit. However, we develop them from scratch because we want somewhat greater generality (not just the simple groups) and also because we do not want implicit constants. For any finite group X, let $P(X)$ denote the smallest index of any proper subgroup of X. Lower bounds for $P(X)$, X a finite classical groups, are listed in [KlL, Table 5.2.A]. First we deal with unitary groups.

Proposition 6.1. *Let $n\geq 3$, $(n,q_0)\neq(3,2)$, $V=\mathbb{F}_{q_0^2}^n$, and let $g\in\mathrm{GU}(V)$ have support $s:=\mathsf{supp}(g)$. Then*

$$|\mathrm{SU}(V)|^{s/2n}\leq|g^{\mathrm{SU}(V)}|\leq|\mathrm{SU}(V)|^{3s/n}.$$

Proof. Let $q:=q_0^2$, so that $V=\mathbb{F}_q^n$. Let d denote the dimension of the centralizer $\underline{C}(g)$ of g in the algebraic group GL_n. Then d is bounded above and below in Proposition 4.2(a). The finite group $\mathbf{C}_{\mathrm{GU}(V)}(g)$ has a normal series, whose factors X_i are unipotent groups of order $q_0^{d_i}$, or $\mathrm{GL}_{m_i}(q_0^{a_i})$ with $2|a_i$, or $\mathrm{GU}_{m_i}(q_0^{a_i})$, with $d_i:=m_i^2a_i$, and $\sum_i d_i=d$. By [LMT, Lemma 4.1(iv)],

$$q_0^{m^2a}\leq|\mathrm{GU}_m(q_0^a)|=q_0^{m^2a}\cdot\prod_{j=1}^m\big(1-\frac{(-1)^j}{q_0^{aj}}\big)\leq\frac{3}{2}q_0^{m^2a};\tag{6.1}$$

also, $3/2 < 2^{0.6} \le q_0^{0.6}$, and $q_0^{n^2-1.5} < |\mathrm{SU}(V)| < q_0^{n^2-1}$. Now we can follow the proof of Proposition 4.2(b), (c), but increasing the upper bound for $\mathbf{C}_{\mathrm{SU}(V)}(g)$ by $q_0^{0.6n}$ and decreasing the lower bound by $(q_0+1)/(q_0-1) \le 3 < q_0^{1.6}$, going down from $\mathbf{C}_{\mathrm{GU}(V)}(g)$ to $\mathbf{C}_{\mathrm{SU}(V)}(g)$. It follows that

$$q_0^{ns-0.6n-2} \le |g^{\mathrm{SU}(V)}| \le q_0^{2ns+n-s^2+0.6}.$$

Now, the statement can be checked directly for $s = 0$ and for $\mathrm{SU}_3(5)$. If $(n, q) \ne (3, 5)$ and $s \le 2$, then

$$|g^{\mathrm{SU}(V)}| \ge P(\mathrm{SU}(V)) > q_0^n > |\mathrm{SU}(V)|^{s/2n}.$$

If $s = 1$, we also have $|g^{\mathrm{SU}(V)}| < q_0^{2n-1} < |\mathrm{SU}(V)|^{3/n}$. In all other cases,

$$ns - 0.6n - 2 \ge \frac{s}{2n}(n^2-1),\ 2ns + n - s^2 + 0.6 \le \frac{3s}{n}(n^2 - 1.5),$$

proving the statement. □

Let J_i denote the Jordan block of size $i \in \mathbb{Z}_{\ge 1}$ and with eigenvalue 1. Then the Jordan canonical form of any unipotent element u in $\mathrm{GL}(V)$ can be written as $\oplus_{i\ge 1} J_i^{n_i}$, meaning it contains $n_i \in \mathbb{Z}_{\ge 0}$ blocks J_i for each $i \ge 1$. Sometimes we will re-order the blocks into the form $\oplus_{k=1}^t J_{m_k}$ with $m_1 \ge m_2 \ge \ldots \ge m_t \ge 1$.

Lemma 6.2. *In the above notation, for any unipotent element $u \in \mathrm{GL}(V)$ we have*

$$\sum_i i n_i^2 + 2\sum_{i<j} i n_i n_j = \sum_{k=1}^t (2km_k - m_k). \tag{6.2}$$

Proof. We induct on the number $r \ge 1$ of distinct sizes of Jordan blocks of u. Suppose $r = 1$, i.e. $u \sim J_m^s$, $t = s$, and $m_1 = \ldots = m_s = m$. Then the left-hand-size of the formula is ms^2, and the right-hand-side is $m\sum_{k=1}^s (2k-1) = ms^2$.

We suppose the formula holds for $r \ge 1$, and prove it for $r+1$. We can present u as $\mathrm{diag}(v, J_m^s)$, where $v = J_{m_1} \oplus J_{m_2} \oplus \ldots \oplus J_{m_t}$, $u = J_{m_1} \oplus J_{m_2} \oplus \ldots \oplus J_{m_{t+s}}$, and $m_{t+1} = \ldots = m_{t+s} = m$. Then, replacing v by u increases the left-hand-side of (6.2) by $ms^2 + 2\sum_{i>m} msn_i = ms^2 + 2mst$, whereas the right-hand-side grows by $\sum_{k=t+1}^{t+s} m(2k-1) = m((t+s)^2 - t^2) = m(s^2 + 2st)$. □

Lemma 6.3. *Let q be an odd prime power, $V = \mathbb{F}_q^n$ be endowed with a non-degenerate, symplectic or orthogonal, bilinear form, and let $G = \mathrm{Sp}(V)$, respectively, $\mathrm{GO}(V)$, denote the corresponding isometry group of the form. Extend the form to $\overline{V} := V \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q$, and let $\underline{G} = \mathrm{Sp}(\overline{V})$, respectively $\mathrm{GO}(\overline{V})$. Let $g = \oplus_i J_i^{n_i} \in G$ be a unipotent element with $s = \mathsf{supp}(g)$, and let $D(g) := \dim \mathbf{C}_{\underline{G}}(g)$. Then the following statements hold.*

(a) *If $G = \mathrm{Sp}(V)$, then*

$$\frac{(n-s)^2}{2} \le D(g) \le \frac{n(n-s)+n}{2} - \frac{1}{2}\sum_{i:2|i} i n_i \le \frac{n(n-s)+n}{2} - \sum_{i:2|i, n_i>0} 1.$$

If $G = \mathrm{GO}(V)$ then

$$\frac{(n-s)^2 - n_1}{2} + \frac{1}{2}\sum_{2|i} n_i \le \frac{(n-s)^2 - n_1}{2} \le D(g) \le \frac{n(n-s)}{2} - \frac{1}{2}\sum_{i:2\nmid i, n_i>0} n_i$$

(b) *If $G = \mathrm{Sp}(V)$, then*

$$(1-1/q)^{n/2} q^{(n-s)^2/2} \le |\mathbf{C}_G(g)| \le q^{(n(n-s)+n)/2}.$$

If $G = \mathrm{GO}(V)$, then

$$(1-1/q)^{n/2}q^{((n-s)^2-n)/2} \le |\mathbf{C}_G(g)| \le q^{(n(n-s)+n/3)/2}.$$

Proof. (a) We will follow in part the proof of [LiSh1, Lemma 3.4(ii)] and note that $s = \sum_i (i-1)n_i$, $n = \sum_i in_i$, so that $n - s = \sum_i n_i$. Suppose $G = \mathrm{Sp}(V)$. By [LiSe, Theorem 3.1(iii)],

$$D(g) = \frac{1}{2}\sum_i in_i^2 + \sum_{i<j} in_in_j + \frac{1}{2}\sum_{i:2\nmid i} n_i. \tag{6.3}$$

Note that

$$\sum_i in_i^2 + 2\sum_{i<j} in_in_j = \big(\sum_i n_i\big)^2 + \sum_i (i-1)n_i^2 + 2\sum_{i<j}(i-1)n_in_j. \tag{6.4}$$

Hence $2D(g) \ge \sum_i in_i^2 + 2\sum_{i<j} in_in_j \ge \big(\sum_i n_i\big)^2 = (n-s)^2$. Next,

$$\begin{aligned} s(n-s)+n &= \big(\sum_i (i-1)n_i\big)\big(\sum_i n_i\big) + \sum_i in_i \\ &\ge \sum_i (i-1)n_i^2 + 2\sum_{i<j}(i-1)n_in_j + \sum_{i:2\nmid i} n_i + \sum_{i:2|i} in_i \\ &\ge 2D_G(g) - (n-s)^2 + \sum_{i:2|i} in_i, \end{aligned}$$

implying the statement for $\mathrm{Sp}(V)$.

Suppose now that $G = \mathrm{GO}(V)$. By [LiSe, Theorem 3.1(iii)],

$$D(g) = \frac{1}{2}\sum_i in_i^2 + \sum_{i<j} in_in_j - \frac{1}{2}\sum_{i:2\nmid i} n_i. \tag{6.5}$$

Using (6.4), we obtain

$$2D(g) \ge \big(\sum_i n_i\big)^2 + \sum_i (i-1)n_i^2 - \sum_{i:2\nmid i} n_i \ge \big(\sum_i n_i\big)^2 + \sum_{2|i} n_i - n_1 = (n-s)^2 + \sum_{2|i} n_i - n_1.$$

Next, again using (6.4), we have

$$\begin{aligned} s(n-s) &= \big(\sum_i (i-1)n_i\big)\big(\sum_i n_i\big) \\ &\ge \sum_i (i-1)n_i^2 + 2\sum_{i<j}(i-1)n_in_j \\ &= 2D_G(g) - (n-s)^2 + \sum_{i:2\nmid i} n_i, \end{aligned}$$

implying the statement for $\mathrm{GO}(V)$.

(b) Suppose $G = \mathrm{Sp}(V)$. By [LiSe, Theorem 7.1(ii)], $|\mathbf{C}_G(g)|$ is a polynomial in q of degree $D(g)$, and

$$|\mathbf{C}_G(g)| = q^{D'} \cdot \prod_{2\nmid i} |\mathrm{Sp}_{n_i}(q)| \cdot \prod_{2|i} |\mathrm{GO}^{\varepsilon_i}_{n_i}(q)|$$

for suitable D' and $\varepsilon_i = \pm$ (note that $2|n_i$ when $2 \nmid i$). Note that

$$\begin{array}{rll} (q-1)^{m/2}q^{m(m+1)/2-m/2} & < |\mathrm{Sp}_m(q)| & < q^{m(m+1)/2}, \\ 2(q-1)^{\lfloor m/2\rfloor}q^{m(m-1)/2-\lfloor m/2\rfloor} & \le |\mathrm{GO}^{\pm}_m(q)| & \le \begin{cases} \frac{2(q+1)}{q}q^{m(m-1)/2}, & m=2, \\ 2q^{m(m-1)/2}, & m \ne 2. \end{cases} \end{array} \tag{6.6}$$

In our case, $q \ge 3$, so $2(q+1)/q < q$, and $\sum_i n_i/2 = (n-s)/2 \le n/2$. It follows that

$$(1-1/q)^{n/2}q^{D(g)} = (q-1)^{n/2}q^{D(g)-n/2} \le |\mathbf{C}_G(g)| < q^{\sum_{2|i} 1+D(g)},$$

Together with (a), this implies the statement for $\mathrm{Sp}(V)$.

Suppose now that $G = \mathrm{GO}(V)$. By [LiSe, Theorem 7.1(iii)], $|\mathbf{C}_G(g)|$ is a polynomial in q of degree $D(g)$, and

$$|\mathbf{C}_G(g)| = q^{D'} \cdot \prod_{2|i} |\mathrm{Sp}_{n_i}(q)| \cdot \prod_{2\nmid i} |\mathrm{GO}^{\varepsilon_i}_{n_i}(q)|$$

for suitable D' and $\varepsilon_i = \pm$ (note that $2|n_i$ when $2|i$). Using (6.6), we get

$$(1-1/q)^{n/2}q^{D(g)} = (q-1)^{n/2}q^{D(g)-n/2} \le |\mathbf{C}_G(g)| < Aq^{D(g)},$$

where $A := \prod_{i:2\nmid i} \alpha_i$, with $\alpha_i = 2$ if $n_i \ne 2$ and $\alpha_i = 2(q+1)/q$ if $n_i = 2$. In particular, $\alpha_i < q^{2n_i/3}$, and so $A \le q^{\sum_{2\nmid i} 2n_i/3}$. Since $n_1 \le \sum_i n_i \le n$, together with (a) this implies the statement for $\mathrm{GO}(V)$. □

In what follows, by $\mathsf{supp}(g)$ for $g \in \mathrm{Spin}^{\varepsilon}_n(q)$ we mean the support of its image in $\Omega^{\varepsilon}_n(q)$. Also, the notation $\mathrm{GL}^{\varepsilon}_m(q)$ means $\mathrm{GL}(\mathbb{F}_q^m)$ when $\varepsilon = +$ and $\mathrm{GU}(\mathbb{F}_{q^2}^m)$ when $\varepsilon = -$.

Proposition 6.4. *Let q be an odd prime power, $V = \mathbb{F}_q^n$ be endowed with a non-degenerate, symplectic or orthogonal, bilinear form, and let $G = \mathrm{Sp}(V)$, respectively, $\mathrm{SO}(V)$, $\Omega(V)$, or $\mathrm{Spin}(V)$. Let $g \in G$ be any element with $s = \mathsf{supp}(g)$. Then the following statements hold.*

(a) *If $2|n$ and $G = \mathrm{Sp}(V)$, then*

$$q^{(n-s)^2/2-0.2n} \le |\mathbf{C}_G(g)| \le q^{n(n-s)/2+0.5n}.$$

In particular, if $2|n \ge 4$, then $|G|^{3s/n} \ge |g^G| \ge |G|^{s/2n}$.

(b) *If $n \ge 3$ and $\Omega(V) \le G \le \mathrm{GO}(V)$, then*

$$q^{(n-s)^2/2-0.7n-1.3} \le |\mathbf{C}_G(g)| \le q^{n(n-s)/2+n/6}.$$

In particular, if $n \ge 7$ and $G = \mathrm{SO}(V)$, $\Omega(V)$, or $\mathrm{Spin}(V)$, then $|G|^{3s/n} \ge |g^G| \ge |G|^{s/3n}$.

