SURJECTIVE WORD MAPS AND BURNSIDE'S p^aq^b THEOREM

ROBERT M. GURALNICK, MARTIN W. LIEBECK, E.A. O'BRIEN, ANER SHALEV, AND PHAM HUU TIEP

Abstract. We prove surjectivity of certain word maps on finite non-abelian simple groups. More precisely, we prove the following: if N is a product of two prime powers, then the word map $(x, y) \mapsto x^N y^N$ is surjective on every finite non-abelian simple group; if N is an odd integer, then the word map $(x, y, z) \mapsto x^N y^N z^N$ is surjective on every finite quasisimple group. These generalize classical theorems of Burnside and Feit-Thompson. We also prove asymptotic results about the surjectivity of the word map $(x, y) \mapsto x^N y^N$ that depend on the number of prime factors of the integer N.

Contents

The first author was partially supported by the NSF grants DMS-1302886 and DMS-1600056, and the Simons Foundation Fellowship 224965. He also thanks the Institute for Advanced Study for its support. The third author was partially supported by the Marsden Fund of New Zealand via grant UOA 1626. The fourth author was supported by ERC Advanced Grant 247034, ISF grant 1117/13 and the Vinik Chair of Mathematics which he holds. The fifth author was partially supported by the NSF grants DMS-1201374 and DMS-1665014, the Simons Foundation Fellowship 305247, the Mathematisches Forschungsinstitut Oberwolfach, and the EPSRC. Parts of the paper were written while the fifth author visited the Department of Mathematics, Harvard University, and Imperial College, London. He thanks Harvard University and Imperial College for generous hospitality and stimulating environments.

The authors thank Frank Lübeck for providing them with the proof of Lemma 7.8.

The authors are grateful to the referee for careful reading and insightful comments on the paper that helped improve both the exposition of the paper and some of its results.

1. Introduction

The theory of word maps on finite non-abelian simple groups – that is, maps of the form $(x_1, \dots, x_k) \mapsto w(x_1, \dots, x_k)$ for some word w in the free group F_k of rank k – has attracted much attention. It was shown in [37, 1.6] that for a given nontrivial word w, every element of every sufficiently large finite simple group G can be expressed as a product of $C(w)$ values of w in G, where $C(w)$ depends only on w; this has been improved to $C(w) = 3$ in [55] and to $C(w) = 2$ in [30, 31, 55]. Improving $C(w)$ to 1 is not possible in general, as is shown by power words x_1^n, which cannot be surjective on any finite group of order non-coprime to n.

Certain word maps are surjective on all groups – namely, those in cosets of the form $x_1^{e_1} \dots x_k^{e_k} F_k'$ where the e_i are integers with $\gcd(e_1, \dots, e_k) = 1$ (see [54, 3.1.1]). The word maps for a small number of other words have been shown to be surjective on all finite simple groups. These include the commutator word $[x_1, x_2]$, whose surjectivity was conjectured by Ore in 1951 and proved in 2010 (see [34] and the references therein).

The main result of this paper is the following.

Theorem 1. *Let p, q be primes, let a, b be non-negative integers, and let $N = p^a q^b$. The word map $(x, y) \mapsto x^N y^N$ is surjective on all finite (non-abelian) simple groups.*

This result generalizes various theorems.

First, it implies the classical Burnside $p^a q^b$-theorem [3], stating that groups of this order are soluble. Indeed, if G is a non-soluble group of order $N = p^a q^b$, then G has a non-abelian composition factor S whose order divides N. Thus S is a (non-abelian) finite simple group satisfying the identity $x^N = 1$, so the word map $x^N y^N$ on S has the trivial image $\{1\}$, contradicting Theorem 1.

Theorem 1 also implies the surjectivity of $x^2 y^2$ and more generally of the words $x^{p^a} y^{p^a}$ (for a prime p), as established in [20, 35]. In [20, Corollary 1.5] it is shown that $x^{6^a} y^{6^a}$ is surjective on all (non-abelian) finite simple groups, again a particular case of Theorem 1.

This theorem is best possible in the sense that it cannot be extended to the case where N is a product of three or more prime powers, since such a number can be the exponent of a simple group. Indeed, the smallest example is that of A_5.

If N_1, N_2 are positive integers such that $N_1 N_2$ is divisible by at most two primes, then $x^{N_1} y^{N_2}$ is surjective on all (non-abelian) finite simple groups, since $(x^{N_2})^{N_1} (y^{N_1})^{N_2} = x^{N_1 N_2} y^{N_1 N_2}$ is surjective by Theorem 1. We also indicate the following consequence (in fact an equivalent reformulation) of Theorem 1:

Corollary 2. *Let π be a set of two primes. If G is a finite non-abelian simple group, then every element of G is a product of two π'-elements.*

To see this, let $\pi := \{p, q\}$. Let $N = p^aq^b$ where p^a is the exponent of a Sylow p-subgroup of G and similarly for q^b. Since every Nth power in G is a π'-element the result follows by Theorem 1.

But some more general questions, including the following, have a negative answer. If N is not divisible by the exponent of a finite simple group G, is x^Ny^N surjective on G? If N is odd, is x^Ny^N surjective on all finite non-abelian simple groups? If $N = p^aq^b$ for some primes p, q, is x^Ny^N surjective on all finite quasisimple groups, or does it hit at least all non-central elements of every quasisimple group? See Remark 8.9.

However, we prove the following result which generalizes the celebrated Feit-Thompson theorem [13]:

Theorem 3. *Let N be an odd positive integer. The word map $(x, y, z) \mapsto x^Ny^Nz^N$ is surjective on all finite quasisimple groups. In fact, every element of every finite quasisimple group is a product of three 2-elements.*

As mentioned above, this result is best possible in the sense that it does not hold for x^Ny^N; it also implies the surjectivity of $x^{N_1}y^{N_2}z^{N_3}$ for odd numbers N_1, N_2, N_3.

A key ingredient of our proof of Theorem 3 is the construction of certain 2-elements in simple groups G of Lie type in odd characteristic that are regular if G is classical (see §7.2) and almost regular if G is exceptional (see §7.4). This construction may be useful in other situations; in particular, it played a key role in the recent proof [33] of [25, Conjecture 6.2]. There are other results of the same flavor as the second statement of Theorem 3, such as [24, Theorem 3.8] where p-elements are considered instead of 2-elements. There is also considerable literature on the case of involutions, see e.g. [46] and the references therein. These imply results like Theorem 3 with longer products $x_1^Nx_2^N \dots x_t^N$, where N is not divisible by the exponent of the simple group in question, see for example [24, Corollary 3.9]. However, the *width* of power maps can grow unbounded on finite simple groups; more precisely, given any integer $t \geq 1$, there exist a finite simple group G and an integer N not divisible by the exponent of G such that the map $(x_1, \dots, x_t) \mapsto x_1^Nx_2^N \dots x_t^N$ is not surjective on G, see e.g. [24, Example 3.2].

Recall that the main results of [30, 31] assert that, given two non-trivial words w_1 and w_2, the product w_1w_2 is surjective on all finite non-abelian simple groups of *sufficiently large* order (depending on w_1 and w_2). In particular, once we fix a positive integer N, the word x^Ny^N is surjective on all sufficiently large simple groups. Theorem 1 (and 3) shows that, for all N of the prescribed form, the word map x^Ny^N (respectively $x^Ny^Nz^N$) is in fact surjective on *all* simple groups (respectively quasisimple groups).

As mentioned above, one cannot generalize Theorem 1 for products of more than two prime powers. However, we prove results of that flavor by imposing asymptotic conditions on the simple groups. If an integer N has the prime factorization $N = \prod_{i=1}^r p_i^{\alpha_i}$ (with $p_1 < \dots < p_r$ and $\alpha_i > 0$), then $\boldsymbol{\omega}(N) := r$ and $\boldsymbol{\Omega}(N) := \sum_{i=1}^r \alpha_i$.

Theorem 4. *Given a positive integer k, there is an explicit positive integer $f(k)$ such that for all positive integers N with $\boldsymbol{\omega}(N) \leq k$, the word map $(x, y) \mapsto x^Ny^N$ is surjective on all finite simple groups S, where S is either an alternating group A_n with $n \geq f(k)$, or a simple Lie-type group of rank $\geq f(k)$ but not of type A or ${}^2A$.*

An explicit upper bound for $f(k)$ in Theorem 4 can be read off from its proof.

For simple classical groups of type A we obtain a somewhat weaker result.

Theorem 5. *Given a positive integer k, there is an explicit positive integer $g(k)$ such that the following statements hold.*

(i) *For all positive integers N with $\boldsymbol{\Omega}(N) \leq k$, the word map $(x, y) \mapsto x^Ny^N$ is surjective on all finite simple groups $S = \mathrm{PSL}_n(q)$, $\mathrm{PSU}_n(q)$ with $n \geq g(k)$.*

(ii) *For all positive integers N with $\boldsymbol{\omega}(N) \leq k$, the word map $(x,y) \mapsto x^N y^N$ is surjective on all finite simple groups $S = \mathrm{PSL}_n(q)$, $\mathrm{PSU}_n(q)$, where $n \geq g(k)$, and q is any prime power such that either $q \geq g(k)$, or $(q-1)|n$ for $S = \mathrm{PSL}_n(q)$, or $(q+1)|n$ for $S = \mathrm{PSU}_n(q)$.*

Example 8.11 shows that there is no analogue of Theorems 1, 4, or 5 for *quasisimple* groups. However, we prove the following asymptotic analogue of Theorem 3 for every N with $\boldsymbol{\omega}(N) \leq k$ (cf. [32, Theorems 2.1, 3.1] for other results in this direction).

Theorem 6. *Given a positive integer k, there is an explicit positive integer $h(k)$ such that for any positive integer N with $\boldsymbol{\omega}(N) \leq k$, the word map $(x,y,z) \mapsto x^N y^N z^N$ is surjective on all finite quasisimple classical groups of rank at least $h(k)$. Furthermore, there is some integer $h'(k)$ such that if $\boldsymbol{\omega}(N) \leq k$ and $n \geq h'(k)$ then the word map $(x,y,z) \mapsto x^N y^N z^N$ is surjective on the double cover $2\mathsf{A}_n$.*

We note that none of Theorems 4–6 holds for finite simple Lie-type groups of bounded rank (over fields of sufficiently large size), cf. Example 8.10. It remains an open question whether Theorem 4 holds for finite simple classical groups of type A of unbounded rank over fields of bounded size.

We use the notation of [26] for finite groups of Lie type. For $\epsilon = \pm$, the group $\mathrm{SL}^\epsilon_n(q)$ is $\mathrm{SL}_n(q)$ when $\epsilon = +$ and $\mathrm{SU}_n(q)$ when $\epsilon = -$, and similarly for $\mathrm{GL}^\epsilon_n(q)$, $\mathrm{PSL}^\epsilon_n(q)$. Also, $E^\epsilon_6(q)$ is $E_6(q)$ if $\epsilon = +$ and ${}^2E_6(q)$ if $\epsilon = -$. We use the convention that if $\epsilon = \pm$ then expressions such as $q - \epsilon$ mean $q - \epsilon 1$.

2. Preliminaries

The following result plays a key role in our proofs.

Theorem 2.1. [24, Theorem 1.1] *Let $\mathcal{G}$ be a simple simply connected algebraic group in characteristic $p > 0$ and let $F : \mathcal{G} \to \mathcal{G}$ be a Frobenius endomorphism such that $G := \mathcal{G}^F$ is quasisimple. There exist (not necessarily distinct) primes r, s_1, s_2, all different from p, and regular semisimple $x, y \in G$ such that $|x| = r$, y is an $\{s_1, s_2\}$-element, and $x^G \cdot y^G \supseteq G \setminus \mathbf{Z}(G)$. In fact $s_1 = s_2$ unless $\mathcal{G}$ is of type B_{2n} or C_{2n}.*

Throughout the paper, by a *finite simple group of Lie type in characteristic p* we mean a simple non-abelian group $S = G/\mathbf{Z}(G)$ for some $G = \mathcal{G}^F$ as in Theorem 2.1. In this notation, let $q = p^f$ denote the common absolute value of the eigenvalues of F acting on the character group of an F-stable maximal torus (so that f is a half-integer if G is a Suzuki-Ree group). For each group G and $S = G/\mathbf{Z}(G)$, we refer to the set $\{r, s_1, s_2\}$ specified in the proof of [24, Theorem 1.1] as $\mathcal{R}(G)$ and $\mathcal{R}(S)$.

Corollary 2.2. *In the notation of Theorem 2.1, let $S = G/\mathbf{Z}(G)$ be simple non-abelian.*

(i) *Theorem 1 holds for S, unless possibly $N = p^a t^b$ with $t \in \{r, s_1, s_2\}$.*
(ii) *Suppose $N = p^a t^b$ for some prime t and $|\mathcal{X}| < |G|/2$, where $\mathcal{X}$ is the set of all elements of G of order divisible by p or by t. The word map $(x,y) \mapsto x^N y^N$ is surjective on G.*

Proof. (i) By [11, Corollary, p. 3661], every non-central element of G is a product of two p-elements. Hence Theorem 1 holds for S if $p \nmid N$. On the other hand, if $N = p^a t^b$ with $t \notin \{r, s_1, s_2\}$, then the elements x and y in Theorem 2.1 are Nth powers, so Theorem 1 again holds for S.

(ii) Let $g \in G$. By assumption, $|G \setminus \mathcal{X}| > |G|/2$, so $g(G \setminus \mathcal{X}) \cap (G \setminus \mathcal{X}) \neq \emptyset$. Hence $g = xy^{-1}$ for some $x, y \in G \setminus \mathcal{X}$. Note that every element of $G \setminus \mathcal{X}$ is an Nth power, whence the claim follows. ∎

Recall that if $a \geq 2$ and $n \geq 3$ are integers and $(a,n) \neq (2,6)$, then $a^n - 1$ has a *primitive prime divisor*, i.e. a prime divisor that does not divide $\prod_{i=1}^{n-1}(a^i-1)$, cf. [67]. In what follows, we fix one such prime divisor for given (a,n) and denote it by $\ell(a,n)$. Next we record the primes r, s_1, s_2 mentioned in Theorem 2.1 in Table 1 (for larger groups G). The third column of Table 1 contains one entry precisely when $s_1 = s_2$.

G	r	s_1, s_2	$(n,q) \neq$
$\mathrm{SL}_n(q)$, $n \geq 4$	$\ell(p, nf)$	$\ell(p,(n-1)f)$	$(6,2),(7,2),(4,4)$
$\mathrm{SU}_n(q)$, $n \geq 5$ odd	$\ell(p,2nf)$	$\ell(p,(n-1)f)$, $n \equiv 1 \bmod 4$ $\ell(p,(n-1)f/2)$, $n \equiv 3 \bmod 4$	$(7,4)$
$\mathrm{SU}_n(q)$, $n \geq 4$ even	$\ell(p,(2n-2)f)$	$\ell(p,nf)$, $n \equiv 0 \bmod 4$ $\ell(p,nf/2)$, $n \equiv 2 \bmod 4$	$(4,2),(6,4)$
$\mathrm{Sp}_{2n}(q)$, $\mathrm{Spin}_{2n+1}(q)$, $n \geq 3$ odd	$\ell(p,2nf)$	$\ell(p,nf)$	$(3,4)$
$\mathrm{Sp}_{2n}(q)$, $\mathrm{Spin}_{2n+1}(q)$, $n \geq 6$ even	$\ell(p,2nf)$	$\ell(p,nf), \ell(p,nf/2)$	$(6,2),(12,2)$
$\mathrm{Sp}_{24}(2)$ $\mathrm{Sp}_{12}(2)$	241 13	13, 7 3, 7	
$\mathrm{Spin}^+_{2n}(q)$, $n \geq 4$	$\ell(p,(2n-2)f)$	$\ell(p,nf)$, n odd $\ell(p,(n-1)f)$, n even	$(4,2)$
$\mathrm{Spin}^-_{2n}(q)$, $n \geq 4$	$\ell(p,2nf)$	$\ell(p,(2n-2)f)$	$(4,2)$
${}^2B_2(q^2)$	$\ell(2,8f)$	$\ell(2,8f)$	$q^2 > 8$
${}^2G_2(q^2)$	$\ell(3,12f)$	$\ell(3,12f)$	$q^2 > 27$
${}^2F_4(q^2)$	$\ell(2,24f)$	$\ell(2,12f)$	$q^2 > 8$
$G_2(q)$	$\ell(p,3f)$	$\ell(p,3f)$	$q \neq 2,4$
${}^3D_4(q)$	$\ell(p,12f)$	$\ell(p,12f)$	
$F_4(q)$	$\ell(p,12f)$	$\ell(p,8f)$	
$E_6(q)_{\mathrm{sc}}$	$\ell(p,9f)$	$\ell(p,8f)$	
${}^2E_6(q)_{\mathrm{sc}}$	$\ell(p,18f)$	$\ell(p,8f)$	
$E_7(q)_{\mathrm{sc}}$	$\ell(p,18f)$	$\ell(p,7f)$	
$E_8(q)$	$\ell(p,24f)$	$\ell(p,20f)$	

TABLE 1. Special primes for simple groups of Lie type

Lemma 2.3. *Let G be a finite group, fix $g_1, g_2 \in G$, and let $g \in G$.*

(i) *Then $g \in g_1^G \cdot g_2^G$ if and only if*

$$\sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g_1)\chi(g_2)\overline{\chi}(g)}{\chi(1)} \neq 0.$$

In particular, $g \in g_1^G \cdot g_2^G$ if

$$\left| \sum_{\chi \in \mathrm{Irr}(G),\ \chi(1)>1} \frac{\chi(g_1)\chi(g_2)\overline{\chi}(g)}{\chi(1)} \right| < \left| \sum_{\chi \in \mathrm{Irr}(G),\ \chi(1)=1} \frac{\chi(g_1)\chi(g_2)\overline{\chi}(g)}{\chi(1)} \right|.$$

(ii) *For $D \in \mathbb{N}$,*

$$\left| \sum_{\chi \in \mathrm{Irr}(G),\ \chi(1) \geq D} \frac{\chi(g_1)\chi(g_2)\overline{\chi}(g)}{\chi(1)} \right| \leq \frac{1}{D} \left(|\mathbf{C}_G(g_1)| \cdot |\mathbf{C}_G(g_2)| \cdot |\mathbf{C}_G(g)| \right)^{1/2}.$$

Proof. The first statement is a well known result of Frobenius. For (ii), note that $|\chi(g)| \leq |\mathbf{C}_G(g)|^{1/2}$ for $\chi \in \mathrm{Irr}(G)$ by the second orthogonality relation for complex characters. By the Cauchy-Schwarz inequality,

$$\sum_{\chi \in \mathrm{Irr}(G)} |\chi(g_1)\chi(g_2)| \leq \left(\sum_{\chi \in \mathrm{Irr}(G)} |\chi(g_1)|^2 \cdot \sum_{\chi \in \mathrm{Irr}(G)} |\chi(g_2)|^2 \right)^{1/2} = \left(|\mathbf{C}_G(g_1)| \cdot |\mathbf{C}_G(g_2)| \right)^{1/2}.$$

■

Lemma 2.4. *Theorem 1 holds for all alternating groups A_n, $5 \leq n \leq 18$, and for all 26 sporadic finite simple groups.*

Proof. For each of these groups G and for every two primes p, q dividing $|G|$, we verify that each $g \in G$ can be written as a product of two $\{p,q\}'$-elements. We do this by applying Lemma 2.3 to the character table of the relevant group. Some of these character tables are available in the Character Table Library of GAP [14]; the remainder were constructed directly using the MAGMA [4] implementation of the algorithm of Unger [65]. ■

Proposition 2.5. *Theorem 1 holds for $S = \mathsf{A}_n$ if $n \geq 19$.*

Proof. Since $n \geq 19$, there are at least 6 consecutive integers in the interval $[\lfloor 3n/4 \rfloor, n]$. In particular, we can find an odd integer m such that $\lfloor 3n/4 \rfloor \leq m < m+4 \leq n$. Suppose now that $N = p^a q^b$. Among m, $m+2$, and $m+4$, at most one integer is divisible by p, and similarly for q. Hence there is some $\ell \in \{m, m+2, m+4\}$ that is coprime to N. According to [2, Corollary 2.1], each $g \in \mathsf{A}_n$ is a product of two ℓ-cycles. Since every ℓ-cycle is an Nth power in S, we are done. ■

Proposition 2.6. *Given a positive integer k, there is some explicit $f(k)$ such that for all $n \geq f(k)$ and for all positive integers N with $\boldsymbol{\omega}(N) \leq k$, the word map $(x,y) \mapsto x^N y^N$ is surjective on $S = \mathsf{A}_n$.*

Proof. Choosing $f(k)$ large enough, we see by an explicit form of the prime number theorem, see e.g. [53], that for every $n \geq f(k)$, the interval $[3n/4, n]$ contains at least $k+1$ distinct primes $p_1, \ldots, p_{k+1}$. Given a positive integer N with at most k distinct primes factors, at least one of the p_i's, call it ℓ, does not divide N, whence all ℓ-cycles are Nth powers. Hence the claim follows from [2, Corollary 2.1]. ■

Lemma 2.7. *If g is a real element of a finite group G, then g is a product of two 2-elements of G.*

Proof. By assumption, $g^{-1} = xgx^{-1}$ for some $x \in G$. Replace x by $x^{|x|_{2'}}$ to obtain a 2-element. Now

$$xgxg = x^2 \cdot x^{-1}gx \cdot g = x^2 \cdot g^{-1} \cdot g = x^2,$$

so xg is a 2-element as well. Since $g = x^{-1} \cdot xg$, the claim follows. ■

In particular, the following is an immediate consequence of Lemma 2.7:

Corollary 2.8. *If G is a finite real group and N is an odd integer, then the word map $(x,y) \mapsto x^N y^N$ is surjective on G.*

Corollary 2.9. *Let q be an odd prime power. Theorem 1 holds for the following simple groups:*

(i) $\mathrm{PSp}_{2n}(q)$ *and* $\Omega_{2n+1}(q)$, *where* $n \geq 3$ *and* $q \equiv 1(\mathrm{mod}4)$;
(ii) $\mathrm{P}\Omega^+_{4n}(q)$, *where* $n \geq 3$ *and* $q \equiv 1(\mathrm{mod}4)$;
(iii) $\mathrm{P}\Omega^-_{4n}(q)$, *where* $n \geq 2$;
(iv) $\mathrm{P}\Omega^+_8(q)$, $\Omega_9(q)$, *and* ${}^3D_4(q)$.

If N is an arbitrary odd integer, then the word map $(x,y) \mapsto x^N y^N$ is surjective on each of these groups. The same conclusion holds for $G = \mathrm{Spin}^-_{4n}(q)$ with $n \geq 2$, and $G = \Omega^+_{4n}(q)$ with $n \geq 2$ and $q \equiv 1 \bmod 4$, and $G = \Omega^+_8(q)$.

Proof. By [64, Theorem 1.2], all of these groups G are real, whence the statement follows from Corollary 2.8 when N is odd. If G is simple and N is even, then the statement follows from Corollary 2.2(i). ∎

Corollary 2.9 implies that Theorem 1 holds for many simple symplectic or orthogonal groups over $\mathbb{F}_q$ when $q \equiv 1(\mathrm{mod}4)$. To handle the groups over $\mathbb{F}_q$ with $q \not\equiv 1(\mathrm{mod}4)$, we use the following result:

Proposition 2.10. *Let S be a non-abelian simple group of Lie type in characteristic p. Suppose $N = p^a t^b$ with $t \in \mathcal{R}(S)$, where $\mathcal{R}(S)$ is defined after Theorem 2.1. The word map $(x,y) \mapsto x^N y^N$ is surjective on G, where $S = G/\mathbf{Z}(G)$ and G is one of the following groups:*

(i) $\mathrm{Sp}_{2n}(q)$, *where* $2|q \geq 8$ *and* $2 \nmid n \geq 3$;
(ii) $\mathrm{Sp}_{2n}(q)$, *where* $2 \nmid q \geq 11$ *and* $2 \nmid n \geq 3$;
(iii) $\Omega_{2n+1}(q)$, *where* $2 \nmid q \geq 7$, $2 \nmid n \geq 3$, *and* $(n,q) \neq (3,7)$;
(iv) $\Omega^\pm_{2n}(q)$, *where* $n \geq 4$, $q \geq 5$, *and* $n \neq 5,7$ *when* $q = 5$.

Proof. By Corollary 2.2(ii), it suffices to show that $|\mathcal{X}| < |G|/2$ for $\mathcal{X} = \mathcal{X}_p \cup \mathcal{X}_t$, where $\mathcal{X}_s$ is the set of all elements of G that have order divisible by s for $s \in \{p,t\}$. We use [19, Theorem 2.3] which states that $|\mathcal{X}_p|/|G| < c(q)$, where

$$c(q) := \begin{cases} 2/(q-1) + 1/(q-1)^2, & G = \mathrm{Sp}_{2n}(q),\ 2|q \\ 3/(q-1) + 1/(q-1)^2, & G = \mathrm{Sp}_{2n}(q),\ 2 \nmid q \\ 2/(q-1) + 2/(q-1)^2, & G = \Omega_{2n+1}(q) \text{ or } \Omega^\pm_{2n}(q). \end{cases}$$

(Note that this result applies to G since $\mathbf{Z}(G)$ is a p'-group.) To estimate $|\mathcal{X}_t|$, observe that every nontrivial t-element x of G is regular semisimple, with $\mathbf{C}_G(x)$ being a conjugate T^g of a fixed maximal torus T of G. Hence if $y \in \mathcal{X}_t$ has the t-part equal to x then $y \in T^g$. It follows that

$$|\mathcal{X}_t|/|G| < |T|/|\mathbf{N}_G(T)|.$$

For cases (i)–(iii), $\mathbf{N}_G(T)/T$ contains a cyclic group of odd order n. Moreover, since the central involution of the Weyl group of G inverts T, cf. [64, Proposition 3.1], $|\mathbf{N}_G(T)/T|$ is even. It follows that $2n$ divides $|\mathbf{N}_G(T)/T|$. If in addition $G \neq \Omega_7(7)$, then

$$\frac{|\mathcal{X}|}{|G|} \leq \frac{|\mathcal{X}_t|}{|G|} + \frac{|\mathcal{X}_p|}{|G|} < \frac{1}{2n} + c(q) < 0.49.$$

In case (iv), we may by Corollary 2.9 assume that $n \geq 5$. Note that T is constructed using two kinds of cyclic maximal tori. The first is

$$T_1 = \mathrm{SO}^+_2(q^m) \cap G \leq \mathrm{SO}^+_{2m}(q)$$

with m odd, where

$$\mathbf{N}_{\Omega^+_{2m}(q)}(T_1)/T_1 \cong C_m.$$

The second is

$$T_2 = \mathrm{SO}^-_2(q^m) \cap G \leq \mathrm{SO}^-_{2m}(q),$$

where

$$\mathbf{N}_{\Omega^-_{2m}(q)}(T_2)/T_2 \hookrightarrow C_m.$$

Furthermore, $m \in \{n-1, n\}$. Hence, if $q \geq 7$, or $q = 5$ and $n \geq 9$, then

$$\frac{|\mathcal{X}|}{|G|} \leq \frac{|\mathcal{X}_t|}{|G|} + \frac{|\mathcal{X}_p|}{|G|} < \frac{1}{n-1} + \frac{1}{q-1} + \frac{2}{(q-1)^2} \leq 1/2,$$

as desired. If $q = 5$ and $n = 6, 8$ then we are done by Corollary 2.9. ∎

Lemma 2.11. *Let G be a finite group and let $g \in G$. If $\mathcal{O}$ is a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-orbit on*

$$\{\chi \in \mathrm{Irr}(G) \mid \chi(g) \neq 0\},$$

then

$$\sum_{\chi \in \mathcal{O}} |\chi(g)|^2 \geq |\mathcal{O}|.$$

In particular,

$$|\{\chi \in \mathrm{Irr}(G) \mid \chi(g) \neq 0\}| \leq |\mathbf{C}_G(g)|.$$

Proof. Note that $\prod_{\chi \in \mathcal{O}} \chi(g)$ is a nonzero algebraic integer fixed by $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, whence it is a nonzero integer. The Cauchy-Schwarz inequality implies that

$$\sum_{\chi \in \mathcal{O}} |\chi(g)|^2 \geq |\mathcal{O}| \cdot |\prod_{\chi \in \mathcal{O}} \chi(g)|^{2/|\mathcal{O}|} \geq |\mathcal{O}|.$$

Let $\mathcal{O}_1, \ldots, \mathcal{O}_t$ denote all of the distinct $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-orbits on $\{\chi \in \mathrm{Irr}(G) \mid \chi(g) \neq 0\}$. The first statement implies that

$$|\mathbf{C}_G(g)| = \sum_{\chi \in \mathrm{Irr}(G),\ \chi(g) \neq 0} |\chi(g)|^2 = \sum_{i=1}^{t} \sum_{\chi \in \mathcal{O}_i} |\chi(g)|^2 \geq \sum_{i=1}^{t} |\mathcal{O}_i|.$$

∎

3. Centralizers of unbreakable elements

3.1. Symplectic and orthogonal groups.

Definition 3.1. Let $\mathrm{Cl}(V) = \mathrm{Sp}(V)$ or $\Omega(V)$ be a finite symplectic or orthogonal group. An element x of $\mathrm{Cl}(V)$ is *breakable* if there is a proper, nonzero, non-degenerate subspace U of V such that $x = x_1 x_2 \in \mathrm{Cl}(U) \times \mathrm{Cl}(U^\perp)$ (with $x_1 \in \mathrm{Cl}(U)$, $x_2 \in \mathrm{Cl}(U^\perp)$), and either

(i) $\mathrm{Cl}(U)$ and $\mathrm{Cl}(U^\perp)$ are both perfect, or

(ii) $\mathrm{Cl}(U^\perp)$ is perfect and $x_1 = \pm 1_U$.

Otherwise, x is *unbreakable*.

Lemma 3.2. *Let $G = \mathrm{Sp}_{2n}(q) = \mathrm{Sp}(V)$ with $n \geq 2$, and assume that $n \geq 4$ if $q = 3$ and that $n \geq 7$ if $q = 2$. If $x \in G$ is unbreakable, then $|\mathbf{C}_G(x)| \leq N$ where N is as in Table 2.*

Proof. Assume first that x is unipotent and q is odd. By [39, 3.12], $V \downarrow x$ is an orthogonal sum of non-degenerate subspaces of the form $W(m)$ and $V(2m)$, where x acts on $W(m)$ as J_m^2, the sum of two Jordan blocks of size m, and on $V(2m)$ as J_{2m}. Note that in general there may be more than one G-conjugacy class of elements with a given Jordan structure. However, if m is even then $W(m) \cong V(m)^2$ as x-modules. For $q > 3$ the symplectic group $\mathrm{Sp}(V(m))$ is perfect for every $m \geq 2$, so the unbreakability of x implies that $V \downarrow x$ is either $W(n)$ with n odd, or $V(2n)$. The corresponding orders of $\mathbf{C}_G(x)$ are given by [39, 7.1],

n	q	N
odd	$q>3, q$ odd	$q^{2n-1}(q^2-1)$
	$q>3, q$ even	$2q^{2n}(q+1)$
	$q=3$	$24\cdot 3^{2n-2}$
even	$q>3, q$ odd	$2q^n$
	$q>3, q$ even	$q^{2n}(q^2-1)$
	$q=3$	$48\cdot 3^{2n+1}$
any	$q=2$	$9\cdot 2^{2n+9}$

TABLE 2. Upper bounds for symplectic groups

and the largest are those in Table 2 for $q>3$ odd. If $q=3$ then $\mathrm{Sp}_2(3)$ is not perfect, so there are more unbreakable possibilities for x:

$V\downarrow x$	$\lvert\mathbf{C}_G(x)\rvert$
$V(2n)$	$2\cdot 3^n$
$V(2n-2)+V(2)$	$4\cdot 3^{n+2}$
$W(n)$ (n odd)	$24\cdot 3^{2n-2}$
$W(n-1)+V(2)$ (n even)	$48\cdot 3^{2n+1}$

Again, the values of $|\mathbf{C}_G(x)|$ are given by [39, 7.1], and the largest are those in Table 2.

Next assume x is unipotent and q is even. Again, $V\downarrow x$ is an orthogonal sum of non-degenerate subspaces of the form $W(m)$ and $V(2m)$ (see [39, Chapter 6]). If $q\geq 4$, the unbreakability of x implies that $V\downarrow x$ is either $W(n)$ or $V(2n)$. The corresponding orders of $\mathbf{C}_G(x)$ are given by [39, 7.3], and the largest are those in Table 2 for $q>2$ even. If $q=2$ then neither $\mathrm{Sp}_2(2)$ nor $\mathrm{Sp}_4(2)$ is perfect, so for $n\geq 7$, the possible $V\downarrow x$ for unbreakable x are of the form $X+Y$, where $X=W(n-k)$ or $V(2n-2k)$ and $Y=W(k)$, $V(2k)$ or $V(2)^k$ for some $k\leq 2$. By [39, 7.3], the largest centralizer order occurs for $W(n-2)+W(2)$, and is at most $9\cdot 2^{2n+9}$, as in Table 2.

Now suppose x is not unipotent and write $x=su$ with semisimple part s and unipotent part u. If $s\in\mathbf{Z}(G)$ then the argument for the unipotent case above applies, so assume $s\notin\mathbf{Z}(G)$. Then

$$\mathbf{C}_G(s)=\mathrm{Sp}_{2r}(q)\times\mathrm{Sp}_{2t}(q)\times\prod\mathrm{GL}_{a_i}^{\epsilon_i}(q^{b_i}),$$

where $2r, 2t$ are the dimensions of the 1- and -1- eigenspaces of s (with $t=0$ for q even), and $r+t+2\sum a_ib_i=n$.

If $q>3$ then the unbreakability of x implies that $r=t=0$ and $a_1b_1=n$; write $a=a_1, b=b_1$. Moreover, in $\mathbf{C}_G(s)=\mathrm{GL}_a^\epsilon(q^b)$, u must be a single Jordan block J_a. So from [39, 7.1], $|\mathbf{C}_G(x)|=|\mathbf{C}_{\mathbf{C}_G(s)}(u)|=(q^b-\epsilon)q^{b(a-1)}\leq q^n+1$, giving the result in this case.

Now consider $q=3$. As x is unbreakable, either $2r$ or $2t$ is equal to $2n-2$, or $a_1b_1\in\{n-1,n\}$. In the former case, $u=u_1u_2\in\mathbf{C}_G(s)=\mathrm{Sp}_{2n-2}(3)\times H$ with $H=\mathrm{Sp}_2(3)$ or $\mathrm{GU}_1(3)$, and unbreakability forces $V_{2n-2}\downarrow u_1$ to be $W(n-1)$ (n even) or $V(2n-2)$. Now [39, 7.1] shows that $|\mathbf{C}_G(x)|$ is less than the bound in Table 2. In the latter case $u=u_1u_2\in\mathbf{C}_G(s)=\mathrm{GL}_a^\epsilon(q^b)\times H$ with either $ab=n$, $H=1$, or $ab=n-1$, $H\in\{\mathrm{Sp}_2(3),\mathrm{GU}_1(3)\}$. If $ab=n$, unbreakability forces u_1 to be J_a or (J_{a-1},J_1); likewise if $ab=n-1$, then $u_1=J_a$. In either case $|\mathbf{C}_G(x)|$ is less than the bound in Table 2.

Finally, suppose $q=2$. Here unbreakability forces either $r\geq n-2$ or $a_1b_1\geq n-2$. If $r\geq n-2$ then $u=u_1u_2\in\mathbf{C}_G(s)=\mathrm{Sp}_{2r}(2)\times H$ with $H\leq\mathrm{Sp}_{2n-2r}(2)$, and $V_{2r}\downarrow u_1$ is $V(2r)$, $W(r)$, or $V(2n-4)+V(2)$ ($r=n-1$) or $W(n-2)+V(2)$ ($r=n-1$). The largest possible value of $|\mathbf{C}_G(x)|$ is less than the value $9\cdot 2^{2n+9}$ in Table 2. If $a_1b_1=n-k\geq n-2$

then, writing $a = a_1, b = b_1$, we see that $u = u_1u_2 \in \mathrm{Sp}_{2k}(2) \times \mathrm{GL}^\epsilon_a(q^b)$. The largest value of $|\mathbf{C}_G(x)|$ occurs when $a = n, b = 1, \epsilon = -1$ and $u = u_2 = (J_{n-2}, J_1^2)$; here $\mathbf{C}_G(x) = \mathbf{C}_{\mathrm{GU}_n(2)}(u)$ again has order less than the bound in Table 2. ∎

Lemma 3.3. *Let $G = \Omega(V) = \Omega^\epsilon_{2n}(q)$ $(n \geq 4)$ or $G = \Omega(V) = \Omega_{2n+1}(q)$ $(n \geq 3$, q odd), and assume further that $\dim V \geq 13$ if $q \leq 3$. If $x \in G$ is unbreakable, then $|\mathbf{C}_G(x)| \leq M$, where M is as in Table 3.*

q	M
$q > 3$	$q^{2n-2}(q+1)^2$
$q = 2$	$3 \cdot 2^{2n+6}$
$q = 3$	$2^6 \cdot 3^{2n+4}\,(\dim V = 2n)$
	$2^4 \cdot 3^{2n+3}\,(\dim V = 2n+1)$

TABLE 3. Upper bounds for orthogonal groups

Proof. First consider the case where $q \geq 4$ is even, so $G = \Omega^\epsilon_{2n}(q)$.

Assume x is unipotent. By [39, Chapter 6], $V \downarrow x$ is an orthogonal sum of non-degenerate subspaces of the form $V(2k)$ (a single Jordan block $J_{2k} \in \mathrm{GO}^\epsilon_{2k}(q) \smallsetminus \Omega^\epsilon_{2k}(q)$) and $W(k)$ (two singular Jordan blocks $J_k^2 \in \Omega^+_{2k}(q)$). Since x is unbreakable, $V \downarrow x$ is $W(n)$ or $V(2n-2k) + V(2k)$ for some k. The order of $\mathbf{C}_G(x)$ is given by [39, 7.1], and the largest value occurs for $W(n)$. It is $q^{2n-3}|\mathrm{Sp}_2(q)|$ for n even, and $q^{2n-2}|\mathrm{SO}^\pm_2(q)|$ for n odd; the former is less than the bound in Table 3 for $q > 3$.

If $x = su$ is non-unipotent with semisimple part s and unipotent part u, then $\mathbf{C}_G(s) = \Omega^\delta_{2k}(q) \times \prod \mathrm{GL}^{\epsilon_i}_{a_i}(q^{b_i})$ with $2k = \dim \mathbf{C}_V(s)$ and $k + \sum a_ib_i = n$. As each $\mathrm{GL}^{\epsilon_i}_{a_i}(q^{b_i}) \leq \Omega_{2a_ib_i}(q)$, the unbreakability of x implies that either $k \geq n-1$ or $a_1b_1 \geq n-1$. In the former case $u = u_1u_2 \in \mathbf{C}_G(s) = \Omega^\delta_{2n-2}(q) \times \mathrm{GL}^\nu_1(q)$, and as in the previous paragraph $|\mathbf{C}_{\Omega^\delta_{2n-2}(q)}(u_1)|$ is at most $q^{2n-5}|\mathrm{Sp}_2(q)|$, which gives the conclusion. In the latter case $u = u_1u_2 \in \mathbf{C}_G(s) = \Omega^\delta_{2k}(q) \times \mathrm{GL}^\nu_a(q^b)$ with $k \leq 1$ and $ab = n-k$, and unbreakability forces $u_2 \in \mathrm{GL}^\nu_a(q^b)$ to be either J_a, or (J_{a-1}, J_1) with $a = n, b = 1$. Then $\mathbf{C}_G(x) = \mathbf{C}_{\mathbf{C}_G(s)}(u)$ has smaller order than the bound in Table 3.

Now consider the case where $q \geq 5$ is odd.

For x unipotent, $V \downarrow x$ is an orthogonal sum of non-degenerate spaces $W(2k)$ (namely, $J_{2k}^2 \in \Omega^+_{4k}(q)$) and $V(2k+1)$ (namely, $J_{2k+1} \in \Omega_{2k+1}(q)$). The unbreakability of x implies that $V \downarrow x = W(n)$ or $V(2n+1)$, giving the conclusion by [39, 7.1].

For $x = su$ non-unipotent, write

$$\mathbf{C}_G(s) = (\Omega_a(q) \times \Omega_b(q) \times \prod \mathrm{GL}^{\epsilon_i}_{a_i}(q^{b_i})) \cap G,$$

where $a = \dim \mathbf{C}_V(s), b = \dim \mathbf{C}_V(-s)$ and $a + b + \sum 2a_ib_i = \dim V$. As $\mathrm{GL}^\epsilon_r(q) \leq \mathrm{SO}_{2r}(q)$ and s has determinant one, b is even. If $a \neq 0$ then $V_a \downarrow u$ is either $W(2k)$ or $V(2k+1)$ and x is breakable. Hence $a = 0$. Moreover, $-1 \in \Omega^+_{4k}(q)$ (see [26, 2.5.13]), so if u_0 is a unipotent element of type $W(2k)$, then $-u_0 \in \Omega^+_{4k}(q)$. Hence by unbreakability, if $b \neq 0$ then either $b = \dim V$ and $V_b \downarrow u = W(n)$, or $V_b \downarrow u$ is a sum of an even number of spaces $V(2k_i+1)$. The former case satisfies the conclusion as above, so assume the latter holds. If there are more than two of the spaces $V(2k_i+1)$, then there exist i, j such that the discriminant of $V(2k_i+1) + V(2k_j+1)$ is a square; if u_1 is the projection of u to this space then $-u_1 = -(J_{2k_1+1}, J_{2k_j+1}) \in \Omega_{2k_i+2k_j+2}(q)$, contradicting unbreakability. Hence either $b = 0$ or $V_b \downarrow u$ is a sum of two spaces $V(2k_i+1)$. Likewise, the projection of u to a factor $\mathrm{GL}^{\epsilon_i}_{a_i}(q^{b_i}))$ has at most two Jordan blocks; here, the only extra point to note is that if $b_i = 1$ and there are three blocks J_1, J_k, J_l with the projection of s to the J_1 block

giving an element of $\Omega_2(q)$, then the projection of s to the other blocks gives elements of $\Omega_{2k}(q), \Omega_{2l}(q)$, and x is breakable.

It follows from all these observations together with [39, 7.1] that the largest value of $|\mathbf{C}_G(x)|$ occurs when either $b = \dim V$ and $V \downarrow u = V(n)^2$ (n odd), or $\mathbf{C}_G(s) = \mathrm{GU}_n(q) \cap G$ and $u = (J_{n/2}^2) \in \mathrm{GU}_n(q)$ (n even). In either case $|\mathbf{C}_G(x)| \leq q^{2n-2}(q+1)^2$, as in Table 3.

Next suppose $q = 3$. Following the proof of the $q = 3$ case of [34, 5.15], for $\dim V = 2n$ the largest possibility for $|\mathbf{C}_G(x)|$ is as in Table 3, and arises when x is unipotent and $V \downarrow x = W(2) + W(n-2)$; note that the larger bound given in [34, 5.15] occurs when $x = -u$ with $V \downarrow u = V(1)^4 + W(n-2)$, but this element x is breakable according to our definition (which is different from the definition in [34]). For $\dim V = 2n+1$ the largest value of $|\mathbf{C}_G(x)|$ is as in [34, 5.15.].

Finally, if $q = 2$ the proof of [34, 5.15] gives the bound in Table 3. ∎

Lemma 3.4. *The following statements hold.*

(i) *Let $q = 2$ or 3, and let $G = Sp(V)$ or $\Omega(V)$ with the assumptions on $\dim V$ as in Lemmas 3.2 and 3.3. Let $\bar{V} = V \otimes_{\mathbb{F}_q} \bar{\mathbb{F}}_q$ and let $\alpha \in \bar{\mathbb{F}}_q$ satisfy either $\alpha^{q-1} = 1$ or $\alpha^{q+1} = 1$. If $x \in G$ is unbreakable, then $\dim \mathrm{Ker}_{\bar{V}}(x - \alpha I) \leq 4$.*

(ii) *Let $q = 5$ and let $G = \Omega(V) = \Omega^{\pm}_{2n}(5)$ with $n \geq 5$. Let $\bar{V} = V \otimes_{\mathbb{F}_q} \bar{\mathbb{F}}_q$ and let $\alpha \in \bar{\mathbb{F}}_q$ satisfy $\alpha^{q-1} = 1$ or $\alpha^{q+1} = 1$. If $x \in G$ is unbreakable, then $\dim \mathrm{Ker}_{\bar{V}}(x - \alpha I) \leq 2$.*

Proof. (i) For $\alpha = \pm 1$ the lemma implies that the number of unipotent Jordan blocks of $\pm x$ is at most 4, which follows from the proofs of Lemmas 3.2 and 3.3. In the other case, α has order $q+1$. A Jordan block of x on $\bar{V}$ with eigenvalue α and dimension k corresponds to a non-degenerate subspace W of V of dimension $2k$ such that x^W lies in $\mathrm{Sp}(W)$ or $\mathrm{SO}(W)$. Hence the unbreakability of x implies that there can be no more than four such blocks.

(ii) If $x = \pm u$ with u unipotent, then the proof of Lemma 3.3 (for the case where $q \geq 5$ is odd) shows that $V \downarrow u$ is $W(n)$ or $V(2k_1+1) + V(2k_2+1)$ for some k_1, k_2, giving the result in this case. Now suppose $x = su$ with semisimple part $s \neq \pm 1$, and let $\mathbf{C}_G(s) = \Omega_a(5) \times \Omega_b(5) \times \prod \mathrm{GL}^{\epsilon_i}_{a_i}(5^{b_i})$ as in Lemma 3.3. That proof shows that $a = 0$, b is even, $V_b \downarrow u$ is the sum of zero or two odd-dimensional spaces $V(2k_i+1)$, and the projection of u to each factor $\mathrm{GL}^{\epsilon_i}_{a_i}(5^{b_i})$ has at most 2 Jordan blocks. The conclusion of (ii) follows. ∎

3.2. **Linear and unitary groups.**

Definition 3.5. (i) An element of the general linear group $\mathrm{GL}_n(2)$ is *breakable* if it lies in a natural subgroup of the form $\mathrm{GL}_a(2) \times \mathrm{GL}_b(2)$ where $a + b = n$, $1 \leq a \leq b$ and $a, b \neq 2$.

(ii) An element of the unitary group $\mathrm{GU}_n(2)$ is *breakable* if it lies in a natural subgroup of the form $\mathrm{GU}_a(2) \times \mathrm{GU}_b(2)$ where $a + b = n$, $1 \leq a \leq b$ and $a, b \neq 2, 3$.

(iii) An element of the general linear or unitary group $\mathrm{GL}^{\epsilon}_n(3)$ is *breakable* if it lies in a natural subgroup of the form $\mathrm{GL}^{\epsilon}_a(3) \times \mathrm{GL}^{\epsilon}_b(3)$ where $a + b = n$, $1 \leq a \leq b$ and $a, b \neq 2$.

(iv) If $q \geq 4$, then an element of $\mathrm{GL}^{\epsilon}_n(q)$ is *breakable* if it lies in a natural subgroup of the form $\mathrm{GL}^{\epsilon}_a(q) \times \mathrm{GL}^{\epsilon}_b(q)$ where $a + b = n$ and $1 \leq a \leq b$.

If $q \geq 4$ and $x \in G = \mathrm{GL}^{\epsilon}_n(q)$ is unbreakable, then

$$|\mathbf{C}_G(x)| \leq \begin{cases} q^n - 1, & \epsilon = +, \\ q^{n-1}(q+1), & \epsilon = -, \end{cases} \tag{3.1}$$

(cf. [34, Lemma 6.7] for the case $\epsilon = -$).

Lemma 3.6. *If $n \geq 7$ and $x \in G = \mathrm{GL}_n(2)$ is unbreakable, then either*

(i) $|\mathbf{C}_G(x)| \leq 2^{n+2}$, *or*

(ii) $|\mathbf{C}_G(x)| = 9 \cdot 2^n$, $2|n$, *and* $x \in \mathrm{GL}_{n/2}(4)$.

Proof. Suppose first that x is unipotent. As it is unbreakable, x has Jordan form J_n, or $J_{n-2} + J_2$. The order of $\mathbf{C}_G(x)$ is given by [39, 7.1], and the maximum possible order is 2^{n+2}, which occurs in the last case.

Now assume that $x = su$ where $s \neq 1$ is the semisimple part and u the unipotent part of x. Then

$$\mathbf{C}_G(s) = \prod_i \mathrm{GL}_{a_i}(2^{b_i}),$$

where $\sum a_i b_i = n$. Moreover, since $x \in \mathbf{C}_G(s)$ is unbreakable, we may assume $a_1 b_1 \in \{n, n-2\}$, and write $a = a_1, b = b_1$. If $ab = n$ then $b \geq 2$. A Jordan block J_c of u as an element of $\mathrm{GL}_a(2^b)$ lies in a natural subgroup $\mathrm{GL}_{cb}(2)$, so the unbreakability of x forces the Jordan form of u in $\mathrm{GL}_a(2^b)$ to be J_a or $J_{a-1} + J_1$ (with $b = 2$ in the latter case). By [39, 7.1], $|\mathbf{C}_G(x)| = |\mathbf{C}_{\mathrm{GL}_a(2^b)}(u)|$ is $2^{b(a-1)}(2^b - 1) < 2^n$ in the former case, and it is $2^{ab} \cdot |\mathrm{GL}_1(2^b)|^2 = 9 \cdot 2^n$ in the latter case, in which case also $2|n$ and $x \in \mathbf{C}_G(s) = \mathrm{GL}_{n/2}(4)$. If $ab = n-2$, then $\mathbf{C}_G(s) \leq \mathrm{GL}_a(2^b) \times \mathrm{GL}_2(2)$ and the Jordan form of u in the first factor must be J_a, whence

$$|\mathbf{C}_G(x)| \leq 2^{b(a-1)} |\mathrm{GL}_1(2^b)||\mathrm{GL}_2(2)| = (2^{n-2} - 2^{n-2-b}) \cdot 6 < 2^{n+2},$$

giving the result in this case. ∎

Lemma 3.7. *If $x \in G = \mathrm{GU}_n(2)$ is unbreakable, then $|\mathbf{C}_G(x)| \leq 2^{n+4} \cdot 3^2$ if $n \geq 10$ and $|\mathbf{C}_G(x)| \leq 2^{48}$ if $n = 9$.*

Proof. (i) Consider the case $n \geq 10$. Suppose first that x is unipotent. As it is unbreakable, x has Jordan form J_n, $J_{n-2} + J_2$ or $J_{n-3} + J_3$. The order of $\mathbf{C}_G(x)$ is given by [39, 7.1], and the maximum possible order is $2^{n+4} \cdot 3^2$, which occurs in the last case.

Suppose that $x = su$ where $s \neq 1$ is the semisimple part and u the unipotent part of x. If $s \in \mathbf{Z}(G)$ then the argument of the previous paragraph applies. If $s \notin \mathbf{Z}(G)$, then

$$\mathbf{C}_G(s) = \prod \mathrm{GU}_{a_i}(2^{b_i}) \times \prod \mathrm{GL}_{c_i}(2^{2d_i}) \leq \prod \mathrm{GU}_{a_i b_i}(2) \times \prod \mathrm{GU}_{2c_i d_i}(2),$$

where $\sum a_i b_i + 2\sum c_i d_i = n$, and all b_i are odd. Moreover, since $x \in \mathbf{C}_G(s)$ is unbreakable, either $a_1 b_1$ or $2c_1 d_1$ lies in the set $\{n, n-2, n-3\}$.

Suppose $a_1 b_1 \in \{n, n-2, n-3\}$, and write $a = a_1, b = b_1$. If $ab = n$ then $b > 1$ since $s \notin \mathbf{Z}(G)$, so $b \geq 3$ (as b is odd). A Jordan block J_c of u as an element of $\mathrm{GU}_a(2^b)$ lies in a natural subgroup $\mathrm{GU}_{cb}(2)$, so the unbreakability of x forces the Jordan form of u in $\mathrm{GU}_a(2^b)$ to be J_a or $J_{a-1} + J_1$ (with $b = 3$ in the latter case). By [39, 7.1], the largest possible value of $|\mathbf{C}_G(x)| = |\mathbf{C}_{\mathrm{GU}_a(2^b)}(u)|$ occurs in the latter case, and is $2^{ab} \cdot |\mathrm{GU}_1(2^b)|^2 = 2^n \cdot 9^2$, proving the result in this case. If $ab = n-2$, then $\mathbf{C}_G(s) = \mathrm{GU}_a(2^b) \times \mathrm{GU}_2(2)$ and the Jordan form of u in the first factor must be J_a, whence

$$|\mathbf{C}_G(x)| \leq 2^{b(a-1)} |\mathrm{GU}_1(2^b)||\mathrm{GU}_2(2)| = (2^{n-2} + 2^{n-2-b}) \cdot 18 < 2^n \cdot 3^2,$$

giving the result in this case. Similarly, if $ab = n-3$ then

$$\begin{aligned} |\mathbf{C}_G(x)| &\leq |\mathbf{C}_{\mathrm{GU}_a(2^b)}(J_a)||\mathrm{GU}_3(2)| = 2^{b(a-1)}(2^b + 1) \cdot 2^3 3^4 \\ &= (2^{n-3} + 2^{n-3-b}) \cdot 2^3 3^4 < 2^{n+4} \cdot 3^2. \end{aligned}$$

Now suppose $2c_1 d_1 \in \{n, n-2, n-3\}$, and write $c = c_1, d = d_1$. If $d = 1$ then the projection of s in $\mathrm{GL}_c(2^{2d})$ is a central element of order 3 which is central in a natural subgroup $\mathrm{GU}_{2c}(2)$, so $\mathbf{C}_G(s)$ has a factor $\mathrm{GU}_{2c}(2)$ rather than $\mathrm{GL}_c(2^2)$. Hence $d > 1$. As

above, the unbreakability of x forces u to have Jordan form J_c as an element of $\mathrm{GL}_c(2^{2d})$. Hence

$$|\mathbf{C}_G(x)| \leq |\mathbf{C}_{\mathrm{GL}_c(2^{2d})}(J_c)| \cdot |\mathrm{GU}_{n-2cd}(2)|,$$

which is a maximum when $cd = n-3$, in which case $|\mathbf{C}_G(x)| \leq 2^{2d(c-1)}(2^{2d}-1) \cdot |\mathrm{GU}_3(2)|$ which is less than $2^n \cdot 3^4$. This completes the proof.

(ii) Suppose now that $n = 9$. Assume first that $x = su$ where $s \in \mathbf{Z}(G)$ and u is unipotent. As x is unbreakable, u has Jordan form J_9, $J_7 + J_2$, $J_6 + J_3$ or J_3^3. The largest centralizer is that of J_3^3, which has order $2^{18}|\mathrm{GU}_3(2)|$, less than 2^{48}.

Now suppose $x = su$ with semisimple part $s \notin \mathbf{Z}(G)$. Then $\mathbf{C}_G(s)$ is as described above. Assuming that $|\mathbf{C}_G(x)| \geq 2^{48}$, the only possibility is that $\mathbf{C}_G(s) = \mathrm{GU}_7(2) \times \mathrm{GU}_2(2)$ (note that $\mathrm{GU}_8(2) \times GU_1(2)$ is not possible as this would imply that x is breakable). If $|\mathbf{C}_G(x)| = |\mathbf{C}_{C_G(s)}(u)| \geq 2^{48}$, then u projects to the identity in $\mathrm{GU}_7(2)$; but then x is breakable, a contradiction. ∎

Lemma 3.8. *If $n \geq 7$ and $x \in G = \mathrm{GL}_n^\epsilon(3)$ is unbreakable, then $|\mathbf{C}_G(x)| \leq 3^{n+2} \cdot 2^4$.*

Proof. For x unipotent the largest centralizer occurs when $x = (J_{n-2}, J_2)$ and has order $3^{n+2} \cdot 2^4$ by [39, 7.1].

Suppose $x = su$ is non-unipotent. If $s \in \mathbf{Z}(G)$ the bound of the previous paragraph applies, so assume $s \notin \mathbf{Z}(G)$. The possibilities for $\mathbf{C}_G(s)$ are:

$$\begin{aligned} \epsilon = +: \ & \mathbf{C}_G(s) = \textstyle\prod \mathrm{GL}_{a_i}(3^{b_i}) \\ \epsilon = -: \ & \mathbf{C}_G(s) = \textstyle\prod \mathrm{GU}_{a_i}(3^{b_i}) \times \prod \mathrm{GL}_{c_i}(3^{2d_i}) \end{aligned}$$

where $\sum a_i b_i = n$ for $\epsilon = +$, and $\sum a_i b_i + 2\sum c_i d_i = n$ and all b_i are odd for $\epsilon = -$. As in the previous proof, the unbreakability assumption implies that $a_1 b_1 \in \{n-2, n\}$ for $\epsilon = +$, and either $a_1 b_1$ or $2c_1 d_1$ is in $\{n-2, n\}$ for $\epsilon = -$. Now we argue as in the previous lemma that none of the possibilities for $u \in \mathbf{C}_G(s)$ give a larger centralizer order than $3^{n+2} \cdot 2^4$. ∎

4. Theorem 1 for linear and unitary groups

4.1. **General inductive argument.** Recall $\mathcal{R}(S)$ from §2, and the notion of unbreakability from Definition 3.5.

Definition 4.1. Given a prime power $q = p^f$, $\epsilon = \pm$, and an integer $N = p^a t^b$ with $t \nmid (q - \epsilon)$ a prime. We say that $G = \mathrm{GL}_n^\epsilon(q)$ satisfies

(i) the condition $\mathsf{P}(N)$ if every $g \in G$ can be written as $g = x^N y^N$ for some $x, y \in G$ with $x^N \in \mathrm{SL}_n^\epsilon(q)$; and
(ii) the condition $\mathsf{P}_u(N)$ if every *unbreakable* $g \in G$ can be written as $g = x^N y^N$ for some $x, y \in G$ with $x^N \in \mathrm{SL}_n^\epsilon(q)$.

First we prove an extension of Theorem 2.1 for $\mathrm{GL}_n^\epsilon(q)$:

Proposition 4.2. *Let $G = \mathrm{GL}_n^\epsilon(q)$ with $n \geq 4$, $q = p^f$, and let $t \nmid p(q - \epsilon)$ be a prime not contained in $\mathcal{R}(\mathrm{SL}_n^\epsilon(q))$. Then $\mathsf{P}(N)$ holds for G and for all $N = p^a t^b$.*

Proof. (i) First we consider the generic case: $\mathcal{R}(\mathrm{SL}_n^\epsilon(q)) = \{r, s_1 = s_2\}$ and r and $s = s_1 = s_2$ are listed in Table 1. In particular, $r = \ell(q, n)$ and $s_1 = \ell(q, n-1)$ when $\epsilon = +$. When $\epsilon = -$, interchanging r and s if necessary, we may assume that r divides $q^n - \epsilon^n$ but not $\prod_{i=1}^{n-1}(q^i - \epsilon^i)$ (so r is a primitive prime divisor of $(\epsilon q)^n - 1$), and similarly, s divides $q^{n-1} - \epsilon^{n-1}$ but not $\prod_{1 \leq i \leq n,\ i \neq n-1}(q^i - \epsilon^i)$.

Since N is coprime to $q - \epsilon$, every central element of G can be written as an Nth power. So it suffices to prove $\mathsf{P}(N)$ for every non-central $g \in G$. Fix a regular semisimple $g_1 \in G$

of order r, in particular $\det(g_1) = 1$, and a regular semisimple $h \in \mathrm{GL}^\epsilon_{n-1}(q)$ of order s. We can choose $d \in \mathrm{GL}^\epsilon_1(q)$ such that $\det(g_2) = \det(g)$ for $g_2 := \mathrm{diag}(h, d)$. Since both g_1 and g_2 have order coprime to N, it suffices to show that $g \in g_1^G \cdot g_2^G$. To this end we apply Lemma 2.3(i).

Consider a character $\chi \in \mathrm{Irr}(G)$ with $\chi(g_1)\chi(g_2) \neq 0$. It follows that $\chi(1)$ is neither of r-defect 0 nor of s-defect 0. On the other hand, the order of the centralizer of every non-central semisimple element of $\mathrm{GL}^\epsilon_n(q)$ is either coprime to r or coprime to s. Hence the Lusztig classification of irreducible characters of G [9] implies that χ belongs to the rational series $\mathcal{E}(G, (z))$ labeled by a central semisimple $z \in G^* \cong G$. It follows that $\chi = \lambda\psi$, where $\lambda(1) = 1$ and ψ is a unipotent character of G. Moreover, as shown in the proof of [47, Theorems 2.1–2.2], ψ is either 1_G or St, the Steinberg character of G. Since $\det(g_1) = 1$ and $\det(g_2) = \det(g)$ by our choice, $\lambda(g_1) = 1$ and $\lambda(g_2)\overline{\lambda}(g) = 1$ for all linear $\lambda \in \mathrm{Irr}(G)$. Finally, since $g \notin \mathbf{Z}(G)$ and $|\mathsf{St}(g_i)| = 1$,

$$\sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g_1)\chi(g_2)\overline{\chi}(g)}{\chi(1)} = (q - \epsilon)\left(1 + \frac{\mathsf{St}(g)}{\mathsf{St}(1)}\right) > 0,$$

so we are done.

(ii) The same arguments apply to the non-generic cases

$$(n, q, \epsilon) = (4, 4, +),\ (6, 4, -), (7, 4, -),$$

if we choose $\mathcal{R}(\mathrm{SL}^\epsilon_n(q))$ to be $\{17, 7\}$, $\{41, 7\}$, or $\{113, 7\}$, respectively. In the remaining cases

$$(n, q, \epsilon) = (6, 2, +),\ (7, 2, +),\ (4, 2, -),$$

the statement follows from [24, Lemma 2.12] if we choose $\mathcal{R}(\mathrm{SL}^\epsilon_n(q))$ to be $\{31\}$, $\{127\}$, or $\{5\}$, respectively (note that $\mathrm{GU}_4(2) \cong C_3 \times \mathrm{SU}_4(2)$). ∎

Our proof of Theorem 1 for linear and unitary groups relies on the following inductive argument:

Proposition 4.3. *Fix a prime power $q = p^f$, an integer $n \geq 4$, and $\epsilon = \pm$. Suppose that there is an integer $n_0 \geq 3$ such that the following statements hold:*

(i) *Let $1 \leq k \leq n_0$ with $k \neq 2$ if $q = 2, 3$, and $k \neq 3$ if $(q, \epsilon) = (2, -)$. Then $\mathsf{P}_u(N)$ holds for $\mathrm{GL}^\epsilon_k(q)$ for every $N = p^a t^b$ with t prime and $t \nmid p(q - \epsilon)$.*

(ii) *For each k with $n_0 < k \leq n$, $\mathsf{P}_u(N)$ holds for $\mathrm{GL}^\epsilon_k(q)$ and for every $N = p^a t^b$ with $t \in \mathcal{R}(\mathrm{SL}^\epsilon_k(q))$.*

If $N = s^a t^b$ for some primes s, t, then the word map $(u, v) \mapsto u^N v^N$ is surjective on $\mathrm{PSL}^\epsilon_n(q)$.

Proof. By Corollary 2.2, we need to consider only the case $N = p^a t^b$ with $t \in \mathcal{R}(\mathrm{SL}^\epsilon_n(q))$; in particular, $t \nmid (q - \epsilon)$. It suffices to show $\mathsf{P}(N)$ holds for $G := \mathrm{GL}^\epsilon_n(q)$ and this choice of N. Indeed, in this case every $g \in \mathrm{SL}^\epsilon_n(q)$ can be written as $x^N y^N$ with $\det(x^N) = \det(y^N) = 1$. Since $\gcd(N, q - \epsilon) = 1$, it follows that $x, y \in \mathrm{SL}^\epsilon_n(q)$.

By (ii), $\mathsf{P}_u(N)$ holds for G. Consider a breakable $g \in G$ and write it as $\mathrm{diag}(g_1, \ldots, g_m)$ lying in the natural subgroup

$$\mathrm{GL}^\epsilon_{k_1}(q) \times \ldots \times \mathrm{GL}^\epsilon_{k_m}(q).$$

Here, $1 \leq k_i < n$, and if $k_i \leq n_0$ then $k = k_i$ fulfills the conditions imposed on k in (i). Furthermore, each g_i is unbreakable. Hence, according to (i), $\mathsf{P}_u(N)$ holds for $\mathrm{GL}^\epsilon_{k_i}(q)$ if $k_i \leq n_0$. If $k_i > n_0$, then by (ii) and Proposition 4.2, $\mathsf{P}_u(N)$ holds for $\mathrm{GL}^\epsilon_{k_i}(q)$ as well. Thus we can write $g_i = x_i^N y_i^N$ with $x_i, y_i \in \mathrm{GL}^\epsilon_{k_i}(q)$ and $\det(x_i^N) = 1$. Letting

$$x := \mathrm{diag}(x_1, \ldots, x_m),\ y := \mathrm{diag}(y_1, \ldots, y_m)$$

we deduce that $g = x^N y^N$ and $\det(x^N) = 1$. Thus $\mathsf{P}(N)$ holds for G, as desired. ∎

4.2. **Induction base.**

Lemma 4.4. *Let $q = p^f \geq 2$, $\epsilon = \pm$, and $N = r^a t^b$ for some primes r, t. Suppose that $S = \mathrm{PSL}_k^\epsilon(q)$ is simple and $k = 2$ or 3. Then the map $(u, v) \mapsto u^N v^N$ is surjective on S.*

Proof. By Corollary 2.2(i), we need to consider only the case $N = p^a t^b$ with $t \in \mathcal{R}(S)$. Let $S = \mathrm{PSL}_3(q)$. By [20, Theorem 7.3], $S \smallsetminus \{1\} \subseteq CC$ where $C = x^S$ or y^S, $|x| = (q^2+q+1)/d$ and $|y| = (q^2-1)/d$, with $d = \gcd(3, q-1)$. In particular, $|x|$ and $|y|$ are coprime. Hence at least one of x, y has order coprime to N, so it is an N-power in S, whence we are done. The case of $\mathrm{PSU}_3(q)$ can be treated similarly using [20, Theorem 7.1]. If $S = \mathrm{PSL}_2(q)$ with $q \geq 7$ odd, then by [20, Theorem 7.1], $S \smallsetminus \{1\} \subseteq CC$ with $C = x^S$ or y^S, $|x| = (q+1)/2$ and $|y| = (q-1)/2$, so we can argue similarly. Finally, assume that $S = \mathrm{SL}_2(q)$ with $q \geq 4$ even. If $t \nmid (q-1)$, then $S \smallsetminus \{1\} \subseteq CC$ with $C = x^S$ and $|x| = q-1$ by [20, Theorem 7.1], so we are done. Assume $t|(q-1)$. Using the character table, we check that $S \smallsetminus \{1\} \subseteq y^S \cdot (y^2)^S$ if $|y| = q+1$, so we are done again. ∎

Lemma 4.5. *Let $q = p^f \geq 4$, $\epsilon = \pm$, and $N = p^a t^b$ for a prime $t \nmid p(q-\epsilon)$. Then $\mathsf{P}_u(N)$ holds for $G = \mathrm{GL}_k^\epsilon(q)$ with $1 \leq k \leq 3$.*

Proof. Clearly the statement holds for $k = 1$. Suppose $k > 1$ and let $g \in G$ be unbreakable. Let $\rho \in \mathbb{F}_q^\times$ and let $\varepsilon \in \mathbb{C}^\times$ have order $q-1 \geq 3$. To establish $\mathsf{P}_u(N)$ for g, we exhibit some N'-elements g_1, g_2 of G such that $g \in g_1^G \cdot g_2^G$ and at least one of g_1, g_2 has determinant 1.