Proof. Write $g = g_{\mathrm{ss}}u$, with g_{ss} the semisimple part and u the unipotent part. Then g preserves the orthogonal decomposition

$$V = V_1 \oplus V_2 \oplus \big(\oplus_{i=3}^{t+2} V_i\big),$$

into non-degenerate subspaces V_i of dimension $\dim V_i = n_i$, where g_{ss} acts as 1 on V_1, -1 on V_2, and

$$\mathbf{C}_{I(V)}(g_{\mathrm{ss}}) = \prod_{i=1}^{t+2} \mathbf{C}_{G\cap I(V_i)}(g_{\mathrm{ss}}) = I(V_1) \times I(V_2) \times \prod_{i=3}^{t+2} \mathrm{GL}^{\varepsilon_i}_{m_i}(q^{a_i}),$$

where $I = \mathrm{Sp}$ or GO, $\varepsilon_i = \pm$, $m_i, a_i \in \mathbb{Z}_{\ge 1}$, and $m_i a_i = n_i/2$. Let u_i denote the image of u in $I(V_i)$ when $i \le 2$, and in $\mathrm{GL}^{\varepsilon_i}_{m_i}(q^{a_i})$ when $i > 2$, and let d_i denote the dimension of its kernel U_i on V_i when $i \le 2$, on $\mathbb{F}_{q^{a_i}}^{m_i}$ when $i > 2$ and $\varepsilon_i = +$, and on $\mathbb{F}_{q^{2a_i}}^{m_i}$ when $i > 2$ and $\varepsilon_i = -$. Then the subspaces $U_i \otimes \overline{\mathbb{F}}_q$ are the distinct eigenspaces for g on $V \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q$; in particular,

$$n - s = \max_i d_i \tag{6.7}$$

Furthermore,

$$\mathbf{C}_{I(V)}(g) = \mathbf{C}_{\mathbf{C}_{I(V)}(g_{\rm ss})}(u) = \prod_{i=1}^{t+2} \mathbf{C}_{\mathbf{C}_{G\cap I(V_i)}(g_{\rm ss})}(u_i). \tag{6.8}$$

(a) Consider the case $G = \mathrm{Sp}(V)$. By (4.2) (and (6.1)), Proposition 4.2(a), and Lemma 6.3(ii), $|\mathbf{C}_{G\cap \mathrm{Sp}(V_i)}(g)| = |\mathbf{C}_{\mathbf{C}_{G\cap \mathrm{Sp}(V_i)}(g_{\rm ss})}(u_i)|$ is bounded below by $(1-1/q)^{n_i/2}q^{d_i^2/2}$. Since $q^{0.4} \geq 3^{0.4} > 1/(1-1/q)$ and $n \geq n_i$, by (6.7)–(6.8) we get $|\mathbf{C}_G(g)| > q^{(n-s)^2/2-0.2n}$. On the other hand, by (6.1), Proposition 4.2(b), and Lemma 6.3(b), $|\mathbf{C}_{G\cap \mathrm{Sp}(V_i)}(g)| = |\mathbf{C}_{\mathbf{C}_{G\cap \mathrm{Sp}(V_i)}(g_{\rm ss})}(u_i)|$ is bounded from the above by $q^{(n_id_i+n_i)/2}$ when $i \leq 2$, and by $q^{n_id_i/2+0.2n_i}$ when $i > 2$, with the extra factor $q^{0.2n_i}$ accounting for $q^{0.2n_i} = q^{0.4m_ia_i} \geq (3/2)^{m_i}$ when $\varepsilon_i = -$. Now $n = \sum_i n_i$, so by (6.7)–(6.8) we get $|\mathbf{C}_G(g)| < q^{n(n-s)/2+n/2}$, proving the first statement. Using

$$q^{n(n+1)/2-0.6} < (9/16)q^{n(n+1)/2} < |G| < q^{n(n+1)/2},$$

(see [LMT, Lemma 4.1(ii)]), we obtain

$$q^{ns/2-0.6} < |g^G| < q^{ns-s^2/2+0.7n}.$$

The second statement is obvious if $s = 0$. If $s \geq 1$ then $ns/2 - 0.6 \geq (s/2n)(n(n+1)/2)$. If $s \geq 2$, then $ns - s^2/2 + 0.7n \leq (3s/n)(n(n+1)/2 - 0.6)$. Finally, if $s = 1$, then g is a transvection (up to a sign), hence $|g^G| = (q^n-1)/2 < |G|^{3/n}$, completing the proof of the second statement.

(b) Now we consider the orthogonal case. By (4.2) (and (6.1)), Proposition 4.2(a), and Lemma 6.3(ii), $|\mathbf{C}_{G\cap \mathrm{GO}(V_i)}(g)| = |\mathbf{C}_{\mathbf{C}_{G\cap \mathrm{GO}(V_i)}(g_{\rm ss})}(u_i)|$ is bounded from below by $(1-1/q)^{n_i/2}q^{d_i^2/2-n_i/2}$. Since $q^{0.4} > 1/(1-1/q)$ and $n \geq n_i$, by (6.7)–(6.8) we get $|\mathbf{C}_{\mathrm{GO}}(V)(g)| > q^{(n-s)^2/2-0.7n}$. On the other hand, by (6.1), Proposition 4.2(b), and Lemma 6.3(b), $|\mathbf{C}_{G\cap \mathrm{GO}(V_i)}(g)| = |\mathbf{C}_{\mathbf{C}_{G\cap \mathrm{GO}(V_i)}(g_{\rm ss})}(u_i)|$ is bounded from the above by $q^{n_id_i/2+n_i/6}$ when $i \leq 2$, and by $q^{n_id_i/2+0.2n_i}$ when $i > 2$, again with the extra factor $q^{0.2n_i}$ accounting for $q^{0.2n_i} = q^{0.4m_ia_i} \geq (3/2)^{m_i}$ when $\varepsilon_i = -$. Now $n = \sum_i n_i$, so by (6.7)–(6.8) we get $|\mathbf{C}_{\mathrm{GO}(V)}(g)| < q^{n(n-s)/2+n/6}$. Since $[\mathrm{GO}(V) : \Omega(V)] = 4$, we have that

$$q^{-1.3}|\mathbf{C}_{\mathrm{GO}(V)}(g)| < |\mathbf{C}_{\mathrm{GO}(V)}(g)|/4 \leq |\mathbf{C}_G(g)| \leq |\mathbf{C}_{\mathrm{GO}(V)}(g)|$$

when $\mathrm{GO}(V) \geq G \geq \Omega(V)$, proving the first statement.

To prove the second statement, we may again assume $s \geq 1$, and note that

$$q^{n(n-1)/2-1.16} < (9/32)q^{n(n-1)/2} < |\Omega(V)| < |\mathrm{SO}(V)| = |\mathrm{Spin}(V)| = 2|\Omega(V)| < q^{n(n-1)/2},$$

if $n \geq 7$, (see [LMT, Lemma 4.1(ii)]). Furthermore, if $\bar{g}$ denotes the image of $g \in \mathrm{Spin}(V)$ in $\Omega(V)$, then $|\mathbf{C}_{\Omega(V)}(\bar{g})| \leq |\mathbf{C}_{\mathrm{Spin}(V)}(g)| \leq 2 \cdot |\mathbf{C}_{\Omega(V)}(\bar{g})|$, and so

$$\frac{|\Omega(V)|}{|\mathbf{C}_{\Omega(V)}(g)|} \leq |g^{\mathrm{Spin}(V)}| \leq \frac{|\mathrm{SO}(V)|}{|\mathbf{C}_{\Omega(V)}(g)|}.$$

Hence, it suffices to prove that

$$|\mathrm{SO}(V)|^{1-3s/n} \leq |\mathbf{C}_{\Omega(V)}(g)| \leq |\mathbf{C}_{\mathrm{SO}(V)}(g)| \leq |\Omega(V)|^{1-s/3n} \cdot q^{-0.64} < |\Omega(V)|^{1-s/3n}/2. \tag{6.9}$$

When $n \geq 8$, or if $n = 7$ but $s = 1$, we have $\frac{(n-s)^2}{2} - 0.7n - 1.3 \geq \big(1 - \frac{3s}{n}\big)\frac{n(n-1)}{2}$. If $s \geq 3$ then we also have $\frac{n(n-s)}{2} + \frac{n}{6} \leq \big(1 - \frac{s}{3n}\big)\big(\frac{n(n-1)}{2} - 1.8\big)$, proving (6.9). Finally, if $s \leq 3$, then $|G|^{s/3n} \leq q^{(n-1)/2} < P(G) \leq |g^G|$; and if $(n,s) = (7,1)$, then $|G|^{3s/n} > q^{17} > q^{2n} > |g^G|$, completing the proof of the second statement. $\square$

Lemma 6.5. *Let q be a power of 2, let n be even, let $V = \mathbb{F}_q^n$ be endowed with a non-degenerate alternating bilinear form $(\cdot|\cdot)$, respectively a quadratic form associated to $(\cdot|\cdot)$, and let $G = \mathrm{Sp}(V)$, respectively, $\mathrm{GO}(V)$, denote the corresponding isometry group of the form(s). Extend the form to $\overline{V} := V \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q$, and let $\underline{G} = \mathrm{Sp}(\overline{V})$, respectively $\mathrm{GO}(\overline{V})$. Let $g = \oplus_i J_i^{n_i} \in G$ be a unipotent element with $s = \mathsf{supp}(g)$, and let $D^\sharp(g) := \dim \mathbf{C}_{\underline{G}}(g)$. Then the following statements hold.*

(a) *If $G = \mathrm{Sp}(V)$, then*

$$\frac{(n-s)^2}{2} \le D^\sharp(g) \le \frac{n(n-s)+n}{2}.$$

If $G = \mathrm{GO}(V)$ then

$$\frac{(n-s)^2-n-n_1}{2} \le D^\sharp(g) \le \frac{n(n-s)}{2} - \frac{1}{2}\sum_{i:2\nmid i, n_i>0} n_i$$

(b) *If $G = \mathrm{Sp}(V)$, then*

$$(1-1/q)^{n/2} q^{(n-s)^2/2} \le |\mathbf{C}_G(g)| \le q^{n(n-s)/2+1.3n}.$$

If $G = \mathrm{GO}(V)$, then

$$(1-1/q)^{n/2} q^{(n-s)^2/2-n} \le |\mathbf{C}_G(g)| \le q^{n(n-s)/2+0.8n}.$$

Proof. (a) The conjugacy classes g^G of unipotent elements in G are best represented in the form [LiSe, (4.4)], where one decomposes the g-module V as

$$\big(\oplus_i W(m_i)^{a_i}\big) \oplus \big(\oplus_j V(2k_j)^{b_j}\big), \tag{6.10}$$

where $b_j \le 2$, $k_1 > k_2 > \cdots$, $m_1 > m_2 > \cdots$, g acts on $W(m_i)$ as $J_{m_i}^2$, and on $V(2k_j)$ as $J(2k_j)$, see [LiSe, Table 4.1]. We again record the Jordan canonical form of g as $\sum_{i=1}^r J_{m_i}$, with $m_1 \ge m_2 \ge \ldots \ge m_r \ge 1$. Then

$$D^\sharp(g) = \sum_{i=1}^r \big(im_i - \chi_V(m_i)\big),$$

where the function χ_V is defined as follows (see [LiSe, Lemma 6.2]):

$$\chi_V(m) = \chi_{V(m)}(m) = \begin{cases} m/2, & G = \mathrm{Sp}(V) \\ m/2+1, & G = \mathrm{GO}(V) \end{cases}$$

if $V(m)$ occurs in (6.10), and

$$\chi_V(m) = \chi_{W(m)}(m) = \begin{cases} \lfloor (m-1)/2 \rfloor, & G = \mathrm{Sp}(V) \\ \lfloor (m+1)/2 \rfloor, & G = \mathrm{GO}(V) \end{cases}$$

otherwise.

Suppose $G = \mathrm{Sp}(V)$. Then $\chi_V(m_i) = m_i/2 - \nu_i$, where $\nu_i = 0$ if $V(m_i)$ occurs in (6.10), $\nu_i = 1$ if $2|m_i$ but $V(m_i)$ does not occur in (6.10), and $\nu_i = 1/2$ if $2 \nmid m_i$. It follows that

$$D^\sharp(g) = \sum_{i=1}^r (im_i - m_i/2) + \sum_{2\nmid m_i} a_i + \nu,$$

where $\nu := 2\sum_i a_i$, with i running over those m_i such that $2|m_i$ but $V(m_i)$ does not occur in (6.10). With g written as $\oplus_i J_i^{n_i}$, we have that $\nu \le \sum_{2|i} n_i \le \frac{1}{2}\sum_{2|i} in_i$, and $\sum_{2\nmid m_i} a_i = \frac{1}{2}\sum_{2\nmid i} n_i$. Using Lemma 6.2 and (6.3), we get

$$D^\sharp(g) = \frac{1}{2}\sum_i in_i^2 + \sum_{i<j} in_i n_j + \frac{1}{2}\sum_{2\nmid i} n_i + \nu = D(g) + \nu.$$

Since $0 \le \nu \le \frac{1}{2}\sum_{2|i} in_i$, together with Lemma 6.3(a), this implies the statement for $\mathrm{Sp}(V)$.

Next suppose that $G = \mathrm{GO}(V)$. Then $\chi_V(m_i) = m_i/2 + \mu_i$, where $\nu_i = 1$ if $V(m_i)$ occurs in (6.10), $\mu_i = 0$ if $2|m_i$ but $V(m_i)$ does not occur in (6.10), and $\mu_i = 1/2$ if $2 \nmid m_i$. It follows that

$$D^\sharp(g) = \sum_{i=1}^{r}(im_i - m_i/2) - \sum_{2\nmid m_i} a_i - \mu,$$

where $\mu := \sum_j b_j$. With g written as $\oplus_i J_i^{n_i}$, we have that $\mu \le \sum_{2|i} n_i$, and $\sum_{2\nmid m_i} a_i = \frac{1}{2}\sum_{2\nmid i} n_i$. Using Lemma 6.2 and (6.5), we get

$$D^\sharp(g) = \frac{1}{2}\sum_i in_i^2 + \sum_{i<j} in_in_j - \frac{1}{2}\sum_{2\nmid i} n_i - \mu = D(g) - \mu.$$

Since $\mu \ge 0$ and $2(n_1 + \sum_{2|i} n_i) \le 2n_1 + \sum_{2|i} in_i \le n + n_1$, together with Lemma 6.3(a), this implies the statement for $\mathrm{GO}(V)$.

(b) By [LiSe, Theorem 7.3(ii)], $|\mathbf{C}_G(g)|$ is a polynomial in q of degree $D^\sharp(g)$, and

$$|\mathbf{C}_G(g)| = 2^{t+\delta}q^{D'} \cdot \prod_{2\nmid m_i} |I_{2a_i}(q)| \cdot \prod_{2|m_i} |\mathrm{Sp}_{2a_i}(q)|$$

for a suitable D'; moreover, I is either Sp or $\mathrm{GO}^\pm$, $0 \le \delta \le 1$, and t is the number of j such that $k_j - k_{j+1} \ge 2$ in (6.10). In particular, $(t + \delta +$ the number of factors GO among the $I_{2a_i})$ is at most $n/2$. Using (6.6) and $(q+1)/q \le 1.5 < q^{0.6}$, we obtain

$$(1-1/q)^{n/2}q^{D^\sharp(g)} = (q-1)^{n/2}q^{D^\sharp(g)-n/2} \le |\mathbf{C}_G(g)| < q^{0.8n+D^\sharp(g)},$$

Now we can apply the estimates in (a) for $D^\sharp(g)$. □

Proposition 6.6. *Let q be a power of 2, $2|n \ge 4$, $V = \mathbb{F}_q^n$ be endowed with a non-degenerate alternating bilinear form $(\cdot|\cdot)$, respectively a quadratic form associated to $(\cdot|\cdot)$, and let $G = \mathrm{Sp}(V)$, respectively, $\mathrm{GO}(V)$ or $\Omega(V)$. Let $g \in G$ be any element with $s = \mathsf{supp}(g)$. Then the following statements hold.*

(a) *If $G = \mathrm{Sp}(V)$, then*

$$q^{(n-s)^2/2-0.5n} \le |\mathbf{C}_G(g)| \le q^{n(n-s)/2+1.3n}.$$

In particular, $|G|^{3s/n} \ge |g^G| \ge |G|^{s/3n}$.

(b) *If $n \ge 8$ and $\Omega(V) \le G \le \mathrm{GO}(V)$, then*

$$q^{(n-s)^2/2-1.5n-1} \le |\mathbf{C}_G(g)| \le q^{n(n-s)/2+0.8n}.$$

In particular, if $n \ge 8$ and $G = \Omega(V)$, then $|G|^{5s/n} \ge |g^G| \ge |G|^{s/3n}$.

Proof. Write $g = g_{\mathrm{ss}}u$, with g_{ss} the semisimple part and u the unipotent part. Then g preserves the orthogonal decomposition

$$V = V_1 \oplus \big(\oplus_{i=2}^{t+1} V_i\big),$$

into non-degenerate subspaces V_i of dimension $\dim V_i = n_i$, where g_{ss} acts as 1 on V_1, and

$$\mathbf{C}_{I(V)}(g_{\mathrm{ss}}) = \prod_{i=2}^{t+1} \mathbf{C}_{G\cap I(V_i)}(g_{\mathrm{ss}}) = I(V_1) \times \prod_{i=2}^{t+1} \mathrm{GL}_{m_i}^{\varepsilon_i}(q^{a_i}),$$

where $I = \mathrm{Sp}$ or GO, $\varepsilon_i = \pm$, $m_i, a_i \in \mathbb{Z}_{\ge 1}$, and $m_ia_i = n_i/2$. Let u_i denote the image of u in $I(V_i)$ when $i = 1$, and in $\mathrm{GL}_{m_i}^{\varepsilon_i}(q^{a_i})$ when $i > 1$, and let d_i denote the dimension of its kernel U_i

on V_i when $i=1$, on $\mathbb{F}_{q^{a_i}}^{m_i}$ when $i>1$ and $\varepsilon_i=+$, and on $\mathbb{F}_{q^{2a_i}}^{m_i}$ when $i>1$ and $\varepsilon_i=-$. Then the subspaces $U_i\otimes\overline{\mathbb{F}}_q$ are the distinct eigenspaces for g on $V\otimes_{\mathbb{F}_q}\overline{\mathbb{F}}_q$; in particular,

$$n-s=\max_i d_i \tag{6.11}$$

Furthermore,

$$\mathbf{C}_{I(V)}(g)=\mathbf{C}_{\mathbf{C}_{I(V)}(g_{\rm ss})}(u)=\prod_{i=1}^{t+1}\mathbf{C}_{\mathbf{C}_{G\cap I(V_i)}(g_{\rm ss})}(u_i). \tag{6.12}$$

(a) Consider the case $G=\mathrm{Sp}(V)$. By (4.2) (and (6.1)), Proposition 4.2(a), and Lemma 6.5(ii), $|\mathbf{C}_{G\cap\mathrm{Sp}(V_i)}(g)|=|\mathbf{C}_{\mathbf{C}_{G\cap\mathrm{Sp}(V_i)}(g_{\rm ss})}(u_i)|$ is bounded below by $q^{d_i^2/2-n_i/2}$. Hence (6.11)–(6.12) imply $|\mathbf{C}_G(g)|>q^{(n-s)^2/2-0.5n}$. On the other hand, by (6.1), Proposition 4.2(b), and Lemma 6.5(b), $|\mathbf{C}_{G\cap\mathrm{Sp}(V_i)}(g)|=|\mathbf{C}_{\mathbf{C}_{G\cap\mathrm{Sp}(V_i)}(g_{\rm ss})}(u_i)|$ is bounded from the above by $q^{n_id_i/2+1.3n_i}$ when $i=1$, and by $q^{n_id_i/2+0.3n_i}$ when $i>1$, with the extra factor $q^{0.3n_i}$ accounting for $q^{0.3n_i}=q^{0.6m_ia_i}>(3/2)^{m_i}$ when $\varepsilon_i=-$. Now $n=\sum_i n_i$, so by (6.11)–(6.12) we get $|\mathbf{C}_G(g)|<q^{n(n-s)/2+1.3n}$, proving the first statement. Using

$$q^{n(n+1)/2-0.84}<(9/16)q^{n(n+1)/2}<|G|<q^{n(n+1)/2},$$

(see [LMT, Lemma 4.1(ii)]), we obtain

$$q^{ns/2-0.8n-0.84}<|g^G|<q^{ns-s^2/2+n}.$$

The second statement is obvious if $s=0$. If $s\geq 4$ then $ns/2-0.8n-0.84\geq(s/3n)(n(n+1)/2)$, and if $1\leq s\leq 3$, then $|G|^{s/3n}\leq|G|^{1/n}<q^{(n+1)/2}<P(G)\leq|g^G|$, showing $|g^G|\geq|G|^{s/3n}$. If $s\geq 2$, then $ns-s^2/2+n\leq(3s/n)(n(n+1)/2-0.84)$. Finally, if $s=1$, then g is a transvection, hence $|g^G|=q^n-1<|G|^{3/n}$, completing the proof of the second statement.

(b) Now we consider the orthogonal case. By (4.2) (and (6.1)), Proposition 4.2(a), and Lemma 6.5(ii), $|\mathbf{C}_{G\cap\mathrm{GO}(V_i)}(g)|=|\mathbf{C}_{\mathbf{C}_{G\cap\mathrm{GO}(V_i)}(g_{\rm ss})}(u_i)|$ is bounded below by $(1-1/q)^{n_i/2}q^{d_i^2/2-1.5n_i}$. Hence (6.11)–(6.12) imply that $|\mathbf{C}_{\mathrm{GO}}(V)(g)|>q^{(n-s)^2/2-1.5n}$. On the other hand, by (6.1), Proposition 4.2(b), and Lemma 6.5(b), $|\mathbf{C}_{G\cap\mathrm{GO}(V_i)}(g)|=|\mathbf{C}_{\mathbf{C}_{G\cap\mathrm{GO}(V_i)}(g_{\rm ss})}(u_i)|$ is bounded from the above by $q^{n_id_i/2+0.8n_i}$ when $i=1$, and by $q^{n_id_i/2+0.3n_i}$ when $i>1$, again with the extra factor $q^{0.3n_i}$ accounting for $q^{0.3n_i}=q^{0.6m_ia_i}>(3/2)^{m_i}$ when $\varepsilon_i=-$. Now $n=\sum_i n_i$, so by (6.11)–(6.12) we get $|\mathbf{C}_{\mathrm{GO}(V)}(g)|<q^{n(n-s)/2+0.8n}$. Since $[\mathrm{GO}(V):\Omega(V)]=2$, we have that

$$|\mathbf{C}_{\mathrm{GO}(V)}(g)|/q\leq|\mathbf{C}_{\mathrm{GO}(V)}(g)|/2\leq|\mathbf{C}_G(g)|\leq|\mathbf{C}_{\mathrm{GO}(V)}(g)|$$

when $\mathrm{GO}(V)\geq G\geq\Omega(V)$, proving the first statement.

To prove the second statement, we may again assume $s\geq 1$, and note that

$$q^{n(n-1)/2-0.84}<(9/16)q^{n(n-1)/2}<|\Omega(V)|<q^{n(n-1)/2},$$

if $n\geq 8$, (see [LMT, Lemma 4.1(ii)]). Hence,

$$q^{ns/2-1.3n-0.84}<|g^G|<q^{ns-s^2/2+2n+1}.$$

If $s\geq 4$ then $ns/2-1.3n-0.84\geq(s/3n)(n(n-1)/2)$, and if $1\leq s\leq 3$, then

$$|G|^{s/3n}\leq|G|^{1/n}<q^{(n-1)/2}<P(G)\leq|g^G|,$$

showing $|g^G|\geq|G|^{s/3n}$. If $s\geq 2$, then $ns-s^2/2+2n+1\leq(5s/n)(n(n-1)/2-0.84)$. If $s=1$ then $g\in\mathrm{GO}(V)\setminus\Omega(V)$ (and we still have $|g^G|\leq q^n-1<|G|^{3/n}$). □

Together, Propositions 4.2, 6.1, 6.4, and 6.6 imply

Corollary 6.7. *Let G be any of the following quasisimple classical groups:* $\mathrm{SL}_n(q)$ *with* $n \geq 2$, $\mathrm{SU}_n(q)$ *with* $n \geq 3$, $\mathrm{Sp}_n(q)$ *with* $2|n \geq 4$, *or* $\Omega_n^{\pm}(q)$ *or* $\mathrm{Spin}_n^{\pm}(q)$ *with* $n \geq 7$. *If* $g \in G$ *has* $s = \mathsf{supp}(g)$, *then* $|G|^{s/3n} \leq |g^G| \leq |G|^{5s/n}$.

Proof of Theorem A. If G is an exceptional group of Lie type, then the statement follows from the main result [LiT, Theorem 1]. Choosing c small enough, we may assume that G is (a quotient of) one of the groups listed in Corollary 6.7; in particular, for $S := g^G$ with $s = \mathsf{supp}(g)$ we have $s/3n \leq \log_{|G|} |S| \leq 5s/n$. Hence the statement follows from Theorem 5.5, by taking $c \leq \sigma/5$. □

In addition to Example 5.7 and Lemma 5.8, we offer another example showing that the term $\log_{|G|} |g^G|$ in Theorem A is optimal, up to a constant.

Example 6.8. Let G be any finite group of Lie type, g a semisimple element, and χ the Steinberg character of G. Then by [St, Theorem 15.5], $|\chi(g)| = |\mathbf{C}_G(g)|_p$, the p-part of $|\mathbf{C}_G(g)|$. For instance, if $G := \mathrm{SL}_n(q)$ and g is a diagonal element with eigenvalue multiplicities $a_1, \ldots, a_m$, then in the large q limit,

$$|g^G| \sim q^{n^2 - \sum_i a_i^2} \sim |G|^{\frac{n^2 - \sum a_i^2}{n^2 - 1}}$$

while

$$|\chi(g)| = q^{\sum_i \binom{a_i}{2}} = \chi(1)^{\frac{\sum_i a_i^2 - \sum a_i}{n^2 - n}},$$

so if $\sum_i a_i^2$ is large compared to $\sum_i a_i$, then

$$1 - \frac{\log |g^G|}{\log |G|} \approx \frac{\log |\chi(g)|}{\log \chi(1)}.$$

7. Squares of conjugacy classes and Thompson's conjecture

In this section we consider situations in which the square of a conjugacy class x^G can be shown to be all or nearly all of G. The main result is Theorem 7.7, which proves Thompson's conjecture for various families of unitary, symplectic, and orthogonal groups. The strategy here is to choose a class x with small centralizer and use the Frobenius formula in conjunction with character estimates to show that every target element g lies in $x^G \cdot x^G$. This breaks down when g has very small support, necessitating a separate analysis of such elements. If g is of the form $\mathrm{diag}(g_1, I_{n-k})$ for some small value of k, and if x is conjugate to an element of the form $\mathrm{diag}(x_1, x_2)$, where x_2 is real and g_1 can be written as a product of two conjugates of x_1, then g lies in $x^G \cdot x^G$. By choosing x carefully, we can hope to treat all elements of bounded support. Of course, the primary eigenvalue of an element of small support need not be 1. Because of this difficulty, our strategy at present assumes congruence conditions relating n and q for orthogonal and unitary groups.

We remark that Ore's conjecture, now a theorem of Liebeck, O'Brien, Shalev, and Tiep [LOST2], plays an important role in the proof of Theorem 7.7, via Lemma 7.5.

For groups of type $\mathrm{PSL}_n(q)$, Thompson's conjecture is already known [EG]. Theorem 7.8 shows that there are many regular semisimple conjugacy classes in $\mathrm{SL}_n(q)$ and $\mathrm{SU}_n(q)$, including all those with irreducible characteristic polynomial, for which the first part of the argument works, and $x^G \cdot x^G$ contains all elements whose support is greater than an absolute constant.

Lemma 7.1. *Let* $V = \mathbb{F}_q^n$ *with* $n \geq 117$. *If* $G := \mathrm{SU}(V)$, $\mathrm{Sp}(V)$, *or* $\Omega(V)$, *and* $g \in G$ *satisfies* $|\mathbf{C}_G(g)| \geq |G|^{6/7}$, *then* V *admits an orthogonal decomposition* $V_1 \oplus V_2$ *of non-degenerate subspaces with* $\dim(V_2) > 2(\dim V)/3$, *such that* $g(V_i) = V_i$, *and* g *acts as a scalar* λ *on* V_2, *with* $\lambda^{q+1} = 1$ *in the* SU*-case and* $\lambda^2 = 1$ *otherwise.*

Proof. Let $D = n(n+1)/2$ when $G = \mathrm{Sp}(V)$ and $D = n(n-1)/2$ when $G = \Omega(V)$. As mentioned in the proofs of Propositions 6.4 and 6.6, $|G| > q^{D-1.16}$. Now, if $g \in G$ has support $s = \mathsf{supp}(g)$, then Propositions 6.4 and 6.6 show that $|\mathbf{C}_G(g)| \le q^{D+1.3n-ns/2}$. If $0 < \varepsilon < 1$ and $|\mathbf{C}_G(g)| \ge |G|^{1-\varepsilon}$, then $D + 1.3n - ns/2 \ge (D - 1.16)(1-\varepsilon)$, and so

$$s < \frac{2\varepsilon D}{n} + 2.6 + \frac{2.32}{n} \le \varepsilon(n+1) + 2.6 + \frac{2.32}{n}.$$

Taking $\varepsilon = 1/7$, when $n \ge 117$ we then have $s < n/6$; in particular, the primary eigenvalue λ of g satisfies $\lambda^{q_0+1} = 1$ in the case $G = \mathrm{SU}(V) \cong \mathrm{SU}_n(q_0)$, respectively $\lambda = \pm 1$ in the remaining cases. By [LaST1, Lemma 6.3.4], V admits a g-invariant orthogonal decomposition $V_1 \oplus V_2$ such that $\dim(V_2) \ge n - 2s > 2n/3$ and g acts as λ on V_2.

The same argument applies to the case $G = \mathrm{SU}(V)$, using the estimates in Proposition 6.1. □

In what follows, we will fix $\mathrm{Cl} \in \{\mathrm{SU}, \mathrm{Sp}, \Omega\}$ and work with $\mathrm{Cl}^\varepsilon_n(q)$, with the convention that, if we choose $\mathrm{Cl} = \mathrm{Sp}$ then all Cl^ε will be Sp (regardless of ε) and $2|n$, and if we choose $\mathrm{Cl} = \mathrm{SU}$ then all Cl^ε will be SU, whereas if we choose $\mathrm{Cl} = \Omega$, then $\mathrm{Cl}^\varepsilon = \Omega^\varepsilon$ with $\varepsilon = \pm$ and also $2|n$ if $2|q$. If $m < n$, then $\mathrm{Cl}^\varepsilon_m(q)$ can be naturally embedded in $\mathrm{Cl}^{\varepsilon'}_n(q)$ via $x \mapsto \mathrm{diag}\big(x, I_{n-m}\big)$. For $g \in \mathrm{Cl}^\varepsilon_m(q)$ and S a normal subset of $\mathrm{Cl}^{\varepsilon'}_n(q)$, where either $(m, \varepsilon) = (n, \varepsilon')$ or $n > m$, we say S *represents* g if the natural embedding of $\mathrm{Cl}^\varepsilon_m(q)$ into $\mathrm{Cl}^{\varepsilon'}_n(q)$ maps g to an element of S. We say an element $x \in G = \mathrm{Cl}^{\varepsilon'}_n(q)$ *covers* g if $x^G \cdot x^G$ represents g.

Lemma 7.2. *If $g \in \mathrm{Cl}^\varepsilon_r(q)$ is covered by $x \in \mathrm{Cl}^\alpha_m(q)$, where $m \ge r$, and y is any real element of $\mathrm{Cl}^\beta_n(q)$, then g is covered by*

$$\mathrm{diag}(x, y) \in \mathrm{Cl}^\alpha_m(q) \times \mathrm{Cl}^\beta_n(q) < \mathrm{Cl}^{\alpha\beta}_{m+n}(q).$$

Proof. By assumption, g viewed as an element of $\mathrm{Cl}_m(q)$ is x_1x_2 for some conjugates x_1, x_2 of x. As y is real, $\mathrm{diag}(x, y)$ is conjugate to $\mathrm{diag}(x_1, y)$ and $\mathrm{diag}(x_2, y^{-1})$. Hence x_1x_2 is covered by $\mathrm{diag}(x, y)$. □

Lemma 7.3. *Let $x \in \mathrm{Cl}^+_{2m}(q)$ and $y \in \mathrm{Cl}^+_{2n}(q)$. If $\mathrm{Cl} = \Omega$ and $2 \nmid q$, assume in addition that $2|m$ and $2|n$. Then $\mathrm{diag}(x, y)$ is conjugate to $\mathrm{diag}(y, x)$ in $\mathrm{Cl}^+_{2m+2n}(q)$.*

Proof. We may assume that $\mathrm{Cl}^+_{2m}(q) = \mathrm{Cl}(U)$, where $U = \oplus_{i=1}^m \mathrm{Span}(u_{2i-1}, u_{2i})$ is an orthogonal sum of 2-spaces, with a Witt basis (u_{2i-1}, u_{2i}) and moreover $\mathsf{Q}(u_{2i-1}) = \mathsf{Q}(u_{2i}) = 0$ if in addition $\mathrm{Cl} = \Omega$ and $2|q$, and with $\mathsf{Q}(u_{2i-1}) = 1$, $\mathsf{Q}(u_{2i}) = -1$, $(u_{2i-1}|u_{2i}) = 0$ when $\mathrm{Cl} = \Omega$ and $2 \nmid q$. Write $\mathrm{Cl}^+_{2n}(q) = \mathrm{Cl}(V)$ with $V = \oplus_{i=1}^n \mathrm{Span}(v_{2i-1}, v_{2i})$ in a similar manner.