(i) Consider the case $G = \mathrm{GL}_2(q)$. Since g is unbreakable, it belongs to class B_1 or A_2, in the notation of [60]. In the first case, g lies in a torus of order q^2-1, and we define $g_1 = \mathrm{diag}(\rho, \rho^{-1})$, and $g_2 = \mathrm{diag}(1, \rho^i)$ if $\det(g) = \rho^i \neq 1$, or $g_2 = g_1$ if $\det(g) = 1$. Using [60, Table II], it is easy to check that

$$\sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g_1)\chi(g_2)\overline{\chi}(g)}{\chi(1)} = (q-1)\left(1 + \frac{1}{q}\right) > 0.$$

Since g_1 and g_2 are N'-elements, we are done. Suppose now that $g \in A_2$, i.e. $g = zu$ with $z \in \mathbf{Z}(G)$ and u a regular unipotent element. Since z is the Nth power of some central element of G, it suffices to show that $u \in g_1^G \cdot g_2^G$ where we again choose $g_2 = g_1$. Using [60, Table II],

$$\sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g_1)\chi(g_2)\overline{\chi}(g)}{\chi(1)} = (q-1)\left(1 - \frac{1}{2(q+1)} \sum_{0 \leq m \neq n \leq q-2} (\varepsilon^{m-n} + \varepsilon^{n-m})^2\right) = \frac{4(q-1)}{q+1},$$

so we are done again.

The same arguments apply in the case $G = \mathrm{GU}_2(q)$, where we choose $g_2 = g_1^2$ if $g = zu$ and u is a regular unipotent element.

(ii) Consider the case $G = \mathrm{GL}_3(q)$, Since g is unbreakable, g belongs to class C_1 (so g lies in a maximal torus of order q^3-1) or A_3 (i.e. g is a scalar multiple of a regular unipotent element), in the notation of [60]. First suppose that $t \neq \ell(q,3)$. By Lemma 4.7 (below) we can find a regular semisimple $g_1 \in \mathrm{GL}_3(q)$ of order $\ell(q,3)m$ such that $\det(g_1) = \det(g)$ and all prime divisors of m divide $q-1$. Note that g_1 belongs to class C_1. Also, define $g_2 = \mathrm{diag}(1, \rho, \rho^{-1}) \in \mathrm{SL}_3(q)$ belonging to class A_6. Using [60, §3], it is easy to check that

$$\left| \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g_1)\chi(g_2)\overline{\chi}(g)}{\chi(1)} \right| > (q-1)\left(1 - \frac{2}{q(q+1)} - \frac{1}{q^3}\right) > 0.$$

Since g_1 and g_2 are N'-elements, we are done. Suppose now that $t = \ell(q,3)$. We choose h to be a regular semisimple element of order $q+1$ in $\mathrm{SL}_2(q)$ and define $g_1 := \mathrm{diag}(h, \det(g))$ so that it belongs to class B_1. Using g_2 as in (i), we observe that

$$\left| \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g_1)\chi(g_2)\overline{\chi}(g)}{\chi(1)} \right| > (q-1)\left(1 - \frac{1}{q^3} - \frac{3(q-2)}{2(q^2+q+1)}\right) > 0,$$

so we are done again.

The same arguments apply in the case $G = \mathrm{GU}_3(q)$. ∎

4.3. **Weil characters of $\mathrm{GL}_n(q)$ and $\mathrm{GU}_n(q)$.** In this subsection we collect some information about *Weil characters* of $\mathrm{GL}_n(q)$ and $\mathrm{GU}_n(q)$ with $n \geq 3$, cf. [62, §§3, 4], [63, §4], that play an essential role in our analysis.

First we consider the linear case: $G = \mathrm{GL}_n(q) = \mathrm{GL}(V)$ with $V = \mathbb{F}_q^n$. Fix a primitive $(q-1)$th root of unity $\delta \in \mathbb{F}_q^\times$ and a primitive $(q-1)$th root of unity $\tilde{\delta} \in \mathbb{C}^\times$. Also, for $x \in G$ and $\alpha \in \overline{\mathbb{F}}_q^\times$, let $e(x,\alpha)$ denote the dimension of the α-eigenspace of x on $V \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q$. Then $\mathrm{SL}(V) = \mathrm{SL}_n(q)$ has $q-1$ complex Weil representations, which are the nontrivial irreducible constituents of the permutation representation of $\mathrm{SL}(V)$ on $V \smallsetminus \{0\}$. The characters of these representations are τ_i, where $0 \leq i \leq q-2$ and

$$\tau_i(g) = \frac{1}{q-1} \sum_{k=0}^{q-2} \tilde{\delta}^{ik} q^{e(g,\delta^k)} - 2\delta_{0,i}. \tag{4.1}$$

Similarly, $G = \mathrm{GL}_n(q)$ has $(q-1)^2$ complex Weil representations, which are the $q-1$ nontrivial irreducible constituents of the permutation representation of $\mathrm{GL}(V)$ on $V \smallsetminus \{0\}$, tensored with one of the $q-1$ representations of degree 1 of $\mathrm{GL}_n(q)$. If we fix a character $\lambda = \lambda_1$ of order $q-1$ of G, then the characters of these representations are $\tau_{i,j}$, where $0 \leq i,j \leq q-2$ and

$$\tau_{i,j}(g) = \left(\frac{1}{q-1} \sum_{k=0}^{q-2} \tilde{\delta}^{ik} q^{e(g,\delta^k)} - 2\delta_{0,i} \right) \cdot \lambda^j(g). \tag{4.2}$$

Note that $\tau_{i,j}$ restricts to τ_i over $\mathrm{SL}_n(q)$.

Now consider the unitary case: $G = \mathrm{GU}_n(q) = \mathrm{GU}(V)$ with $V = \mathbb{F}_{q^2}^n$. Fix a primitive $(q+1)$th root of unity $\xi \in \mathbb{F}_{q^2}^\times$ and a primitive $(q+1)$th root of unity $\tilde{\xi} \in \mathbb{C}^\times$. Again, for $x \in G$ and $\alpha \in \overline{\mathbb{F}}_q^\times$, let $e(x,\alpha)$ denote the dimension of the α-eigenspace of x on $V \otimes_{\mathbb{F}_{q^2}} \overline{\mathbb{F}}_q$. Then $\mathrm{SU}(V) = \mathrm{SU}_n(q)$ has $q+1$ complex Weil characters ζ_i, where $0 \leq i \leq q$ and

$$\zeta_i(g) = \frac{(-1)^n}{q+1} \sum_{k=0}^{q} \tilde{\xi}^{ik} (-q)^{e(g,\xi^k)}. \tag{4.3}$$

Next, $G = \mathrm{GU}_n(q)$ has $(q+1)^2$ complex Weil characters $\zeta_{i,j}$, where $0 \leq i,j \leq q$ and

$$\zeta_{i,j}(g) = \frac{(-1)^n}{q+1} \sum_{k=0}^{q} \tilde{\xi}^{ik} (-q)^{e(g,\xi^k)} \cdot \lambda^j(g), \tag{4.4}$$

where $\lambda = \lambda_1$ is a fixed linear character of order $q+1$ of G. Note that $\zeta_{i,j}$ restricts to ζ_i over $\mathrm{SU}_n(q)$.

Lemma 4.6. *Let $G = \mathrm{GL}_n^\epsilon(q)$ with $n \geq 3$ and $\epsilon = \pm$. Suppose that $y \in G$ satisfies the condition $\sum_{l=0}^{q-2} e(y,\delta^l) \leq 1$ if $\epsilon = +$ and $\sum_{l=0}^{q} e(y,\xi^l) \leq 1$ if $\epsilon = -$. If $\chi \in \mathrm{Irr}(G)$ is an irreducible Weil character, then $|\chi(y)| \leq 1$.*

Proof. Consider the case $\epsilon = +$. By assumption, $e(y, \delta^l)$ is at most 1 for $0 \le l \le q-2$, and in fact it can equal 1 for at most one value l_0. In particular,

$$-1 = \frac{1}{q-1}(q-1) - 2 \le \tau_{0,0}(y) \le \frac{1}{q-1}(q+q-2) - 2 = 0.$$

Assume now that $i > 0$. If such l_0 exists, then

$$\tau_{i,0}(y) = \frac{1}{q-1}\left(\tilde{\delta}^{il_0}(q-1) + \sum_{l=0}^{q-2}\tilde{\delta}^{il}\right) = \tilde{\delta}^{il_0}.$$

If no such l_0 exists, then

$$\tau_{i,0}(y) = \frac{1}{q-1}\sum_{l=0}^{q-2}\tilde{\delta}^{il} = 0.$$

As $|\tau_{i,j}(y)| = |\tau_{i,0}(y)|$, the claim follows. Similar arguments apply to the case $\epsilon = -$. □

4.4. **Induction step: Generic case.** We need the following simple observation:

Lemma 4.7. *Let $G = \mathrm{GL}_n^\epsilon(q)$ with $n \ge 3$ and let T be a cyclic torus of order $q^n - \epsilon^n$ of G. Suppose there is a prime s that divides $q^n - \epsilon^n$ but not $\prod_{i=1}^{n-1}(q^i - \epsilon^i)$. For every $g \in G$, there exists a regular semisimple $h \in T$ of order sm for some $m \in \mathbb{N}$ such that $\det(h) = \det(g)$ and all prime divisors of m divide $q - \epsilon$.*

Proof. Let $\Delta \cong C_{q-\epsilon}$ denote the image of G under the determinant map det. Note that det maps T onto Δ. The condition on s implies that every $x \in T$ of order divisible by s is regular semisimple and $s \nmid (q-\epsilon)$. It follows that det maps $T_1 \ge \mathbf{O}_s(T)$ into 1 and T_2 onto Δ, where $T = T_1 \times T_2$, $|T_1|$ is coprime to $q-\epsilon$, and all prime divisors of $|T_2|$ divide $q-\epsilon$. Hence we can choose $x \in \mathbf{O}_s(T)$ of order s and $y \in T_2$ such that $\det(y) = \det(g)$ and set $h := xy$. □

Proposition 4.8. *Suppose $G = \mathrm{GL}_n(q)$ with $n \ge 4$, $q = p^f \ge 4$, and $t \in \mathcal{R}(\mathrm{SL}_n(q))$. Then $\mathsf{P}_u(N)$ holds for G and for every $N = p^a t^b$.*

Proof. Consider an unbreakable $g \in G$ and a regular semisimple $g_1 \in \mathrm{SL}_n(q)$ of order $s \in \mathcal{R}(G) \smallsetminus \{t\}$. Denote

$$\mathrm{Irr}(G/[G,G]) = \{\lambda_i = (\lambda_1)^i \mid 0 \le i \le q-2\}.$$

(i) First we consider the case $n \ge 6$. Choose

$$D = \frac{(q^n-1)(q^{n-1}-q^2)}{(q-1)(q^2-1)}.$$

By [62, Theorem 3.1], every irreducible character of $\mathrm{SL}_n(q)$ of degree less than D is either the principal character, or an irreducible Weil character τ_i as given in (4.1). It follows that the characters in $\mathrm{Irr}(G)$ of degree less than D are exactly the $q-1$ linear characters λ_i and $(q-1)^2$ irreducible Weil characters $\tau_{i,j}$, $0 \le i,j \le q-2$ as given in (4.2). Using Lemma 4.7, we can choose a regular semisimple $g_2 \in G$ of order sm where all prime divisors of m divide $q-1$ and $\det(g_2) = \det(g)$. In particular,

$$|\mathbf{C}_G(g_i)| \le q^n - 1,$$

and

$$\sum_{i=0}^{q-2}\lambda_i(g_1)\lambda_i(g_2)\overline{\lambda}_i(g) = q-1. \tag{4.5}$$

By (3.1) and Lemma 2.3,

$$\left|\sum_{\chi\in\mathrm{Irr}(G),\ \chi(1)\geq D}\frac{\chi(g_1)\chi(g_2)\overline{\chi}(g)}{\chi(1)}\right|\leq\frac{(q^n-1)^{3/2}}{D}\leq(q-1)\left(1-\frac{1}{q^2+q+1}\right).\tag{4.6}$$

The choice of g_i and the unbreakability of g ensure that each $y\in\{g,g_1,g_2\}$ satisfies the assumption of Lemma 4.6 and so

$$|\tau_{i,j}(y)|\leq 1.\tag{4.7}$$

It follows that if $n\geq 5$ then

$$\left|\sum_{0\leq i,j\leq q-2}\frac{\tau_{i,j}(g_1)\tau_{i,j}(g_2)\overline{\tau}_{i,j}(g)}{\tau_{i,j}(1)}\right|\leq\frac{(q-1)^3}{q^n-q}<\frac{q-1}{q(q^2+q+1)}.\tag{4.8}$$

Together with (4.6), this implies that

$$\left|\sum_{\chi\in\mathrm{Irr}(G),\ \chi(1)>1}\frac{\chi(g_1)\chi(g_2)\overline{\chi}(g)}{\chi(1)}\right|\leq(q-1)\left(1-\frac{1}{q^2+q+1}+\frac{1}{q(q^2+q+1)}\right)<q-1.$$

Hence $g\in g_1^G\cdot g_2^G$ by (4.5) and Lemma 2.3(i). Since both g_1 and g_2 have order coprime to N, we are done.

(ii) Next we consider the case $n=5$. Setting $s':=\ell(q,3)$ and using Lemma 4.7, we can choose a regular semisimple $h\in\mathrm{GL}_3(q)$ of order $s'm$, where all prime divisors of m divide $q-1$ and $\det(h)=\det(g)$. Also, let $h'\in\mathrm{GL}_2(q)$ be conjugate (over $\overline{\mathbb{F}}_q$) to $\mathrm{diag}(\beta,\beta^{-1})$, where $\beta\in\overline{\mathbb{F}}_q^\times$ has order $q+1$. Setting $g_2=\mathrm{diag}(h,h')$, the orders of g_1 and g_2 are coprime to N, $\det(g_2)=\det(g)$, and $e(g_2,\delta^l)=0$ for $0\leq l\leq q-2$. In particular, (4.7) and (4.8) hold. Next, we choose $D=q^4(q^5-1)/(q-1)$, yielding

$$\left|\sum_{\chi\in\mathrm{Irr}(G),\ \chi(1)\geq D}\frac{\chi(g_1)\chi(g_2)\overline{\chi}(g)}{\chi(1)}\right|\leq\frac{(q^5-1)^{3/2}}{D}\leq\frac{q-1}{q^{3/2}}\leq\frac{q-1}{8}.\tag{4.9}$$

Now, using [41], we check that if $\psi\in\mathrm{Irr}(\mathrm{SL}_5(q))$ has positive s-defect and positive s'-defect and $\psi(1)<D$, then either ψ is the principal character or a Weil character, or $s=\ell(q,4)$ and ψ is the unique character of degree $q^2(q^5-1)/(q-1)$. In either case, ψ extends to G. In fact, in the latter case, an extension φ of ψ to G is the unipotent character labeled by the partition $(3,2)$ (see [7, §13.8]). On the other hand, $\tau_{0,0}$ (as defined in (4.2)) is the unipotent character of G labeled by the partition $(4,1)$. It follows by [22, Lemma 5.1] that

$$\varphi=(1_G+\tau_{0,0}+\varphi)-(1_G+\tau_{0,0})=\rho_2-\rho_1,$$

where ρ_i is the permutation character of the action of G on the set of i-dimensional subspaces of the natural module $\mathbb{F}_q^5$ for $i=1,2$. Therefore,

$$\varphi(g_1)=\rho_2(g_1)-\rho_1(g_1)=0-1=-1,\ \varphi(g_2)=\rho_2(g_2)-\rho_1(g_2)=1-0=1.$$

Also, the extensions of ψ to G are $\varphi\lambda_i$, $0\leq i\leq q-2$, and $|\varphi(g)|\leq(q^5-1)^{1/2}$ by (3.1). Certainly, $\chi(g_1)\chi(g_2)=0$ unless χ has positive s-defect and positive s'-defect. Hence, combining with (4.8), we deduce that

$$\left|\sum_{\chi\in\mathrm{Irr}(G),\ 1<\chi(1)<D}\frac{\chi(g_1)\chi(g_2)\overline{\chi}(g)}{\chi(1)}\right|\leq\frac{q-1}{q(q^2+q+1)}+(q-1)\frac{(q^5-1)^{1/2}}{\psi(1)}\leq\frac{q-1}{32}.$$

Together with (4.9), this implies that

$$\left|\sum_{\chi\in\mathrm{Irr}(G),\ \chi(1)>1}\frac{\chi(g_1)\chi(g_2)\overline{\chi}(g)}{\chi(1)}\right|\le(q-1)\left(\frac{1}{8}+\frac{1}{32}\right)<q-1,$$

so we are done as before.

(iii) Here we consider the case $n=4$. Since g is unbreakable, g belongs to class A_5, C_2, or E_1, in the notation of [60]. In the two latter cases, note that the G-conjugacy class of such an element g is completely determined by $|g|$ and the eigenvalues of g acting on $\overline{\mathbb{F}}_q^4$. On the other hand, G contains a natural subgroup $H\cong\mathrm{GL}_2(q^2)$, and H contains an element h with the same spectrum and order as g. Hence we may assume $g=h\in H$. As $N=p^at^b$ and $t\nmid(q^2-1)$, we can now apply Lemma 4.5 (if h is unbreakable) to get $g=x^Ny^N$ for some $x\in\mathrm{SL}_2(q^2)<\mathrm{SL}_4(q)$ and $y\in H$. Such a decomposition certainly exists if h is breakable in H (i.e. $h\in\mathrm{GL}_1(q^2)\times\mathrm{GL}_1(q^2)$).

It remains therefore to consider the case $g\in A_5$, i.e. $g=zu$, where $z\in\mathbf{Z}(G)$ and u is a regular unipotent element. By [7, Corollary 8.3.6], $|\chi(g)|\le1$ for all $\chi\in\mathrm{Irr}(G)$. Choosing $D=(q-1)(q^3-1)$ and g_2 of order sm as in (i), by the Cauchy-Schwarz inequality,

$$\left|\sum_{\chi\in\mathrm{Irr}(G),\ \chi(1)\ge D}\frac{\chi(g_1)\chi(g_2)\overline{\chi}(g)}{\chi(1)}\right|\le\frac{(q^4-1)}{(q-1)(q^3-1)}<1.35.$$

Using [60], we check that all irreducible characters of G of degree less than D are linear or Weil characters. Hence (4.7) implies that

$$\left|\sum_{\chi\in\mathrm{Irr}(G),\ 1<\chi(1)<D}\frac{\chi(g_1)\chi(g_2)\overline{\chi}(g)}{\chi(1)}\right|\le\frac{(q-1)^3}{q^4-q}<0.11.$$

It follows that

$$\left|\sum_{\chi\in\mathrm{Irr}(G),\ \chi(1)>1}\frac{\chi(g_1)\chi(g_2)\overline{\chi}(g)}{\chi(1)}\right|<1.35+0.11=1.46<q-1,$$

so we are done. ∎

Proposition 4.9. *Suppose $G=\mathrm{GU}_n(q)$ with $n\ge4$, $q=p^f\ge4$, and $t\in\mathcal{R}(\mathrm{SU}_n(q))$. Then $\mathsf{P}_u(N)$ holds for G and for every $N=p^at^b$.*

Proof. Consider an unbreakable $g\in G$ and a regular semisimple $g_1\in\mathrm{SU}_n(q)$ of order $s\in\mathcal{R}(G)\smallsetminus\{t\}$. Denote

$$\mathrm{Irr}(G/[G,G])=\{\lambda_i=(\lambda_1)^i\mid0\le i\le q\}.$$

(i) First we consider the case $n\ge6$. If $n\ge7$, then using Lemma 4.7, we can choose a regular semisimple $g_2\in G$ of order sm where all prime divisors of m divide $q+1$ and $\det(g_2)=\det(g)$. If $n=6$, then we set $s':=\ell(q,6)\ge7$ and use Lemma 4.7 to get a regular semisimple $h\in\mathrm{GU}_3(q)$ of order $s'm$, where $\det(h)=\det(g)$ and all prime divisors of m divide $q+1$. We also set $h':=(h_{s'})^{-1}$ and $g_2=\mathrm{diag}(h,h')$. Then $g_2\in G$ is regular semisimple, and $\det(g_2)=\det(g)$. In either case

$$|\mathbf{C}_G(g_i)|\le(q^{n-1}+1)(q+1).$$

Choose

$$D=\begin{cases}(q^n-(-1)^n)(q^{n-1}-q^2)/(q+1)(q^2-1), & n\ge7,\\ (q+1)(q^3+1)(q^5+1)/2, & n=6.\end{cases}$$

If $n \geq 7$, then by [62, Theorem 4.1], every irreducible character of $\mathrm{SU}_n(q)$ of degree less than D is either the principal character, or an irreducible Weil character ζ_i as defined in (4.3). Hence, the characters in $\mathrm{Irr}(G)$ of degree less than D are exactly the $q+1$ linear characters λ_i, and $(q+1)^2$ irreducible Weil characters $\zeta_{i,j}$ with $0 \leq i,j \leq q$ as defined in (4.4). Suppose $n = 6$ and $\psi \in \mathrm{Irr}(\mathrm{SU}_6(q))$ has positive s-defect 0 and positive s'-defect. Using [41], we check that either ψ is the principal character of a Weil character, or $\psi(1) \geq D$. Again, if $\chi \in \mathrm{Irr}(G)$, $\chi(1) < D$, and $\chi(g_1)\chi(g_2) \neq 0$, then χ is either a linear character, or a Weil character.

The choice of g_1 and g_2 ensures that

$$\sum_{i=0}^{q} \lambda_i(g_1)\lambda_i(g_2)\overline{\lambda}_i(g) = q+1. \tag{4.10}$$

By (3.1) and Lemma 2.3,

$$\left| \sum_{\chi \in \mathrm{Irr}(G),\ \chi(1) \geq D} \frac{\chi(g_1)\chi(g_2)\overline{\chi}(g)}{\chi(1)} \right| < \frac{((q+1)(q^{n-1}+1))^{3/2}}{D} < \frac{2(q+1)}{3}. \tag{4.11}$$

The choice of g_i and the unbreakability of g ensure that each $y \in \{g, g_1, g_2\}$ satisfies the assumption of Lemma 4.6, and so

$$|\zeta_{i,j}(y)| \leq 1. \tag{4.12}$$

It follows that if $n \geq 5$ then

$$\left| \sum_{0 \leq i,j \leq q} \frac{\zeta_{i,j}(g_1)\zeta_{i,j}(g_2)\overline{\zeta}_{i,j}(g)}{\zeta_{i,j}(1)} \right| \leq \frac{(q+1)^3}{q^n - q} \leq \frac{(q+1)^2}{q(q-1)^2}. \tag{4.13}$$

Together with (4.11), this implies that

$$\left| \sum_{\chi \in \mathrm{Irr}(G),\ \chi(1) > 1} \frac{\chi(g_1)\chi(g_2)\overline{\chi}(g)}{\chi(1)} \right| \leq (q+1)\left(\frac{2}{3} + \frac{1}{7}\right) < q+1.$$

Hence $g \in g_1^G \cdot g_2^G$ by (4.10) and Lemma 2.3(i). Since both g_1 and g_2 have order coprime to N, we are done.

(ii) Next we consider the case $n = 5$. Setting $s' := \ell(q,6)$ and using Lemma 4.7 we can choose a regular semisimple $h \in \mathrm{GU}_3(q)$ of order $s'm$, where all prime divisors of m divide $q+1$ and $\det(h) = \det(g)$. Also, let $h' \in \mathrm{GU}_2(q)$ be conjugate (over $\overline{\mathbb{F}}_q$) to $\mathrm{diag}(\alpha, \alpha^{-1})$, where $\alpha \in \mathbb{F}_q^\times$ has order $q-1$. Setting $g_2 = \mathrm{diag}(h, h')$, the orders of g_1 and g_2 are coprime to N, $\det(g_2) = \det(g)$, and $e(g_2, \xi^l) = 0$ for $0 \leq l \leq q$. In particular, (4.12) and (4.13) hold. Next, we choose $D = q^4(q^5+1)/(q+1)$, yielding

$$\left| \sum_{\chi \in \mathrm{Irr}(G),\ \chi(1) \geq D} \frac{\chi(g_1)\chi(g_2)\overline{\chi}(g)}{\chi(1)} \right| \leq \frac{(q+1)(q^4+1)(q^4(q+1))^{1/2}}{D} < \frac{q+1}{5}. \tag{4.14}$$

Now, using [41], we check that if $\psi \in \mathrm{Irr}(\mathrm{SU}_5(q))$ has positive s-defect and positive s'-defect and $\psi(1) < D$, then either ψ is the principal character or a Weil character, or $s = \ell(q,4)$ and ψ is the unique character of degree $q^2(q^5+1)/(q+1)$. In either case, ψ extends to G. In fact, in the latter case, an extension φ of ψ to G is the unipotent character labeled by the partition $(3,2)$ (see [7, §13.8]). Letting σ be the unipotent character of G labeled by the partition $(3,1,1)$, of degree $q^3(q^2+1)(q^2-q+1)$, we check that

$$\rho = 1_G + \varphi + \sigma$$

is the (rank 3) permutation character of the action of G on the set of isotropic 1-dimensional subspaces of the natural module $\mathbb{F}_{q^2}^5$, cf. [56, Table 2]. Note that σ has s-defect 0 and s'-defect 0. It follows that $\sigma(g_1) = \sigma(g_2) = 0$, so

$$\varphi(g_1) = \rho(g_1) - 1 = 0 - 1 = -1,\ \varphi(g_2) = \rho(g_2) - 1 = 2 - 1 = 1.$$

Also, the extensions of ψ to G are $\varphi\lambda_i$, $0 \le i \le q$, and $|\varphi(g)| \le (q^4(q+1))^{1/2}$ by (3.1). Certainly, $\chi(g_1)\chi(g_2) = 0$ unless χ has positive s-defect and positive s'-defect. Hence, combining with (4.13), we deduce that

$$\left|\sum_{\chi\in\mathrm{Irr}(G),\ 1<\chi(1)<D} \frac{\chi(g_1)\chi(g_2)\overline{\chi}(g)}{\chi(1)}\right| \le \frac{(q+1)^2}{q(q-1)^2} + (q+1)\frac{(q^4(q+1))^{1/2}}{\psi(1)} < \frac{q+1}{7}.$$

Together with (4.14), this implies that

$$\left|\sum_{\chi\in\mathrm{Irr}(G),\ \chi(1)>1} \frac{\chi(g_1)\chi(g_2)\overline{\chi}(g)}{\chi(1)}\right| \le (q+1)\left(\frac{1}{5}+\frac{1}{7}\right) < q+1,$$

so we are done as before.

(iii) Here we consider the case $n = 4$. Since g is unbreakable, g belongs to class A_5, C_2, or E_1, in the notation of [51]. In the two latter cases, note that the G-conjugacy class of such an element g is completely determined by $|g|$ and the eigenvalues of g acting on $\overline{\mathbb{F}}_q^4$. On the other hand, G contains a natural subgroup $H \cong \mathrm{GL}_2(q^2)$, and H contains an element h with the same spectrum and order as g. Hence we may assume $g = h \in H$. As $N = p^at^b$ and $t \nmid (q^2-1)$, we can now apply Lemma 4.5 (if h is unbreakable) to get $g = x^Ny^N$ for some $x \in \mathrm{SL}_2(q^2) < \mathrm{SL}_4(q)$ and $y \in H$. Such a decomposition certainly exists if h is breakable in H (i.e. $h \in \mathrm{GL}_1(q^2) \times \mathrm{GL}_1(q^2)$).

It remains therefore to consider the case $g \in A_5$, i.e. $g = zu$, where $z \in \mathbf{Z}(G)$ and u is a regular unipotent element. By [7, Corollary 8.3.6], $|\chi(g)| \le 1$ for all $\chi \in \mathrm{Irr}(G)$. Choosing $D = (q+1)(q^3+1)$ and g_2 of order sm as in (i) (when $n \ge 7$), by the Cauchy-Schwarz inequality,

$$\left|\sum_{\chi\in\mathrm{Irr}(G),\ \chi(1)\ge D} \frac{\chi(g_1)\chi(g_2)\overline{\chi}(g)}{\chi(1)}\right| \le \frac{(q^3+1)(q+1)}{(q+1)(q^3+1)} = 1 \le \frac{q+1}{5}.$$

Using [51], we check that all irreducible characters of G of degree less than D are linear or Weil characters. Hence (4.12) implies that

$$\left|\sum_{\chi\in\mathrm{Irr}(G),\ 1<\chi(1)<D} \frac{\chi(g_1)\chi(g_2)\overline{\chi}(g)}{\chi(1)}\right| \le \frac{(q+1)^2}{q(q-1)^2} < \frac{q+1}{7}.$$

It follows that

$$\left|\sum_{\chi\in\mathrm{Irr}(G),\ \chi(1)>1} \frac{\chi(g_1)\chi(g_2)\overline{\chi}(g)}{\chi(1)}\right| < (q+1)\left(\frac{1}{5}+\frac{1}{7}\right) < q+1,$$

so we are done. ∎

Corollary 4.10. *Theorem 1 holds for $G = \mathrm{PSL}_n^\epsilon(q)$ with $q = p^f \ge 4$, $\epsilon = \pm$, and $n \ge 2$.*

Proof. The case $n = 2, 3$ follows from Lemma 4.4. If $n \ge 4$, then we choose $n_0 = 3$ and apply Proposition 4.3. Note that condition (i) of that proposition is satisfied by Lemma 4.5, and (ii) holds by Propositions 4.8 and 4.9. Hence we are done by Proposition 4.3. ∎

4.5. **Induction step: Small fields.**

Proposition 4.11. *Suppose $G = \mathrm{GL}_n(2)$ with $n \geq 8$ and $t \in \mathcal{R}(G)$. Then $\mathsf{P}_u(N)$ holds for G and for every $N = 2^a t^b$.*

Proof. Consider an unbreakable $g \in G$ and choose

$$D = (2^n - 1)(2^{n-1} - 4)/3.$$

By [62, Theorem 3.1], $\mathrm{Irr}(G)$ contains exactly two characters of degree less than D: namely, 1_G and $\tau = \tau_0$. In fact $\tau(1) = 2^n - 2$ and $\rho = \tau + 1_G$ is the permutation character of the action of G on the set of nonzero vectors of the natural module $V = \mathbb{F}_2^n$. Choose regular semisimple elements $g_1 = g_2$ of order $s \in \mathcal{R}(G) \smallsetminus \{t\}$; in particular, $|\mathbf{C}_G(g_i)| \leq 2^n - 1$. Note that $\rho(g_i) \in \{0, 1\}$, so $|\tau(g_i)| \leq 1$. Also, $|\mathbf{C}_G(g)| \leq 9 \cdot 2^n$ by Lemma 3.6. It follows that

$$\frac{|\tau(g_1)\tau(g_2)\tau(g)|}{\tau(1)} \leq \frac{3 \cdot 2^{n/2}}{2^n - 2} < 0.189.$$

If $n \geq 9$, then by Lemma 2.3(ii)

$$\left| \sum_{\chi \in \mathrm{Irr}(G),\ \chi(1) \geq D} \frac{\chi(g_1)\chi(g_2)\overline{\chi}(g)}{\chi(1)} \right| \leq \frac{(2^n - 1) \cdot 3 \cdot 2^{n/2}}{D} = \frac{9 \cdot 2^{n/2}}{2^{n-1} - 4} < 0.809.$$

If $n = 8$ and $|\mathbf{C}_G(g)| \leq 2^{n+2}$, then

$$\left| \sum_{\chi \in \mathrm{Irr}(G),\ \chi(1) \geq D} \frac{\chi(g_1)\chi(g_2)\overline{\chi}(g)}{\chi(1)} \right| \leq \frac{(2^n - 1) \cdot 2 \cdot 2^{n/2}}{D} = \frac{6 \cdot 2^{n/2}}{2^{n-1} - 4} < 0.775.$$

Thus, in each of these cases,

$$\left| \sum_{\chi \in \mathrm{Irr}(G),\ \chi(1) > 1} \frac{\chi(g_1)\chi(g_2)\overline{\chi}(g)}{\chi(1)} \right| < 0.809 + 0.189 = 0.998,$$

whence $g \in g_1^G \cdot g_2^G$ by Lemma 2.3(i). Since both g_1 and g_2 have order coprime to N, we are done in these cases. In the remaining case, by Lemma 3.6, $G = \mathrm{GL}_8(2)$ and $g \in H := \mathrm{GL}_4(4) = \mathbf{Z}(H) \times S$ with $\mathbf{Z}(H) \cong C_3$ and $S \cong \mathrm{SL}_4(4)$. Thus we can write $g = zh$ with $z \in \mathbf{Z}(H)$ and $h \in S$. Applying Corollary 4.10 to $\mathrm{SL}_4(4)$, we deduce that $h = x^N y^N$ for some $x, y \in S$. Certainly, $z = z_1^N$ for some $z_1 \in \mathbf{Z}(H)$. It follows that $g = (z_1 x)^N y^N$, and we are done again. ∎

Proposition 4.12. *Suppose $G = \mathrm{GL}_n(3)$ with $n \geq 8$ and $t \in \mathcal{R}(\mathrm{SL}_n(3))$. Then $\mathsf{P}_u(N)$ holds for G and for every $N = 3^a t^b$.*

Proof. Consider an unbreakable $g \in G$, so $|\mathbf{C}_G(g)| \leq 3^{n+2} \cdot 2^4$ by Lemma 3.8. First, we use Lemma 4.7 to get a regular semisimple element g_1 of order sm, where $s \in \mathcal{R}(G) \smallsetminus \{t\}$, m is a 2-power, and $\det(g_1) = \det(g)$. Next we fix a regular semisimple $h \in \mathrm{SL}_{n-2}(3)$ of order $s' = \ell(3, n-2)$ and $h' \in \mathrm{SL}_2(3)$ of order 4, and set $g_2 := \mathrm{diag}(h, h')$. In particular, $|\mathbf{C}_G(g_i)| \leq 3^n - 1$. Also, we choose

$$D = 3^{3n-9}.$$

By Lemma 2.3(ii),

$$\left| \sum_{\chi \in \mathrm{Irr}(G),\ \chi(1) \geq D} \frac{\chi(g_1)\chi(g_2)\overline{\chi}(g)}{\chi(1)} \right| \leq \frac{(3^n - 1) \cdot 4 \cdot 3^{(n+2)/2}}{3^{3n-9}} < \frac{4}{3^{3n/2-10}} \leq \frac{4}{9}.$$

Now we estimate character ratios for $\chi \in \mathrm{Irr}(G)$ with $\chi(1) < D$ and $\chi(g_1)\chi(g_2) \neq 0$. The latter condition implies that χ has positive s-defect and positive s'-defect. Applying [5, Theorem 3.4], χ can be only one of the following:

- two linear characters $\lambda_{0,1}$,
- two of the four Weil characters $\tau_{i,j}$ with $0 \leq i \leq 1$ as listed in (4.2), and, possibly,
- two characters $\varphi_{0,1} = \varphi\lambda_{0,1}$. Here, φ is the unipotent character of G labeled by the partition $(n-2,2)$, of degree $(3^n-1)(3^{n-1}-9)/16$.

The elements $g_{1,2}$ have the property that $\sum_{\delta\in\mathbb{F}_3^\times} e(g_i,\delta) \leq 1$. Hence, the estimate (4.7) holds by Lemma 4.6. It follows that

$$\sum_{0\leq i,j\leq 1} \frac{|\tau_{i,j}(g_1)\tau_{i,j}(g_2)\overline{\tau}_{i,j}(g)|}{\tau_{i,j}(1)} \leq \frac{2\cdot 4\cdot 3^{n/2+1}}{(3^n-3)/2} \leq \frac{8}{13}.$$

On the other hand, $\tau_{0,0}$ is the unipotent character of G labeled by the partition $(n-1,1)$. It follows by [22, Lemma 5.1] that

$$\varphi = (1_G + \tau_{0,0} + \varphi) - (1_G + \tau_{0,0}) = \rho_2 - \rho_1,$$

where ρ_i is the permutation character of the action of G on the set of i-dimensional subspaces of the natural module $\mathbb{F}_3^n$ for $i = 1, 2$. Observe that $\rho_2(g_1) = 0$ and $\rho_1(g_1) = 0$ or 1. Therefore,

$$|\varphi(g_1)| = |\rho_2(g_1) - \rho_1(g_1)| = |\rho_1(g_1)| \leq 1,\ \varphi(g_2) = \rho_2(g_2) - \rho_1(g_2) = 1 - 0 = 1.$$

This implies that

$$\left|\sum_{i=0}^{1} \frac{\varphi_i(g_1)\varphi_i(g_2)\overline{\varphi}_i(g)}{\varphi_i(1)}\right| \leq \frac{2\cdot 4\cdot 3^{n/2+1}}{(3^n-1)(3^{n-1}-9)/16} \leq \frac{128}{(3^{n/2-1}-1)(3^{n-1}-9)} < 0.003.$$

In summary,

$$\left|\sum_{\chi\in\mathrm{Irr}(G),\ \chi(1)>1} \frac{\chi(g_1)\chi(g_2)\overline{\chi}(g)}{\chi(1)}\right| < \frac{4}{9} + \frac{8}{13} + 0.003 < 1.07.$$

Our choice of g_1 and g_2 ensures that

$$\sum_{i=0}^{1} \lambda_i(g_1)\lambda_i(g_2)\overline{\lambda}_i(g) = 2.$$

Hence $g \in g_1^G \cdot g_2^G$ by Lemma 2.3(i), so we are done since $|g_1|$ and $|g_2|$ are both coprime to N. ∎

Proposition 4.13. *Suppose $G = \mathrm{GU}_n(3)$ with $n \geq 7$ and $t \in \mathcal{R}(\mathrm{SU}_n(3))$. Then $\mathsf{P}_u(N)$ holds for G and for every $N = 3^at^b$.*

Proof. Consider an unbreakable $g \in G$, so $|\mathbf{C}_G(g)| \leq 3^{n+2}\cdot 2^4$ by Lemma 3.8. First, we use Lemma 4.7 to get a regular semisimple g_1 of order sm, where $s \in \mathcal{R}(G) \smallsetminus \{t\}$, m is a 2-power, and $\det(g_1) = \det(g)$. Then we choose

$$s' := \begin{cases} \ell(q, 2n-4), & n \equiv 1 \bmod 2, \\ \ell(q, n-2), & n \equiv 2 \bmod 4, \\ \ell(q, (n-2)/2), & n \equiv 0 \bmod 4, \end{cases}$$

(with $q = 3$). Note that $s' | (q^{n-2} - (-1)^{n-2})$ but $s' \nmid \prod_{i=1, i\neq n-2}^{n} (q^i - (-1)^i)$. Next, we fix $\alpha \in \overline{\mathbb{F}}_3^\times$ of order $q^{n-2} - (-1)^n$ and choose a regular semisimple $h \in \mathrm{GU}_{n-2}(3)$ that is conjugate over $\overline{\mathbb{F}}_3$ to

$$\mathrm{diag}\left(\alpha, \alpha^{-q}, \alpha^{q^2}, \ldots, \alpha^{(-q)^{n-3}}\right).$$

Note that $\det(h) \in \mathbb{F}_9^\times$ has order 4. Hence there is some $\beta \in \mathbb{F}_9^\times$ of order q^2-1 so that $\det(h) = \beta^2$. We fix $h' = \mathrm{diag}(\beta, \beta^{-q}) \in \mathrm{GU}_2(3)$, and set $g_2 := \mathrm{diag}(h, h')$. In particular, $g_2 \in \mathrm{SU}_n(3)$ is s'-singular, g_i is an N'-element and $|\mathbf{C}_G(g_i)| \le 4(3^{n-1}+1)$ for $i = 1, 2$.

Recall the Weil characters $\zeta_{i,j}$, $0 \le i, j \le q$, defined in (4.4). The elements $g_{1,2}$ satisfy the assumption of Lemma 4.6, hence the estimate (4.12) holds for $y = g_i$. Also,

$$e(g, \xi^l) \le n/2 \tag{4.15}$$

whenever $n \ge 7$. (Indeed, otherwise $U = \mathrm{Ker}(g - \xi^l \cdot 1_V)$ has dimension $\ge (n+1)/2$ in the natural G-module $V := \mathbb{F}_{q^2}^n$. It follows that U cannot be totally singular, so U contains at least one anisotropic vector u. In this case, g fixes the decomposition

$$V = \langle u \rangle_{\mathbb{F}_{q^2}} \oplus (\langle u \rangle_{\mathbb{F}_{q^2}})^\perp.$$

In other words, $g \in \mathrm{GU}_1(q) \times \mathrm{GU}_{n-1}(q)$, so g is breakable, a contradiction.) As $n \ge 7$, we deduce that $e(g, \xi^l) \le n-4$, whence

$$|\zeta_{i,j}(g)| \le \frac{(q+1)q^{n-4}}{q+1} = q^{n-4}, \tag{4.16}$$

so

$$\sum_{0 \le i,j \le q} \frac{|\zeta_{i,j}(g_1)\zeta_{i,j}(g_2)\overline{\zeta}_{i,j}(g)|}{\zeta_{i,j}(1)} \le \frac{16 \cdot 3^{n-4}}{(3^n-3)/4} < 0.8. \tag{4.17}$$

Choosing

$$D = \begin{cases} (3^n-1)(3^{n-1}-1)(3^{n-2}-27)/896, & n \ge 8, \\ 3^{16}, & n = 7, \end{cases}$$

by Lemma 2.3(ii)

$$\left| \sum_{\chi \in \mathrm{Irr}(G),\ \chi(1) \ge D} \frac{\chi(g_1)\chi(g_2)\overline{\chi}(g)}{\chi(1)} \right| \le \frac{4(3^{n-1}+1) \cdot 4 \cdot 3^{(n+2)/2}}{D} < 0.76. \tag{4.18}$$

Now we estimate character ratios for $\chi \in \mathrm{Irr}(G)$ with $\chi(1) < D$ and $\chi(g_1)\chi(g_2) \ne 0$. The latter condition implies that χ has positive s-defect and positive s'-defect. Applying [34, Proposition 6.6] for $n \ge 8$, χ can be only one of the following:

- 4 linear characters λ_i, $0 \le i \le 3$;
- (at most 12 of the) 16 Weil characters $\zeta_{i,j}$ with $0 \le i \le 3$, and
- 4 characters $\varphi_i = \varphi\lambda_i$, $0 \le i \le 3$, if $s|(q^{n-1} + (-1)^n)$. Here, φ is the unipotent character of G labeled by the partition $(n-2, 2)$, of degree

$$\varphi(1) = (3^n - (-1)^n)(3^{n-1} + 9(-1)^n)/32.$$

This conclusion also holds for $n = 7$. (Indeed, for $n = 7$, using [41] we can check that if $\sigma \in \mathrm{Irr}(\mathrm{SU}_7(q))$ has positive s-defect and positive s'-defect and $\sigma(1) < D$, then σ is the restriction to $\mathrm{SU}_7(q)$ of one of the above characters of $\mathrm{GU}_7(q)$.)

Let ψ denote the unipotent character of G labeled by the partition $(n-2, 1, 1)$, of degree

$$\psi(1) = (3^n + 3(-1)^n)(3^n - 9(-1)^n)/32.$$

It is well known, see e.g. [56, Table 2], that $\rho := 1_G + \varphi + \psi$ is the permutation character of the action of G on the set of isotropic 1-dimensional subspaces of the natural module V. Recall we need to consider φ only when $s|(q^{n-1} + (-1)^n)$, so ψ has s-defect 0 and s'-defect 0. In particular, $\psi(g_1) = \psi(g_2) = 0$. Therefore,

$$\varphi(g_1) = \rho(g_1) - 1 = 0 - 1 = -1,\ \varphi(g_2) = \rho(g_2) - 1 = 2 - 1 = 1.$$

Since $|\varphi(g)| \le 4 \cdot 3^{n/2+1}$,

$$\left| \sum_{i=0}^{q} \frac{\varphi_i(g_1)\varphi_i(g_2)\overline{\varphi}_i(g)}{\varphi_i(1)} \right| \le \frac{4 \cdot 4 \cdot 3^{n/2+1}}{(3^n-1)(3^{n-1}-9)/32} < 0.05.$$

Together with (4.15) and (4.18), this implies that

$$\left| \sum_{\chi \in \mathrm{Irr}(G),\ \chi(1)>1} \frac{\chi(g_1)\chi(g_2)\overline{\chi}(g)}{\chi(1)} \right| < 0.8 + 0.76 + 0.05 = 1.61.$$

Our choice of g_1 and g_2 ensures that

$$\sum_{i=0}^{q} \lambda_i(g_1)\lambda_i(g_2)\overline{\lambda}_i(g) = 4.$$

Hence $g \in g_1^G \cdot g_2^G$ by Lemma 2.3(i), so we are done since $|g_1|$ and $|g_2|$ are both coprime to N. ∎

Proposition 4.14. *Suppose $G = \mathrm{GU}_n(2)$ with $n \ge 9$ and $t \in \mathcal{R}(\mathrm{SU}_n(2))$. Then $\mathsf{P}_u(N)$ holds for G and for every $N = 2^a t^b$.*

Proof. Consider an unbreakable $g \in G$, so $|\mathbf{C}_G(g)| \le 2^{n+4} \cdot 3^2$ when $n \ge 10$ and $|\mathbf{C}_G(g)| \le 2^{48}$ when $n = 9$ by Lemma 3.7.

(i) First, we use Lemma 4.7 to get a regular semisimple element g_1 of order sm, where $s \in \mathcal{R}(G) \smallsetminus \{t\}$, m is a 3-power, and $\det(g_1) = \det(g)$. If $n \ge 10$, we can find a regular semisimple $g_2 \in \mathrm{SU}_n(2)$ of order s. In particular, g_i is an N'-element and $|\mathbf{C}_G(g_i)| \le 3(2^{n-1}+1)$ for $i = 1, 2$. Fix $\xi \in \mathbb{F}_{q^2}^\times$ of order $q+1$. Again, note that the elements $g_{1,2}$ satisfy the assumption of Lemma 4.6, hence (4.12) holds for $y = g_i$.

If $n = 9$, we choose $s' := 43$ and fix a regular semisimple $h \in \mathrm{SU}_7(2)$ of order 43. Also, we fix $h' \in \mathrm{SU}_2(2)$ of order 3 and set $g_2 := \mathrm{diag}(h, h')$. In particular, $|\mathbf{C}_G(g_2)| = 9(2^7+1)$, and $e(g_2, \xi^l)$ equals 0 for $l = 0$ and 1 for $l = 1, 2$. Direct computation shows that $|\zeta_{i,j}(g_2)| = 1$ for all i, j. Thus, for $n \ge 9$ and $y \in \{g_1, g_2\}$,

$$|\zeta_{i,j}(y)| \le 1. \tag{4.19}$$

(ii) Choosing

$$D = \begin{cases} (2^n+1)(2^{n-1}-1)(2^{n-2}-27)/81, & n \ge 10, \\ 2^{22} \cdot 7 \cdot (2^9+1), & n = 9, \end{cases}$$

by Lemma 2.3(ii), for $n \ge 10$,

$$\left| \sum_{\chi \in \mathrm{Irr}(G),\ \chi(1) \ge D} \frac{\chi(g_1)\chi(g_2)\overline{\chi}(g)}{\chi(1)} \right| \le \frac{3(2^{n-1}+1) \cdot 3 \cdot 2^{n/2+2}}{D} < 0.37. \tag{4.20}$$

Now we estimate character ratios for $\chi \in \mathrm{Irr}(G)$ with $\chi(1) < D$ and $\chi(g_1)\chi(g_2) \ne 0$. The latter condition implies that χ has positive s-defect and positive s'-defect. Applying [34, Proposition 6.6] for $n \ge 10$, χ can be only one of the following:

- 3 linear characters λ_i, $0 \le i \le 2$;
- at most 6 of the 9 Weil characters $\zeta_{i,j}$ with $0 \le i \le 2$, and
- (some of the) 27 characters $D_\alpha^\circ \lambda_i$, $0 \le i \le 2$, $\alpha \in \mathrm{Irr}(S)$ with $S := \mathrm{GU}_2(2)$ (see [34, Proposition 6.3] for the definition of D_α°).

This conclusion also holds for $n = 9$. (Indeed, for $n = 9$, using [41] we can check that if $\sigma \in \mathrm{Irr}(\mathrm{SU}_9(2))$ has positive s-defect and positive s'-defect and $\sigma(1) < D$, then σ is the restriction to $\mathrm{SU}_9(2)$ of one of the above characters of $\mathrm{GU}_9(2)$.)

Next, the inequality (4.15) implies that $e(g,\xi^l) \le n-5$ as $n \ge 9$, so

$$|\zeta_{i,j}(g)| \le \frac{(q+1)q^{n-5}}{q+1} = q^{n-5}.$$

It now follows from (4.19) that

$$\sum_{0\le i,j\le q} \frac{|\zeta_{i,j}(g_1)\zeta_{i,j}(g_2)\overline{\zeta}_{i,j}(g)|}{\zeta_{i,j}(1)} \le \frac{6\cdot 2^{n-5}}{(2^n-2)/3} < 0.57. \tag{4.21}$$

(iii) Now we assume that $n \ge 10$. We already observed that $\sum_{l=0}^{2} e(g_i,\xi^l) \le 1$. Thus g_i satisfies the conclusion (i) of [34, Lemma 6.7]. Hence it also satisfies the conclusion (ii) of [34, Proposition 6.9]. Thus

$$|D^\circ_\alpha(g_i)| \le \begin{cases} 2, & \alpha(1)=1, \alpha \ne 1_S,\\ 3, & \alpha = 1_S,\\ 4, & \alpha(1)=2. \end{cases}$$

Since $|\varphi(g)| \le 3\cdot 2^{n/2+2}$,

$$\left|\sum_{\chi=D^\circ_\alpha\lambda_i} \frac{\chi(g_1)\chi(g_2)\overline{\chi}(g)}{\chi(1)}\right| \le 3^2\cdot 2^{n/2+2}\cdot\left(\frac{5\cdot 2^2+3^2}{(2^n-1)(2^{n-1}-4)/9} + \frac{3\cdot 4^2}{(2^n-2)(2^n-4)/9}\right) < 1.06.$$

Together with (4.21) and (4.20), this implies that

$$\left|\sum_{\chi\in\mathrm{Irr}(G),\ \chi(1)>1} \frac{\chi(g_1)\chi(g_2)\overline{\chi}(g)}{\chi(1)}\right| < 0.57+0.37+1.06 = 2.$$

Our choice of g_1 and g_2 ensures that

$$\sum_{i=0}^{q} \lambda_i(g_1)\lambda_i(g_2)\overline{\lambda}_i(g) = 3.$$

Hence $g \in g_1^G\cdot g_2^G$ by Lemma 2.3(i), so we are done since $|g_1|$ and $|g_2|$ are both coprime to N.

(iv) Finally, we handle the case $n=9$. Now $\chi = D^\circ_\alpha\lambda_i$ can have positive s-defect and positive s'-defect only when $t=19$, $s=17$, $\alpha = 1_S$. In this case, $\varphi := D^\circ_{1_S}$ is the unipotent character of G labeled by the partition $(n-2,2)$, of degree

$$\varphi(1) = (2^9+1)(2^8-4)/9 = 14364.$$

Let ψ denote the unipotent character of G labeled by the partition $(n-2,1,1)$, of degree

$$\psi(1) = (2^9-2)(2^9+4)/9 = 29240.$$

Again, $\rho := 1_G+\varphi+\psi$ is the permutation character of the action of G on the set of isotropic 1-dimensional subspaces of the natural module V, see e.g. [56, Table 2]. Recall we need to consider φ only when $s=17$ (and $s'=43$), so ψ has s-defect 0 and s'-defect 0. In particular, $\psi(g_1)=\psi(g_2)=0$. Therefore,

$$\varphi(g_i) = \rho(g_i) - 1 = 0 - 1 = -1.$$

Recall that $e(g,\xi^l) \le 4$ for all unbreakable $g \in \mathrm{GU}_9(q)$ and $0 \le l \le 2$. Arguing as in the proof of [34, Proposition 6.9], we obtain

$$|\varphi(g)| = |D^\circ_{1_S}(g)| \le 2^8+1 = 257.$$

It follows that

$$\left|\sum_{\chi=\varphi\lambda_i,\ 0\le i\le 2}\frac{\chi(g_1)\chi(g_2)\overline{\chi}(g)}{\chi(1)}\right|\le\frac{3\cdot 257}{14364}<0.06.$$

By Lemma 2.3(ii),

$$\left|\sum_{\chi\in\mathrm{Irr}(G),\ \chi(1)\ge D}\frac{\chi(g_1)\chi(g_2)\overline{\chi}(g)}{\chi(1)}\right|\le\frac{(765\cdot 1161)^{1/2}\cdot 2^{24}}{2^{22}\cdot 7\cdot 513}<1.05.$$

In summary,

$$\left|\sum_{\chi\in\mathrm{Irr}(G),\ \chi(1)>1}\frac{\chi(g_1)\chi(g_2)\overline{\chi}(g)}{\chi(1)}\right|<0.57+0.06+1.05=1.68,$$

so we are done again. ∎

Lemma 4.15. *Let $q=p=2,3$ and $\epsilon=\pm$.*

(i) *Suppose that $3\le k\le 4$ and $k\ne 3$ if $(q,\epsilon)=(2,-)$. Then $\mathsf{P}(N)$ holds for $\mathrm{GL}_k^\epsilon(q)$ and for every $N=p^at^b$ with $t\ne p$ a prime and $t\nmid(q-\epsilon)$. Also, Theorem 1 holds for $\mathrm{PSL}_k^\epsilon(q)$.*

(ii) *Let $\mathrm{GL}_k^\epsilon(q)$ be one of the following groups:*
   (a) *$\mathrm{GL}_n(2)$ or $\mathrm{GL}_n(3)$, with $5\le n\le 7$;*
   (b) *$\mathrm{GU}_n(2)$ with $5\le n\le 8$;*
   (c) *$\mathrm{GU}_n(3)$ with $n=5,6$.*
   Then $\mathsf{P}_u(N)$ holds for $\mathrm{GL}_k^\epsilon(q)$ and for every $N=p^at^b$ with $t\in\mathcal{R}(\mathrm{SL}_k^\epsilon(q))$.

Proof. Direct calculations similar to those of Lemma 2.4. ∎

Corollary 4.16. *Theorem 1 holds for $G=\mathrm{PSL}_n^\epsilon(q)$ with $q=p^f=2,3$, $\epsilon=\pm$, $n\ge 3$, and $(n,q,\epsilon)\ne(3,2,-)$.*

Proof. The case $n=3,4$ follows from Lemma 4.15(i). Suppose now that $n\ge 5$. Then we choose $n_0=4$ and apply Proposition 4.3. Note that condition (i) of that proposition is verified by Lemma 4.15(i), and (ii) holds by Propositions 4.11, 4.12, 4.13, 4.14, and Lemma 4.15(ii). Hence we are done by Proposition 4.3. ∎

5. Theorem 1 for symplectic and orthogonal groups

5.1. **General inductive argument.** Recall $\mathcal{R}(G)$ from §2, and the notion of unbreakability for symplectic and orthogonal groups from Definition 3.1.

Definition 5.1. Given a prime power $q=p^f$, a finite symplectic or orthogonal group $G=\mathrm{Cl}(V)=\mathrm{Cl}_n(q)$, and an integer $N=p^at^b$ with $t>2$ a prime. We say that

(i) G satisfies the condition $\mathsf{P}(N)$ if every $g\in G$ can be written as $g=x^Ny^N$ for some $x,y\in G$; and
(ii) G satisfies the condition $\mathsf{P}_u(N)$ if every *unbreakable* $g\in G$ can be written as $g=x^Ny^N$ for some $x,y\in G$.

Our proof of Theorem 1 for symplectic and orthogonal groups relies on the following inductive argument:

Proposition 5.2. *Given a prime power $q=p^f$, an integer $n\ge 4$, let $V=\mathbb{F}_q^n$ be a finite symplectic or quadratic space, and let $G:=\mathrm{Cl}(V)=\mathrm{Cl}_n(q)$ be perfect, with $\mathrm{Cl}=\mathrm{Sp}$ or Ω. Suppose that there is an integer $n_0\ge 4$ with the following properties:*

(i) *If* $1 \le k \le n_0$ *and* $\mathrm{Cl}_k(q)$ *is perfect, then* $\mathsf{P}_u(N)$ *holds for* $\mathrm{Cl}_k(q)$ *and for every* $N = p^a t^b$ *with* $t \ne 2, p$ *any prime; and*

(ii) *For each* k *with* $n_0 < k \le n$, $\mathsf{P}_u(N)$ *holds for* $\mathrm{Cl}_k(q)$ *and for every* $N = p^a t^b$ *with* $t \in \mathcal{R}(\mathrm{Cl}_k(q))$.

If $N = s^a t^b$ *for some primes* s, t, *then the word map* $(u, v) \mapsto u^N v^N$ *is surjective on* $G/\mathbf{Z}(G)$.

Proof. By Corollary 2.2, we need to consider only the case $N = p^a t^b$ with $t \in \mathcal{R}(\mathrm{Cl}_n(q))$; in particular, $t > 2$. It suffices to show $\mathsf{P}(N)$ holds for G. According to (ii), $\mathsf{P}_u(N)$ holds for G. Consider a breakable $g \in G$ and write it as $\mathrm{diag}(g_1, \dots, g_m)$ lying in the natural subgroup

$$\mathrm{Cl}(U_1) \times \ldots \times \mathrm{Cl}(U_i) \cong \mathrm{Cl}_{k_1}(q) \times \ldots \times \mathrm{Cl}_{k_m}(q)$$

that corresponds to an orthogonal decomposition $V = U_1 \oplus \ldots \oplus U_m$. Here, $1 \le k_i < n$, and for each i either $\mathrm{Cl}_{k_i}(q)$ is perfect or $g_i = \pm 1_{U_i}$. Relabeling the elements g_i suitably, we may assume that there is some $m' \le m$ such that g_i is unbreakable if $1 \le i \le m'$ and $g_i = \pm 1_{U_i}$ if $i > m'$. Hence, according to (i), $\mathsf{P}_u(N)$ holds for $\mathrm{Cl}_{k_i}(q)$ if $k_i \le n_0$ and $i \le m'$. Suppose $k_i > n_0$. Then $\mathsf{P}_u(N)$ holds for $\mathrm{Cl}_{k_i}(q)$ if $t \in \mathcal{R}(\mathrm{Cl}_{k_i}(q))$ by (ii). If $t \notin \mathcal{R}(\mathrm{Cl}_{k_i}(q))$, then by Theorem 2.1 every non-central element of G is a product of two N'-elements, so it is a product of two Nth powers. Furthermore, all central elements of $\mathrm{Cl}_{k_i}(q)$ are Nth powers. Hence $\mathsf{P}_u(N)$ holds for $\mathrm{Cl}_{k_i}(q)$ in this case as well. Thus for $i \le m'$ we can write $g_i = x_i^N y_i^N$ with $x_i, y_i \in \mathrm{Cl}(U_i)$. Setting

$$U := U_1 \oplus \ldots \oplus U_{m'},\ W = U_{m'+1} \oplus \ldots \oplus U_m,\ h := \mathrm{diag}(g_{m'+1}, \dots, g_m) \in \mathrm{Iso}(W),$$

(where $\mathrm{Iso}(W) = \mathrm{Sp}(W)$ if $\mathrm{Cl} = \mathrm{Sp}$ and $\mathrm{Iso}(W) = \mathrm{GO}(W)$ if $\mathrm{Cl} = \Omega$), we see that either $|h| = 1$, or p and N are odd and $|h| = 2$. In particular, $h = h^N$ in either case. Letting

$$x := \mathrm{diag}(x_1, \dots, x_{m'}) \in \mathrm{Cl}(U),\ y := \mathrm{diag}(y_1, \dots, y_{m'}) \in \mathrm{Cl}(U)$$

we deduce that $g = x^N y^N h^N = x^N (yh)^N$. Also, $x, y \in G$, $g = \mathrm{diag}(g', h) \in G$ with $g' := \mathrm{diag}(g_1, \dots, g_{m'}) \in \mathrm{Cl}(U) \le G$. It follows that $h \in G$, so $\mathsf{P}(N)$ holds for G, as desired. ∎

5.2. **Induction base.**

Lemma 5.3. *Let* $q = p^f$ *and let* $N = p^a t^b$ *with* $t \ne 2, p$ *any prime. Then* $\mathsf{P}(N)$ *holds for* $G = \mathrm{SL}_2(q)$ *with* $q \ge 4$, *and for* $\mathrm{Sp}_4(q)$ *with* $q \ge 3$.

Proof. (i) Consider the case $G = \mathrm{SL}_2(q)$. If $t \nmid (q-1)$, then we check that $X^G \cdot X^G = G$ for $X = x\mathbf{Z}(G)$ and $x \in G$ of order $q-1$. On the other hand, if $t \nmid (q+1)$, then $Y_1^G \cdot Y_2^G \supseteq G \setminus \{1\}$ for $Y_i = y^i \mathbf{Z}(G)$, $i = 1, 2$, and $y \in G$ of order $q+1$. Since N is odd, we are done in both cases.

(ii) Consider the case $G = \mathrm{Sp}_4(q)$ with $2|q$. The character table of G is given in [12]. Suppose that $t|(q^2+1)$. We fix a regular semisimple $x_1 \in G$ of order $q-1$ belonging to the class $B_1(1,2)$ and a regular semisimple $x_2 \in G$ of order $q+1$ belonging to the class $B_4(1,2)$, in the notation of [12, Table IV-1]. There are 3 non-principal characters of G that are nonzero at both x_1 and x_2: namely, $\theta_{1,2}$ of degree $q(q^2+1)/2$, and St of degree q^4. For every $1 \ne g \in G$,

$$\sum_{1_G \ne \chi \in \mathrm{Irr}(G)} \frac{|\chi(x_1)\chi(x_2)\chi(g)|}{\chi(1)} \le 2 \cdot \frac{q(q+1)/2}{q(q^2+1)/2} + \frac{q}{q^4} < 1,$$

so we are done by Lemma 2.3(i).

Suppose now that $t \nmid (q^2+1)$. Then at least one of x_1 and x_2 has order coprime to N; denote it by x. We also fix a regular semisimple $y \in G$ of order q^2+1 belonging to the

class $B_5(1)$. There are at most 2 non-principal characters of G that are nonzero at both x and y: namely, St and possibly a character θ of degree $\geq q(q-1)^2/2$. For every $1 \neq g \in G$,

$$\sum_{1_G \neq \chi \in \mathrm{Irr}(G)} \frac{|\chi(x)\chi(y)\chi(g)|}{\chi(1)} \leq \frac{q(q-1)/2}{q(q-1)^2/2} + \frac{q}{q^4} < 1,$$

so we are done by Lemma 2.3(i).

(iii) Assume that $G = \mathrm{Sp}_4(q)$ with $q \geq 7$ odd. The character table of G is given in [59]. If $t \nmid (q^2+1)$, then the statement follows from [20, Theorem 7.3]. So we assume that $t|(q^2+1)$. Fix a regular semisimple $x_1 \in G$ of order q^2-1 belonging to the class $B_2(1)$ and a regular semisimple $x_2 \in G$ of order $(q^2-1)/2$ belonging to the class $B_5(1,1)$, in the notation of [59]. There are 3 non-principal characters of G that are nonzero at both x_1 and x_2: namely, $\theta_{1,2}$ of degree $q(q^2+1)/2$, and St of degree q^4. For every $1 \neq g \in G$,

$$\sum_{1_G \neq \chi \in \mathrm{Irr}(G)} \frac{|\chi(x_1)\chi(x_2)\chi(g)|}{\chi(1)} \leq 2 \cdot \frac{q(q+1)/2}{q(q^2+1)/2} + \frac{q}{q^4} < 1,$$

so we are done by Lemma 2.3(i). ∎

Lemma 5.4. *Let G be one of the following groups:*

(i) $\mathrm{Sp}_{2n}(2)$ *with* $3 \leq n \leq 6$, $\mathrm{Sp}_{2n}(3)$ *with* $2 \leq n \leq 5$, *and* $\mathrm{Sp}_{2n}(4)$ *with* $n = 2, 3$;
(ii) $\Omega_{2n+1}(3)$ *with* $3 \leq n \leq 5$;
(iii) $\Omega^{\pm}_{2n}(2)$ *with* $4 \leq n \leq 6$, $\Omega^{\pm}_{2n}(3)$ *with* $4 \leq n \leq 6$, *and* $\Omega^{\pm}_8(4)$.

Let $N = p^at^b$ where p is the defining characteristic of G and $t \in \mathcal{R}(G)$. Then $\mathsf{P}(N)$ holds.

Proof. Direct calculations similar to those of Lemma 2.4. ∎

5.3. **Induction step: Symplectic groups.**

Proposition 5.5. *Suppose $G = \mathrm{Sp}_{2n}(q)$ with $n \geq 3$, $q = p^f \geq 7$ odd, and $t \in \mathcal{R}(G)$. Then $\mathsf{P}_u(N)$ holds for G and for every $N = p^at^b$.*

Proof. Consider an unbreakable $g \in G$; in particular,

$$|\mathbf{C}_G(g)| \leq \begin{cases} 2q^n, & 2|n, \\ q^{2n-1}(q^2-1), & 2 \nmid n \end{cases}$$

by Lemma 3.2. Let $V = \mathbb{F}_q^{2n}$ denote the natural module for G. Inside $\mathrm{Sp}_{2n-2}(q)$ we can find a regular semisimple element x_- of order $s_- = \ell(q, 2n-2)$, and, if $2|n$, a regular semisimple element x_+ of order $s_+ = \ell(q, n-1)$. For $\nu = \pm$, we fix $y_\nu \in \mathrm{Sp}_2(q)$ of order $q - \nu$.