First we assume that $n = 1$, and either $\mathrm{Cl} = \mathrm{SU}$, Sp, or $2|q$ and $\mathrm{Cl} = \Omega$. Then the linear transformation

$$f : u_1 \mapsto v_1,\ u_2 \mapsto v_2,\ u_3 \mapsto u_1,\ u_4 \mapsto u_2,\ u_5 \mapsto u_3, \dots$$
$$u_{2m-3} \mapsto u_{2m-1},\ u_{2m} \mapsto u_{2m-2},\ v_1 \mapsto u_{2m-1},\ v_2 \mapsto u_{2m}$$

belongs to $\mathrm{SU}(U \oplus V)$, respectively $\mathrm{Sp}(U \oplus V)$. Suppose $2|q$ and $\mathrm{Cl} = \Omega$. Then f fixes the maximal totally singular subspace $\mathrm{Span}(u_1, u_3, \dots, u_{2m-1}, v_1)$ of $U \oplus V$, hence $f \in \Omega(U \oplus V)$ by [KlL, Lemma 2.5.8].

Next suppose that $n = 2$, $2 \nmid q$, and $\mathrm{Cl} = \Omega$, and consider the linear transformation

$$f : u_1 \mapsto v_1,\ u_2 \mapsto v_2,\ u_3 \mapsto v_3,\ u_4 \mapsto v_4, u_5 \mapsto u_1,\ u_6 \mapsto u_2, u_7 \mapsto u_3,\ u_8 \mapsto u_4, \dots,$$
$$u_{2m-1} \mapsto u_{2m-5},\ u_{2m} \mapsto u_{2m-4},\ v_1 \mapsto u_{2m-3},\ v_2 \mapsto u_{2m-2},\ v_3 \mapsto u_{2m-1},\ v_4 \mapsto u_{2m}.$$

Clearly $f \in \mathrm{GO}(U \oplus V)$, but we want to show that $f \in \Omega(U \oplus V)$. Note that

$$u_1 \mapsto v_1 \mapsto u_{2m-3} \mapsto u_{2m-7} \mapsto \dots \mapsto u_5 \mapsto u_1,$$

is an $(m/2+1)$-cycle, which is a product of $m/2$ reflections of the form

$$\rho_w : x \mapsto x - \frac{2(x|w)}{(w|w)}w$$

with $w = u_1 - v_1, v_1 - u_{2m-3}, \ldots, u_5 - u_1$, each of norm $\mathsf{Q}(w) = 2$. The same holds for the sequence starting at u_3. The two sequences starting at u_2 and u_4 each give us a product of $m/2$ reflections of the form ρ_w with $\mathsf{Q}(w) = -2$. Thus f is a product of $2m$ reflections, whence $\det(f) = 1$, and its spinor norm is the class of $2^m(-2)^m$, a square since $2|m$. Hence $f \in \Omega(U \oplus V)$ in this case as well.

The above f moves v_1, v_2, respectively $v_1, \ldots, v_4$, to the front of $u_1, \ldots, u_{2m}$. In the general case of any n, a sequence of such transformations moves $v_1, \ldots, v_{2n}$ to the front of $u_1, \ldots, u_{2m}$, and thus conjugates $\mathrm{diag}(x, y)$ to $\mathrm{diag}(y, x)$. □

Lemma 7.4. *Suppose $r, m, n \in \mathbb{Z}_{\geq 1}$, and moreover $2|m$ and $2|n$ if $\mathrm{Cl} = \Omega$ and $2 \nmid q$. If the elements $g_1, \ldots, g_k \in \mathrm{Cl}_r^\alpha(q)$ are all covered by a real element $x \in \mathrm{Cl}_{2m}^+(q)$ and the elements $h_1, \ldots, h_l \in \mathrm{Cl}_s^\beta(q)$ are all covered by a real element $y \in \mathrm{Cl}_{2n}^+(q)$, then the g_i and h_j are all covered by the real element $\mathrm{diag}(x, y) \in \mathrm{Cl}_{2m+2n}^+(q)$.*

Proof. The assumptions and Lemma 7.3 imply that the elements

$$z_1 := \mathrm{diag}(x, y),\ z_2 := \mathrm{diag}(x, y^{-1}),\ z_3 := \mathrm{diag}(y, x),\ z_4 := \mathrm{diag}(y, x^{-1})$$

are all in the same conjugacy class C. Conjugating z_1 and z_2 by elements in $\mathrm{Cl}_{2m}^+(q) \times I_{2n}$ and multiplying together, we see that every $\mathrm{diag}(g_i, I_{2m+2n-r})$ belongs to C^2. Conjugating z_3 and z_4 by elements in $I_{2m} \times \mathrm{Cl}_{2n}^+(q)$ and multiplying, we see that every $\mathrm{diag}(h_j, I_{2m+2n-s})$ lies in C^2. □

Lemma 7.5. *For every positive integer $r \geq 1$, every element $g \in \mathrm{Cl}_r^\alpha(q)$ is covered by a real element in $\mathrm{Cl}_{4m}^+(q)$, where $\max(6, r) \leq 2m \leq r + 3$, and $2|m$ if $\mathrm{Cl} = \Omega$ and $2 \nmid q$.*

Proof. Embedding $\mathrm{Cl}_r^\alpha(q)$ in $\mathrm{Cl}_{2m}^+(q)$ and replacing g by $\mathrm{diag}(g, I_s)$ for a suitable s, we may assume that $g \in \mathrm{Cl}_{2m}^+(q)$ with m as specified. (Note that for the case of Ω_r^-, we take $m = r/2 + 1$.) By [LOST2, Theorem 1], every g in $\mathrm{Cl}_{2m}^+(q)$ is a commutator $xyx^{-1}y^{-1}$. By Lemma 7.3, $z := \mathrm{diag}(x, x^{-1}) \in \mathrm{Cl}_{4m}^+(q)$ is conjugate to $\mathrm{diag}(x^{-1}, x) = z^{-1}$, and thus z is real. Conjugating z^{-1} by $\mathrm{diag}(y, I_{2m})$ we see that z is also conjugate to $t := \mathrm{diag}(yx^{-1}y^{-1}, x)$. It follows that $\mathrm{diag}(g, I_{2m}) = zt$ lies in the square of the conjugacy class of z. □

Lemma 7.6. *For all positive integers k and prime powers q, there exists a positive integer r and a real element $x \in \mathrm{Cl}_{2r}^+(q)$, both depending on k and q, such that x covers every element of $\mathrm{Cl}_l^\alpha(q)$ for all integers $l \in [1, k]$ and $\alpha = \pm$.*

Proof. Let N denote the sum of the conjugacy class numbers of all $\mathrm{Cl}_l^\alpha(q)$ with $1 \leq l \leq k$ and $\alpha = \pm$. By Lemma 7.5, each such class g_i is covered by a real class x_i in $\mathrm{Cl}_{4m_i}^+(q)$. The statement now follows from Lemma 7.4, by taking $r = 2\sum_{i=1}^N m_i$ and $x := \mathrm{diag}(x_1, \ldots, x_N)$. □

In the next theorem, we remark that the congruence conditions on q ensure that the central extension of G which lies in $\mathrm{GL}_n(\bar{\mathbb{F}}_q)$ has a large enough center that every element of G of small support can be represented by an $n \times n$ matrix for which the primary eigenvalue is 1, as needed for (7.7). In particular, when n and q are odd we have no results about $\Omega_n(q)$ because the center of $\mathrm{SO}_n(q)$ is trivial, and we do not know how to show that elements of small support with principal eigenvalue -1 lie in S^2.

Theorem 7.7. *Let q be a prime power and let $G \in \{\mathrm{PSU}_n(q), \mathrm{PSp}_n(q), \mathrm{P}\Omega_n^\varepsilon(q)\}$. Suppose that $(q+1)|n$ in the SU-case, and that, if $2 \nmid q$ then $2|n$ and $\varepsilon = (-1)^{n(q-1)/4}$ in the Ω-case. If n is sufficiently large, then there exists a conjugacy class S in G such that $S^2 = G$.*

Proof. (a) Ellers and Gordeev [EG, Table 1] already proved Thompson's conjecture for simple classical groups when $q \geq 8$. Hence it suffices to prove the theorem for $q \leq 7$ and $n \geq 117$ sufficiently large. For consistency with the $\mathrm{Cl}_n^\varepsilon(q)$ notation, in the PSU-case, we write $\mathrm{Cl}_n(q^2) = \mathrm{SU}_n(q)$, $\mathbb{F} := \mathbb{F}_{q^2}$, and $V := \mathbb{F}^n$; otherwise, $\mathrm{Cl}_n(q)$ is $\mathrm{Sp}_n(q)$ or $\Omega_n^\pm(q)$, $\mathbb{F} := \mathbb{F}_q$, and $V := \mathbb{F}^n$. Replacing G by $G = \mathrm{Cl}(V)$, it suffices to prove that there exists a real conjugacy class S in G such that S^2 contains a scalar multiple of every non-central element $g \in G$.

(b) By Lemma 7.1, if $g \in G$ satisfies $|\mathbf{C}_G(g)| \geq |G|^{6/7}$, then V admits an orthogonal decomposition $V_1 \oplus V_2$ with $\dim(V_2) > 2\dim(V)/3$, such that $g(V_i) = V_i$, and g acts as a scalar λ on V_2, with $\lambda^{q+1} = 1$ in the SU-case and $\lambda^2 = 1$ otherwise. By Theorem 4.5, if $|\mathbf{C}_G(g)| \leq |G|^{6/7}$, then there exists $\delta > 0$, independent of V, such that

$$|\chi(g)| \leq \chi(1)^{1-\delta} \tag{7.1}$$

for every irreducible character of G. By [GLT2, Theorem 1.3], there exists $\alpha > 0$ (depending on δ) such that if $x \in G$ satisfies $|\mathbf{C}_G(x)| \leq |G|^\alpha$, then

$$|\chi(x)| \leq \chi(1)^{\delta/3} \tag{7.2}$$

for all irreducible characters χ. By the Frobenius formula, $g \in G$ lies in $x^G \cdot x^G$ if

$$\sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(x)^2 \bar{\chi}(g)}{\chi(1)} > 0. \tag{7.3}$$

By [LiSh3, Theorem 1.2], $\sum_{1_G \neq \chi \in \mathrm{Irr}(G)} \chi(1)^{-\delta/3} \to 0$ when $n \to \infty$. Hence, if n is large enough and both (7.1) and (7.2) hold, then

$$\sum_{\chi \neq 1_G} \frac{|\chi(x)^2 \bar{\chi}(g)|}{\chi(1)} < 1,$$

implying (7.3) . We fix $B > 0$ such that if x satisfies (7.2) and g satisfies (7.1), then $\dim(V) \geq B$ implies $g \in x^G \cdot x^G$.

(c) For any sufficiently large integer d, if V has an orthogonal decomposition $V_3 \oplus V_4$, and

$$x = \mathrm{diag}(x_3, x_4) \in \mathrm{Cl}(V_3) \times \mathrm{Cl}(V_4) < \mathrm{Cl}(V) = G,$$

where $\dim(V_3) > d\dim(V_4)$ and the characteristic polynomial of x_3 has no irreducible factors of degree $< d$, then

$$|\mathbf{C}_G(x)| \leq |\mathbf{C}_{\mathrm{GL}(V)}(x)| < |G|^\alpha. \tag{7.4}$$

Indeed, suppose $d > 4\alpha$ and $n = \dim(V)$ is sufficiently large such that

$$n\left(\frac{\alpha}{4} - \frac{1}{d}\right) > 1.3.$$

The assumptions imply that any eigenspace of x has dimension at most

$$\dim(V_4) + \dim(V_3)/d < 2\dim(V_3)/d \leq 2n/d,$$

hence $s := \mathsf{supp}(x) \geq n - 2n/d$. By Propositions 6.4 and 6.6,

$$|\mathbf{C}_G(x)| \leq q^{n(n-s)/2+1.3n} \leq q^{n^2/d+1.3n} < q^{\alpha n^2/4} < |G|^\alpha$$

in the non-SU cases. In the SU-case we argue similarly, using Proposition 6.1. Fix such a d.

(d) We now fix a non-degenerate space W over $\mathbb{F}$ of dimension $\geq d$, unitary if $G = \mathrm{SU}(V)$, symplectic if $G = \mathrm{Sp}(V)$, and quadratic of type + if $G = \Omega(V) \cong \Omega_n^\varepsilon(q)$, and a real semisimple element $h \in \mathrm{Cl}(W)$ whose characteristic polynomial has no irreducible factors over $\mathbb{F}$ of degree less than d. (For instance, $\mathrm{SU}_{4d}(q)$ and its subgroup $\mathrm{Sp}_{4d}(q)$ contain a semisimple element of order

$(q^{2d}+1)/\gcd(2,q-1)$ as does $\Omega^-_{4d}(q)$; moreover, such an element is real by [TZ2, Proposition 3.1]. Next, $\Omega^+_{4d}(q) > \Omega^-_{2d}(q)\times\Omega^-_{2d}(q)$ contains a semisimple element of order $(q^d+1)/\gcd(2,q-1)$, which is again real by [TZ2, Proposition 3.1].)

Next, we fix some integer

$$k > \max(B, \dim(W)) \tag{7.5}$$

and apply Lemma 7.6 to find a non-degenerate space V_0 over $\mathbb{F}$, unitary if $G=\mathrm{SU}(V)$, symplectic if $G=\mathrm{Sp}(V)$, and quadratic if $G=\Omega(V)$, and a real element $y_k\in\mathrm{Cl}(V_0)$ such that y_k covers every element in $\mathrm{Cl}^\beta_l(|\mathbb{F}|)$, $1\le l\le k$. By Lemma 7.2, if y_k is replaced by $\mathrm{diag}(y_k,z)$ for any real element z in any $\mathrm{Cl}^\gamma_s(|\mathbb{F}|)$, it still has the above covering property. We may therefore assume that $\dim(V_0)$ lies in any desired congruence class modulo $\dim(W)$, and that V_0 is also of type ε when $G=\Omega^\varepsilon_n(q)$.

Suppose that n is sufficiently large. Then we can write $n=\dim(V)=\dim(V_0)+N\dim(W)$, with N sufficiently large, and that V is isometric to $V_0\oplus W^N$.

We claim that if V_0 and y_k are fixed as above, $N > d\dim(V_0)/\dim(W)$ is sufficiently large,

$$V := V_0\oplus\underbrace{W\oplus W\oplus\cdots\oplus W}_{N},$$

and

$$x_N := \mathrm{diag}\big(y_k,\underbrace{h,h,\dots,h}_{N}\big)\in\mathrm{Cl}(V_0)\times\mathrm{Cl}(W)^N<\mathrm{Cl}(V)=G,$$

then for every $g\in\mathrm{Cl}(V)$, subject to the hypothesis on (n,q,ε) (which guarantees that $\mathbf{Z}(G)\cong C_2$ in the case of Sp/Ω with $2\nmid q$ and $\mathbf{Z}(G)\cong C_{q+1}$ in the case $G=\mathrm{SU}(V)$), zg lies in $(x_N)^G\cdot(x_N)^G$ for some $z\in\mathbf{Z}(G)$.

Let $f_\lambda(g)$ denote the maximum dimension of V_2 where

$$V = V_1\oplus V_2 \tag{7.6}$$

is a g-stable orthogonal splitting and g acts as a scalar λ on V_2, with $\lambda^{q+1}=1$ in the SU-case and $\lambda=\pm1$ otherwise; and let $f(g)=\max_\lambda f_\lambda(g)$.

To prove the claim in general, we divide into three cases.

(d1) $f(g)\ge\dim(V)-k$.

In this case, we may assume $\dim(V_2)\ge 4$ in the decomposition (7.6) for some eigenvalue λ. Hence, in the case $G=\Omega(V)$, g is centralized by elements u in any chosen $\Omega(V_2)$-coset in $\mathrm{GO}(V_2)$. Likewise, in the case $G=\mathrm{SU}(V)$, g is centralized by elements u in any chosen $\mathrm{SU}(V_2)$-coset in $\mathrm{GU}(V_2)$. Conjugating g using elements in $\mathrm{Sp}(V)$, $\mathrm{GU}(V)$, or $\mathrm{GO}(V)$, and then by suitable elements like u in the case $G=\mathrm{SU}(V)$ or $\Omega(V)$, and replacing g by zg for a suitable $z\in\mathbf{Z}(G)$ if necessary, we may assume that

$$g=\mathrm{diag}(g_1,I_{f(g)})\in\mathrm{Cl}(V_1)\times\mathrm{Cl}(V_2)<\mathrm{Cl}(V). \tag{7.7}$$

As $\dim V_1\le k$, g_1 is covered by y_k, so as h is real, Lemma 7.2 implies g belongs to $(x_N)^G\cdot(x_N)^G$.

(d2) $f(g)\le 2\dim(V)/3$.

This condition implies (7.1) for g by the argument of (b). The choice of N guarantees that $d\dim(V_0)<N\dim(W)$, hence (7.4) holds for x_N. Now we deduce (7.2) for x_N, which implies $g\in(x_N)^G\cdot(x_N)^G$.

(d3) $\dim(V)-k>f(g)>2\dim(V)/3$.

Recall $n = \dim(V)$. When N is large enough, we have $2f(g) - n > n/3 > \dim(V_0)$. Let t denote the largest integer such that

$$e := \dim(V_0) + t\dim(W) \le 2f(g) - n. \tag{7.8}$$

By the choice of t, $e > 2f(g) - n - \dim(W)$. Hence

$$e - (3f(g) - 2n) > n - f(g) - \dim(W) > k - \dim(W) > 0$$

by (7.5) and (d3). Together with (7.8), this implies that

$$\frac{n-e}{2} \le f(g) - e < \frac{2(n-e)}{3}. \tag{7.9}$$

Arguing as in part (d1) we may assume that $f(g) = f_1(g)$ and that

$$g = \mathrm{diag}(I_{\dim(V_0)+t\dim(W)}, g_1) \in \mathrm{Cl}(V_0 \oplus W^t) \times \mathrm{Cl}(W^{N-t}) < \mathrm{Cl}(V).$$

Note that x_N is conjugate to both

$$\mathrm{diag}\big(y_k, \underbrace{h, \dots, h}_{t}, \underbrace{h, \dots, h}_{N-t}\big) \in \mathrm{Cl}(V_0) \times \mathrm{Cl}(W)^t \times \mathrm{Cl}(W)^{N-t} < \mathrm{Cl}(V)$$

and

$$\mathrm{diag}\big(y_k^{-1}, \underbrace{h^{-1}, \dots, h^{-1}}_{t}, \underbrace{h, \dots, h}_{N-t}\big) \in \mathrm{Cl}(V_0) \times \mathrm{Cl}(W)^t \times \mathrm{Cl}(W)^{N-t} < \mathrm{Cl}(V).$$

Conjugating each element by an element of the form

$$(I_{\dim(V_0)+t\dim(W)}, v) \in \mathrm{Cl}(V_0 \oplus W^t) \times \mathrm{Cl}(W)^{N-t} < \mathrm{Cl}(V),$$

it suffices to prove that g_1 is contained in the square of the conjugacy class in $\mathrm{Cl}(W^{N-t})$ of

$$x' := \mathrm{diag}\big(\underbrace{h, \dots, h}_{N-t}\big).$$

By the choice of h, inequality (7.4) holds for x', which implies (7.2) for x'. The construction of g_1 shows that $f_1(g_1) = f_1(g) - e = f(g) - e$, and $\dim(W^{N-t}) = n - e$, so

$$\frac{1}{2}\dim(W^{N-t}) \le f_1(g_1) < \frac{2}{3}\dim(W^{N-t})$$

by (7.9). It follows that $f(g_1) = f_1(g_1) < 2\dim(W^{N-t})/3$, and so g_1 satisfies (7.1). As

$$\dim(W^{N-t}) = n - e \ge n - (2f(g) - n) \ge 2(n - f(g)) > 2k > B$$

by (7.8), it follows that g_1 is in the square of the conjugacy class of x', completing the proof. □

Theorem 7.8. *For all $A > 0$, there exists $B > 0$ such that the following statement holds for all $n \in \mathbb{Z}_{\ge 1}$ and all prime powers q. If $G = \mathrm{SL}_n^{\varepsilon}(q)$ for some $\varepsilon = \pm$ and the characteristic polynomial of a semisimple element $x \in G$ factors, over $\mathbb{F}_q$ if $\varepsilon = +$ and over $\mathbb{F}_{q^2}$ if $\varepsilon = -$, into pairwise distinct irreducible polynomials $P_1, \dots, P_k$ of degrees $\deg P_i \ge n/A$ for all i, then $x^G \cdot x^G$ contains every element $g \in G$ of support $\ge B$. In particular, the square of the conjugacy class of a Singer element in $\mathrm{SL}_n(q)$ covers all elements $g \in \mathrm{SL}_n(q)$ for which $\mathsf{supp}(g)$ exceeds an absolute constant value.*

Proof. Since the support of an element of $\tilde{G} := \mathrm{GL}_n^{\varepsilon}(q)$ is at most n, by enlarging B, we are free to make $n \ge A$ as large as we wish. Also note that $k \le A$.

Note that the element x is regular semisimple, and $T := \mathbf{C}_{\tilde{G}}(x)$ is a maximal torus, so of order at most $(q+1)^n$. Moreover, the image of T under the determinant map is the same as of $\tilde{G}$. Hence

the conjugacy class of x in G is the same as its class in $\tilde{G}$. Let $g \in G$. To show that $g \in x^G \cdot x^G$, it suffices to prove that

$$\sum_{\chi \in \mathrm{Irr}(\tilde{G})} \frac{\chi(x)^2 \bar{\chi}(g)}{\chi(1)} \neq 0.$$

As $\det(g) = \det(x) = 1$, for every character χ of degree 1 we have $\chi(x) = \chi(x)^2\bar{\chi}(g) = 1$. Therefore, it suffices to prove that

$$\sum_{\{\chi \in \mathrm{Irr}(\tilde{G}) | \chi(1) > 1\}} \frac{|\chi(x)|^2 |\chi(g)|}{\chi(1)} < q - \varepsilon. \tag{7.10}$$

For any fixed $\epsilon > 0$, choosing B sufficiently large, the contribution of characters χ satisfying $\chi(1) \geq q^{\epsilon n^2}$ to (7.10) is $o(1)$. Indeed, consider any such character χ and any irreducible constituent ψ of $\chi|_G$. Since $\tilde{G}/G \cong C_{q-\varepsilon}$, by Clifford's theorem we have $\chi|_G = \psi_1 + \ldots + \psi_t$, where $\psi_1 = \psi, \ldots, \psi_t$ are distinct $\tilde{G}$-conjugates of ψ, and $t|(q-\varepsilon)$. By Theorem 5.5,

$$|\psi_i(g)| \leq \psi_i(1)^{1-\sigma B/n} = (\chi(1)/t)^{1-\sigma B/n},$$

and so $|\chi(g)| \leq t(\chi(1)/t)^{1-\sigma B/n}$. As $\chi(1) \geq (q+1)^2 \geq t^2$, we obtain

$$|\chi(g)/\chi(1)| \leq \chi(1)^{-\sigma B/2n} \leq q^{-\varepsilon\sigma Bn/2}.$$

Since $|T| \leq (q+1)^n < q^{2n}$, it follows that the contribution of all these characters to (7.10) is at most

$$q^{-\varepsilon\sigma Bn/2} \sum_{\chi} |\chi(x)|^2 \leq q^{-\varepsilon\sigma Bn/2}|T| < q^{2n(1-\varepsilon\sigma B/4)}$$

which is $o(1)$ when B is large enough.

Any irreducible character χ of $\tilde{G}$ belongs to the rational Lusztig series labeled by a semisimple element s in the dual group which can be identified with $\tilde{G}$. Consider the case $s \notin \mathbf{Z}(\tilde{G})$. Then $L := \mathbf{C}_{\tilde{G}}(s)$ is a proper Levi subgroup of $\tilde{G}$. Hence $\chi = \pm R_L^G(\varphi)$ is Lusztig induced from an irreducible character φ of L, see [DM, Theorem 13.25]. We claim that either $\chi(x) = 0$ or $\chi(1) \geq q^{n^2/A^2-1}$. Indeed, assume that $\chi(x) \neq 0$. As x is regular semisimple, the Steinberg characters $\mathsf{St}_{\tilde{G}}$ of $\tilde{G}$ and St_L of L take values ± 1 at x. Applying [DM, Proposition 9.6] we have

$$0 \neq \chi(x) = \pm(\mathsf{St}_{\tilde{G}} \cdot \chi)(x) = \pm \mathrm{Ind}_L^G(\mathsf{St}_L \cdot \varphi)(x),$$

and so x is contained in a conjugate of L. If $L = \mathrm{GL}_a^{\pm}(q^b)$ with $ab = n$, then $b > 1$ as $s \notin \mathbf{Z}(\tilde{G})$, and so $\chi(1) \geq q^{n^2/4-2}$ by [GLT1, Lemma 5.8]. Thus we may assume L is of type $\mathrm{GL}_{m_1}^{\pm}(q^{a_1}) \times \ldots \times \mathrm{GL}_{m_r}^{\pm}(q^{a_r})$ with $r \geq 2$ and each $m_i a_i$ is a sum of some n_j's; in particular, $m_i a_i \geq n/A$. Using [GLT1, Lemma 5.1(vi)], we then have $\chi(1) \geq [G:L]_{p'} \geq q^{m_1(n-m_1)}/2 \geq q^{n^2/A^2-1}$.

It remains therefore to consider the case $s \in \mathbf{Z}(\tilde{G})$, i.e. χ is a unipotent character times a linear character, so on g and x, it can be treated as a unipotent character (but each such character occurs $q-\varepsilon$ times). Each unipotent character χ is associated to a partition $\lambda(\chi)$ of n, and the value of χ at the regular semisimple element x is given, up to a sign, by the value at the permutation $\pi \in \mathsf{S}_n$, which is a product of k cycles of length $n_1, \ldots, n_k$, of the irreducible character of S_n associated to $\lambda(\chi)$, see e.g. [LM, Proposition 3.3]. As π consists of k cycles, by [LaSh2, Theorem 7.2], $|\chi(x)| \leq 2^{k-1}k!$, which is bounded in terms of A.

Note that χ has level $j = n - \lambda_1$ by [GLT1, Theorem 3.9]. If $\lambda_1 \leq n/2$, then $\chi(1) \geq q^{n^2/4-2}$ by [GLT1, Theorem 1.2(ii)], and, as before, the contribution of all such unipotent characters to the left hand side of (7.10) is $o(1)$. Hence it remains to consider the characters χ with $\lambda_1 > n/2$; any such unipotent character is irreducible over G, see [GLT1, Corollary 8.6]. For any fixed positive value of

$j = n - \lambda_1 < n/2$, the number of partitions of n with largest part λ_1 is $p(n-\lambda_1)$ (where $p(\cdot)$ is the partition function), and the degree of the associated unipotent character is at least $q^{j(n-j)-1} > q^{nj/3}$ by [GLT1, Theorem 1.2(i)]. For these characters χ, $\mathsf{supp}(g) \geq B$ implies by Theorem 5.5 that $|\chi(g)|/\chi(1) < q_0^j$ with $q_0 := q^{\sigma B/3}$. Note that $\sum_{j=1}^{\infty} 1/(q_0^j - 1) < \sum_{j=1}^{\infty} q_0^{-j+1}/(q_0 - 1) < 1/(q_0 - 2)$, and so

$$\sum_{j=1}^{\infty} \frac{p(j)}{q_0^j} < \sum_{j=1}^{\infty} \frac{2^j}{q_0^j} = \frac{2}{q_0 - 2},$$

which is $o(1)$ when B is large enough. Hence, the contribution of these characters to (7.10) is less than $2^{k-1}k!(e^{1/(q_0-2)} - 1)(q - \varepsilon) = o(q - \varepsilon)$, and the theorem follows. □

Since this paper was written, Theorem 7.8 has been generalized: see [LTT, Theorem 1.1].

8. Further applications

8.1. **Mixing time of random walks on Cayley graphs.** Recall that the mixing time of a probability distribution P on a finite group G is the smallest integer n such that $\|P^{*n} - U_G\|_1 < 1/e$, where U_G denotes the uniform distribution on G. The mixing time of a generating set S of G means the mixing time of the uniform distribution U_S on S. The theorem of Diaconis and Shahshahani [DS] asserts that for the set of transpositions of S_n, the mixing time is asymptotic to $\frac{n \log n}{2}$. By comparison, every element in S_n is the product of at most $n-1$ transpositions.

For any constants C_1 and C_2 there exists $\epsilon > 0$ so that if n is sufficiently large and S is any conjugacy class in S_n of permutations fixing all but C_1 points, a random product of less than $C_2 n$ elements has probability greater than $1/2$ of fixing more than ϵn elements. Thus the mixing time for conjugacy classes of bounded support is superlinear in n, implying that for symmetric and alternating groups, the maximum ratio of mixing time over covering number for conjugacy classes goes to ∞.

In this section, we show that the situation is different for finite simple groups of Lie type. Liebeck and Shalev proved [LiSh2, Corollary 1.2] that if G is such a group and S is a conjugacy class of G, then the diameter of the Cayley graph $\Gamma(G, S)$ is less than $C\frac{\log |G|}{\log |S|}$, where C is an absolute constant. Note that this bound is optimal up to a constant factor.

In this subsection, we prove the same result, though with a different constant, for mixing time. (The special example of transvections in $\mathrm{SL}_n(q)$ was handled by Hildebrand [Hi]; furthermore, the case of semisimple classes whose centralizer is a Levi subgroup is treated in [BLST, Theorem 1.12].) This improves on the previously known upper bound $O\big(\frac{\log^3 |G|}{\log^2 |S|}\big)$ [LiSh2, Corollary 1.14], and proves a conjecture of Shalev [Sh, 4.3]. It also resolves a conjecture made by Lubotzky in [Lu, p.179], stating that, if G is a finite simple group (of Lie type) and S is a non-trivial conjugacy class of G, then the mixing time of the Cayley graph $\Gamma(G, S)$ is linearly bounded above in terms of the diameter of $\Gamma(G, S)$.

Theorem 8.1. *There exists an absolute constant C' such that if $S = g^G$ is any non-trivial conjugacy class in a finite simple group G of Lie type, then the mixing time of the random walk on the Cayley graph $\Gamma(G, S)$ is less than $C'\frac{\log |G|}{\log |S|}$.*

Proof. Let c denote the constant in Theorem A. We choose $C' > 26/c + 1$, so $N \geq C'\frac{\log |G|}{\log |S|} - 1$ implies $N \geq \frac{26 \log |G|}{c \log |S|}$, whence

$$c\frac{\log |S|}{\log |G|} > \frac{26}{N}.$$

By Theorem A, this implies $|\chi(g)| \leq \chi(1)^{1-\frac{26}{N}}$, so

$$|\chi(g)|^N \leq \chi(1)^{N-26}.$$

To prove the theorem, it suffices to prove that for all $x \in G$, the probability that the product of N i.i.d. random variables with distribution U_S gives x is within $1/e|G|$ of $1/|G|$. By the Frobenius formula, this probability is

$$\frac{1}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g)^N \bar{\chi}(x)}{\chi(1)^{N-1}}.$$

By [FG, Theorem 1.1], $|\mathrm{Irr}(G)| \leq 27.2q^r$, if G is of Lie type of rank r defined over $\mathbb{F}_q$, and $\chi(1) > q^{r/3}$ by [LaSe] when $1_G \neq \chi \in \mathrm{Irr}(G)$. Now,

$$\sum_{\chi \neq 1_G} \frac{|\chi(g)^N \bar{\chi}(x)|}{\chi(1)^{N-1}} \leq \sum_{\chi \neq 1_G} \chi(1)^{-24} \frac{|\chi(g)|^N}{\chi(1)^{N-26}} \leq \sum_{\chi \neq 1_G} \chi(1)^{-24} \leq \frac{|\mathrm{Irr}(G)|}{\min_{\chi \neq 1_G} \chi(1)^{24}}.$$

This is less than

$$\frac{27.2q^r}{q^{8r}} \leq \frac{27.2}{128} < \frac{1}{e}.$$

In fact, given any $\varepsilon > 0$, we have $27.2/q^{7r} < \varepsilon$, except possibly for a finite number of possibilities for (q, r). This proves Lubotzky's conjecture [Lu, p. 179] (since, as noted above, the diameter of $\Gamma(G, S)$ is of the same magnitude as $(\log |G|)/(\log |S|)$. □

Proposition 8.2. *There exists an absolute constant $C'' > 0$ such that if S is a non-trivial conjugacy class in a finite simple group G of Lie type, then the mixing time of the random walk on the Cayley graph $\Gamma(G, S)$ is greater than $C'' \frac{\log |G|}{\log |S|}$.*

Proof. Since $\frac{\log |G|}{\log |S|}$ is bounded in bounded rank, we may assume without loss of generality that the rank of G is as large as we wish, in particular that G is classical. By Corollary 6.7, $\frac{\log |G|}{\log |S|} \leq \frac{n}{5\mathsf{supp}(g)}$, so it suffices to prove that the mixing time for $\Gamma(G, S)$ is greater than $m := \lfloor \frac{n}{2\mathsf{supp}(g)} \rfloor$, where $S = g^G$. Every element in S^m has support $\leq m\mathsf{supp}(g) \leq n/2$ by Lemma 5.1. Therefore, the characteristic polynomial of each such element has at least $n/2$ irreducible factors. By [LaSh3, Proposition 3.4], the proportion of elements of G satisfying this property is $o(1)$, so

$$\|U_{g^G}^{*m} - U_G\|_1 = 2 - o(1) > \frac{1}{e}.$$

□

Theorem 8.1 and Proposition 8.2 imply that the diameter and the mixing time of $\Gamma(G, S)$ are linearly bounded in terms of one another, and so are of the same magnitude, for all non-trivial conjugacy classes S in all simple groups of Lie type G; and they have the same magnitude as $\mathrm{rank}(G)/\mathsf{supp}(g)$, as shown by Corollary 6.7.