(a) Here we consider the case $2|n$, and set

$$g_1 := \mathrm{diag}(x_+, y_+),\ g_2 := \mathrm{diag}(x_-, y_-)$$

so each g_i is an N'-element and $|\mathbf{C}_G(g_i)| \leq (q^{n-1}+1)(q+1)$. We also choose

$$D = \frac{(q^n-1)(q^n-q)}{2(q+1)}.$$

It follows that

$$\sum_{\chi \in \mathrm{Irr}(G),\ \chi(1) \geq D} \frac{|\chi(g_1)\chi(g_2)\overline{\chi}(g)|}{\chi(1)} \leq \frac{(q^{n-1}+1)(q+1)(2q^n)^{1/2}}{D} < 0.54. \tag{5.1}$$

By [62, Theorem 5.2] the only non-principal irreducible characters of G of degree less than D are the four irreducible Weil characters: $\eta_{1,2}$ of degree $(q^n-1)/2$ and $\xi_{1,2}$ of degree $(q^n+1)/2$. The choice of g_i implies that $\mathrm{Ker}(g_i \pm 1_V) = 0$. Hence, by [23, Lemma 2.4],

$$|\omega(g_i)|,\ |\omega(zg_i)| \le 1,$$

where $\omega = \eta_1 + \xi_1$ is a reducible Weil character of G and $z \in G$ is the central involution. Note that

$$|\omega(g_i)| = |\eta_1(g_i) + \xi_1(g_i)|,\ |\omega(zg_i)| = |\eta_1(g_i) - \xi_1(g_i)|.$$

It follows that

$$|\eta_1(g_i)| = \frac{|(\eta_1(g_i) + \xi_1(g_i)) + (\eta_1(g_i) - \xi_1(g_i))|}{2} \le \frac{|\omega(g_i)| + |\omega(zg_i)|}{2} \le 1.$$

Similarly,

$$|\eta_j(g_i)| \le 1,\ |\xi_j(g_i)| \le 1,\ \forall i,j = 1,2. \tag{5.2}$$

It follows that

$$\sum_{\chi \in \mathrm{Irr}(G),\ 1<\chi(1)<D} \frac{|\chi(g_1)\chi(g_2)\overline{\chi}(g)|}{\chi(1)} \le \frac{4 \cdot (2q^n)^{1/2}}{(q^n-1)/2} < 0.24.$$

Together with (5.1), this implies that

$$\sum_{\chi \in \mathrm{Irr}(G),\ \chi(1)>1} \frac{|\chi(g_1)\chi(g_2)\overline{\chi}(g)|}{\chi(1)} < 0.54 + 0.24 = 0.78,$$

whence $g \in g_1^G \cdot g_2^G$. Since both g_1 and g_2 are N'-elements, we are done.

(b) Next we consider the case $n \ge 3$ odd. Here we choose

$$D = \begin{cases} (q^{2n}-1)(q^{n-1}-q)/2(q^2-1), & n \ge 5, \\ q^4(q^3-1)(q-1)/2, & n = 3, \end{cases}$$

so

$$\sum_{\chi \in \mathrm{Irr}(G),\ \chi(1)\ge D} \frac{|\chi(g_1)\chi(g_2)\overline{\chi}(g)|}{\chi(1)} \le \frac{(q^{n-1}+1)(q+1)(q^{2n-1}(q^2-1))^{1/2}}{D} < 0.15. \tag{5.3}$$

Using [50, Theorem 1.1] for $n \ge 7$ and [41] for $n = 5$, we show that every non-principal irreducible character of G of degree less than D is one of the following:

(b1) four irreducible Weil characters $\eta_{1,2}$, $\xi_{1,2}$ as above;

(b2) four unipotent characters α_ν, β_ν, $\nu = \pm$, of degree

$$\alpha_\nu(1) = \frac{(q^n-\nu)(q^n+\nu q)}{2(q-1)},\ \beta_\nu(1) = \frac{(q^n+\nu)(q^n+\nu q)}{2(q+1)};$$

(b3) two characters of degree $(q^{2n}-1)/2(q+1)$, two of degree $(q^{2n}-1)/2(q-1)$, $(q-1)/2$ of degree $(q^{2n}-1)/(q+1)$, and $(q-3)/2$ of degree $(q^{2n}-1)/2(q-1)$.

Note that $\mathcal{R}(G)$ consists of two primes and contains t; denote $\mathcal{R}(G) \setminus \{t\} =: \{s\}$. Since $t \in \mathcal{R}(G)$, there is an $\epsilon = \pm$ such that $t|(q^n - \epsilon)$. Now, we choose a regular semisimple element g_1 of order s and take $g_2 := \mathrm{diag}(x_-, y_\epsilon)$ of order $(q-\epsilon)s_-$. In particular, $|\mathbf{C}_G(g_i)| \le (q^{n-1}+1)(q+1)$. If $n = 3$, then we check using [41] that the characters $\chi \in \mathrm{Irr}(G)$ with $1 < \chi(1) < D$ and such that χ has positive s-defect and positive s_--defect are described in (b1) and (b2). Thus, in all cases, in considering characters χ of G of degree less than D and computing $\chi(g_1)\chi(g_2)$ we can restrict to the ones in (b1)–(b3).

Note that all characters in (b3) have s-defect 0, so vanish at g_1. Next, β_ϵ and $\alpha_{-\epsilon}$ have s-defect 0, whence

$$\beta_\epsilon(g_1) = \alpha_{-\epsilon}(g_1) = 0.$$

Likewise, β_+ and α_+ have s_--defect 0, whence

$$\beta_+(g_2) = \alpha_+(g_2) = 0.$$

Consider the case $\epsilon = -$. We have shown that $\chi(g_1)\chi(g_2) = 0$ for $\chi = \alpha_+, \beta_+, \beta_-$, and

$$\alpha_+(g_1) = \alpha_+(g_2) = 0.$$

On the other hand, $\rho := 1_G + \alpha_+ + \alpha_-$ is just the permutation character of the action of G on the set of 1-spaces of V, cf. [56, Table 2]. The choice of g_i ensures that $\rho(g_i) = 0$, whence

$$\alpha_-(g_1) = \alpha_-(g_2) = -1.$$

Assume now that $\epsilon = +$. We have shown that $\chi(g_1)\chi(g_2) = 0$ for $\chi = \alpha_+, \beta_+, \alpha_-$, and

$$\beta_+(g_1) = \beta_+(g_2) = 0.$$

On the other hand, as shown in [61], $\zeta := \beta_+ + \beta_-$ is just the restriction to G of the character $\zeta_{0,0}$ of $\mathrm{GU}_{2n}(q)$ as defined in (4.4) when we embed

$$G = \mathrm{Sp}_{2n}(q) \hookrightarrow \mathrm{SU}_{2n}(q) \lhd \mathrm{GU}_{2n}(q).$$

The choice of g_i ensures that $\zeta(g_i) = 0$, whence

$$\beta_-(g_1) = \beta_-(g_2) = -1.$$

The same arguments as in (a) show that (5.2) holds in this case as well. Observe that, for $\mu = \pm 1$, $U_\mu := \mathrm{Ker}(g - \mu \cdot 1_V)$ has dimension at most n, as otherwise it cannot be totally isotropic, so g acts as the multiplication by μ on a 2-dimensional non-degenerate subspace of U, contrary to the assumption that g is unbreakable. Using [23, Lemma 2.4], we see that

$$|\omega(g)|,\ |\omega(zg)| \le q^{n/2},$$

so, arguing as in the above proof of (5.2), we obtain

$$|\eta_i(g)|,\ |\xi_i(g)| \le q^{n/2}.$$

Certainly, $|\gamma(g)| \le |\mathbf{C}_G(g)|^{1/2} \le (q^{2n-1}(q^2-1))^{1/2}$ for $\gamma = \alpha_-, \beta_-$. In summary,

$$\sum_{\chi \in \mathrm{Irr}(G),\ 1<\chi(1)<D} \frac{|\chi(g_1)\chi(g_2)\overline{\chi}(g)|}{\chi(1)} \le \frac{4 \cdot q^{n/2}}{(q^n-1)/2} + \frac{(q^{2n-1}(q^2-1))^{1/2}}{(q^n-1)(q^n-q)/2(q-1)} < 0.53.$$

Together with (5.3), this implies that

$$\sum_{\chi \in \mathrm{Irr}(G),\ \chi(1)>1} \frac{|\chi(g_1)\chi(g_2)\overline{\chi}(g)|}{\chi(1)} < 0.15 + 0.53 = 0.68,$$

whence $g \in g_1^G \cdot g_2^G$. Since both g_1 and g_2 are N'-elements, we are done. ∎

To handle the symplectic groups over $\mathbb{F}_3$, we need an explicit description of low-degree complex characters of $\mathrm{Sp}_{2n}(3)$.

Lemma 5.6. *Let $G = \mathrm{Sp}_{2n}(3)$ with $n \ge 6$ and let $D := (3^{2n}-1)(3^{n-1}-3)/16$. Then*

$$\{\chi \in \mathrm{Irr}(G) \mid 1 < \chi(1) < D\}$$

consists of the following 13 characters:

(i) *four irreducible Weil characters η, $\bar\eta$ of degree $(3^n-1)/2$, ξ, $\bar\xi$ of degree $(3^n+1)/2$;*

(ii) *four characters $\mathsf{S}^2(\xi)$, $\wedge^2(\eta)$, $\xi\bar\xi - 1_G$, and $\eta\bar\eta - 1_G$, of respective degree*

$$\frac{(3^n+1)(3^n+3)}{8},\ \frac{(3^n-1)(3^n-3)}{8},\ \frac{(3^n-1)(3^n+3)}{4},\ \frac{(3^n+1)(3^n-3)}{4};$$

(iii) *two characters $\mathsf{S}^2(\eta)$, $\wedge^2(\xi)$ of degree $(3^{2n}-1)/8$, and three characters $\xi\bar\eta$, $\bar\xi\eta$, $\xi\eta = \bar\xi\bar\eta$ of degree $(3^{2n}-1)/4$.*

Also, $\mathsf{S}^2(\eta) = \bar{\wedge}^2(\xi)$.

Proof. Applying [50, Theorem 1.1], we deduce that the degrees, and the multiplicity for each degree of non-principal irreducible character of G of degree less than D are as listed above. The proof of [45, Proposition 5.4] shows that the six characters $\mathsf{S}^2(\xi)$, $\wedge^2(\eta)$, $\xi\bar{\xi} - 1_G$, $\eta\bar{\eta} - 1_G$, $\mathsf{S}^2(\eta)$, and $\wedge^2(\xi)$ have the degrees listed in (ii) and (iii). It also shows that $\xi\bar{\eta}$ and $\bar{\xi}\eta$ are two distinct irreducible constituents (of a certain real character τ) of degree $(3^{2n}-1)/4$, so they are non-real. On the other hand, $\xi\eta$ is the unique irreducible constituent of degree $(3^{2n}-1)/4$ of a certain real character σ, whence it must be real. We have therefore identified the three characters of degree $(3^{2n}-1)/4$. Finally,

$$[\mathsf{S}^2(\eta) + \wedge^2(\eta), \bar{\mathsf{S}^2}(\xi) + \bar{\wedge}^2(\xi)] = [\eta^2, \bar{\xi}^2] = [\xi\eta, \bar{\xi}\bar{\eta}] = 1,$$

so $\mathsf{S}^2(\eta) = \bar{\wedge}^2(\xi)$, since the involved characters are all irreducible, and only $\mathsf{S}^2(\eta)$ and $\bar{\wedge}^2(\xi)$ have equal degree. ∎

Proposition 5.7. *Suppose* $G = \mathrm{Sp}_{2n}(3)$ *with* $n \geq 6$, *and* $t \in \mathcal{R}(G)$. *Then* $\mathsf{P}_u(N)$ *holds for* G *and for every* $N = 3^a t^b$.

Proof. (i) Consider an unbreakable $g \in G$; in particular,

$$|\mathbf{C}_G(g)| \leq 16 \cdot 3^{2n+2} \tag{5.4}$$

by Lemma 3.2. Let $V = \mathbb{F}_3^{2n}$ denote the natural module for G. Inside $\mathrm{Sp}_{2n-2}(3)$ we can find a regular semisimple element x_- of order $s_- = \ell(3, 2n-2)$ and a regular semisimple element x_+ of order $s_+ = \ell(3, n-1)$. We fix $y \in \mathrm{Sp}_2(3)$ of order 4. If n is even, we set

$$g_1 := \mathrm{diag}(x_+, y),\ g_2 := \mathrm{diag}(x_-, y),$$

whereas for odd n, we choose a regular semisimple $g_1 \in G$ of order $s \in \mathcal{R}(G) \setminus \{t\}$ and set $g_2 := \mathrm{diag}(x_-, y)$. In particular, g_i is an N'-element and $|\mathbf{C}_G(g_i)| \leq 4 \cdot (3^{n-1}+1)$ for $i = 1, 2$. We also choose

$$D = \frac{(3^{2n}-1)(3^{n-1}-3)}{16}.$$

Then the characters $\chi \in \mathrm{Irr}(G)$ with $1 < \chi(1) < D$ are described in Lemma 5.6.

The choice of g_i implies that $\mathrm{Ker}(g_i \pm 1_V) = 0$. Hence, as in the proof of Proposition 5.5,

$$|\chi(g_i)| \leq 1,\ \forall \chi \in \{\xi, \eta\}. \tag{5.5}$$

On the other hand, $\dim_{\mathbb{F}_3} \mathrm{Ker}(g \pm 1_V) \leq 4$ by Lemma 3.4. Arguing as in part (a) of the proof of Proposition 5.5, we obtain

$$|\chi(g)| \leq 3^2,\ \forall \chi \in \{\xi, \eta\}. \tag{5.6}$$

It follows that

$$\sum_{\chi \in \{\xi, \bar{\xi}, \eta, \bar{\eta}\}} \frac{|\chi(g_1)\chi(g_2)\overline{\chi}(g)|}{\chi(1)} \leq \frac{4 \cdot 3^2}{(3^n-1)/2} < 0.099. \tag{5.7}$$

Let $\mathcal{X}$ denote the set of nine characters listed in Lemma 5.6(ii), (iii). Observe that x_ν has prime order s_ν for $\nu = \pm$. Hence

$$\mathrm{Ker}(g_i^2 - 1_V) = 0,\ \dim_{\mathbb{F}_3} \mathrm{Ker}(g_i^2 + 1_V) \leq 2.$$

This in turn implies that

$$|\omega(g_i^2)| \leq 1,\ |\omega(z g_i^2)| \leq 3$$

for the reducible Weil character $\omega = \xi + \eta$ and the central involution $z \in G$. Arguing as in part (a) of the proof of Proposition 5.5, we obtain

$$|\chi(g_i^2)| \leq (1+3)/2 = 2,\ \forall \chi \in \{\xi, \eta\}.$$

Together with (5.5), this implies that

$$|\chi(g_i)| \le 3/2,\ \forall \chi \in \mathcal{X}. \tag{5.8}$$

(ii) Here we assume that $n \ge 7$. If $2|n$, then the four characters listed in Lemma 5.6 have either s_+-defect 0, or s_--defect 0. If $2 \nmid n$, then the five characters listed in Lemma 5.6 have s-defect 0. Thus, at most five characters from $\mathcal{X}$ can be nonzero at both g_1 and g_2. Also, $|\chi(g)| \le 4 \cdot 3^{n+1}$ for all $\chi \in \mathrm{Irr}(G)$ by (5.4). Using (5.8), we see that

$$\sum_{\chi \in \mathcal{X}} \frac{|\chi(g_1)\chi(g_2)\overline{\chi}(g)|}{\chi(1)} \le \frac{5 \cdot (3/2)^2 \cdot 4 \cdot 3^{n+1}}{(3^n-1)(3^n-3)/8} < 0.495.$$

On the other hand,

$$\sum_{\chi \in \mathrm{Irr}(G),\ \chi(1) \ge D} \frac{|\chi(g_1)\chi(g_2)\overline{\chi}(g)|}{\chi(1)} \le \frac{4(3^{n-1}+1) \cdot 4 \cdot 3^{n+1})}{D} < 0.354.$$

Together with (5.7), these estimates imply that

$$\sum_{\chi \in \mathrm{Irr}(G),\ \chi(1) > 1} \frac{|\chi(g_1)\chi(g_2)\overline{\chi}(g)|}{\chi(1)} < 0.099 + 0.495 + 0.354 = 0.948,$$

whence $g \in g_1^G \cdot g_2^G$. Since both g_1 and g_2 are N'-elements, we are done.

(iii) We may now assume that $n = 6$. In this case $\mathcal{R}(G) = \{7, 13, 73\}$ and $|g_1| = 44$, $|g_2| = 244$. Using [41], we check that G has exactly 30 irreducible characters χ that have both positive 11-defect and positive 41-defect: namely, 1_G, four Weil characters, five characters from $\mathcal{X}$ and listed in Lemma 5.6(iii), four characters $\psi_{1,2,3,4}$ with two of each of the degrees

$$D = 15 \cdot (3^{12}-1),\ D_1 := 15 \cdot (3^4+1) \cdot (3^8+3^4+1),$$

and 16 more, of degree larger than $D_2 := 3^{19}$. In particular,

$$\sum_{\chi \in \mathrm{Irr}(G),\ \chi(1) \ge D_2} \frac{|\chi(g_1)\chi(g_2)\overline{\chi}(g)|}{\chi(1)} \le \frac{4 \cdot (3^{n-1}+1) \cdot 4 \cdot 3^{n+1}}{D_2} < 0.0074. \tag{5.9}$$

Next we strengthen the bound on $|\chi(g)|$ for $\chi \in \mathcal{X}$. Consider $\lambda = \pm 1$ and write $g = uv = vu$, with u unipotent and v semisimple. Let $\tilde{V} := V \otimes_{\mathbb{F}_3} \overline{\mathbb{F}}_3$. Note that if $w \in U_\lambda := \mathrm{Ker}(g^2 - \lambda \cdot 1_{\tilde{V}})$, then w belongs to $W_\mu := \mathrm{Ker}(v - \mu \cdot 1_{\tilde{V}})$ for some μ with $\mu^2 = \lambda$. Now g^2 acts on W_μ as $\lambda u'^2$, where $u' := u_{W_\mu}$ is unipotent. Next, observe that

$$\dim_{\overline{\mathbb{F}}_3} \mathrm{Ker}(u'^2 - 1_{W_\mu}) = \dim_{\overline{\mathbb{F}}_3} \mathrm{Ker}(u' - 1_{W_\mu}).$$

It then follows from Lemma 3.4 that

$$\dim_{\overline{\mathbb{F}}_3} U_\lambda = \dim_{\overline{\mathbb{F}}_3} \mathrm{Ker}(g - \mu_0 \cdot 1_{\tilde{V}}) + \dim_{\overline{\mathbb{F}}_3} \mathrm{Ker}(g + \mu_0 \cdot 1_{\tilde{V}}) \le 8,$$

where μ_0 is a fixed square root μ_0 of λ. In turn, this implies by [23, Lemma 2.4] that

$$|\omega(g^2)|,\ |\omega(zg^2)| \le 3^4.$$

Arguing as in part (a) of the proof of Proposition 5.5, we obtain

$$|\chi(g^2)| \le 3^4,\ \forall \chi \in \{\xi, \eta\}.$$

Using this bound and (5.6), we see that

$$|\chi(g)| \le 3^4,\ \forall \chi \in \mathcal{X}.$$

Since only five characters from $\mathcal{X}$ can be nonzero at both g_1 and g_2, this last estimate together with (5.8) yields

$$\sum_{\chi\in\mathcal{X}}\frac{|\chi(g_1)\chi(g_2)\overline{\chi}(g)|}{\chi(1)}\le\frac{5\cdot(3/2)^2\cdot 3^4}{(3^{2n}-1)/8}<0.0138. \tag{5.10}$$

Finally, we estimate character ratios for the four characters $\psi_{1,2,3,4}$ of degree D and D_1. Since $|g_2|=4\cdot 61$, $\chi(g)=0$ if and only if $\chi\in\mathrm{Irr}(G)$ has degree divisible by 61. Using [41], we check that

$$\mathrm{Irr}_{61'}(G):=\{\chi\in\mathrm{Irr}(G)\mid 61\nmid\chi(1)\}$$

consists of exactly 343 characters. (Another way to check it is to observe that since $P\in\mathrm{Syl}_{61}(G)$ is cyclic, the *McKay conjecture* holds for G, i.e.

$$|\mathrm{Irr}_{61'}(G)|=|\mathrm{Irr}_{61'}(\mathbf{N}_G(P))|.$$

Direct computation shows that

$$\mathbf{N}_G(P)=(C_{244}\rtimes C_{10})\times\mathrm{Sp}_2(3)$$

has exactly 343 irreducible characters of degree coprime to 61.) Certainly,

$$\mathrm{Irr}_{61'}(G)\setminus\{\psi_{1,2,3,4}\}$$

is a union of some $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-orbits. Hence, by Lemma 2.11,

$$\sum_{\chi\in\mathrm{Irr}(G)\setminus\{\psi_{1,2,3,4}\}}|\chi(g_2)|^2=\sum_{\chi\in\mathrm{Irr}_{61'}(G)\setminus\{\psi_{1,2,3,4}\}}|\chi(g_2)|^2\ge|\mathrm{Irr}_{61'}(G)\setminus\{\psi_{1,2,3,4}\}|=343-4=339.$$

Since $\sum_{\chi\in\mathrm{Irr}(G)}|\chi(g_2)|^2=|\mathbf{C}_G(g_2)|=4\cdot(3^5+1)=976$,

$$\sum_{j=1}^{4}|\psi_j(g_2)|^2\le 976-339=637.$$

Recall that $|\psi_j(g)|\le 4\cdot 3^7$ by (5.4) and $|\psi_j(g_1)|^2\le|\mathbf{C}_G(g_1)|=4\cdot(3^5-1)=968$. By the Cauchy-Schwarz inequality,

$$\sum_{j=1}^{4}\frac{|\psi_j(g_1)\psi_j(g_2)\overline{\psi}_j(g)|}{\psi_j(1)}\le\frac{4\cdot 3^7\cdot 968^{1/2}}{D}\cdot(\sum_{j=1}^{4}|\psi_j(g_2)|^2)^{1/2}=\frac{4\cdot 3^7\cdot(968\cdot 637)^{1/2}}{15\cdot(3^{12}-1)}<0.8618.$$

Together with (5.7), (5.9), (5.10), this implies that

$$\sum_{\chi\in\mathrm{Irr}(G),\ \chi(1)>1}\frac{|\chi(g_1)\chi(g_2)\overline{\chi}(g)|}{\chi(1)}<0.099+0.0138+0.8618+0.0074=0.982,$$

whence $g\in g_1^G\cdot g_2^G$. Since both g_1 and g_2 are N'-elements, we are again done. ∎

Proposition 5.8. *Suppose $G=\mathrm{Sp}_{2n}(q)$ with $n\ge 3$, $2|q$, and $t\in\mathcal{R}(G)$. Assume that $n\ge 4$ if $q=4$, and $n\ge 7$ if $q=2$. Then $\mathsf{P}_u(N)$ holds for G and for every $N=2^at^b$.*

Proof. Consider an unbreakable $g\in G$; in particular,

$$|\mathbf{C}_G(g)|\le B:=\begin{cases}q^{2n}(q^2-1), & 2|n,q\ge 4\\ 2q^{2n}(q+1), & 2\nmid n,q\ge 4\\ 9\cdot q^{2n+9}, & q=2\end{cases}$$

by Lemma 3.2. Let $V=\overline{\mathbb{F}}_q^{2n}$ denote the natural module for G. Inside $\mathrm{Sp}_{2n-2}(q)$ we can find a regular semisimple element x_- of order $s_-=\ell(q,2n-2)$, and, if $2|n$, a regular semisimple element x_+ of order $s_+=\ell(q,n-1)$. We fix $y\in\mathrm{Sp}_2(q)$ of order $q+1$. Let $\mathcal{W}$ denote the set of $q+3$ Weil characters

$$\alpha_n,\ \beta_n,\ \rho_n^1,\ \rho_n^2,\ \zeta_n^i,\ 1\le i\le q/2,\ \tau_n^j,\ 1\le j\le q/2-1$$

(as described in [23, Table 1]). Assuming $n \geq 4$ and choosing

$$D := \frac{(q^{2n}-1)(q^{n-1}-1)(q^{n-1}-q^2)}{2(q^4-1)},$$

we see by [23, Corollary 6.2] that $\mathcal{W}$ is precisely the set $\{\chi \in \mathrm{Irr}(G) \mid 1 < \chi(1) < D\}$.

(i) Here we consider the case $2|n$, and set

$$g_1 := \mathrm{diag}(x_+, y),\ g_2 := \mathrm{diag}(x_-, y)$$

so that each g_i is an N'-element and $|\mathbf{C}_G(g_i)| \leq (q^{n-1}+1)(q+1)$. In particular,

$$\sum_{\substack{\chi \in \mathrm{Irr}(G),\\ \chi(1) \geq D}} \frac{|\chi(g_1)\chi(g_2)\overline{\chi}(g)|}{\chi(1)} \leq \frac{(q^{n-1}+1)(q+1)\cdot B^{1/2}}{D} < \begin{cases} 0.8293, & n=4 \\ 0.1956, & n \geq 6. \end{cases} \tag{5.11}$$

If $\chi \in \{\alpha_n, \beta_n, \rho_n^1, \rho_n^2\}$ then χ has s_ν-defect 0 for some $\nu = \pm$, so $\chi(g_1)\chi(g_2) = 0$. For $\gamma \in \overline{\mathbb{F}}_q^\times$, the choice of g_i implies that $\dim_{\overline{\mathbb{F}}_q} \mathrm{Ker}(g_i - \gamma \cdot 1_V)$ equals 0 if $\gamma^{q-1} = 1$, and is at most 1 if $\gamma^{q+1} = 1$; in fact, it equals 1 for exactly two primitive $(q+1)$th roots of unity in $\overline{\mathbb{F}}_q^\times$. Hence, by formulae (1) and (4) of [23],

$$|\tau_n^j(g_i)| = 0,\ |\zeta_n^j(g_i)| \leq b,$$

where $b := 2$ if $q \geq 4$ and $b := 1$ if $q = 2$. For $n \geq 6$, it follows that

$$\sum_{\chi \in \mathrm{Irr}(G),\ 1<\chi(1)<D} \frac{|\chi(g_1)\chi(g_2)\overline{\chi}(g)|}{\chi(1)} \leq \frac{q}{2} \cdot \frac{b^2 \cdot (q^{2n}(q^2-1))^{1/2}}{(q^{2n}-1)/(q+1)} < 0.7956.$$

Suppose that $n = 4$ and $q \geq 4$. Observe that $\dim_{\overline{\mathbb{F}}_q} \mathrm{Ker}(g_i - \gamma \cdot 1_V) \leq 4$ for $\gamma \in \overline{\mathbb{F}}_q^\times$ with $\gamma^{q+1} = 1$. (Indeed, this bound is obvious if $\gamma \neq 1$. If $\gamma = 1$, it follows from the condition that g is unbreakable.) Hence, formula (4) of [23] implies that $|\zeta_n^j(g)| \leq q^4$, so

$$\sum_{\chi \in \mathrm{Irr}(G),\ 1<\chi(1)<D} \frac{|\chi(g_1)\chi(g_2)\overline{\chi}(g)|}{\chi(1)} \leq \frac{q}{2} \cdot \frac{b^2 \cdot q^4}{(q^8-1)/(q+1)} < 0.1564.$$

Together with (5.11), this implies that

$$\sum_{\chi \in \mathrm{Irr}(G),\ \chi(1)>1} \frac{|\chi(g_1)\chi(g_2)\overline{\chi}(g)|}{\chi(1)} < \begin{cases} 0.8293 + 0.1564 = 0.9857, & n=4 \\ 0.1956 + 0.7956 = 0.9912, & n \geq 6 \end{cases}$$

whence $g \in g_1^G \cdot g_2^G$. Since both g_1 and g_2 are N'-elements, we are done.

(ii) From now on we assume $2 \nmid n$. By Proposition 2.10 we may assume that $n \geq 5$. We choose a regular semisimple element g_1 of order $s \in \mathcal{R}(G) \smallsetminus \{t\}$ and take $g_2 := \mathrm{diag}(x_-, y)$. In particular, again $|\mathbf{C}_G(g_i)| \leq (q^{n-1}+1)(q+1)$. Note that all characters ζ_n^j and τ_n^j have s-defect 0, so vanish at g_1. Next, the choice of g_i implies that, for $\gamma \in \overline{\mathbb{F}}_q^\times$, $\dim_{\overline{\mathbb{F}}_q} \mathrm{Ker}(g_i - \gamma \cdot 1_V)$ equals 0 if $\gamma^{q-1} = 1$, and is at most 1 if $\gamma^{q+1} = 1$; in fact, it equals 1 for exactly two primitive $(q+1)$th roots of unity in $\overline{\mathbb{F}}_q^\times$. Using formulae (1), (3), (4), and (6) of [23], we obtain

$$(\rho_n^1 + \rho_n^2)(g_i) = -1,\ (\alpha_n + \beta_n)(g_1) = 1,\ (\alpha_n + \beta_n)(g_2) = -1.$$

Furthermore, exactly one character among α_n, β_n, and exactly one character among ρ_n^1, ρ_n^2, have s-defect zero. It follows that

$$|\chi(g_1)| \leq 1,\ \forall \chi \in \{\alpha_n, \beta_n, \rho_n^1, \rho_n^2\}.$$

Likewise, β_n and ρ_n^2 have s_--defect 0, so

$$\beta_n(g_2) = \rho_n^2(g_2) = 0,\ |\alpha_n(g_2)| = |\rho_n^1(g_2)| = 1.$$

We also observe that $\alpha_n(g_1) = 0$ if $s|(q^n-1)$ and $\rho_n^1(g_1) = 0$ if $s|(q^n+1)$. We have shown that, among the characters in $\mathcal{W}$, exactly one character can be nonzero at both g_1 and g_2. Denoting this character by ψ,

$$|\psi(g)|/\psi(1) \le 0.95,\ |\psi(g)| \le B^{1/2},\ |\psi(g_i)| \le 1. \tag{5.12}$$

Here, the first bound follows from the main result of [16].

(iii) Assume in addition that $n \ge 9$ if $q = 2$. Now

$$\sum_{\chi\in\mathrm{Irr}(G),\ 1<\chi(1)<D} \frac{|\chi(g_1)\chi(g_2)\overline{\chi}(g)|}{\chi(1)} \le \frac{B^{1/2}}{(q^n-1)(q^n-q)/2(q+1)} < 0.8003.$$

On the other hand,

$$\sum_{\chi\in\mathrm{Irr}(G),\ \chi(1)\ge D} \frac{|\chi(g_1)\chi(g_2)\overline{\chi}(g)|}{\chi(1)} \le \frac{(q^{n-1}+1)(q+1)\cdot B^{1/2}}{D} < 0.0478.$$

It follows that

$$\sum_{\chi\in\mathrm{Irr}(G),\ \chi(1)>1} \frac{|\chi(g_1)\chi(g_2)\overline{\chi}(g)|}{\chi(1)} < 0.8003 + 0.0478 = 0.8481,$$

whence $g \in g_1^G \cdot g_2^G$. Since both g_1 and g_2 are N'-elements, we are done.