8.2. **McKay graphs and products of irreducible characters.** Let G be any finite group, $\mathrm{Irr}(G)$ the set of irreducible characters, and χ a complex character of G. Recall [LiST1] that the *McKay graph* $\mathcal{M}(G, \chi)$ associated to χ is the directed graph on vertex set $\mathrm{Irr}(G)$ such that there is an edge from χ_1 to χ_2 if and only if χ_2 is a constituent of $\chi\chi_1$. This graph is connected if and only if χ is faithful [Bu, Chapter XV, Theorem IV]. One also considers random walks on $\mathcal{M}(G, \chi)$, starting from any vertex $\alpha \in \mathrm{Irr}(G)$ and with the transition probability from vertex χ_1 to vertex χ_2 equal to $\langle \chi\chi_1, \chi_2 \rangle_G \cdot \chi_2(1)/\chi(1)\chi_1(1)$ (proportional to the dimension of the χ_2-homogeneous component in a representation affording $\chi\chi_1$), see [Fu, §1].

For groups of Lie type, we now settle in the affirmative a question of Liebeck, Shalev, and Tiep [LiST1, Conjecture 1] (note that the case of alternating groups is handled in [LiST2, Theorem 2]). In fact, we prove a slightly stronger result, in which, by $\chi^*(1)$ we mean the sum of degrees of distinct irreducible constituents of a character χ. As discussed in [LiST1], this upper bound on the diameter is optimal.

Theorem 8.3. *There exists an absolute constant γ such that for every finite simple group G and every faithful (not necessarily irreducible) character χ of G, the diameter of the McKay graph of χ is less than $\gamma \frac{\log |G|}{\log \chi^*(1)}$.*

Proof. Let χ_1 be an irreducible constituent of largest degree of χ. If G is of Lie type, then the results of [FG] and [LaSe] imply that $\chi_1(1) \geq k(G)^{1/6}$. It follows that $\chi_1(1) \leq \chi^*(1) \leq \chi_1(1)^7$. If $G = \mathsf{A}_n$, then for n sufficiently large, [LiSh4, Theorem 1.1(i)] implies that the number of distinct irreducible characters of G of degree $\leq \chi_1(1)$ is less than $\chi_1(1)^2$, so the same inequalities hold. Thus in all cases $\log \chi^*(1)$ and $\log \chi_1(1)$ are of the same magnitude. Hence it suffices to prove the conjecture in the case χ is irreducible.

The theorem is known for alternating groups [LiST2, Theorem 2] and for Lie-type groups of bounded rank r [LiST1, Theorem 2], so without loss of generality, we may assume $r \geq 9$ and G is classical. Choose $\gamma = 7/c + 1$, where c is defined as in Theorem A. Let χ_1 and χ_2 denote irreducible characters of a finite simple group G of classical type. Let

$$N := \left\lceil \frac{7}{c} \cdot \frac{\log |G|}{\log \chi(1)} \right\rceil \leq \gamma \frac{\log |G|}{\log |\chi(1)|}.$$

Then,

$$\langle \chi^N \chi_1, \chi_2 \rangle_G = \frac{1}{|G|} \sum_{g \in G} \chi(g)^N \chi_1(g) \overline{\chi}_2(g) = \frac{1}{|G|} \sum_{S = g^G \subset G} |S| \chi(g)^N \chi_1(g) \overline{\chi}_2(g),$$

where the last sum is taken over conjugacy classes $S = g^G$. To prove this is non-zero, it suffices to prove

$$\sum_{S = g^G \neq \{1\}} |S| |\chi(g)|^N |\chi_1(g)| |\overline{\chi}_2(g)| < \chi(1)^N \chi_1(1) \chi_2(1).$$

As $|\chi_i(g)| \leq \chi_1(1)$, it suffices to prove that

$$\sum_{S = g^G \neq \{1\}} |S| \Big(\frac{|\chi(g)|}{\chi(1)} \Big)^N < 1.$$

By Theorem A and since $N \geq (7/c)(\log |G|)/(\log \chi(1))$, it suffices to prove

$$\sum_{S \neq \{1\}} |S| \chi(1)^{-7 \frac{\log |S|}{\log \chi(1)}} = \sum_{S \neq \{1\}} \frac{1}{|S|^6} < 1.$$

Clearly,

$$\sum_{S \neq \{1\}} \frac{1}{|S|^6} < \frac{k(G)}{\min_{S \neq \{1\}} |S|^6}.$$

By [FG, Theorem 1.1], $|\mathrm{Irr}(G)| \leq 27.2 q^r$. Now, $|S|$ is the degree of a permutation representation of G, so by [KlL, Table 5.2.A], this is greater than q^r, so $|S|^6 > q^{6r} > 32 q^r$. □

Random walks on some McKay graphs defined for S_n and $\mathrm{GL}_n(q)$ are studied in [Fu, Theorems 4.1, 5.1]. The following result determines the asymptotic of the convergence rate (to the stationary distribution) of random walks on general McKay graphs for simple groups of Lie type.

Theorem 8.4. *There exist absolute constants $C_1 > C_2 > 0$ such that the following statements hold for any non-trivial irreducible character χ of any finite simple group G of Lie type. The convergence rate of the random walk on the McKay graph of χ starting from any vertex $\alpha \in \mathrm{Irr}(G)$ is less than $C_1 \frac{\log |G|}{\log \chi(1)}$, and more than $C_2 \frac{\log |G|}{\log \chi(1)}$ if $\alpha = 1_G$.*

This means that in any sequence of examples, the difference in total variation, between the stationary probability distribution and the distribution obtained from any initial state after at least $C_1 \frac{\log |G|}{\log \chi(1)}$ steps, goes to 0, while the total variation difference after at most $C_2 \frac{\log |G|}{\log \chi(1)}$ steps remains bounded away from 0.

Proof. Let K_α^l denote the probability measure given by taking l steps from the starting vertex $\alpha \in \mathrm{Irr}(G)$, and let π denote the stationary distribution, which is known to be the Plancherel measure $\pi(\beta) = \beta(1)^2/|G|$, see [Fu, §2]. If

$$\|P - Q\| = \frac{1}{2} \sum_{\beta \in \mathrm{Irr}(G)} |P(\beta) - Q(\beta)|$$

denotes the total variation distance between two probabilistic measures P and Q on $\mathrm{Irr}(G)$, then [Fu, Lemmas 2.1, 3.1] shows that

$$4\|K_\alpha^l - \pi\|^2 \leq \sum_{S = x^G \neq \{1\}} |\frac{\chi(x)}{\chi(1)}|^{2l} |S| |\frac{\alpha(x)}{\alpha(1)}|^2.$$

Clearly, $|\alpha(x)| \leq \alpha(1)$. Applying Theorem A and choosing $l \geq (4/c) \log |G| / \log \chi(1)$, we obtain $|\chi(x)/\chi(1)|^{2l} \leq \chi(1)^{-8 \log_{\chi(1)} |S|} = |S|^{-8}$, and so

$$4\|K_\alpha^l - \pi\|^2 \leq \sum_{S = x^G \neq \{1\}} \frac{1}{|S|^7},$$

which is less than $1/q^r$ if G is of rank r over $\mathbb{F}_q$, as shown in the proof of Theorem 8.3.

For the lower bound, for any $l < (1/4) \frac{\log |G|}{\log \chi(1)}$, we see that χ^l cannot contain any irreducible character β of degree $\geq |G|^{1/4}$ (e.g. the Steinberg character), and thus $K_{1_G}^l(\beta) = 0$. Taking C_2 small enough, we may assume that the rank r of G is large enough, so that $|\mathrm{Irr}(G)| \leq 27.2 q^r \leq |G|^{1/3}$. For such l and G, now we have

$$2\|K_{1_G}^l - \pi\| \geq \sum_{\beta(1) \geq |G|^{1/4}} \frac{\beta(1)^2}{|G|} = 1 - \sum_{\gamma(1) < |G|^{1/4}} \frac{\gamma(1)^2}{|G|} > 1 - \frac{|G|^{1/2} |\mathrm{Irr}(G)|}{|G|} \geq 1 - |G|^{-1/6} > 2/3.$$

□

The next result generalizes Theorem 8.3 and proves a conjecture of Gill [Gi]. Note that the case $G = \mathrm{PSL}_n(q)$ or $\mathrm{PSU}_n(q)$, with q large enough compared to n, was handled in [LiST2, Theorem 3(ii)]; on the other hand, the case of alternating groups is still open.

Theorem 8.5. *There exists an absolute constant δ such that for all finite simple groups of Lie type G and all non-trivial $\chi_1, \chi_2, \ldots, \chi_m \in \mathrm{Irr}(G)$, if $\chi_1(1)\chi_2(1) \ldots \chi_m(1) \geq |G|^\delta$, then $\chi_1 \chi_2 \ldots \chi_m$ contains every irreducible character of G.*

Proof. Suppose G has bounded rank $r \leq l$. Taking $\delta \geq 245 l^2$, we see that the condition $\prod_{i=1}^m \chi_i(1) \geq |G|^\delta$ implies that $m \geq 490 l^2$, since $|\chi_i(1)| \leq |G|^{1/2}$. It follows from [LiST2, Theorem 3(i)] that $\prod_{i=1}^m \chi_i$ contains $\mathrm{Irr}(G)$.

Hence we may assume that $r \geq 9$ and G is classical. Choose $\delta \geq 7/c$. For any $\theta \in \mathrm{Irr}(G)$, we have

$$\langle \prod_{i=1}^{m} \chi_i, \theta \rangle_G = \frac{1}{|G|} \sum_{g \in G} \prod_i \chi_i(g) \overline{\theta}(g) = \frac{1}{|G|} \sum_{S = g^G \subset G} |S| \prod_i \chi_i(g) \overline{\theta}(g),$$

where the last sum is taken over conjugacy classes $S = g^G$. To prove this is non-zero, it suffices to prove

$$\sum_{S = g^G \neq \{1\}} |S| |\prod_i \chi_i(g)| |\overline{\theta}(g)| < \prod_i \chi_i(1) \theta(1).$$

As $|\theta(g)| \leq \theta(1)$, it suffices to prove that

$$\sum_{S = g^G \neq \{1\}} |S| \prod_i \frac{|\chi_i(g)|}{\chi_i(1)} < 1.$$

By Theorem A we have $|\chi_i(g)/\chi_i(1)| \leq \chi_i(1)^{-c \log_{|G|} |S|}$, hence

$$\sum_{S = g^G \neq \{1\}} |S| \prod_i \frac{|\chi_i(g)|}{\chi_i(1)} \leq \sum_{S \neq \{1\}} |S| (\prod_i \chi_i(1))^{-c \log_{|G|} |S|}.$$

Since $\prod_i \chi_i(1) \geq |G|^{\delta}$, we now have

$$\sum_{S = g^G \neq \{1\}} |S| \prod_i \frac{|\chi_i(g)|}{\chi_i(1)} \leq \sum_{S \neq \{1\}} |S| \cdot |S|^{-c\delta} \leq \sum_{S \neq \{1\}} \frac{1}{|S|^6} < 1,$$

the last inequality already established in the proof of Theorem 8.3. □

The next result proves [LiST2, Conjecture 4] for simple groups of Lie type.

Corollary 8.6. *There exists an absolute constant δ' such that for all finite simple groups of Lie type G of rank r and all non-trivial $\chi_1, \chi_2, \ldots, \chi_m \in \mathrm{Irr}(G)$, if $m \geq \delta' r$, then $\chi_1 \chi_2 \ldots \chi_m$ contains every irreducible character of G.*

Proof. Take $\delta' = 12\delta$, with δ the constant in Theorem 8.5. Since $\chi_i(1) \geq q^{r/3}$ by [LaSe] and $|G| \leq q^{4r^2}$ if G is defined over $\mathbb{F}_q$, we have $\prod_{i=1}^{m} \chi_i(1) \geq q^{12\delta r^2/3} \geq |G|^{\delta}$. Hence the statement follows from Theorem 8.5. □

Taking $\chi_1 = \ldots = \chi_m = \chi$ in Corollary 8.6, we obtain the following consequence, which was proved in [LiST1, Theorem 3] for q large enough compared to n (but with a much smaller constant).

Corollary 8.7. *There exists an absolute constant δ' such that for all finite simple groups $\mathrm{PSL}_n(q)$ and $\mathrm{PSU}_n(q)$ and all non-trivial $\chi \in \mathrm{Irr}(G)$, if $m \geq \delta'(n-1)$, then χ^m contains every irreducible character of G.*

8.3. **Power word maps on simple groups.** Recall that $\mathrm{GL}_n^{\varepsilon}(q)$ denotes $\mathrm{GL}(\mathbb{F}_q^n)$ if $\varepsilon = +$ and $\mathrm{GU}(\mathbb{F}_{q^2}^n)$ if $\varepsilon = -$, and similarly for $\mathrm{SL}_n^{\varepsilon}(q)$ and $\mathrm{PSL}_n^{\varepsilon}(q)$. The notion of the *level* $\mathfrak{l}(\chi)$ of a character χ of $\mathrm{GL}_n^{\varepsilon}(q)$ and $\mathrm{SL}_n^{\varepsilon}(q)$ was introduced in [GLT1, Definitions 1, 2]. The following result gives a somewhat better bound than [GLT1, Theorem 1.6(iii), (iv)], which is needed in Theorem 8.10 below.

Proposition 8.8. *Let q be any prime power, $n \geq 1$, $G = \mathrm{GU}_n(q)$ or $\mathrm{SU}_n(q)$, and $\chi \in \mathrm{Irr}(G)$.*

(i) *If $\mathfrak{l}(\chi) \leq \sqrt{n - 3/4} - 1/2$, then $|\chi(g)| < 1.93 \chi(1)^{1 - 1/n}$ for all $g \in G \smallsetminus \mathbf{Z}(G)$.*

(ii) *If $\mathfrak{l}(\chi) \leq \sqrt{n/2 - 1}$, then $|\chi(g)| < 1.93 \chi(1)^{\max(1 - 1/2\mathfrak{l}(\chi), 1 - \mathsf{supp}(g)/n)}$ for all $g \in G$.*

Proof. We follow the proof of [GLT1, Theorem 1.6(iii), (iv)], and assume first that $j := \mathfrak{l}(\chi) \geq 3$. Using [GLT1, Lemma 5.1(iii)] we see that

$$|\mathrm{GU}_j(q)|/q^{j^2} \leq (q+1)(q^2-1)(q^3+1)/q^6 < 1.266.$$

Hence we can use [GLT1, (8.18)] with the improved bound $|S| < 1.266q^{j^2}$ for $S := \mathrm{GU}_j(q)$, which leads to the improved upper bound $0.747q^{(n-1)j}$ for $|S|\big(q^{n(j-1)} + \sqrt{16.52q^{j^2+j-1}}q^{n(j-2)}\big)$, and obtain

$$|\chi(1)| \geq \frac{q^{nj}(1-0.747q^{-j})}{|S|\alpha(1)} > \frac{0.906q^{nj}}{|S|\alpha(1)},\ |\chi(g)| < \frac{1.747q^{(n-1)j}}{|S|\alpha(1)}$$

if $\chi = D^\circ_\alpha$ for $\alpha \in \mathrm{Irr}(S)$ in the notation of [GLT1, Theorem 1.1].