(iv) Now we consider the case $(n,q) = (7,2)$ and choose

$$D_1 := \frac{q^{35}(q^7-1)(q^7-q)}{2(q+1)}.$$

Using [41], we check that there is only one character $\chi \in \mathrm{Irr}(G)$ with $1 < \chi(1) < D_1$ that has both positive s-defect and s_--defect, namely the character ψ described in (ii). Now using (5.12)

$$\sum_{\chi\in\mathrm{Irr}(G),\ 1<\chi(1)<D_1} \frac{|\chi(g_1)\chi(g_2)\overline{\chi}(g)|}{\chi(1)} \le \frac{|\psi(g)|}{\psi(1)} < 0.95.$$

On the other hand,

$$\sum_{\chi\in\mathrm{Irr}(G),\ \chi(1)\ge D_1} \frac{|\chi(g_1)\chi(g_2)\overline{\chi}(g)|}{\chi(1)} \le \frac{(q^6+1)(q+1)\cdot B^{1/2}}{D_1} < 0.01.$$

It follows that

$$\sum_{\chi\in\mathrm{Irr}(G),\ \chi(1)>1} \frac{|\chi(g_1)\chi(g_2)\overline{\chi}(g)|}{\chi(1)} < 0.95 + 0.01 = 0.96,$$

and we are done again. ∎

5.4. **Induction step: Orthogonal groups.**

Proposition 5.9. *Suppose $G = \Omega_{2n+1}(q)$ with $n \ge 3$, $q = p^f$ odd, and $t \in \mathcal{R}(G)$. Assume that $n \ge 6$ if $q = 3$. Then $\mathsf{P}_u(N)$ holds for G and for every $N = p^a t^b$.*

Proof. By Corollary 2.9 and Proposition 2.10, we may assume that $q = 3$ and $n \ge 6$. Let $V = \overline{\mathbb{F}}_q^{2n+1}$ denote the natural module for G, and let

$$F_0 := \{\gamma \in \overline{\mathbb{F}}_q^\times \mid \gamma^{q\pm1} = 1\}.$$

Consider an unbreakable $g \in G$; in particular, $|\mathbf{C}_G(g)| \le B := 2^4 \cdot q^{2n+3}$ by Lemma 3.3. Let $\mathcal{X}$ denote the set of $q+4$ characters described in [34, Proposition 5.7]: each is of the form D_α° for $\alpha \in \mathrm{Irr}(S)$ and $S := \mathrm{Sp}_2(q)$. Choosing

$$D := q^{4n-8},$$

we see by [34, Corollary 5.8] that $\mathcal{X}$ is precisely the set $\{\chi \in \mathrm{Irr}(G) \mid 1 < \chi(1) < D\}$. If $\gamma \in F_0$, then

$$\dim_{\overline{\mathbb{F}}_q} \mathrm{Ker}(g - \gamma \cdot 1_V) \leq 4$$

by Lemma 3.4. Following the proof of [34, Proposition 5.11], one can show that

$$|D_\alpha(g)| \leq q^4 \cdot \alpha(1). \tag{5.13}$$

Now we choose $g_1 = g_2$ to be a regular semisimple element of order $s \in \mathcal{R}(G) \smallsetminus \{t\}$, so that g_i is an N'-element and $|\mathbf{C}_G(g_i)| \leq (q^{n-1}+1)(q+1)$. In particular,

$$\sum_{\substack{\chi \in \mathrm{Irr}(G),\\ \chi(1) \geq D}} \frac{|\chi(g_1)\chi(g_2)\overline{\chi}(g)|}{\chi(1)} \leq \frac{(q^{n-1}+1)(q+1)\cdot B^{1/2}}{D} < 0.35. \tag{5.14}$$

The choice of g_i implies that

$$\dim_{\overline{\mathbb{F}}_q} \mathrm{Ker}(g - \gamma \cdot 1_V) \leq 1$$

for all $\gamma \in F_0$. Following the proof of [34, Proposition 5.11], one can show that

$$|D_\alpha(g)| \leq q \cdot \alpha(1). \tag{5.15}$$

In the notation of [34, Table I], if $\alpha \neq \xi_{1,2}$, then $D^\circ_\alpha = D_\alpha$. In this case, it follows from (5.13) and (5.15) for $\chi = D^\circ_\alpha$ that

$$\frac{|\chi(g_1)\chi(g_2)\overline{\chi}(g)|}{\chi(1)} \leq \frac{q^6 \cdot \alpha(1)^3}{\chi(1)} < (1.1)\frac{q^6 \cdot \alpha(1)^2}{(q^{2n}-1)/(q^2-1)}.$$

In the case $\alpha = \xi_{1,2}$ (of degree $(q+1)/2$), for $\chi = D^\circ_\alpha = D_\alpha - 1_G$,

$$\frac{|\chi(g_1)\chi(g_2)\overline{\chi}(g)|}{\chi(1)} \leq \frac{(q^4\alpha(1)+1)(q\alpha(1)+1)^2}{\chi(1)} < (1.4)\frac{q^6 \cdot \alpha(1)^2}{(q^{2n}-1)/(q^2-1)}.$$

It follows that

$$\begin{aligned}\textstyle\sum_{\chi \in \mathrm{Irr}(G),\ 1<\chi(1)<D} \frac{|\chi(g_1)\chi(g_2)\overline{\chi}(g)|}{\chi(1)} &\leq (1.4)\frac{q^6}{(q^{2n}-1)/(q^2-1)} \cdot \textstyle\sum_{\alpha \in \mathrm{Irr}(S)} \alpha(1)^2 \\ &= (1.4)\frac{q^6 \cdot q(q^2-1)}{(q^{2n}-1)/(q^2-1)} < 0.26.\end{aligned}$$

Together with (5.14), this implies that

$$\sum_{\chi \in \mathrm{Irr}(G),\ \chi(1)>1} \frac{|\chi(g_1)\chi(g_2)\overline{\chi}(g)|}{\chi(1)} < 0.35 + 0.26 = 0.61.$$

whence $g \in g_1^G \cdot g_2^G$. Since both g_1 and g_2 are N'-elements, we are done. ∎

Proposition 5.10. *Suppose $G = \Omega^\epsilon_{2n}(q)$ and $q = 2, 4$, $\epsilon = \pm$, and $t \in \mathcal{R}(G)$. Assume that $n \geq 5$ if $q = 4$, and $n \geq 7$ if $q = 2$. Then $\mathsf{P}_u(N)$ holds for G and for every $N = 2^a t^b$.*

Proof. (i) Consider an unbreakable $g \in G$; in particular,

$$|\mathbf{C}_G(g)| \leq B := \begin{cases} 3 \cdot q^{2n+6}, & q = 2 \\ 25 \cdot q^{2n-2}, & q = 4 \end{cases}$$

by Lemma 3.3. We also choose

$$D := \begin{cases} q^{4n-10}, & n \geq 6, (n,q) \neq (7,2), \\ q^{4n-8}, & (n,q) = (7,2), \\ q^3(q^3-1)(q^5-1)(q-1)^2/2, & n = 5, q = 4. \end{cases}$$

Consider the prime $s \in \mathcal{R}(G) \setminus \{t\}$. If $s|(q^{n-1}+1)$ with $q = 2$ and $\epsilon = +$, then we choose $g_1 = \mathrm{diag}(x_1, y_1)$, where $x_1 \in \Omega^-_{2n-2}(q)$ is regular semisimple of order s and $y_1 \in \Omega^-_2(q)$ has order $q+1$. In all other cases, we choose a regular semisimple $g_1 \in G$ of order s.

If $s|(q^{n-1}+1)$ and $(n, q, \epsilon) = (7, 2, +)$, then choose $g_2 := \mathrm{diag}(x_2, y_2)$, where $x_2 \in \Omega^-_{2n-4}(q)$ is regular semisimple of order $s_\epsilon = \ell(q, 2n-4) = 11$, and $y_2 \in \Omega^-_4(q)$ of order $\ell(q, 4) = 5$. In all other cases, let $g_2 := g_1$.

Our choices of g_i imply that each g_i is an N'-element, and $|\mathbf{C}_G(g_i)| \le (q+1)(q^{n-1}+1)$. It follows that

$$\sum_{\substack{\chi \in \mathrm{Irr}(G),\\ \chi(1) \ge D}} \frac{|\chi(g_1)\chi(g_2)\overline{\chi}(g)|}{\chi(1)} \le \frac{(q^{n-1}+1)(q+1)\cdot B^{1/2}}{D} < \begin{cases} 0.10, & n \ge 5, q = 4 \\ 0.33, & n \ge 7, q = 2. \end{cases} \tag{5.16}$$

(ii) Now we estimate character values for the characters in

$$\mathcal{X} := \{\chi \in \mathrm{Irr}(G) \mid 1 < \chi(1) < D\}.$$

By [50, Theorem 1.3], when $n \ge 6$ and $(n, q) \ne (7, 2)$ the set $\mathcal{X}$ consists of $q+1$ characters:

- φ of degree $(q^n - \epsilon)(q^{n-1} + \epsilon q)/(q^2-1)$,
- ψ of degree $(q^{2n} - q^2)/(q^2-1)$,
- ζ_i of degree $(q^n - \epsilon)(q^{n-1} - \epsilon)/(q+1)$ for $1 \le i \le q/2$, and
- σ of degree $(q^n - \epsilon)(q^{n-1} + \epsilon)/(q-1)$ if $q = 4$.

If $(n, q) = (7, 2)$ and $\chi \in \mathcal{X}$ has positive s-defect, then using [41] we show that χ must be one of these $q+1$ characters. Likewise, if $(n, q) = (5, 4)$ and $\chi \in \mathcal{X}$ has positive s-defect and positive s_ϵ-defect, then using [41] we check that χ is again one of these characters.

Let $V = \mathbb{F}_q^{2n}$ denote the natural module for G. Then

$$\rho_0 = 1_G + \varphi + \psi \tag{5.17}$$

is the rank 3 permutation character of the action of G on singular 1-spaces of V, see [56, Table 1]. It is shown in [21] that

$$\rho_0 = 1_G + \psi + \sigma + \sum_{i=1}^{q/2} \zeta_i \tag{5.18}$$

is the permutation character of the action of G on non-singular 1-spaces of V (we use the convention that $\sigma = 0$ for $q = 2$). We can identify G with its dual group G^*, cf. [7]. Then the non-identity elements of the natural subgroup $\Omega^-_2(q)$ of G break into $q/2$ conjugacy classes with representatives t_i, $1 \le i \le q/2$, and

$$\mathbf{C}_G(t_i) = \Omega^{-\epsilon}_{2n-2}(q) \times \Omega^-_2(q).$$

All these semisimple elements have connected centralizer in the underlying algebraic group. Hence, these classes yield $q/2$ semisimple characters in $\mathrm{Irr}(G)$, which can then be identified with ζ_i, $1 \le i \le q/2$. If $q = 4$ then ζ_1 and ζ_2 are Galois conjugate and $\mathbb{Q}(\zeta_i) = \mathbb{Q}(\sqrt{5})$. (Indeed, let ω denote a primitive 5th root of unity in $\mathbb{C}$, so that $\mathbb{Q}(\omega + \omega^{-1}) = \mathbb{Q}(\sqrt{5})$. Let $\gamma : \omega \mapsto \omega^2$ be a generator of $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$. Following the proof of [49, Lemma 9.1], one can show that $\mathbb{Q}(\zeta_i) \subseteq \mathbb{Q}(\omega)$, and γ sends ζ_1 to ζ_2. Moreover, since s_i is real, $\mathbb{Q}(\zeta_i)$ is fixed by $\gamma^2 : \omega \mapsto \omega^{-1}$. It follows that $\mathbb{Q}(\zeta_i) \subseteq \mathbb{Q}(\omega)^{\gamma^2} = \mathbb{Q}(\sqrt{5})$. As ζ_1 and ζ_2 are distinct Galois conjugates, we conclude that $\mathbb{Q}(\zeta_i) = \mathbb{Q}(\sqrt{5}.)$ In particular, since the g_j are chosen to be $5'$-elements, $\zeta_i(g_j) \in \mathbb{Q}$, so

$$\zeta_1(g_i) = \zeta_2(g_i) \tag{5.19}$$

when $q = 4$.

(iii) Here we determine character values for the element g_1 of order s.

Suppose that $s = \ell(q, 2n-2)$. Then ψ has s-defect 0, so $\psi(g_1) = 0$. Similarly, $\sigma(g_1) = 0$ if $\epsilon = +$ and $\zeta_i(g_1) = 0$ if $\epsilon = -$. Next,

$$(\rho_0(g_1), \rho_1(g_1)) = \begin{cases} (0, q+1), & \epsilon = +, q = 4, \\ (0, 0), & \epsilon = +, q = 2, \\ (2, q-1), & \epsilon = -. \end{cases}$$

It follows by (5.17)–(5.19) that

$$\varphi(g_1) = \pm 1, \text{ and } \begin{cases} \zeta_i(g_1) = 2, & \text{if } \epsilon = +, q = 4, \\ \zeta_i(g_1) = -1, & \text{if } \epsilon = +, q = 2, \\ \sigma(g_1) = q-2, & \text{if } \epsilon = -. \end{cases}$$

Suppose that either $s = \ell(q, 2n)$ and $\epsilon = -$, or $s = \ell(q, n)$ with $2 \nmid n$ and $\epsilon = +$. Then φ, ζ_i, and σ all have s-defect 0, so they all vanish at g_1. Also, $\rho_0(g_1) = 0$, so (5.17) implies that $\psi(g_1) = -1$.

The remaining case is that $s = \ell(q, n-1)$, $\epsilon = +$, and $2|n$. Then ψ and ζ_i have s-defect 0, so they vanish at g_1. Also, $\rho_0(g_1) = 2$, so (5.17) implies that $\varphi(g_1) = 1$. Similarly, $\rho_1(g_1) = q-1$, so (5.17) implies that $\sigma(g_1) = q-2$.

(iv) Suppose $n \geq 5$ and $q = 4$. The analysis in (iii) shows that there are at most 3 characters $\chi \in \mathcal{X}$ that can be nonzero at $g_1 = g_2$, in which case $|\chi(g_1)\chi(g_2)| \leq 4$. Also, one character in $\mathcal{X}$ has degree $\geq d := (q^n-1)(q^{n-1}-q)/(q^2-1)$ and all others have degree $\geq 3d$. It follows that

$$\sum_{\chi \in \mathrm{Irr}(G),\ 1<\chi(1)<D} \frac{|\chi(g_1)\chi(g_2)\overline{\chi}(g)|}{\chi(1)} \leq \frac{4 \cdot 5 \cdot q^{n-1}}{(q^n-1)(q^{n-1}-q)/(q^2-1)} \cdot \left(1 + \frac{2}{3}\right) < 0.497.$$

Suppose $n \geq 7$ and $q = 2$. The analysis in (iii) shows that there are at most 2 characters $\chi \in \mathcal{X}$ that can be nonzero at g_1, in which case $|\chi(g_1)| \leq 1$. If $n \geq 8$, then

$$\sum_{\chi \in \mathrm{Irr}(G),\ 1<\chi(1)<D} \frac{|\chi(g_1)\chi(g_2)\overline{\chi}(g)|}{\chi(1)} \leq \frac{2 \cdot 3^{1/2} \cdot q^{n+3}}{(q^n-1)(q^{n-1}-q)/(q^2-1)} < 0.658.$$

If $(n, q) = (7, 2)$, then the analysis in (iii) shows that the only case where two characters $\chi \in \mathcal{X}$ are nonzero at g_1 is when $\epsilon = +$, $s = \ell(q, 2n-2)$ and $\chi = \varphi$, ζ_1. In this case, φ has s_ϵ-defect 0, so it vanishes at g_2. Furthermore,

$$\rho_0(g_2) = \rho_1(g_2) = 0,$$

so (5.17) and (5.18) imply that

$$\psi(g_2) = -1, \ \zeta_1(g_2) = 0,$$

so no character $\chi \in \mathcal{X}$ can be nonzero at both g_1 and g_2. In all other cases, only one $\chi \in \mathcal{X}$ can be nonzero at $g_1 = g_2$ and $|\chi(g_1)\chi(g_2)| \leq 1$. It follows that

$$\sum_{\chi \in \mathrm{Irr}(G),\ 1<\chi(1)<D} \frac{|\chi(g_1)\chi(g_2)\overline{\chi}(g)|}{\chi(1)} \leq \frac{3^{1/2} \cdot q^{n+3}}{(q^n+1)(q^{n-1}-q)/(q^2-1)} < 0.666.$$

Combining with (5.16), we are done in all cases. ∎

Proposition 5.11. *Suppose that $G = \Omega^\epsilon_{2n}(q)$, where $n \geq 5$, $q = 3, 5$, and $\epsilon = \pm$. Assume that $t \in \mathcal{R}(G)$, $2 \nmid n$ if $q = 5$, and $n \geq 7$ if $q = 3$. Then $\mathsf{P}_u(N)$ holds for G and for every $N = q^a t^b$.*

Proof. (i) Consider an unbreakable $g \in G$; in particular,

$$|\mathbf{C}_G(g)| \leq B = \begin{cases} 2^6 \cdot q^{2n+4}, & q = 3 \\ 6^2 \cdot q^{2n-2}, & q = 5 \end{cases}$$

by Lemma 3.3. We also choose

$$D := \begin{cases} q^{4n-10}, & (n,q) \neq (7,3),(5,5), \\ q^{19}, & (n,q) = (7,3), \\ q^3(q^3-1)(q^5-1)(q-1)^2/2, & (n,q) = (5,5). \end{cases}$$

For $(n,q) \neq (5,5)$, we fix regular semisimple $g_1 = g_2 \in G$ of order $s \in \mathcal{R}(G) \smallsetminus \{t\}$.

Suppose now that $(n,q) = (5,5)$. First, we fix a regular semisimple $u_1 \in \Omega_6^{-\epsilon}(5)$ of order $\ell := 7$ if $\epsilon = +$ and $\ell := 31$ if $\epsilon = -$, and a regular semisimple $u_2 \in \Omega_4^-(5)$ of order 13, and set $g_1 = \mathrm{diag}(u_1, u_2)$. If $t \nmid (q^5 - \epsilon)$, we fix a regular semisimple $g_2 \in G$ of order $s \in \mathcal{R}(G) \smallsetminus \{t\}$. Note that the central involution z of $\mathrm{SO}_8^-(5)$ does *not* belong to $\Omega_8^-(5)$. Also, a generator v_2 of $\mathrm{SO}_2^{-\epsilon}(5)$ does not belong to $\Omega_2^{-\epsilon}(5)$ and has two distinct eigenvalues ν, ν^{-1} of order $q - \epsilon$. Choosing a regular semisimple $v_1 \in \Omega_8^-(5)$ of order s, we can now set $g_2 := \mathrm{diag}(zv_1, v_2)$ in the case $t|(q^5 - \epsilon)$.

Our choice of g_i implies that each g_i is an N'-element, and $|\mathbf{C}_G(g_i)| \leq (q+1)(q^{n-1}+1)$. It follows that

$$\sum_{\substack{\chi \in \mathrm{Irr}(G), \\ \chi(1) \geq D}} \frac{|\chi(g_1)\chi(g_2)\overline{\chi}(g)|}{\chi(1)} \leq \frac{(q+1)(q^{n-1}+1) \cdot B^{1/2}}{D} < \begin{cases} 0.14, & (n,q) \neq (7,3) \\ 0.40, & (n,q) = (7,3). \end{cases} \tag{5.20}$$

Also, g_2 is always s-singular. Furthermore, g_1 is ℓ-singular when $(n,q) = (5,5)$.

(ii) Now we estimate character values for the characters in

$$\mathcal{X} := \{\chi \in \mathrm{Irr}(G) \mid 1 < \chi(1) < D\}.$$

By [50, Theorem 1.4], when $(n,q) \neq (7,3)$, $(5,5)$, the set $\mathcal{X}$ consists of $q+4$ characters:

- $\varphi = D_{1_S} - 1_G$ of degree $(q^n - \epsilon)(q^{n-1} + q\epsilon)/(q^2-1)$,
- $\psi = D_{\mathsf{St}} - 1_G$ of degree $(q^{2n} - q^2)/(q^2-1)$,
- D_{ξ_i} of degree $(q^n - \epsilon)(q^{n-1} + \epsilon)/2(q-1)$ for $1 \leq i \leq 2$,
- D_{η_i} of degree $(q^n - \epsilon)(q^{n-1} - \epsilon)/2(q+1)$ for $1 \leq i \leq 2$,
- D_{θ_j} of degree $(q^n - \epsilon)(q^{n-1} - \epsilon)/(q+1)$ for $1 \leq j \leq (q-1)/2$, and
- D_{χ_j} of degree $(q^n - \epsilon)(q^{n-1} + \epsilon)/(q-1)$ for $1 \leq j \leq (q-3)/2$.

The characters D_α of G with $\alpha \in \mathrm{Irr}(S)$ and $S := \mathrm{Sp}_2(q)$ are constructed in [34, Proposition 5.7]. If $(n,q) = (7,3)$ and $\chi \in \mathcal{X}$ has positive s-defect, then using [41] we show that χ must be one of these $q+4$ characters. If $(n,q) = (5,5)$ and $\chi \in \mathcal{X}$ has positive s-defect and positive ℓ-defect, then using [41] we again show that χ must be one of these characters.

Let $V = \overline{\mathbb{F}}_q^{2n}$ denote the natural module for G and let $F_0 := \{\lambda \in \overline{\mathbb{F}}_q^\times \mid \lambda^{q\pm 1} = 1\}$. By Lemma 3.4,

$$\dim_{\overline{\mathbb{F}}_q} \mathrm{Ker}(g - \lambda \cdot 1_V) \leq c$$

for all $\lambda \in F_0$, where $c := 4$ for $q = 3$ and $c = 2$ for $n = 5$. Hence, arguing as in the proof of [34, Proposition 5.11], we show that

$$|D_\alpha(g)| \leq q^c \cdot \alpha(1) \tag{5.21}$$

for every $\alpha \in \mathrm{Irr}(S)$. On the other hand, by our choice of g_i,

$$\dim_{\overline{\mathbb{F}}_q} \mathrm{Ker}(g_i - \lambda \cdot 1_V) \leq e_i$$

for all $\lambda \in F_0$ and $i = 1, 2$, where $e_i := 2$ if $(n,q) \neq (5,5)$, $e_1 := 0$ and $e_2 \leq 1$ if $(n,q) = (5,5)$. Arguing as in the proof of [34, Proposition 5.11], we obtain

$$|D_\alpha(g_i)| \leq q^{e_i} \cdot \alpha(1) \tag{5.22}$$

for every $\alpha \in \mathrm{Irr}(S)$.

(iii) Recall that $D^\circ_\alpha = D_\alpha - k_\alpha \cdot 1_G$ where $k_\alpha = 1$ if $\alpha = 1_S$ or St and $k_\alpha = 0$ otherwise cf. [34, Table II]. Suppose that $q = 3$ and $n \geq 8$. Then $\alpha(1) \leq 3$ for all $\alpha \in \mathrm{Irr}(S)$. It now follows from (5.21) and (5.22) that

$$\sum_{\chi\in\mathrm{Irr}(G),\ 1<\chi(1)<D} \frac{|\chi(g_1)\chi(g_2)\overline{\chi}(g)|}{\chi(1)} \leq \frac{7\cdot(3^3+1)^2\cdot(3^5+1)}{(3^n-1)(3^{n-1}-3)/8} < 0.75.$$

Together with (5.20), this implies that $g \in g_1^G \cdot g_2^G$, so we are done in this case.

Assume now that either $q = 5$ or $(n, q) = (7, 3)$; in particular, either $s|(q^n - \epsilon)$ or $s|(q^{n-1}+1)$. In the former case, all $\chi \in \mathcal{X}$ but $\psi = D_{\mathsf{St}} - 1_G$ have s-defect 0, so vanish at g_i. Also, $\mathsf{St}(1) = q$, whence by (5.21) and (5.22)

$$\sum_{\chi\in\mathcal{X}} \frac{|\chi(g_1)\chi(g_2)\overline{\chi}(g)|}{\chi(1)} \leq \frac{(q^{e_1+1}+1)(q^{e_2+1}+1)(q^{c+1}+1)}{(q^{2n}-q^2)/(q^2-1)} < 0.33.$$

In the latter case, the only $\chi \in \mathcal{X}$ that have positive s-defect are $\varphi = D_{1_S} - 1_G$, and $k = (q+1)/2$ or $(q+3)/2$ characters D_{α_i}, $1 \leq i \leq k$ with

$$\sum_{i=1}^{k} \alpha_i(1)^2 \leq (q+1)^2(q-2)/2.$$

Moreover, $\varphi(1) \geq d_1 := (q^n-1)(q^{n-1}-q)/(q^2-1)$ and $D_{\alpha_i}(1) \geq \alpha_i(1)d$. In this case, using (5.21) and (5.22), we obtain

$$\sum_{\chi\in\mathcal{X}} \frac{|\chi(g_1)\chi(g_2)\overline{\chi}(g)|}{\chi(1)} \leq \frac{(q^{e_1}+1)(q^{e_2}+1)(q^c+1)}{d} + \sum_{i=1}^{k} \frac{q^{e_1+e_2}\alpha_i(1)^2\cdot q^c\alpha_i(1)}{\alpha_i(1)d} < 0.44.$$

In either case, together with (5.20), this implies that $g \in g_1^G \cdot g_2^G$, so we are again done. ∎

5.5. **Completion of the proof of Theorem 1 for classical groups.**

Proposition 5.12. *Theorem 1 holds for all finite non-abelian simple symplectic or orthogonal groups.*

Proof. Let $G = \mathrm{Cl}_n(q)$ be such that $G/\mathbf{Z}(G)$ is simple non-abelian and $q = p^f$. By Corollary 2.2(i), we need to prove the surjectivity of the word map $(x, y) \mapsto x^N y^N$ only in the case $N = p^a t^b$ with $t \in \mathcal{R}(G)$. In particular, $t \neq 2, p$.

First we consider the case $G = \mathrm{Sp}_{2m}(q)$. By Lemma 5.3, we may assume that $m \geq 3$. We are also done by Corollary 2.9 if $q \equiv 1 \bmod 4$. For the remaining cases, we take $n_0 = 4$ if $q \geq 7$, $n_0 = 6$ if $q = 4$, and $n_0 = 6$ if $q = 2$, and set $n = 2m$. Note that condition (i) of Proposition 5.2 holds by Lemmas 5.3 and 5.4. Next, condition (ii) of Proposition 5.2 holds by Propositions 5.5, 5.7, and 5.8. Hence we are done by Proposition 5.2.

Next assume that $G = \Omega^\pm_{2m}(q)$ with $m \geq 3$ and $2|q$. Then we are done by Proposition 2.10 if $q \geq 8$ and $m \geq 4$. Since

$$\begin{array}{l} \Omega_3(q) \cong \mathrm{PSL}_2(q),\ \Omega^+_4(q) \cong \mathrm{SL}_2(q) \circ \mathrm{SL}_2(q),\ \Omega^-_4(q) \cong \mathrm{PSL}_2(q^2), \\ \Omega_5(q) \cong \mathrm{PSp}_4(q),\ \Omega^+_6(q) \cong \mathrm{SL}_4(q)/Z,\ \Omega^-_6(q) \cong \mathrm{SU}_4(q)/Z \end{array} \tag{5.23}$$

(for all q and for a suitable central 2-subgroup Z), cf. [26, Proposition 2.9.1], we are done in the case $m = 2, 3$ by the results of §4. In the remaining cases of $q = 2, 4$ and $n = 2m \geq 8$, we take $n_0 = 8$ for $q = 4$ and $n_0 = 12$ for $q = 2$. Note that condition (i) of Proposition 5.2 holds by Lemmas 5.3 and 5.4 for $8 \leq k \leq n_0$, and by the isomorphisms in (5.23) for $k = 4, 6$. Next, condition (ii) of Proposition 5.2 holds by Proposition 5.10. Hence we are done by Proposition 5.2.

Finally, let $G = \Omega^\pm_n(q)$ with $n \geq 7$ and q odd. Then we take $n_0 = 6$ if $q > 3$ and $n_0 = 12$ if $q = 3$. Note that condition (i) of Proposition 5.2 holds for $1 < k \leq 6$ by

the isomorphisms in (5.23) and Lemma 5.3, and for $7 \le k \le n_0$ by Lemma 5.4. Next, condition (ii) of Proposition 5.2 holds by Proposition 5.9 when $2 \nmid k$, by Proposition 2.10 if $2|k$, $q \ge 5$, and $(k,q) \ne (10,5)$, $(14,5)$, and by Proposition 5.11 if $2|k$, and $q = 3$ or $(k,q) = (10,5)$, $(14,5)$. Hence we are done by Proposition 5.2. ∎

6. Theorem 1 for exceptional groups

Lemma 6.1. *Theorem 1 holds for the Suzuki groups ${}^2B_2(q^2)$ with $q^2 \ge 8$ and the Ree groups ${}^2G_2(q^2)$ with $q^2 \ge 27$.*

Proof. Let S be one of these groups. Note that $|S|$ is divisible by at least four different odd primes. Hence we can find a prime divisor $\ell > 2$ of $|S|$ that is coprime to both q^2 and N, and a semisimple $x \in S$ of order ℓ. By [20, Theorem 7.1], $x^S \cdot x^S \supseteq S \setminus \{1\}$, whence the claim follows. ∎

Lemma 6.2. *Theorem 1 holds for the following: ${}^2F_4(2)'$; $G_2(q)$ with $q = 3, 4$; ${}^3D_4(q)$ with $q = 2, 4$; $F_4(2)$; $E_6(2)$; ${}^2E_6(2)$.*

Proof. The cases ${}^2F_4(2)'$, $G_2(3)$, $G_2(4)$ were checked directly using their character tables. For the remainder, by Corollary 2.2(i), it suffices to prove Theorem 1 for $N = p^a t^b$, where p is the defining characteristic and $t \in \mathcal{R}(G) = \{r, s\}$, which is $\{13\}$, $\{241\}$, $\{13, 17\}$, $\{73, 17\}$, $\{19, 17\}$, respectively. This was done by direct calculations similar to those of Lemma 2.4. ∎

In what follows, let $\Phi'_{24} := q^4 + q^3\sqrt{2} + q^2 + q\sqrt{2} + 1$.

Lemma 6.3. *Let S be one of $G_2(q)$, ${}^3D_4(q)$, ${}^2F_4(q)$, $F_4(q)$, $E_6^\epsilon(q)$, $E_7(q)$, $E_8(q)$ where $q = p^f$. Define the primes r, s as follows:*

S	r	s	$\lvert\mathbf{N}_S(T_r) : T_r\rvert$	$\lvert\mathbf{N}_S(T_s) : T_s\rvert$
$G_2(q)$	$\ell(p, 3f)$		6	
${}^3D_4(q)$	$\ell(p, 12f)$		4	
${}^2F_4(q^2)$	$\ell(2, 24f)\lvert\Phi'_{24}$		12	
$F_4(q)$	$\ell(p, 12f)$	$\ell(p, 8f)$	12	8
$E_6(q)$	$\ell(p, 9f)$	$\ell(p, 8f)$	9	8
${}^2E_6(q)$	$\ell(p, 18f)$	$\ell(p, 8f)$	9	8
$E_7(q)$	$\ell(p, 18f)$	$\ell(p, 7f)$	18	14
$E_8(q)$	$\ell(p, 24f)$	$\ell(p, 20f)$	24	20

For $t \in \{r, s\}$ let $x_t \in \mathcal{X}_t$, where $\mathcal{X}_t$ is the set of t-singular elements in S.

(i) $\mathbf{C}_S(x_t) = T_t$, *where T_t is a uniquely determined maximal torus of S.*

(ii) $|\mathbf{N}_S(T_t) : T_t|$ *is as in the table.*

(iii) $|\mathcal{X}_t| < |S|/|N_S(T_t) : T_t|$.

(iv) *If $S \ncong G_2(q)$, ${}^3D_4(q)$, then $|\mathcal{X}_t| < |S|/8$.*

Proof. We know that x_t lies in some maximal torus T_t of S. The orders of maximal tori are given by [6]. Inspection shows that for each t there is a unique possible order $|T_t|$ divisible by t, as follows, where in most cases we give also the label of T_t in [6] (and $d = (3, q - \epsilon)$ and $e = (2, q - 1)$):

S	$\lvert T_r\rvert$, label	$\lvert T_s\rvert$, label
$G_2(q)$	q^2+q+1	
${}^3D_4(q)$	q^4-q^2+1	
${}^2F_4(q^2)$	Φ'_{24}	
$F_4(q)$	$q^4-q^2+1,\ F_4$	$q^4+1,\ B_4$
$E_6^\epsilon(q)$	$(q^6+\epsilon q^3+1)/d,\ E_6(a_1)$	$(q^4+1)(q^2-1)/d,\ D_5$
$E_7(q)$	$(q^6-q^3+1)(q+1)/e,\ E_7$	$(q^7-1)/e,\ A_6$
$E_8(q)$	$q^8-q^4+1,\ E_8(a_1)$	$q^8-q^6+q^4-q^2+1,\ E_8(a_2)$

Write $S=(\mathcal{G}^F)'$, where $\mathcal{G}$ is the corresponding adjoint algebraic group and F a Frobenius endomorphism of $\mathcal{G}$. By [58, II,4.4], $\mathbf{C}_\mathcal{G}(x_t)$ is connected. Then $\mathbf{C}_\mathcal{G}(x_t)=\mathcal{D}\mathcal{Z}$ where $\mathcal{D}$ is semisimple and $\mathcal{Z}$ is a torus. If $\mathcal{D}\neq 1$ then $\mathcal{D}^F$ contains a subsystem $\mathrm{SL}_2(q)$ or $\mathrm{SU}_3(q)$ subgroup D, so $x_t\in\mathbf{C}_S(D)$. However $\mathbf{C}_S(D)$ does not have order divisible by t. Hence $\mathcal{D}=1$ and $\mathbf{C}_\mathcal{G}(x_t)$ is a maximal torus, whence $\mathbf{C}_S(x_t)=T_t$, proving (i).

Part (ii) follows from the tables in [6, pp. 312–315].

By (i), every element of $\mathcal{X}_t$ lies in a unique conjugate of T_t, and the number of these conjugates is $|S:\mathbf{N}_S(T_t)|$; also, $1\notin\mathcal{X}_t$. This gives (iii), and (iv) follows immediately. ∎

Proposition 6.4. *Theorem 1 holds for the simple exceptional group $S=G/\mathbf{Z}(G)$, where G is one of the following groups:*

(i) $G_2(q)$, $q\geq 5$;
(ii) ${}^3D_4(q)$, $q\neq 2,4$;
(iii) ${}^2F_4(q^2)$, $q^2\geq 8$;
(iv) $F_4(q)$, $q\geq 5$;
(v) $E_6(q)_{\mathrm{sc}}$ *or* ${}^2E_6(q)_{\mathrm{sc}}$, $q\geq 3$;
(vi) $E_7(q)_{\mathrm{sc}}$ *or* $E_8(q)$.

Proof. By Corollary 2.2(i), it suffices to prove Theorem 1 in the case $N=p^at^b$ with $p|q$ and $t\in\mathcal{R}(G)=\{r,s\}$.

First we consider the case $S=G_2(q)$ with $q\geq 5$; in particular, $t=\ell(p,3f)$ (with $q=p^f$ as usual). Note that $|\mathcal{X}_p|/|S|\leq 2/(q-1)-1/(q-1)^2<0.31$ for $q\geq 7$ by [19, Theorem 3.1], and $|\mathcal{X}_p|/|S|\leq 1-0.68=0.32$ for $q=5$ by [42]. Lemma 6.3 implies that

$$\frac{|\mathcal{X}_t|}{|S|}+\frac{|\mathcal{X}_p|}{|S|}<\frac{1}{6}+0.32<\frac{1}{2},$$

so we are done by Corollary 2.2(ii).

We can argue similarly in other cases. In the case $S={}^3D_4(q)$ with $q\geq 5$, by Lemma 6.3 and [19, Theorem 3.1],

$$\frac{|\mathcal{X}_t|}{|S|}+\frac{|\mathcal{X}_p|}{|S|}<\frac{1}{4}+\frac{1}{q-1}\leq\frac{1}{2},$$

so we are done. Also, note that the odd q case is covered by Corollary 2.9.

Suppose $S={}^2F_4(q^2)$ with $q^2\geq 8$. By [20, Theorem 7.3], $S\smallsetminus\{1\}\subseteq x^S\cdot x^S$ for a regular semisimple $x\in S$ of order Φ'_{24}. It remains therefore to consider the case $t|\Phi'_{24}$. By Lemma 6.3 and [19, Theorem 3.1],

$$\frac{|\mathcal{X}_t|}{|S|}+\frac{|\mathcal{X}_p|}{|S|}<\frac{1}{12}+\frac{2}{q^2-1}-\frac{1}{(q^2-1)^2}<\frac{1}{2}.$$

Next we consider the case $S=F_4(q)$ with $q\geq 5$. Note that $|\mathcal{X}_p|/|S|\leq 2/(q-1)-1/(q-1)^2<0.3056$ for $q\geq 7$ by [19, Theorem 3.1], and $|\mathcal{X}_p|/|S|\leq 1-0.6619=0.3381$

for $q = 5$ by [42]. It follows by Lemma 6.3 that

$$\frac{|\mathcal{X}_t|}{|S|} + \frac{|\mathcal{X}_p|}{|S|} \leq \frac{1}{8} + 0.3381 < \frac{1}{2}.$$

For cases (v) and (vi), we note that $|\mathcal{X}_p|/|G| \leq 1/(q-1) \leq 1/3$ for $q \geq 4$ by [19, Theorem 3.1], and $|\mathcal{X}_p|/|G| \leq 1 - 0.6627 = 0.3373$ for $q = 3$ by [42]. It follows by Lemma 6.3 that

$$\frac{|\mathcal{X}_t|}{|G|} + \frac{|\mathcal{X}_p|}{|G|} \leq \frac{1}{8} + 0.3373 < \frac{1}{2},$$

so we are done.

If $G = E_8(q)$, then G has two maximal tori $T_{1,2}$ of order $q^8 - 1$ and Φ_{15}, and t is coprime to both $|T_{1,2}|$. According to [43, Theorem 10.1], T_i contains a regular semisimple element s_i for $i = 1, 2$, such that $\mathrm{Irr}(G)$ contains exactly two irreducible characters χ with $\chi(s_1)\chi(s_2) \neq 0$, namely 1_G and St. Since $|\mathsf{St}(s_i)| = 1$, it follows that

$$\sum_{\chi \in \mathrm{Irr}(G)} \frac{|\chi(s_1)\chi(s_2)\chi(g)|}{\chi(1)} = 1 + \frac{|\mathsf{St}(g)|}{\mathsf{St}(1)} > 0,$$

so $g \in s_1^G \cdot s_2^G$ for all $1 \neq g \in G$, and we are done.

Finally, let $G = E_7(2)$, so that $t \in \{19, 127\}$. Consider $s_1 \in G$ of order 73 and $s_2 \in G$ of order 43. Using [41], we check that the only $\chi \in \mathrm{Irr}(G)$ that has positive 73-defect and positive 43-defect are 1_G and St. Hence $s_1^G \cdot s_2^G = G \setminus \{1\}$ and we are done as above. ∎

Lemma 6.5. *The following statements hold.*

(i) *Let $G = F_4(4)$ and let $x \in G$ be a non-semisimple element such that $|\mathbf{C}_G(x)| > 3 \cdot 4^{19}$. Then there is a quasisimple classical subgroup S in characteristic 2 of G such that $|\mathbf{Z}(S)|$ is a 3-power and $x \in S$.*

(ii) *Let $G = F_4(3)$ and let $x \in G$ be a non-semisimple element such that $|\mathbf{C}_G(x)| > 3^{19}$. Then there is a quasisimple classical subgroup S in characteristic 3 of G such that $|\mathbf{Z}(S)|$ is a 2-power and $x \in S$.*

Proof. (i) Suppose first that x is unipotent. Following [39, Table 22.2.4], the bound on $|\mathbf{C}_G(x)|$ forces x to be in one of the following unipotent classes:

$$A_1,\ \tilde{A}_1,\ (\tilde{A}_1)_2,\ A_1\tilde{A}_1,\ A_2\,(2\text{ classes}),\ \tilde{A}_2\,(2\text{ classes}),\ B_2\,(2\text{ classes}).$$

In the first two cases x lies in a subgroup $\mathrm{SL}_2(4)$. The third class $(\tilde{A}_1)_2$ has representative $x = u_{1232}(1)u_{2342}(1)$ (see [39, Table 16.2 and (18.1)]). This is centralized by the long root groups $U_{\pm 0100}$, and these generate $A \cong \mathrm{SL}_2(4)$. Then $x \in \mathbf{C}_G(A) = \mathrm{Sp}_6(4)$. The class $A_1\tilde{A}_1$ has a representative in a subgroup $A_1(4)\tilde{A}_1(4)$, which is contained in a subgroup $\mathrm{Sp}_8(4)$. Representatives of the four classes with labels $A_2, \tilde{A}_2$ lie in subgroups $\mathrm{SL}_3(4)$ or $\mathrm{SU}_3(4)$. Finally, representatives of the classes with label B_2 lie in a subgroup $\mathrm{Sp}_4(4)$.

Now suppose x is non-unipotent, with Jordan decomposition $x = su$, where $s \neq 1$ is semisimple and u unipotent. As x is assumed non-semisimple, $u \neq 1$. Then $\mathbf{C}_G(s)$ is a subsystem subgroup of order greater than $3 \cdot 4^{19}$, and the only possibility is that $\mathbf{C}_G(s) = C_3 \times \mathrm{Sp}_6(4)$. But then $u \in \mathrm{Sp}_6(4)$ has centralizer of order greater than 4^{19}, which is impossible for a nontrivial unipotent element of $\mathrm{Sp}_6(4)$.

(ii) This is similar to (i). Suppose x is unipotent. Then x lies in one of the classes

$$A_1,\ \tilde{A}_1\,(2\text{ classes}),\ A_1\tilde{A}_1,\ A_2\,(2\text{ classes}),\ \tilde{A}_2.$$

For the $A_1\tilde{A}_1$ class, as above x lies in a subgroup $\mathrm{Spin}_9(3)$. Each of the other class representatives lies in a subgroup $\mathrm{SL}_3(3)$ or $\mathrm{SU}_3(3)$.

Now suppose x is non-unipotent, so $x = su$ with semisimple and unipotent parts $s, u \neq 1$. Then $\mathbf{C}_G(s)$ is a subsystem subgroup of type B_4, A_1C_3, T_1C_3 or T_1B_3, where T_1 denotes a 1-dimensional torus. The last two cases are not possible, as in (i). In the first case, $x \in \mathbf{C}_G(s) = \mathrm{Spin}_9(3)$. So assume finally that $\mathbf{C}_G(s)$ is of type A_1C_3, and let $u = u_1u_2$ with $u_1 \in \mathrm{SL}_2(3)$, $u_2 \in \mathrm{Sp}_6(3)$. If $u_2 \neq 1$ then

$$|\mathbf{C}_G(x)| \leq |\mathrm{SL}_2(3)| \cdot |\mathbf{C}_{\mathrm{Sp}_6(3)}(u_2)| < 3^{19}.$$

Hence $u_2 = 1$ and $x = su \in \mathrm{SL}_2(3) < \mathrm{SL}_3(3)$. This completes the proof. ∎

Lemma 6.6. *Theorem 1 holds for the simple exceptional groups $G = F_4(q)$ with $q = 3, 4$.*

Proof. By Corollary 2.2(i), it suffices to prove Theorem 1 in the case $N = q^at^b$ with $t \in \mathcal{R}(G) = \{r, s\}$.

Suppose that $t \nmid \Phi_8$. Then G has two maximal tori $T_{1,2}$ of orders $(q^2-1)(q^2+q+1)$ and q^4+1, which are coprime to N. It is shown in [43, Theorem 10.1] that T_i contains a regular semisimple element s_i for $i = 1, 2$, such that $\mathrm{Irr}(G)$ contains exactly two irreducible characters χ with $\chi(s_1)\chi(s_2) \neq 0$, namely 1_G and St. It follows that $G \smallsetminus \{1\} = s_1^G \cdot s_2^G$, so we are done as in the proof of Proposition 6.4.

Now consider the case where $t|\Phi_8$. Choose regular semisimple $s_1 = s_2 \in G$ of (prime) order $s = \Phi_{12}$. Using [41], we check that if $\chi \in \mathrm{Irr}(G)$, $1 < \chi(1) < q^{18}$, and $\chi(s_1)\chi(s_2) \neq 0$ (in particular, χ has positive s-defect), then $\chi = \chi_{1,2}$ with

$$\chi_1(1) = q\Phi_1^2\Phi_3^2\Phi_8,\ \chi_2(1) = q\Phi_2^2\Phi_6^2\Phi_8.$$

It suffices to show that every nontrivial $g \in G$ belongs to $s_1^G \cdot s_2^G$. This is indeed the case if g is semisimple by [17], so we assume g is non-semisimple. Moreover, if $|\mathbf{C}_G(g)| > B$, where $B := 3^{19}$ for $q = 3$ and $B := 3 \cdot 4^{19}$ for $q = 4$, then by Lemma 6.5 we can embed G in a quasisimple classical subgroup S in characteristic q with $|\mathbf{Z}(S)|$ coprime to N, in which case we are done by applying Theorem 1 to $S/\mathbf{Z}(S)$. So we may assume that $|\mathbf{C}_G(g)| \leq B$. Next observe that χ_i is rational-valued (as it is the unique character in $\mathrm{Irr}(G)$ of its degree), and $\chi_i(1) \equiv \pm 1 \bmod s$. It follows that $\chi_i(s_1) \in \mathbb{Z}$ and $\chi_i(s_1) \equiv \pm 1 \bmod s$. Since $|\chi_i(s_1)| \leq |\mathbf{C}_G(s_1)|^{1/2} = s^{1/2}$, we conclude that $\chi_i(s_1) = \pm 1$. It follows that

$$\sum_{i=1}^{2} \frac{|\chi_i(s_1)\chi_i(s_2)\chi_i(g)|}{\chi_i(1)} \leq \frac{B^{1/2}}{\chi_1(1)} + \frac{B^{1/2}}{\chi_2(1)} < 0.87.$$

On the other hand, since $|\mathbf{C}_G(s_i)| = \Phi_{12}$,

$$\sum_{\chi \in \mathrm{Irr}(G),\ \chi(1) \geq q^{18}} \frac{|\chi(s_1)\chi(s_2)\chi(g)|}{\chi(1)} \leq \frac{B^{1/2}\Phi_{12}}{q^{18}} < \frac{1}{q^4} \leq \frac{1}{81}.$$

It follows that $g \in s_1^G \cdot s_2^G$, as stated. ∎

In summary, we have proved the following.

Corollary 6.7. *Theorem 1 holds for all finite non-abelian simple exceptional groups of Lie type.*

Proof of Theorem 1. The case of simple groups of Lie type is completed by Proposition 5.12 for classical groups and Corollary 6.7 for exceptional groups. Alternating and sporadic groups are handled by Lemma 2.4 and Proposition 2.5. ∎

7. Odd power word maps

7.1. **Preliminaries.**

Lemma 7.1. *Let S be a finite non-abelian simple group. To prove Theorem 3 for all quasisimple groups G with $G/\mathbf{Z}(G) \cong S$, it suffices to prove it for the $2'$-universal cover H of S, that is, $H/\mathbf{Z}(H) \cong S$ and $|\mathbf{Z}(H)|$ is the $2'$-part of the order of the Schur multiplier of S.*

Proof. It suffices to prove Theorem 3 for the universal cover L of S. By assumption, Theorem 3 holds for $H = L/Z$, where $Z \leq \mathbf{Z}(L)$ is a 2-group. Thus every $g \in L$ can be written in the form $g = xyzt$, where x, y, z are 2-elements of L and $t \in Z$. It follows that $g = xy(zt)$ is a product of three 2-elements in L. ∎

Lemma 7.2. *Theorem 3 holds for all quasisimple covers of alternating groups $S = \mathsf{A}_n$ with $n \geq 5$. Moreover, every element of S is a product of two 2-elements.*

Proof. The cases $S = \mathsf{A}_6, \mathsf{A}_7$ are checked directly using [8]. By Lemma 7.1, it suffices to prove Theorem 3 for $G = \mathsf{A}_n$.

(i) First we show that if $g = (1, 2, \ldots, m)$ is an m-cycle with $m = 2k + 1 \geq 5$, then $g = x_1y_1 = x_2y_2$, where $x_i, y_i \in \mathsf{S}_m$ have order 2 or 4, and moreover $x_1, y_1 \in \mathsf{A}_m$, $x_2, y_2 \in \mathsf{S}_m \setminus \mathsf{A}_m$. Indeed, g is inverted by the involution

$$x := (1, 2k + 1)(2, 2k) \ldots (k - 1, k + 3)(k, k + 2).$$

Setting $y := xg$, we get $y^2 = xgxg = g^{-1}g = 1$, so $g = xy$. Next, we set

$$x' := (1, 2k + 1)(2, 2k) \ldots (k - 1, k + 3),\ y' := x'g.$$

A computation establishes that $|x'| = 2$, $|y'| = 4$, and $g = x'y'$. Since exactly one of x, x' belongs to A_m and $g \in \mathsf{A}_m$, the claims follow.

(ii) Now we show that every $g \in \mathsf{A}_n$ is a product of two 2-elements. Indeed, if g is real in A_n then the statement follows from Lemma 2.7. Since g is always real in S_n, we may assume that g is not real in A_n, so it is not centralized by any *odd* permutation in S_n. Thus $g = g_1g_2 \ldots g_s$ is a product of $s \geq 1$ disjoint cycles, where g_i is an n_i-cycle, $3 \leq n_1 < n_2 < \ldots < n_s$, and n_i is odd for all i. We may assume that

$$\mathsf{S}_n \geq X_1 \times X_2 \times \ldots \times X_s,$$

where $X_i \cong \mathsf{S}_{n_i}$ and $g_i \in X_i$.

Suppose $n_1 \geq 5$. Then, according to (i) we can write $g_i = x_iy_i$ where $x_i, y_i \in [X_i, X_i] \cong \mathsf{A}_{n_i}$ are 2-elements. Hence $g = xy$ with $x := x_1x_2 \ldots x_s$ and $y := y_1y_2 \ldots y_s$, as desired.

Assume now that $n_1 = 3$. Since g is not real in A_n and $n \geq 5$, we observe that $s \geq 2$. Again by (i), for $i \geq 2$ we can write $g_i = x_iy_i$, where $x_i, y_i \in X_i$ are 2-elements; moreover, $x_i, y_i \in [X_i, X_i]$ if $i \geq 3$ and $x_2, y_2 \in X_2 \setminus [X_2, X_2]$. We may assume that $g_1 = (1, 2, 3)$ and write $g_1 = x_1y_1$ with $x_1 = (1, 3)$, $y_1 = (1, 2)$. Now setting $x := x_1x_2 \ldots x_s$ and $y := y_1y_2 \ldots y_s$, again $g = xy$ is a product of two 2-elements in A_n. ∎

Lemma 7.3. *Let S be a non-abelian simple group of Lie type in characteristic 2. Theorem 3 holds for all quasisimple covers of S.*

Proof. The case $S = {}^2F_4(2)'$ is checked directly using [8]; and $S = \mathsf{A}_6$ follows from Lemma 7.2. Suppose now that $S \ncong \mathsf{A}_6, {}^2F_4(2)'$. Then there is a quasisimple Lie-type group H of simply connected type such that H is a $2'$-universal cover of S. According to [11, Corollary, p. 3661], every non-central element of H is a product of two 2-elements. For $g \in \mathbf{Z}(H)$, consider a non-central 2-element t of H. Again $gt^{-1} = xy$ for some 2-elements x, y of H, so $g = xyt$ is a product of three 2-elements. Hence we are done by Lemma 7.1. ∎

Lemma 7.4. (i) *Theorem 3 holds for the quasisimple group G if $G/\mathbf{Z}(G)$ is one of the following simple groups: a sporadic group,* $\mathrm{PSU}_4(3)$, $\mathrm{PSp}_6(3)$, $\Omega_7(3)$, $\mathrm{PSp}_8(3)$.

(ii) *Suppose that $G = \mathrm{GU}_n(3)$ with $3 \leq n \leq 6$. Each $g \in G$ can be written as $g = xyz$, where x, y, z are 2-elements of G and* $\det(x) = \det(y) = 1$.

Proof. These statements were established using direct calculations similar to those of Lemma 2.4. ∎

7.2. **Regular 2-elements in classical groups in odd characteristic.** We show that finite classical groups in odd characteristic admit regular 2-elements with prescribed determinant or spinor norm.

We begin with the general linear and unitary groups.

Lemma 7.5. *Let $G = \mathrm{GL}_n^\epsilon(q)$ with $n \geq 1$, $\epsilon = \pm 1$, q an odd prime power and let $\mu_{q-\epsilon} := \{\lambda \in \overline{\mathbb{F}}_q^\times \mid \lambda^{q-\epsilon} = 1\}$. For every 2-element δ of $\mu_{q-\epsilon}$, there exists a regular 2-element $s = s_n(\delta)$ of G, such that* $\det(s) = \delta$ *and s has at most two eigenvalues β that belong to $\mu_{q-\epsilon}$ (and each such eigenvalue appears with multiplicity one).*

Proof. (i) First we consider the special case $n = 2^m \geq 2$ and construct a regular 2-element s_m of G. Fix $\gamma \in \overline{\mathbb{F}}_q^\times$ with $|\gamma| = (q^{2^m} - 1)_2 \geq 8$. Using the embeddings

$$\mathrm{GL}_1(q^{2^m}) \hookrightarrow \mathrm{GL}_{2^{m-1}}(q^2) \hookrightarrow \mathrm{GL}_{2^m}^\epsilon(q) = G,$$

we can find $s_m \in G$ which is conjugate over $\overline{\mathbb{F}}_q$ to

$$\mathrm{diag}(\gamma, \gamma^{q\epsilon}, \gamma^{(q\epsilon)^2}, \ldots, \gamma^{(q\epsilon)^{n-1}}).$$

It is straightforward to check that all eigenvalues of s_m appear with multiplicity one and have order $(q^{2^m} - 1)_2$; in particular, s_m is regular.

(ii) If $n = 1$, then we set $s_1(\delta) = \delta$. Suppose $n = 2$. If $\delta \neq 1$, then we choose $s_2(\delta) := \mathrm{diag}(1, \delta)$. If $\delta = 1$, then we can choose $\alpha = \pm 1$ such that $q \equiv \alpha \bmod 4$ and take

$$s_2(1) \in C_{q-\alpha} \hookrightarrow \mathrm{SL}_2^\epsilon(q) < G$$

with $|s_2(1)| = 4$. Note that $|s_n(\delta)| < (q^2 - 1)_2$ for all $\delta \in \mu_{q-\epsilon}$ and $n = 1, 2$.

Consider the case $n \geq 3$ odd and write

$$n = 2^{m_1} + 2^{m_2} + \ldots + 2^{m_t} + 1$$

with $m_1 > m_2 > \ldots > m_t \geq 1$. Setting

$$s := \mathrm{diag}(s_{m_1}, s_{m_2}, \ldots, s_{m_t}, \alpha) \in \mathrm{GL}_{2^{m_1}}^\epsilon(q) \times \ldots \times \mathrm{GL}_{2^{m_t}}^\epsilon(q) \times \mathrm{GL}_1^\epsilon(q) < G,$$

with $\alpha := \delta / \prod_{i=1}^t \det(s_{m_i})$, we deduce that $\det(s) = \delta$ and all eigenvalues of s appear with multiplicity one, as required.

(iii) We may now assume that

$$n = 2^{m_1} + 2^{m_2} + \ldots + 2^{m_t}$$

with $m_1 > m_2 > \ldots > m_t \geq 1$.

Suppose first that $m_t = 1$. We choose

$$s := \mathrm{diag}(s_{m_1}, s_{m_2}, \ldots, s_{m_{t-1}}, s_2(\alpha)) \in \mathrm{GL}_{2^{m_1}}^\epsilon(q) \times \ldots \times \mathrm{GL}_{2^{m_{t-1}}}^\epsilon(q) \times \mathrm{GL}_2^\epsilon(q) < G,$$

with $\alpha := \delta / \prod_{i=1}^t \det(s_{m_i})$, so that $\det(s) = \delta$. The construction of s ensures that all eigenvalues of s appear with multiplicity one, so s is regular.

If $a := m_t \geq 2$, then we rewrite

$$n = 2^{a_1} + 2^{a_2} + \ldots + 2^{a_{t-1}} + 2^{a_t} + 2^{a_{t+1}} + \ldots + 2^{a_k},$$

where $a_i = m_i$ for $1 \le i \le t-1$, $k = t+a-1$, and $(a_t, a_{t+1}, \ldots, a_k) = (a-1, a-2, \ldots, 2, 1, 1)$. Now we can choose

$$s := \mathrm{diag}(s_{a_1}, s_{a_2}, \ldots, s_{a_{k-1}}, s_2(\alpha)) \in \mathrm{GL}^\epsilon_{2^{a_1}}(q) \times \ldots \times \mathrm{GL}^\epsilon_{2^{a_{k-1}}}(q) \times \mathrm{GL}^\epsilon_2(q) < G,$$

with $\alpha := \delta / \prod_{i=1}^{k-1} \det(s_{a_i})$. Again $\det(s) = \delta$, and all eigenvalues of s appear with multiplicity one, as desired.

The last condition on s can be checked easily in all cases. ∎

Lemma 7.6. *Let $G = \mathrm{Sp}_{2n}(q)$ with $n \ge 1$ and q an odd prime power. There exists a regular 2-element s of G (and neither 1 nor -1 is an eigenvalue of s).*

Proof. First we consider the special case $n = 2^m \ge 2$. We fix $\gamma \in \overline{\mathbb{F}}_q^\times$ with $|\gamma| = (q^{2^m} - 1)_2 \ge 8$ and use the element s_m constructed in part (i) of the proof of Lemma 7.5 via the embeddings

$$\mathrm{GL}_1(q^{2^m}) \hookrightarrow \mathrm{GL}_{2^m}(q) \hookrightarrow \mathrm{Sp}_{2n}(q) = G.$$

Note that s_m is conjugate over $\overline{\mathbb{F}}_q$ to

$$\mathrm{diag}(\gamma, \gamma^q, \gamma^{q^2}, \ldots, \gamma^{q^{n-1}}, \gamma^{-1}, \gamma^{-q}, \gamma^{-q^2}, \ldots, \gamma^{-q^{n-1}}).$$

In particular, all eigenvalues of s_m appear with multiplicity one and have order $(q^{2^m} - 1)_2$, whence s_m is regular.

Consider the general case

$$n = 2^{m_1} + 2^{m_2} + \ldots + 2^{m_t}$$

with $m_1 > m_2 > \ldots > m_t \ge 0$ and $t \ge 1$. If $m_t \ge 1$, set

$$s := \mathrm{diag}(s_{m_1}, s_{m_2}, \ldots, s_{m_t}) \in \mathrm{Sp}_{2^{m_1}}(q) \times \ldots \times Sp_{2^{m_t}}(q) \le G.$$

If $m_t = 0$, then we can choose

$$s := \mathrm{diag}(s_{m_1}, s_{m_2}, \ldots, s_{m_{t-1}}, s_2(1)) \in \mathrm{Sp}_{2^{m_1}}(q) \times \ldots \times Sp_{2^{m_{t-1}}}(q) \times \mathrm{Sp}_2(q) < G,$$

where $s_2(1)$ is constructed in part (ii) of the proof of Lemma 7.5. It is easy to check that s has the desired properties. ∎

Recall that the *spinor norm* $\theta(g)$ of $g \in \mathrm{SO}^\epsilon_n(q)$ is defined in [26, pp. 29–30].

Lemma 7.7. *Let $G = \mathrm{SO}^\epsilon_n(q)$ with $n \ge 2$, $\epsilon = \pm 1$, q an odd prime power. For $\delta = \pm 1$, there exists a regular 2-element $s = s^\epsilon_n(\delta)$ of G, such that $\theta(s) = \delta$; moreover, every $\beta \in \mathbb{F}_{q^2}^\times$ can appear as an eigenvalue of s with multiplicity at most two, and multiplicity two can occur only when $\beta = \pm 1$.*

Proof. (i) First we consider the special case $n = 2^{m+1} \ge 4$. We fix $\gamma \in \overline{\mathbb{F}}_q^\times$ with $|\gamma| = (q^{2^m} - 1)_2 \ge 8$ and use the element s_m constructed in part (i) of the proof of Lemma 7.5 via the embeddings

$$\mathrm{GL}_1(q^{2^m}) \hookrightarrow \mathrm{GL}_{2^m}(q) \hookrightarrow \mathrm{SO}^+_n(q)$$

Note that s_m is conjugate over $\overline{\mathbb{F}}_q$ to

$$\mathrm{diag}(\gamma, \gamma^q, \gamma^{q^2}, \ldots, \gamma^{q^{2^m-1}}, \gamma^{-1}, \gamma^{-q}, \gamma^{-q^2}, \ldots, \gamma^{-q^{2^m-1}}).$$

In particular, all eigenvalues of s_m appear with multiplicity one and have order $(q^{2^m} - 1)_2$, whence s_m is regular. As an element of $\mathrm{GL}_{2^m}(q)$, s_m has determinant

$$\nu := \gamma^{1+q+q^2+\ldots+q^{2^m-1}} = \gamma^{(q^{2^m}-1)/(q-1)}.$$

It follows that $\nu^{(q-1)/2} = \gamma^{(q^{2^m}-1)/2} = -1$, so $\theta(s_m) = -1$ by [26, Lemma 2.7.2].

(ii) Suppose that $n = 2$. We take $s^\epsilon_2(-1) \in \mathrm{SO}^\epsilon_2(q) \cong C_{q-\alpha}$ of order $(q - \epsilon)_2$, and $s^\epsilon_2(1) = I_2$.

Next suppose that $n = 4$ and choose $\alpha = \pm 1$ such that $q \equiv \alpha \bmod 4$. We also fix $s_0 \in \mathrm{SO}_2^\alpha(q)$ of order $(q-\alpha)_2 \geq 4$ so that $\theta(s_0) = -1$ (note that we can take $s_0 = s_2^\alpha(-1)$). Since $\mathrm{SO}_4^\epsilon(q) > \mathrm{SO}_2^\alpha(q) \times \mathrm{SO}_2^{\epsilon\alpha}(q)$, we can choose

$$s_4^+(1) = \mathrm{diag}(-I_2, I_2),\ s_4^-(1) = \mathrm{diag}(s_0, -I_2),\ s_4^+(-1) = \mathrm{diag}(s_0, -I_2),\ s_4^-(-1) = \mathrm{diag}(s_0, I_2).$$

Note that $|s_n^\epsilon(\delta)| < (q^2-1)_2$ for all $\delta = \pm 1$ and $n = 2, 4$. Also, we need later the fact that $s_4^\epsilon(-\epsilon)$ does not have 1 as an eigenvalue.

(iii) Suppose that $6 \leq n \equiv 2 \bmod 4$. We write

$$n = 2^{m_1+1} + 2^{m_2+1} + \ldots + 2^{m_t+1} + 2$$

with $m_1 > m_2 > \ldots > m_t \geq 1$, and choose

$$s := \mathrm{diag}(s_{m_1}, s_{m_2}, \ldots, s_{m_t}, s_2^\epsilon(\alpha)) \in \mathrm{SO}^+_{2^{m_1+1}}(q) \times \ldots \times \mathrm{SO}^+_{2^{m_t+1}}(q) \times \mathrm{SO}_2^\epsilon(q) < G$$

with $\alpha := (-1)^t\delta$, so that $\theta(s) = \delta$.

Consider the case $n \equiv 0 \bmod 4$ and write

$$n = 2^{m_1+1} + 2^{m_2+1} + \ldots + 2^{m_t+1}$$

with $m_1 > m_2 > \ldots > m_t \geq 1$. We can rewrite

$$n = 2^{a_1+1} + 2^{a_2+1} + \ldots + 2^{a_{t-1}+1} + 2^{a_t+1} + 2^{a_{t+1}+1} + \ldots + 2^{a_k+1},$$

where $a_i = m_i$ for $1 \leq i \leq t-1$, $k = t + m_t - 1$, and

$$(a_t, a_{t+1}, \ldots, a_k) = \begin{cases} (m_t - 1, m_t - 2, \ldots, 2, 1, 1), & m_t \geq 2, \\ (m_t), & m_t = 1. \end{cases}$$

Now we can choose

$$s := \mathrm{diag}(s_{a_1}, s_{a_2}, \ldots, s_{a_{k-1}}, s_4^\epsilon(\alpha)) \in \mathrm{SO}^+_{2^{a_1+1}}(q) \times \ldots \times \mathrm{SO}^+_{2^{a_{k-1}+1}}(q) \times \mathrm{SO}_4^\epsilon(q) < G$$

with $\alpha := (-1)^{k-1}\delta$, so that $\theta(s) = \delta$.

(iv) From now on, we may assume

$$n = 2^{m_1+1} + 2^{m_2+1} + \ldots + 2^{m_t+1} + 1$$

with $m_1 > m_2 > \ldots > m_t \geq 0$ and $t \geq 1$. Again choose $\alpha = \pm 1$ such that $4|(q - \alpha)$.

If $m_t = 0$, then we choose

$$s := \begin{cases} \mathrm{diag}(s_{m_1}, s_{m_2}, \ldots, s_{m_{t-1}}, s_{m_t}, 1), & \delta = (-1)^t, \\ \mathrm{diag}(s_{m_1}, s_{m_2}, \ldots, s_{m_{t-1}}, -I_2, 1), & \delta = (-1)^{t-1}, \end{cases}$$

and note that $s \in \mathrm{SO}^+_{2^{m_1+1}}(q) \times \ldots \times \mathrm{SO}^+_{2^{m_{t-1}+1}}(q) \times \mathrm{SO}_2^\alpha(q) \times \mathrm{SO}_1(q) < G$.

Finally, suppose that $m_t \geq 1$. We rewrite

$$n = 2^{a_1+1} + 2^{a_2+1} + \ldots + 2^{a_{t-1}+1} + 2^{a_t+1} + 2^{a_{t+1}+1} + \ldots + 2^{a_k+1} + 1,$$

where $a_i = m_i$ for $1 \leq i \leq t-1$, $k = t + m_t - 1$, and

$$(a_t, a_{t+1}, \ldots, a_k) = \begin{cases} (m_t - 1, m_t - 2, \ldots, 2, 1, 1), & m_t \geq 2, \\ (m_t), & m_t = 1. \end{cases}$$

Next, we set

$$s := \mathrm{diag}(s_{a_1}, s_{a_2}, \ldots, s_{a_{k-1}}, s_4^\beta(-\beta), 1)$$

which belongs to

$$\mathrm{SO}^+_{2^{a_1+1}}(q) \times \ldots \times \mathrm{SO}^+_{2^{a_{k-1}+1}}(q) \times \mathrm{SO}_4^\beta(q) \times \mathrm{SO}_1(q) < G,$$

where $\beta = (-1)^k\delta$.

In all cases, one can verify that $\theta(s) = \delta$, and s has the desired properties. ∎

7.3. **Proof of Theorem 3 for classical groups in odd characteristics.** First we deal with special linear and unitary groups in dimensions 3 and 4.

The CHEVIE project [15] provides *generic character tables* for the groups $\mathrm{SL}_3(q)$ and $\mathrm{SU}_3(q)$; these are symbolic parametrized descriptions of the character tables of all of these groups. To establish Lemma 7.8, it suffices to prove that

$$c_{x,y,z} = \frac{|x^G| \cdot |y^G|}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(x)\chi(y)\chi(z^{-1})}{\chi(1)} > 0,$$

for all $x, y, z \in G$. While, in principle there is a function which computes $c_{x,y,z}$ from the generic tables, its application is often difficult because the result may depend in a complicated way on the parameters for a conjugacy class. We thank Frank Lübeck for providing us with the following alternative proof of this result.

Lemma 7.8. *Let q be a power of an odd prime and let G be one of the groups $\mathrm{SL}_n(q)$ or $\mathrm{SU}_n(q)$ with $n \in \{3, 4\}$. Every element of G is a product of three 2-elements in G.*

Proof. We choose conjugacy classes carefully, such that only very few character values from the generic character tables are needed (and these are also available for $n = 4$).

We first consider $G = \mathrm{SL}_3(q)$ or $G = \mathrm{SU}_3(q)$. Let $c \in \mathbb{F}_{q^2}^\times$ have order $(q^2-1)_2$. Since $q-1$ and $q+1$ are even, $c \notin \mathbb{F}_q$, $c \neq c^q$ and $c \neq c^{-q}$.

Let x be a regular semisimple element with eigenvalues $\{c, c^q, c^{-q-1}\}$ (in case SL), or $\{c, c^{-q}, c^{q-1}\}$ (in case SU). The centralizer of x in G is a maximal torus of order q^2-1. Let y be a regular semisimple element of the maximal torus of order $q^2 \pm q + 1$.

By inspecting the generic character tables for SL_3 and SU_3 in CHEVIE, we notice that there are only two irreducible characters which both have a non-zero value on the conjugacy classes of x and y (the trivial character and the Steinberg character of degree q^3). This can be explained in terms of Deligne-Lusztig theory and Lusztig's Jordan decomposition of characters, see [10, 13.16]: The only semisimple element of the dual group of G whose centralizer contains maximal tori of types of the centralizers of x and of y is the trivial element. From information about the values of Deligne-Lusztig characters, it follows that only unipotent characters can be non-zero on both x and y. Which unipotent characters have this property can be read from the character table of the Weyl group of G, isomorphic to the symmetric group on 3 points, because up to sign this describes the values of unipotent characters on regular semisimple elements.

Now let $z \in G$. Observe that

$$c_{x,y,z} = \frac{|x^G| \cdot |y^G|}{|G|}(1 - \frac{\mathsf{St}(z^{-1})}{q^3}).$$

Hence $c_{x,y,z} > 0$ for every non-central element z. The case $z = x$ shows that y is the product of two 2-power elements, so every non-central z is a product of three 2-power elements.

For some q there are non-trivial z in the center of G. To show that such z can be written as product of three 2-power elements, we have a closer look at the generic character table to establish that $c_{x,x,xz} > 0$. We can compute readily a sufficient lower bound for this number: for example, in $\mathrm{SL}_3(q)$ there are $q-2$ irreducible characters of degree q^2+q+1 whose value on x and xz are some root of unity; for a lower bound we can substitute the corresponding terms in $c_{x,x,xz}$ by $-(q-2)/(q^2+q+1)$.