Suppose $j = 2$, and let $\chi = D^\circ_\alpha$ for $\alpha \in \mathrm{Irr}(S)$ and $k := n - \mathsf{supp}(g)$. In the notation of [GLT1, §8.3], $N' = 1$, so $D'_\alpha(1) \leq q^2\sqrt{2}$ in [GLT1, (8.17)], and instead of [GLT1, (8.18)] we now have

$$\chi(1) \geq \frac{q^{2n} - |S|(q^n + q^2\sqrt{2})}{|S|/\alpha(1)},\ |\chi(g)| \leq \frac{q^{2k} + |S|(q^n + q^2\sqrt{2})}{|S|/\alpha(1)}. \tag{8.1}$$

Also, $|S| = |\mathrm{GU}_2(q)| \leq 1.125q^4$, hence $|S|(q^n + q^2\sqrt{2})$ is less than $0.588q^{2n-2}$ when $n \geq 7$ and less than $0.588q^{1.5n}$ when $n \geq 10$. Now we can repeat the rest of the proof of [GLT1, Theorem 1.6(iii), (iv)] verbatim to obtain the result for $j \geq 2$.

The estimates are trivial if $j = 0$ or if $g \in \mathbf{Z}(G)$, i.e. $k := n - \mathsf{supp}(g) = 0$. If $j = 1$, then, as shown in the proof [GLT1, Theorem 1.6(iii)], we have $\chi(1) \geq (q^n - q)/(q+1)$, and

$$|\chi(g)| \leq \frac{q^{n-1}+q}{q+1},\ |\chi(g)| \leq \begin{cases} q^k < 1.93\chi(1)^{1/2}, & k \leq (n-1)/2, \\ (2q^k+q)/(q+1) < 1.93\chi(1)^{k/n}, & k \geq n/2, \end{cases}$$

yielding the result. □

Proposition 8.9. *There exists an integer $N \geq 1$ such that the following statement holds for any prime power q, any integer $n \geq N$, any integer a with $n/3 \leq a \leq 2n/3$, and any $\varepsilon = \pm$. If $G = \mathrm{SL}^\varepsilon_n(q)$ and $s, t \in G$ are regular semisimple elements belonging to maximal tori T_1 of type $T_{a,n-a}$ and T_2 of type $T_{a+1,n-a-1}$, then $s^G \cdot t^G$ contains every non-central element $g \in G$, except possibly when $q = 2$ and g is a scalar multiple of a transvection.*

Proof. Let $\chi \in \mathrm{Irr}(G)$ be such that $\chi(s)\chi(t) \neq 0$. As shown in the proof of [GLOST, Proposition 8.4], χ is a unipotent character χ^λ labeled by a partition $\lambda \vdash n$, and $|\chi(s)\chi(t)| \leq 16$. The choices for λ are listed in [LaST1, Corollary 3.1.3]: either $\lambda = (n-j, 1^j)$ with $0 \leq j \leq n-1$, or its largest part λ_1 satisfies $n - \lambda_1 \geq \min(a, n-a) - 1 \geq n/3 - 1$, and there are at most $4an \leq 8n^2/3$ of them.

Since $g \notin \mathbf{Z}(G)$, we have that $\mathsf{supp}(g) \geq 1$. Note that $\mathfrak{l}(\chi) = n - \lambda_1$ by [GLT1, Theorem 3.9]. Next, by [GLT1, Theorem 1.3], if $\mathfrak{l}(\chi) \geq n_0 := \sqrt{n}/5$, then $\chi(1) > q^{n_0(n-n_0)-3}$. Hence, applying Theorem 5.5 we now have

$$\Sigma_1 := \sum_{\chi \in \mathrm{Irr}(G),\ \mathfrak{l}(\chi) \geq n_0} \frac{|\chi(s)\chi(t)\bar{\chi}(g)|}{\chi(1)} \leq \frac{16 \cdot 8n^2/3}{q^{\sigma(n_0(n-n_0)-3)/n}} = O\big(\frac{n^2}{2^{\sqrt{n}/6}}\big).$$

Choosing N large enough, we have that $\Sigma_1 \leq 0.01$.

Now we look at χ with $\chi(s)\chi(t) \neq 0$ and $\mathfrak{l}(\chi) < n_0$. By the above considerations, $\chi = \chi^{(n-j,1^j)}$ with $0 \leq j = \mathfrak{l}(\chi) < n_0 < n/3$. The Murnaghan-Nakayama rule applied to $\chi(s)$, $\chi(t)$ and the hook partition $(n-j, 1^j)$ shows that $|\chi(s)\chi(t)| = 1$, see [LaST1, Proposition 3.1.1, Corollary 3.1.2]. On

the other hand, since $\mathfrak{l}(\chi) < n_0$, [GLT1, Theorem 1.6(ii)] and Proposition 8.8(ii) apply to χ (when N is large enough) and yield $|\chi(g)| < 1.93\chi(1)^{1-1/n}$. We also have by [LMT, Lemma 4.1] that

$$\chi^{(n-j,1^j)}(1) = q^{j(j+1)/2}\frac{\prod_{i=n-j}^{n-1}(q^i-\varepsilon^i)}{\prod_{i=1}^{j}(q^i-\varepsilon^i)} > q^{nj-j(j+1)/2-2}. \tag{8.2}$$

In particular, when N is large enough, $\chi(1)^{1/n} > q^{j-1/49}$, and so

$$\Sigma_2 := \sum_{\chi\in\mathrm{Irr}(G),\ 1\le\mathfrak{l}(\chi)<n_0}\frac{|\chi(s)\chi(t)\bar\chi(g)|}{\chi(1)} \le \sum_{j=1}^{n_0}\frac{1.93}{q^{j-1/49}} < \sum_{j=1}^{\infty}\frac{1.93q^{1/49}}{q^j}.$$

If $q \ge 3$, then $\Sigma_2 < 0.99$ and so $\Sigma_1 + \Sigma_2 < 1$, showing $g \in s^G \cdot t^G$.

From now on we assume $q = 2$. If g is semisimple, then $g \in s^G \cdot t^G$ by [GT, Lemma 5.1]. Hence we may assume that $\mathsf{supp}(g) \ge 2$. First we note that

$$\Sigma_3 := \sum_{\chi\in\mathrm{Irr}(G),\ 4\le\mathfrak{l}(\chi)<n_0}\frac{|\chi(s)\chi(t)\bar\chi(g)|}{\chi(1)} \le \sum_{j=4}^{n_0}\frac{1.93}{2^{j-1/49}} < \sum_{j=4}^{\infty}\frac{1.93\cdot 2^{1/49}}{2^j} < 0.25.$$

Next we bound $|\chi(g)/\chi(1)|$ for $1 \le j \le 3$. If $j = 1$, then $\chi(1) \ge (2^n-2)/3$ and $|\chi(g)| \le (2^{n-2}+4)/3$ by [TZ1, Lemma 4.1], hence $|\chi(g)|/\chi(1) < 0.26$ when N is large enough. For $j = 2$, (8.1) implies $|\chi(g)|/\chi(1) < (1.1)q^{-4} < 0.07$ when N is large enough. When $j = 3$, $\chi(1) > q^{3n-8}$ by (8.2), and so $|\chi(g)/\chi(1)| < 1.93\chi(1)^{-1/n} < (1.1)(1.93)q^{-3} < 0.27$ (when N is large enough) by [GLT1, Theorem 1.6(ii)] and Proposition 8.8(ii). It follows that

$$\sum_{1_G\ne\chi\in\mathrm{Irr}(G)}\frac{|\chi(s)\chi(t)\bar\chi(g)|}{\chi(1)} \le \Sigma_1+\Sigma_3+0.26+0.07+0.27 = 0.86,$$

again showing $g \in s^G \cdot t^G$. □

Now we can answer an open question raised in [GLOST] and prove the following result, which strengthens Theorems 4 and 5 of [GLOST]. As shown in [GLOST, Example 8.10], the statement does not hold for simple groups of Lie-type of bounded rank.

Theorem 8.10. *There exists a function $f : \mathbb{Z}_{\ge1} \to \mathbb{Z}_{\ge1}$ such that the following statement holds. For any integer $k \ge 1$ and any integer $N \ge 1$ with at most k distinct prime divisors, the power word map $(x, y) \mapsto x^N y^N$ is surjective on any alternating group A_n with $n \ge f(k)$ and any simple classical group of rank $r \ge f(k)$.*

Proof. Fix any $k \ge 1$. By [GLOST, Theorem 4], it suffices to prove the theorem for any finite classical group $S = \mathrm{PSL}_n^\varepsilon(q)$ with n sufficiently large. Recall [Zs] that if $m \ge 7$, then $(\varepsilon q)^m - 1$ admits a primitive prime divisor ℓ_m, that is a prime divisor which is coprime to $\prod_{i=1}^{m-1}((\varepsilon q)^i - 1)$. Choosing $n \ge 12k + 24$, we can find $k + 1$ integers a_i, $1 \le i \le k + 1$, such that

$$n/3 \le a_1 < a_2 < \ldots < a_{k+1} < n/2,\ a_{i+1} - a_i \ge 2 \text{ for all } i. \tag{8.3}$$

Then, for each i, we can find a regular semisimple element $s_i \in G := \mathrm{SL}_n^\varepsilon(q)$ of order $\ell_{a_i}\ell_{n-a_i}$ belonging to a maximal torus of type $T_{a_i,n-a_i}$ and a regular semisimple element $t_i \in G$ of order $\ell_{a_i+1}\ell_{n-a_i-1}$ belonging to a maximal torus of type $T_{a_i+1,n-a_i-1}$. Condition (8.3) ensures that $\gcd(|s_i|\cdot|t_i|, |s_j|\cdot|t_j|) = 1$ whenever $i \ne j$. Since N has most k distinct prime factors, it follows that N is coprime to $|s_{i_0}|\cdot|t_{i_0}|$ for some i_0 and so both s_{i_0} and t_{i_0} are N^{th} powers in G.

Now assume n is sufficiently large and consider any $g \in G \setminus \mathbf{Z}(G)$. If $q \ge 3$, or if $q = 2$ but g is not a scalar multiple of a transvection, then g belongs to $s_{i_0}^G \cdot t_{i_0}^G$ by Proposition 8.9, and so it is a product of two N^{th} powers. Suppose now that $q = 2$ and g is a transvection. Since $n \ge 12k + 24$,

we can find $k+1$ odd integers $9 \le n_1 < n_2 < \ldots < n_{k+1} < n$. By [GLOST, Theorem 2.1], for each i, g embedded in $\mathrm{SL}^{\varepsilon}_{n_i}(q)$ is a product $u_i v_i$ where $|u_i| = \ell_{n_i}$ and $|v_i| = \ell_{n_i - 1}$. Arguing as above, we see that N is coprime to $|u_{j_0}| \cdot |v_{j_0}|$ for some j_0, hence $g = u_{j_0} v_{j_0}$ is again a product of two N^{th} powers. □

8.4. **Fibers of product morphisms on semisimple algebraic groups.** Our character estimates have consequences for the geometry of semisimple algebraic groups in all characteristics, of which the following result is a sample.

Theorem 8.11. *There exists a constant C with the following property. Let K be an algebraically closed field and $\underline{G}$ a simple algebraic group over K. Let $\underline{S}_1, \ldots, \underline{S}_k$ be conjugacy classes in $\underline{G}$, and $\underline{X} := \underline{S}_1 \times \cdots \times \underline{S}_k$. If $\dim \underline{X} \ge C \dim \underline{G}$, then the multiplication morphism $\mu_K \colon \underline{X} \to \underline{G}$ is flat.*

Proof. As conjugacy classes are non-singular varieties, $\underline{X}$ and $\underline{G}$ are both non-singular, so by miracle flatness, the theorem is equivalent to the statement that for all $g \in \underline{G}(K)$, $\mu_K^{-1}(g)$ has dimension $\dim \underline{X} - \dim \underline{G}$.

If $\tilde{\underline{G}}$ denotes the simply connected cover of $\underline{G}$, $\tilde{\underline{S}}_i := \underline{S}_i \times_{\underline{G}} \tilde{\underline{G}}$, $\tilde{\underline{X}} := \prod_i \underline{S}_i$, and $\tilde{\mu}_K \colon \tilde{\underline{X}} \to \tilde{\underline{G}}$ denotes the product morphism, then the natural morphisms $\pi_G \colon \tilde{\underline{G}} \to \underline{G}$ and $\pi_X \colon \tilde{\underline{X}} \to \underline{X}$ are finite and surjective. If $g \in \underline{G}(K)$, then

$$\mu^{-1}(g) = \bigcup_{\tilde{g} \in \pi_G^{-1}(g)} \pi_X(\tilde{\mu}^{-1}(\tilde{g})),$$

and

$$\dim \pi_X(\tilde{\mu}_K^{-1}(\tilde{g})) = \dim \tilde{\mu}^{-1}(\tilde{g}).$$

We may therefore reduce to the case that $\underline{G}$ is simply connected.

Next, we assume that K is algebraic over $\mathbb{F}_p$ for some prime p. If $\underline{G}_0$ denotes the split, simply connected simple algebraic group over $\mathbb{F}_p$ with the same Dynkin diagram as $\underline{G}$, then $\underline{G}_0 \times_{\mathbb{F}_p} K$ is isomorphic to $\underline{G}$. We fix an isomorphism. Via this isomorphism, all varieties $\underline{S}_i$ are defined over some common finite extension $\mathbb{F}_q$ of $\mathbb{F}_p$.

Fixing q, we define $\tilde{G} := \underline{G}_0(\mathbb{F}_q)$, $\tilde{S}_i := \underline{S}_i(\mathbb{F}_q)$, $\tilde{X} := \tilde{S}_1 \times \cdots \times \tilde{S}_k$, and the multiplication map $\tilde{\mu}_q \colon \tilde{X} \to \tilde{G}$. It suffices to prove that for $\tilde{g} \in \tilde{G}$, $\tilde{\mu}_q^{-1}(\tilde{g})$ has $O(q^{\dim \underline{X} - \dim \underline{G}})$ elements, where the implicit constant depends on $\underline{G}$ and the $\underline{S}_i$ but not on q.

Let Z denote the center of $\tilde{G}$, and $G := \tilde{G}/Z$. Let S_i, X, and μ denote the counterparts for G to $\tilde{S}_i$, $\tilde{X}$, and $\tilde{\mu}$. Then

$$\mu^{-1}(g) = \sum_{\{\tilde{g} \in \tilde{G} \mid \pi_G(\tilde{g}) = g\}} \pi_X(\tilde{\mu}_q^{-1}(\tilde{g})),$$

so it suffices to prove that $\mu^{-1}(g) = O(q^{\dim \underline{X} - \dim \underline{G}})$.

Now,

$$\pi^{-1}(g) = \{(s_1, \ldots, s_k) \in X \mid s_1 \cdots s_k = 1\}.$$

Writing $S_i = x_i^G$, we have

$$|\pi^{-1}(g)| = \frac{|X|}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(x_1) \cdots \chi(x_k) \bar{\chi}(g)}{\chi(1)^{k-1}}.$$

We claim that each $\tilde{S}_i$ is a union of $O(1)$ conjugacy classes in G, where the implicit constant does not depend on $\underline{S}_i$ or q. This follows from the analogous claim for $\tilde{G}$-conjugacy classes in $\tilde{S}_i$. To prove this, consider the subvariety $\underline{W}$ of $\underline{G}_0 \times \underline{G}_0$ consisting of commuting pairs $(\tilde{g}_1, \tilde{g}_2)$. The fiber $\underline{W}_{\tilde{g}_1}$ of this variety over $\tilde{g}_1 \in \underline{G}_0(\mathbb{F}_q)$ is the centralizer of $\tilde{g}_1$ in $\underline{G}_0$. By [EGA IV, Corollaire 9.7.9],

the number of geometric components of the fiber is a constructible function on $\underline{G}_0$, so it is bounded above. The number of points of the algebraic group $\underline{W}_{\tilde{g}_1}$ over $\mathbb{F}_q$ is at most $C(q+1)^{\dim \underline{W}_{\tilde{g}_1}}$, where C is the number of components. Likewise, the number of points of $\underline{G}_0$ over $\mathbb{F}_q$ is at least $(q-1)^{\dim \underline{G}_0}$. Thus, the size of the conjugacy class of $\tilde{g}_1$ in $\underline{G}_0(\mathbb{F}_q)$ is bounded below by a positive constant multiple of $q^{\dim \underline{G}_0 - \dim \underline{W}_{\tilde{g}_1}}$. By the Lang-Weil estimate, the number of $\mathbb{F}_q$-points on the conjugacy class of $\tilde{g}_1$ in the algebraic group $\underline{G}_0$ is at least $(1-o(1))q^{\dim \underline{G}_0 - \dim \underline{W}_{\tilde{g}_1}}$. This gives an upper bound on the number of $\underline{G}(\mathbb{F}_q)$-conjugacy classes in S_i and therefore an upper bound on the number of G-conjugacy classes in S_i.

We may therefore pick representatives x_i of each S_i and prove that the number of k-tuples $(s_1, \dots, s_k)$ such that $s_1 \cdots s_k = 1$ and each s_i is conjugate in G to x_i is $O(|X|/|G|)$. By Theorem A,

$$\frac{|\chi(x_1)\cdots\chi(x_k)\bar{\chi}(g)|}{\chi(1)^{k-1}} \le \chi(1)^{2-c\frac{\sum_{i=1}^k \log|S_i|}{\log|G|}}.$$

As $\log|S_i| = (\dim \underline{S}_i)\log q + O(1)$, we have

$$\sum_{i=1}^k \log|S_i| = (\dim \underline{X})\log q + O(1),$$

so

$$|\pi^{-1}(g)| = \frac{|X|}{|G|}\Big(1 + O\Big(\sum_{\chi\neq 1}\chi(1)^{2-c\frac{\dim \underline{X}}{\dim \underline{G}}+o(1)}\Big)\Big).$$

By [LiSh3, Theorem 1.1], if $\dim \underline{X} > \frac{2+(2/h)}{c}\dim \underline{G}$, then

$$|\pi^{-1}(g)| = \frac{|X|}{|G|}(1+o(1)) = O(q^{\dim \underline{X} - \dim \underline{G}}),$$

where the $o(1)$ term goes to 0 independently of the choices of conjugacy classes as $q \to \infty$. This implies the theorem for $K \cong \bar{\mathbb{F}}_q$.

For the general case, let $\mathcal{G}$ denote the Chevalley scheme over $\mathbb{Z}$ with the same Dynkin diagram as $\underline{G}$. Fix an isomorphism between $\mathcal{G}_K$ and $\underline{G}$. Choose representatives $x_1, \dots, x_k$ for $S_1, \dots, S_k$ in $\underline{G}$. Via the isomorphism, we can identify all the x_i as points $\mathcal{X}_i$ on $\underline{G}(A)$, where A is a finitely generated $\mathbb{Z}$-algebra. By [GLT2, Lemma 8.2], there exists a dense open affine subscheme $\operatorname{Spec} B$ of $\operatorname{Spec} A$ and for each i a locally closed B-subscheme $\mathcal{S}_i$ of $\mathcal{G}_B$ so that for every field F and every F-point of $\operatorname{Spec} B$, $\mathcal{S}_{iF}$ is the conjugacy class of the specialization $\mathcal{X}_{iF}$.

Now consider the multiplication morphism $\mu_B \colon \mathcal{S}_1 \times \cdots \times \mathcal{S}_k \to \mathcal{G}_B$. By [EGA IV, Proposition 9.5.5], the set of points of $\mathcal{G}_B$ over which every fiber of μ_B has dimension $\dim \underline{X} - \dim \underline{G}$ is constructible and contains every point of $\mathcal{G}_B$ with finite residue field. As $\mathcal{G}_B$ is of finite type over B, it is of finite type over $\mathbb{Z}$ and therefore Jacobson [EGA IV, Corollaire 10.4.6]; moreover, the closed points of $\mathcal{G}_B$ are exactly the points with finite residue field [EGA IV, Lemme 10.4.11.1]. In a Jacobson scheme, by definition, the closed points are very dense, so by [EGA IV, Proposition 10.1.2], the only constructible subset of $\mathcal{G}_B$ containing all closed points is the whole set. Thus, the fiber dimension condition holds for all fibers of μ_B and therefore for all fibers of μ_K. □

We remark that, replacing the constant C above by $2C+1$, we can prove that μ_K is faithfully flat. Indeed, it suffices to prove that μ_K is surjective. If $\dim \underline{X} > (2C+1)\dim \underline{G}$, then there exists j such that the multiplication maps $\mu_K \colon \underline{X}_1 \times \cdots \underline{X}_j \to \underline{G}$ and $\nu_K \colon \underline{X}_{j+1} \times \cdots \times \underline{X}_k \to \underline{G}$ are flat and therefore dominant. By Chevalley's theorem, the images of μ_K and ν_K are dense constructible sets. As the intersection of two dense open subsets is non-empty, the same is true for dense constructible

subsets, and it follows that the product of two such subsets on an algebraic group covers the whole group.

A related result, in the case $\underline{S}_1 = \ldots = \underline{S}_k$ and with the explicit constant $C = 120$, was recently proved in [LiSi, Theorem 1].

References

[AH] Z. Arad and M. Herzog, *Products of conjugacy classes in groups*, Lecture Notes in Mathematics, **1112**, Springer-Verlag, Berlin, 1985.

[BLST] R. Bezrukavnikov, M. Liebeck, A. Shalev, and Pham Huu Tiep, Character bounds for finite groups of Lie type. *Acta Math.* **221** (2018), no. 1, 1–57.

[Bu] W. Burnside, *Theory of groups of finite order*, 2nd ed., Cambridge Univ. Press, Cambridge, 1911.

[DS] P. Diaconis and M. Shahshahani, Generating a random permutation with random transpositions. *Z. Wahrsch. Verw. Gebiete* **57** (1981), no. 2, 159–179.

[DM] F. Digne and J. Michel, *Representations of finite groups of Lie type*, London Math. Soc. Student Texts **21**, Cambridge University Press, 1991.

[Du] R. Durrett, *Probability: theory and examples*. Fourth edition. Cambridge Series in Statistical and Probabilistic Mathematics, **31**. Cambridge University Press, Cambridge, 2010.

[EG] E.W. Ellers and N. Gordeev, On the conjectures of J. Thompson and O. Ore. *Trans. Amer. Math. Soc.* **350** (1998), no. 9, 3657–3671.

[EGA IV] A. Grothendieck, Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. III. Inst. Hautes Études Sci. Publ. Math. No. 28 (1966), 255 pp.

[FL] S. Fomin and N. Lulov, On the number of rim hook tableaux. *J. Math. Sci. (New York)* **87** (1997), no. 6, 4118–4123.

[Fu] J. Fulman, Convergence rates of random walk on irreducible representations of finite groups. *J. Theor. Probab.* **21** (2008), 193–211.

[FG] J. Fulman and R.M. Guralnick, Bounds on the number and sizes of conjugacy classes in finite Chevalley groups with applications to derangements. *Trans. Amer. Math. Soc.* **364** (2012), no. 6, 3023–3070.

[GLL] S. Garion, M. Larsen, and A. Lubotzky, Beauville surfaces and finite simple groups. *J. Reine Angew. Math.* **666** (2012), 225–243.

[Gi] N. P. Gill, blog post, `https://nickpgill.github.io/a-rodgers-saxl-conjecture-for-characters`.

[Gl] D. Gluck, Sharper character value estimates for groups of Lie type. *J. Algebra* **174** (1995), no. 1, 229–266.

[Gr] J.A. Green, The characters of the finite general linear groups. *Trans. Amer. Math. Soc.* **80** (1955), 402–447.

[GLT1] R.M. Guralnick, M. Larsen, and Pham Huu Tiep, Character levels and character bounds. *Forum Math. Pi* **8** (2020), e2, 81 pp.

[GLT2] R.M. Guralnick, M. Larsen, and Pham Huu Tiep, Character levels and character bounds for finite classical groups, *Invent. Math.* **235** (2023), 151–210.

[GLOST] R.M. Guralnick, M.W. Liebeck, E.A. O'Brien, A. Shalev, and Pham Huu Tiep, Surjective word maps and Burnside's $p^a q^b$ theorem. *Invent. Math.* **213** (2018), 589–695.

[GT] R.M. Guralnick and Pham Huu Tiep, Lifting in Frattini covers and a characterization of finite solvable groups. *J. Reine Angew. Math.* **708** (2015), 49–72.

[Hi] M. Hildebrand, Generating random elements in $SL_n(\mathbb{F}_q)$ by random transvections. *J. Alg. Comb.* **1** (1992), 133–150.

[KlL] P.B. Kleidman and M. W. Liebeck, *The subgroup structure of the finite classical groups*, London Math. Soc. Lecture Note Ser. no. **129**, Cambridge University Press, 1990.

[LaSe] V. Landazuri and G. M. Seitz, On the minimal degrees of projective representations of the finite Chevalley groups. *J. Algebra* **32** (1974), 418–443.

[LMT] M. Larsen, G. Malle, and Pham Huu Tiep, The largest irreducible representations of simple groups. *Proc. London Math. Soc.* **106** (2013), 65–96.

[LaSh1] M. Larsen and A. Shalev, Characters of symmetric groups: sharp bounds and applications. *Invent. Math.* **174** (2008), no. 3, 645–687.

[LaSh2] M. Larsen and A. Shalev, Word maps and Waring type problems. *J. Amer. Math. Soc.* **22** (2009), no. 2, 437–466.

[LaSh3] M. Larsen and A. Shalev, On the distribution of values of certain word maps. *Trans. Amer. Math. Soc.* **368** (2016), no. 3, 1647–1661.

[LaST1] M. Larsen, A. Shalev and Pham Huu Tiep, The Waring problem for finite simple groups. *Ann. of Math.* **174** (2011), no. 3, 1885–1950.

[LaST2] M. Larsen, A. Shalev and Pham Huu Tiep, Probabilistic Waring problems for finite simple groups. *Ann. of Math.* **190** (2019), no. 2, 561–608.

[LTT] M. Larsen, J. Taylor, and Pham Huu Tiep, Character bounds for regular semisimple elements and asymptotic results on Thompson's conjecture. *Math. Z.* **303** (2023), no. 2, Paper No. 47, 45 pp.

[LM] C. Lassueur and G. Malle, Simple endotrivial modules for linear, unitary and exceptional groups. *Math. Z.* **280** (2015), no. 3–4, 1047–1074.

[Li] M.W. Liebeck, Character ratios for finite groups of Lie type, and applications, *Finite simple groups: thirty years of the Atlas and beyond*, 193–208, Contemp. Math., **694**, Amer. Math. Soc., Providence, RI, 2017.

[LOST1] M.W. Liebeck, E.A. O'Brien, A. Shalev, and Pham Huu Tiep, The Ore conjecture. *J. Eur. Math. Soc. (JEMS)* **12** (2010), no. 4, 939–1008.

[LOST2] M.W. Liebeck, E.A. O'Brien, A. Shalev, and Pham Huu Tiep, Commutators in finite quasisimple groups. *Bull. Lond. Math. Soc.* **43** (2011), no. 6, 1079–1092.

[LSS] M.W. Liebeck, G. Schul, and A. Shalev, Rapid growth in finite simple groups. *Trans. Amer. Math. Soc.* **369** (2017), no. 12, 8765–8779.

[LiSe] M.W. Liebeck and G.M. Seitz, *Unipotent and nilpotent elements in simple algebraic groups and Lie algebras*, Math. Surveys and Monographs, Amer. Math. Soc., vol. **180** (2012).

[LiSh1] M.W. Liebeck and A. Shalev, Simple groups, permutation groups, and probability. *J. Amer. Math. Soc.* **12** (1999), 497–520.

[LiSh2] M.W. Liebeck and A. Shalev, Diameters of simple groups: sharp bounds and applications. *Ann. of Math.* **154** (2001), 383–406.

[LiSh3] M.W. Liebeck and A. Shalev, Character degrees and random walks in finite groups of Lie type. *Proc. London Math. Soc.* **90** (2005), 61–86.

[LiSh4] M.W. Liebeck and A. Shalev, Fuchsian groups, finite simple groups and representation varieties. *Invent. Math.* **159** (2005), no. 2, 317–367.

[LiST1] M.W. Liebeck, A. Shalev, and Pham Huu Tiep, On the diameters of McKay graphs for finite simple groups. *Israel J. Math.* **241** (2021), no. 1, 449–464.

[LiST2] M.W. Liebeck, A. Shalev, and Pham Huu Tiep, McKay graphs for alternating groups and classical groups. *Trans. Amer. Math. Soc.* **374** (2021), no. 8, 5651–5676.

[LiSi] M.W. Liebeck and I.I. Simion, Covering numbers for simple algebraic groups. *Vietnam J. Math.* **51** (2023), no. 3, 605–616.

[LiT] M.W. Liebeck and Pham Huu Tiep, Character ratios for exceptional groups of Lie type. *Int. Math. Res. Not. IMRN* (2023), no. 14, 12477–12511.

[LifM] N. Lifshitz and A. Marmor, Bounds for characters of the symmetric group: A hypercontractive approach, arXiv:2308.08694.

[Lu] A. Lubotzky, Cayley graphs: eigenvalues, expanders and random walks, *Surveys in combinatorics*, 1995 (Stirling), 155–189, London Math. Soc. Lecture Note Ser. **218**, Cambridge Univ. Press, Cambridge, 1995.

[MS] T.W. Müller and J-C. Schlage-Puchta, Character theory of symmetric groups, subgroup growth of Fuchsian groups, and random walks. *Adv. Math.* **213** (2007), no. 2, 919–982.

[RŚ] A. Rattan and P. Śniady, Upper bound on the characters of the symmetric groups for balanced Young diagrams and a generalized Frobenius formula. *Adv. Math.* **218** (2008), 673–695.

[Ro] Y. Roichman, Upper bound on the characters of the symmetric groups. *Invent. Math.* **125** (1996), 451–485.

[Sh] A. Shalev, Conjugacy classes, growth and complexity, *Finite simple groups: thirty years of the Atlas and beyond*, 209–221, Contemp. Math. **694**, Amer. Math. Soc., Providence, RI, 2017.

[St] R. Steinberg, *Endomorphisms of linear algebraic groups*. Mem. Amer. Math. Soc., No. **80** American Mathematical Society, Providence, R.I., 1968.

[TT] J. Taylor and Pham Huu Tiep, Lusztig induction, unipotent supports, and character bounds. *Trans. Amer. Math. Soc.* **373** (2020), no. 12, 8637–8676.

[TZ1] Pham Huu Tiep and A.E. Zalesskii, Some characterizations of the Weil representations of the symplectic and unitary groups. *J. Algebra* **192** (1997), 130–165.

[TZ2] Pham Huu Tiep and A.E. Zalesskii, Real conjugacy classes in algebraic groups and finite groups of Lie type. *J. Group Theory* **8** (2005), 291–315.

[Zs] K. Zsigmondy, Zur Theorie der Potenzreste. *Monatsh. Math. Phys.* **3** (1892), 265–284.

Email address: mjlarsen@indiana.edu

Department of Mathematics, Indiana University, Bloomington, IN 47405, U.S.A.

Email address: pht19@math.rutgers.edu

Department of Mathematics, Rutgers University, Piscataway, NJ 08854-8019, U.S.A.