Now we turn to the case $G = \mathrm{SL}_4(q)$ and $G = \mathrm{SU}_4(q)$. In this case the center of G has order 2 or 4, so there is nothing to show for center elements. All groups of type $\mathrm{SL}_n(q)$ contain pairs of regular semisimple elements such that only two characters are non-zero

on both elements. But for $n = 4$ there are no such pairs containing 2-power elements, therefore we need a slightly more complicated argument than before.

Let $c \in \mathbb{F}_{q^2}^\times$ have order $(q^2-1)_2$. Now $c \neq c^{-1}$ and $c \neq c^{\pm q}$, and G contains a regular 2-power element x with eigenvalues $\{c, c^q, c^{-1}, c^{-q}\}$; its centralizer in G is a maximal torus of order $(q^2-1)(q \pm 1)$. We choose as y a regular element of a cyclic maximal torus of order $q^3 \pm 1$. With the same arguments as sketched in the $\mathrm{SL}_3/\mathrm{SU}_3$-case, we find that only unipotent characters can have non-zero value on both x and y. The unipotent characters of G are obtained by restricting the unipotent characters of $\mathrm{GL}_4(q)$ or $\mathrm{GU}_4(q)$, respectively. These are available in CHEVIE, and their values are all given by evaluating polynomials over the integers at q.

There are three unipotent characters with non-zero value on x and y, and we can compute the precise values of $c_{x,x,y}$ and $c_{x,y,z}$ for every non-central $z \in G$. For all resulting polynomials, it is easy to see that they evaluate to a positive number for all prime powers q. This shows that y is a product of two 2-power elements, so every non-central element is a product of three 2-power elements. ∎

Proposition 7.9. *Theorem 3 holds for all quasisimple covers of $S = \mathrm{PSL}_n(q)$, if $n \geq 5$ and $2 \nmid q$.*

Proof. (i) By Lemma 7.1, it suffices to prove Theorem 3 for $G = \mathrm{SL}_n(q)$. Let $s = s_n(1) \in G$ be as constructed in Lemma 7.5. It suffices to show that every $g \in G$ is a product of three conjugates of s, which is equivalent to

$$\sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(s)^3 \bar{\chi}(g)}{\chi(1)^2} \neq 0. \tag{7.1}$$

As $|\chi(g)/\chi(1)| \leq 1$, it suffices to prove

$$\sum_{1_G \neq \chi \in \mathrm{Irr}(G)} \frac{|\chi(s)|^3}{\chi(1)} < 1. \tag{7.2}$$

Set

$$D := \begin{cases} (q^n-1)(q^{n-1}-q^2)/(q-1)(q^2-1), & (n,q) \neq (6,3), \\ (q^5-1)(q^3-1), & (n,q) = (6,3). \end{cases}$$

By [62, Theorem 3.1], every character $\chi \in \mathrm{Irr}(G)$ of degree less than D is either 1_G or one of $q-1$ irreducible Weil characters τ_i, $0 \leq i \leq q-2$, as defined in (4.1).

(ii) Consider the case $n \geq 6$. The construction of s in Lemma 7.5 shows that

$$|\mathbf{C}_G(s)| \leq \begin{cases} (q^n-1)/(q-1), & (n,q) \neq (6,3), \\ (q^4-1)(q^2-1)/(q-1), & (n,q) = (6,3). \end{cases}$$

Hence

$$\sum_{\chi \in \mathrm{Irr}(G),\ \chi(1) \geq D} \frac{|\chi(s)|^3}{\chi(1)} < \frac{|\mathbf{C}_G(s)|^{1/2}}{D} \cdot \sum_{\chi \in \mathrm{Irr}(G)} |\chi(s)|^2 = \frac{|\mathbf{C}_G(s)|^{3/2}}{D} < 0.9099.$$

Next we estimate $|\tau_i(s)|$. Recall that $1_G + \tau_0$ is just the permutation character of G acting on the set of 1-spaces of $\mathbb{F}_q^n$. In the notation of §4.3, by Lemma 7.5, $e(g, \delta^l) \leq 1$ for all $0 \leq l \leq q-2$ and equality can be attained at most twice. It follows that s fixes at most two 1-spaces, i.e. $0 \leq \tau_0(s) + 1 \leq 2$, so $|\tau_0(s)| \leq 1$. Arguing as in the proof of Lemma 4.6, for $1 \leq i \leq q-2$ we obtain

$$|\tau_i(s)| \leq \frac{q + q + 1 \cdot (q-3)}{q-1} = 3.$$

Hence

$$\sum_{\chi\in\mathrm{Irr}(G),\ 1<\chi(1)<D}\frac{|\chi(s)|^3}{\chi(1)}=\sum_{i=0}^{q-2}\frac{|\tau_i(s)|^3}{\tau_i(1)}\le\frac{1+(q-2)\cdot 3^3}{(q^n-q)/(q-1)}<0.0772.$$

Thus

$$\sum_{1_G\ne\chi\in\mathrm{Irr}(G)}\frac{|\chi(s)|^3}{\chi(1)}<0.9099+0.0772=0.9871,$$

so we are done by (7.2).

(iii) Assume now that $n=5$. The construction of s in Lemma 7.5 implies that $|\mathbf{C}_G(s)|\le q^4-1$; furthermore, $\sum_{l=0}^{q-2}e(g,\delta^l)\le 1$ and so, by Lemma 4.6, $|\tau_i(s)|\le 1$ for all i. Arguing as in (ii), we obtain

$$\sum_{\chi\in\mathrm{Irr}(G),\ \chi(1)\ge D}\frac{|\chi(s)|^3}{\chi(1)}<\frac{(q^4-1)^{1.5}}{q^2(q^5-1)/(q-1)},$$

$$\sum_{\chi\in\mathrm{Irr}(G),1<\chi(1)<D}\frac{|\chi(s)|^3}{\chi(1)}=\sum_{i=0}^{q-2}\frac{|\tau_i(s)|^3}{\tau_i(1)}\le\frac{q-1}{(q^5-q)/(q-1)}.$$

Thus

$$\sum_{1_G\ne\chi\in\mathrm{Irr}(G)}\frac{|\chi(s)|^3}{\chi(1)}<\frac{(q^4-1)^{1.5}}{q^2(q^5-1)/(q-1)}+\frac{q-1}{(q^5-q)/(q-1)}<\frac{q^4+q-1}{(q^5-q)/(q-1)}<1,$$

so we are done again. ∎

Proposition 7.10. *Theorem 3 holds for all quasisimple covers of $S=\mathrm{PSU}_n(q)$, if $n\ge 5$ and $q\ge 5$ is odd, or if $(n,q)=(5,3)$.*

Proof. (i) By Lemma 7.1, it suffices to prove Theorem 3 for $G=\mathrm{SU}_n(q)$. Let $s=s_n(1)\in G$ be as constructed in Lemma 7.5. It suffices to show that every $g\in G$ is a product of three conjugates of s. Hence, it suffices to prove (7.2). Set

$$D:=\frac{(q^n-1)(q^{n-1}-q^2)}{(q-1)(q^2-1)}.$$

By [62, Theorem 4.1], every character $\chi\in\mathrm{Irr}(G)$ of degree less than D is either 1_G or one of $q+1$ irreducible Weil characters ζ_i, $0\le i\le q$, as defined in (4.3).

Consider the case $n\ge 6$. The construction of s in Lemma 7.5 shows that

$$|\mathbf{C}_G(s)|\le\begin{cases}(q+1)^{n-1}, & n\ge 8,\\ (q^4-1)(q+1)^2, & n=7,\\ (q^4-1)(q+1), & n=6.\end{cases}$$

Hence, as in the proof of Lemma 7.9,

$$\sum_{\chi\in\mathrm{Irr}(G),\ \chi(1)\ge D}\frac{|\chi(s)|^3}{\chi(1)}<\frac{|\mathbf{C}_G(s)|^{3/2}}{D}<0.6992.$$

Next we estimate $|\zeta_i(s)|$. In the notation of §4.3, by Lemma 7.5, $e(g,\xi^l)\le 1$ for all $0\le l\le q$ and equality can be attained at most twice. Arguing as in the proof of Lemma 4.6, we obtain

$$|\zeta_i(s)|\le\frac{q+q+1\cdot(q-1)}{q+1}=\frac{3q-1}{q+1}.$$

Hence

$$\sum_{\chi\in\mathrm{Irr}(G),\ 1<\chi(1)<D}\frac{|\chi(s)|^3}{\chi(1)}=\sum_{i=0}^{q}\frac{|\zeta_i(s)|^3}{\zeta_i(1)}\le\frac{(q+1)((3q-1)/(q+1))^3}{(q^n-q)/(q+1)}<0.1467.$$

Thus

$$\sum_{1_G\neq\chi\in\mathrm{Irr}(G)}\frac{|\chi(s)|^3}{\chi(1)}<0.6992+0.1467=0.8459,$$

so we are done by (7.2).

(ii) Assume now that $n=5$. The construction of s in Lemma 7.5 implies that $|\mathbf{C}_G(s)|\leq q^4-1$; furthermore, $\sum_{l=0}^{q}e(g,\xi^l)\leq 1$, hence $|\zeta_i(s)|\leq 1$ for all i by Lemma 4.6. Set

$$D=(q-1)(q^2+1)(q^5+1)/(q-1).$$

Using [41], we check that if $\chi\in\mathrm{Irr}(G)$ satisfies $1<\chi(1)<D$ then χ is either one of $q+1$ Weil characters ζ_i, $0\leq i\leq q$, or one of $q+1$ characters α_i, $0\leq i\leq q$, where

$$\alpha_0(1)=q^2(q^5+1)/(q+1),\ \alpha_i(1)=(q^2+1)(q^5+1)/(q+1),\ 1\leq i\leq q.$$

Inspecting the character table of $\mathrm{GU}_5(q)$ as given in [52], we observe that each α_i extends to $\mathrm{GU}_5(q)$ and $|\alpha_i(s)|\leq 1$. Hence,

$$\sum_{\chi\in\mathrm{Irr}(G),1<\chi(1)<D}\frac{|\chi(s)|^3}{\chi(1)}=\sum_{i=0}^{q}\frac{|\zeta_i(s)|^3}{\zeta_i(1)}+\sum_{i=0}^{q}\frac{|\zeta_i(s)|^3}{\zeta_i(1)}\leq\frac{2(q+1)}{(q^5-q)/(q+1)}<0.1334.$$

On the other hand,

$$\sum_{\chi\in\mathrm{Irr}(G),\ \chi(1)\geq D}\frac{|\chi(s)|^3}{\chi(1)}<\frac{(q^4-1)^{1.5}}{(q-1)(q^2+1)(q^5+1)/(q-1)}<0.5866.$$

Thus

$$\sum_{1_G\neq\chi\in\mathrm{Irr}(G)}\frac{|\chi(s)|^3}{\chi(1)}<0.1334+0.5866=0.72,$$

so we are done again. ∎

For $\mathrm{PSU}_n(3)$, respectively $\mathrm{PSp}_{2n}(q)$, we again employ the notion of breakable elements as defined in Definition 3.5(iii), respectively Definition 3.1.

Proposition 7.11. *Theorem 3 holds for all quasisimple covers of $S=\mathrm{PSU}_n(3)$ if $n\geq 5$.*

Proof. By Lemma 7.1, it suffices to prove Theorem 3 for $L:=\mathrm{SU}_n(3)$. Consider the following statements for $G:=\mathrm{GU}_n(3)$:

$$\mathsf{Q}(n):\ \begin{array}{l}\text{Every } g\in G \text{ can be written as } g=xyz,\\ \text{where } x,y,z\in G \text{ are 2-elements and } \det(x)=\det(y)=1,\end{array}$$

$$\mathsf{Q}_u(n):\ \begin{array}{l}\text{Every unbreakable } g\in G \text{ can be written as } g=xyz,\\ \text{where } x,y,z\in G \text{ are 2-elements and } \det(x)=\det(y)=1,\end{array}$$

By Lemma 7.4(ii), $\mathsf{Q}(n)$ holds for $3\leq n\leq 6$. It is straightforward to check that Theorem 3 holds for L with $n\geq 7$ once we show that $\mathsf{Q}_u(n)$ holds.

We now prove $\mathsf{Q}_u(n)$ for $n\geq 7$. Consider an unbreakable $g\in G$. Lemma 3.8 implies that $|\mathbf{C}_G(g)|\leq 3^{n+2}\cdot 2^4$. Let $s_1=s_2:=s_n(1)$ and $s_3:=s_n(\det(g))$, where $s_n(\delta)$ is constructed in Lemma 7.5; in particular, $|\mathbf{C}_G(s_i)|\leq 4^n$. Choosing

$$D:=(3^n-1)(3^{n-1}-9)/32,$$

by the Cauchy-Schwarz inequality,

$$\sum_{\chi\in\mathrm{Irr}(G),\ \chi(1)\geq D}\frac{|\chi(s_1)\chi(s_2)\chi(s_3)\bar{\chi}(g)|}{\chi(1)^2}<\frac{(4^n)^{3/2}(3^{n+2}\cdot 2^4)^{1/2}}{((3^n-1)(3^{n-1}-9)/32)^2}\leq 0.4866.$$

By [34, Proposition 6.6], the characters $\chi \in \mathrm{Irr}(G)$ of degree less than D consist of 4 linear characters and 4^2 Weil characters $\zeta_{i,j}$, $0 \le i,j \le 3$. Arguing as in the proof of Lemma 4.6, we obtain

$$|\zeta_{i,j}(s_k)| \le \frac{q+q+1\cdot(q-1)}{q+1} = \frac{3q-1}{q+1} = 2$$

for $q = 3$. Together with (4.16), this implies that

$$\sum_{\substack{\chi\in\mathrm{Irr}(G),\\ 1<\chi(1)<D}} \frac{|\prod_{k=1}^3 \chi(s_k)\cdot\bar\chi(g)|}{\chi(1)^2} = \sum_{\substack{\chi=\zeta_{i,j}\\ 0\le i,j\le 3}} \frac{|\prod_{k=1}^3 \chi(s_k)\cdot\bar\chi(g)|}{\chi(1)^2} \le \frac{4^2\cdot 2^3\cdot 3^{n-4}}{((3^n-3)/4)^2} < 0.0117.$$

Since

$$\sum_{\chi\in\mathrm{Irr}(G),\ \chi(1)=1} \frac{\chi(s_1)\chi(s_2)\chi(s_3)\bar\chi(g)}{\chi(1)^2} = 4,$$

we conclude that

$$\sum_{\chi\in\mathrm{Irr}(G)} \frac{\chi(s_1)\chi(s_2)\chi(s_3)\bar\chi(g)}{\chi(1)^2} \ne 0,$$

i.e. $g \in (s_1)^G\cdot(s_2)^G\cdot(s_3)^G$, as stated. ∎

Proposition 7.12. *Theorem 3 holds for all quasisimple covers of $S = \mathrm{PSp}_{2n}(q)$ if $n \ge 1$, $2 \nmid q$, and $(n,q) \ne (1,3)$.*

Proof. (i) Consider the case $n = 1$. The cases $\mathrm{PSp}_2(5) \cong \mathrm{Sp}_2(4)$, $\mathrm{PSp}_2(7) \cong \mathrm{SL}_3(2)$, and $\mathrm{PSp}_2(9) \cong \mathsf{A}_6$ are covered by Lemma 7.3, so we may assume $q \ge 11$. By Lemma 7.1, it suffices to prove Theorem 3 for $L := \mathrm{Sp}_2(q)$. Using the character table of L as given in [10], it is straightforward to check that $g \in s^L\cdot s^L\cdot s^L$ for all $g \in L$ if $|s| = 4$.

From now on we may assume $n \ge 2$. Hence by Lemma 7.1, it suffices to prove Theorem 3 for $L := \mathrm{Sp}_{2n}(q)$. If $q \equiv 1 \bmod 4$, then L is real by [63, Theorem 1.2], whence we are done by Lemma 2.7. Also, the case $\mathrm{PSp}_4(3) \cong \mathrm{SU}_4(2)$ is covered by Lemma 7.3. Note that Theorem 3 holds for $\mathrm{Sp}_6(3)$ and $\mathrm{Sp}_8(3)$ by Lemma 7.4(i). So we may assume $q \equiv 3 \bmod 4$ and $(n,q) \ne (2,3), (3,3), (4,3)$.

(ii) It suffices to prove that every unbreakable $g \in L$ is a product of three 2-elements of L. By Lemma 3.2,

$$|\mathbf{C}_L(g)| \le B := \begin{cases} 2q^n, & 2|n,\ q\ge 5,\\ 48\cdot 3^{2n+1}, & 2|n,\ q=3,\\ q^{2n-1}(q^2-1), & 2\nmid q.\end{cases}$$

Let s be as constructed in Lemma 7.6; in particular,

$$|\mathbf{C}_L(s)| \le C := \begin{cases} q^2-1, & n=2,\\ (q^2-1)(q+1), & n=3,\\ (q+1)^n, & n\ge 4.\end{cases}$$

Choosing

$$D := (q^n-1)(q^n-q)/2(q+1),$$

by the Cauchy-Schwarz inequality,

$$\sum_{\chi\in\mathrm{Irr}(L),\ \chi(1)\ge D} \frac{|\chi(s)^3\cdot\bar\chi(g)|}{\chi(1)^2} < \frac{C^{3/2}\cdot B^{1/2}}{D^2} \le 0.5255.$$

By [62, Theorem 5.2], the characters $\chi \in \mathrm{Irr}(L)$ of degree less than D consist of 1_L and four Weil characters: $\eta_{1,2}$ of degree $(q^n-1)/2$ and $\xi_{1,2}$ of degree $(q^n-1)/2$. Recall by

Lemma 7.6 that neither 1 nor -1 is an eigenvalue of s. Hence, (5.2) holds for s. Since $|\chi(g)| \le \chi(1)$,

$$\sum_{\chi\in\mathrm{Irr}(L),\ 1<\chi(1)<D} \frac{|\chi(s)^3\cdot\bar\chi(g)|}{\chi(1)^2} \le \sum_{\chi\in\mathrm{Irr}(L),\ 1<\chi(1)<D} \frac{|\chi(s)^3|}{\chi(1)} \le \frac{4}{(q^n-1)/2} < 0.1668.$$

Thus

$$\sum_{1_L\ne\chi\in\mathrm{Irr}(L)} \frac{|\chi(s)^3\cdot\bar\chi(g)|}{\chi(1)^2} < 0.5255 + 0.1668 = 0.6923,$$

so $g \in s^L\cdot s^L\cdot s^L$, as stated. ∎

Proposition 7.13. *Theorem 3 holds for all quasisimple covers of $S = \mathrm{P}\Omega^\epsilon_m(q)$ if $m \ge 7$ and $2 \nmid q$.*

Proof. By Lemma 2.7 and [63, Theorem 1.2], we may assume that $m \ne 8, 9$ and $q \equiv 3 \bmod 4$ if $m = 7$. Note that Theorem 3 holds for $\Omega_7(3)$ by Lemma 7.4. By Lemma 7.1, it suffices to prove Theorem 3 for $L := \Omega^\epsilon_m(q)$. Let $s = s^\epsilon_m(1) \in L$ be as constructed in Lemma 7.7.

(i) First we consider the case $m = 2n$; in particular, $n \ge 5$. The construction of s implies that

$$|\mathbf{C}_L(s)| \le C := \begin{cases} (q^4-1)(q+1), & n = 5,\\ (q+1)^n, & n \ge 6.\end{cases}$$

Choosing

$$D := \begin{cases} q^{4n-10}, & (n,\epsilon) \ne (5,-),\\ (q-1)(q^2+1)(q^3-1)(q^4+1), & (n,\epsilon) = (5,-),\end{cases}$$

by the Cauchy-Schwarz inequality,

$$\sum_{\chi\in\mathrm{Irr}(L),\ \chi(1)\ge D} \frac{|\chi(s)^3|}{\chi(1)} < \frac{C^{3/2}}{D} \le 0.135.$$

By [34, Propositions 5.3, 5.7], the characters $\chi \in \mathrm{Irr}(L)$ of degree less than D consist of 1_L and $q+4$ characters D°_α, $\alpha \in \mathrm{Irr}(X)$, where $X := \mathrm{Sp}_2(q)$. By Lemma 7.7, each $\beta \in \mathbb{F}^\times_{q^2}$ can appear as an eigenvalue of s of multiplicity at most 2. Arguing as in the proof of [34, Proposition 5.11], we obtain that $|D_\alpha(s)| \le q^2\alpha(1)$. Recalling that D°_α equals D_α if $\alpha \ne 1_X$, St_X and $D_\alpha - 1_L$ otherwise, cf. [34, Table II], for $n \ge 6$

$$\sum_{\substack{\chi\in\mathrm{Irr}(L),\\ 1<\chi(1)<D}} \frac{|\chi(s)^3|}{\chi(1)} \le \sum_{\alpha=1_X,\mathsf{St}_X} \frac{(q^2\alpha(1)+1)^3}{D^\circ_\alpha(1)} + \sum_{\substack{\alpha\in\mathrm{Irr}(X),\\ \alpha\ne 1_X,\mathsf{St}_X}} \frac{(q^2\alpha(1))^3}{D^\circ_\alpha(1)} < 0.849.$$

Consider the case $n = 5$. If $4|(q-\epsilon)$, then each $\beta \in \mathbb{F}^\times_{q^2}$ can appear as an eigenvalue of s of multiplicity at most 1, so arguing as above $|D_\alpha(s)| \le q\alpha(1)$. Suppose that $4 \nmid (q-\epsilon)$. In this case, the only eigenvalue β of s that belongs to $\mathbb{F}^\times_{q^2}$ is -1 and its multiplicity is 2. In the notation of the proof of [34, Proposition 5.11], for every $x \in X$

$$|\omega(xs)| \le q^{\dim\mathrm{Ker}(xs-I_{2m})/2} = q^{\dim\mathrm{Ker}(x+I_2)}.$$

When x runs over X, $\dim\mathrm{Ker}(x+I_2)$ is 2 only for $x = -I_2$, it is 1 for q^2-1 elements, and it is 0 for the rest. Hence,

$$|D_\alpha(s)| \le \frac{1}{|X|}\sum_{x\in X} |\omega(xs)\overline{\alpha(x)}| \le \frac{\alpha(1)}{|X|}(q^2 + q\cdot(q^2-1) + 1\cdot(q(q^2-1)-q^2)) = 2\alpha(1).$$

We have shown that $|D_\alpha(s)| \le q\alpha(1)$. Hence,

$$\sum_{\substack{\chi \in \mathrm{Irr}(L),\\ 1<\chi(1)<D}} \frac{|\chi(s)^3|}{\chi(1)} \le \sum_{\alpha=1_X,\mathsf{St}_X} \frac{(q\alpha(1)+1)^3}{D^\circ_\alpha(1)} + \sum_{\substack{\alpha \in \mathrm{Irr}(X),\\ \alpha \ne 1_X,\mathsf{St}_X}} \frac{(q\alpha(1))^3}{D^\circ_\alpha(1)} < 0.329.$$

Thus in all cases

$$\sum_{1_L \ne \chi \in \mathrm{Irr}(L)} \frac{|\chi(s)^3|}{\chi(1)} < 1,$$

so $g \in s^L \cdot s^L \cdot s^L$ by (7.2), as stated.

(ii) Now we consider the case $m = 2n+1 \ge 11$. Again $|\mathbf{C}_L(s)| \le (q+1)^n$. Set $D := q^{4n-8}$. By the Cauchy-Schwarz inequality

$$\sum_{\chi \in \mathrm{Irr}(L),\ \chi(1)\ge D} \frac{|\chi(s)^3|}{\chi(1)} < \frac{C^{3/2}}{D} \le 0.062.$$

By [34, Corollary 5.8], the characters $\chi \in \mathrm{Irr}(L)$ of degree less than D consist of 1_L and $q+4$ characters D°_α, $\alpha \in \mathrm{Irr}(X)$. By Lemma 7.7, each $\beta \in \mathbb{F}_{q^2}^\times$ can appear as an eigenvalue of s of multiplicity at most e, where we can choose $e = 2$ for $n \ge 6$ and $e = 1$ for $n = 5$. Arguing as in the proof of [34, Proposition 5.11], we obtain that $|D_\alpha(s)| \le q^e\alpha(1)$. Recalling that D°_α equals D_α if $\alpha \ne \xi_{1,2}$ (the two Weil characters of degree $(q+1)/2$ of X) and $D_\alpha - 1_L$ otherwise, cf. [34, Table I],

$$\sum_{\chi \in \mathrm{Irr}(L),\ 1<\chi(1)<D} \frac{|\chi(s)^3|}{\chi(1)} \le \sum_{\alpha=\xi_{1,2}} \frac{(q^2\alpha(1)+1)^3}{D^\circ_\alpha(1)} + \sum_{\alpha \in \mathrm{Irr}(X),\ \alpha \ne \xi_{1,2}} \frac{(q^2\alpha(1))^3}{D^\circ_\alpha(1)} < 0.281,$$

so we are done by (7.2).

(iii) Finally, we consider the case $m = 7$, so $q \ge 7$. Theorem 3 holds for

$$\Omega_3(q) \cong \mathrm{PSL}_2(q),\ \Omega_4^+(q) \cong \mathrm{SL}_2(q) \circ \mathrm{SL}_2(q),\ \Omega_4^-(q) \cong \mathrm{PSL}_2(q^2),\ \Omega_5(q) \cong \mathrm{PSp}_4(q)$$

by Proposition 7.12, and for $\mathrm{Spin}_6^+(q) \cong \mathrm{SL}_4(q)$, $\mathrm{Spin}_6^-(q) \cong \mathrm{SU}_4(q)$ by Lemma 7.8. Hence, if $g \in L = \Omega_7(q)$ is breakable in the sense of Definition 3.1, then g is a product of three 2-elements of L. If $g \in L$ is unbreakable then $|\mathbf{C}_L(g)| \le q^4(q+1)^2$ by Lemma 3.3. Also, $\chi(1) \ge q^4+q^2+1$ for all $1_L \ne \chi \in \mathrm{Irr}(L)$ by [62, Theorem 1.1]. As $|\mathbf{C}_L(s)| \le (q+1)^3$, by the Cauchy-Schwarz inequality,

$$\sum_{1_L \ne \chi \in \mathrm{Irr}(L)} \frac{|\chi(s)^3 \cdot \bar\chi(g)|}{\chi(1)^2} \le \frac{(q+1)^{4.5} \cdot q^2(q+1)}{(q^4+q^2+1)^2} < 0.757,$$

so we are done as well. ∎

7.4. **Proof of Theorem 3 for exceptional groups in odd characteristics.** Our goal is to prove the following result, which, together with the results of §§7.1 and 7.3, completes the proof of Theorem 3.

Theorem 7.14. *Let G be a quasisimple group such that $G/\mathbf{Z}(G)$ is an exceptional simple group of Lie type in odd characteristic. Then every element of G is a product of three 2-elements.*

The proof consists of a series of lemmas. The first is immediate from [40].

Lemma 7.15. *Let G be as in Theorem 7.14, and let χ be a nontrivial irreducible character of G. Then $\chi(1) \ge N$, where N is as in Table 4.*

Lemma 7.16. *If G is as in Theorem 7.14, then G has a 2-element s such that $|\mathbf{C}_G(s)| \le C$, where C is as in Table 4.*

G	N	C
$E_8(q)$	$q(q^6+1)(q^{10}+1)(q^{12}+1)$	q^8-1
$E_7(q)$	$q(q^{14}-1)(q^6+1)/(q^4-1)$	$(q+1)^2q^7$
$E_6^\epsilon(q)\,(\epsilon=\pm)$	$q(q^4+1)(q^6+\epsilon q^3+1)$	$(q^4-1)(q-\epsilon)^2$, $q\equiv\epsilon \bmod 4$
		$(q-\epsilon)q^7$, $q\equiv-\epsilon \bmod 4$
$F_4(q)$	q^8+q^4+1	$(q+1)^3q^3$
$G_2(q)\,(q>3)$	q^3-1	q^2-1
${}^3D_4(q)$	$q(q^4-q^2+1)$	$(q^3-1)(q+1)$
${}^2G_2(q)\,(q>3)$	q^2-q+1	$q+1$

TABLE 4. Bounds for character degrees and centralizers

Proof. For the most part we construct the element s within a suitable product of classical groups inside G, using the methods of §7.2.

For $G=E_8(q)$ we work in a subsystem subgroup A of type A_8. This has shape $d.L_9(q).e$, where $e=(3,q-1)$ and $d=(9,q-1)/e$ (see for example [36, Table 5.1]); the derived subgroup is a quotient of $\mathrm{SL}_9(q)$ by a central subgroup Z. We will define s in $\mathrm{SL}_9(q)$, and identify it with its image modulo Z. Choose $\gamma\in\mathbb{F}_{q^8}$ of order $(q^8-1)_2$, and define $s_8\in\mathrm{GL}_1(q^8)\leq\mathrm{GL}_8(q)$ to be conjugate over $\bar{\mathbb{F}}_q$ to $\mathrm{diag}(\gamma,\gamma^q,\gamma^{q^2},\dots,\gamma^{q^7})$. Let $s=\mathrm{diag}(s_8,\alpha)\in\mathrm{SL}_9(q)$, where $\alpha^{-1}=\det(s_8)$. Then $|\mathbf{C}_A(s)|=q^8-1$. Now, by [39, 11.2],

$$\mathcal{L}(E_8)\downarrow A_8=\mathcal{L}(A_8)+V_{A_8}(\lambda_3)+V_{A_8}(\lambda_6).$$

Here $V_{A_8}(\lambda_3)\cong\wedge^3(V_9)$, the wedge-cube of the natural module for $\mathrm{SL}_9(q)$, and $V_{A_8}(\lambda_6)$ is the dual of this. Since $\gamma^{q^i+q^j+q^k}$ cannot equal 1 for distinct i,j,k between 0 and 7, and also $\gamma^{q^i+q^j}$ cannot lie in $\mathbb{F}_q$, the element s has no nonzero fixed points in $\wedge^3(V_9)$, so $\dim\mathbf{C}_{\mathcal{L}(E_8)}(s)=8$. Hence $\mathbf{C}_G(s)$ is a maximal torus, so $\mathbf{C}_G(s)=\mathbf{C}_A(s)$ of order q^8-1.

Next consider $G=E_7(q)$. We will work in the simply connected version of G; the element s we construct works equally well for the adjoint version. Let A be a subsystem subgroup of type $A_2^\epsilon A_5^\epsilon$ ($\epsilon=\pm1$), where $q\equiv-\epsilon \bmod 4$. This has the subgroup $\mathrm{SL}_3^\epsilon(q)\circ\mathrm{SL}_6^\epsilon(q)$ of index $(3,q-\epsilon)$. Let $\gamma\in\mathbb{F}_{q^4}$ have order $(q^4-1)_2$, and define $\alpha=\gamma^{(q^2+1)(\epsilon q+1)}$, $\beta=\gamma^{2(\epsilon q+1)}$. Now define $s_1\in\mathrm{SL}_3^\epsilon(q)$, $s_2\in\mathrm{SL}_6^\epsilon(q)$ so that they are conjugate over $\bar{\mathbb{F}}_q$ to

$$\mathrm{diag}(\gamma^{-2},\gamma^{-2\epsilon q},\beta)\in\mathrm{SL}_3,\ \ \mathrm{diag}(\gamma,\gamma^{\epsilon q},\gamma^{q^2},\gamma^{\epsilon q^3},1,\alpha)\in\mathrm{SL}_6,$$

respectively. Let $s=s_1s_2\in A$. Then $|\mathbf{C}_A(s)|=(q^4-1)(q^2-1)(q-\epsilon)$. From [39, 11.8],

$$\mathcal{L}(E_7)\downarrow A_2A_5=\mathcal{L}(A_2A_5)+(V_{A_2}(\lambda_1)\otimes V_{A_5}(\lambda_2))+(V_{A_2}(\lambda_2)\otimes V_{A_5}(\lambda_4)).$$

Here $V_{A_2}(\lambda_1)\otimes V_{A_5}(\lambda_2)\cong V_3\otimes\wedge^2(V_6)$, where V_3,V_6 are the natural modules for SL_3 and SL_6. One checks that s has fixed space of dimension 1 on this module (coming from the product of the eigenvalues $\beta,1,\alpha$). Hence $\dim\mathbf{C}_{\mathcal{L}(E_7)}(s)=9$, and so over $\bar{\mathbb{F}}_q$ we deduce that $\mathbf{C}_{E_7}(s)=A_1T_6$, where T_6 denotes a torus of rank 6. It follows that $|\mathbf{C}_G(s)|=|A_1(q)|\cdot|T_6(q)|$. As $\mathbf{C}_G(s)$ contains $\mathbf{C}_A(s)$, of the order given above, $|\mathbf{C}_G(s)|\leq|A_1(q)|(q^4-1)(q+1)^2<(q+1)^2q^7$.

If $G=E_6^\epsilon(q)$, then we work in a subsystem subgroup A of type A_1A_5 containing $\mathrm{SL}_2(q)\circ\mathrm{SL}_6^\epsilon(q)$. Again let $\gamma\in\mathbb{F}_{q^4}$ have order $(q^4-1)_2$ and define $s_2\in\mathrm{SL}_6^\epsilon(q)$ as the previous paragraph. Define $s_1\in\mathrm{SL}_2(q)$ to be conjugate over $\bar{\mathbb{F}}_q$ to $\mathrm{diag}(\gamma^{2(q+\epsilon)},\gamma^{-2(q+\epsilon)})$ if $q\equiv\epsilon \bmod 4$, and to I_2 otherwise. Set $s=s_1s_2$. Then $|\mathbf{C}_A(s)|$ is equal to $(q^4-1)(q-\epsilon)^2$ if $q\equiv\epsilon \bmod 4$, and to $|A_1(q)|(q^4-1)(q-\epsilon)$ otherwise. By [39, 11.10],

$$\mathcal{L}(E_6)\downarrow A_1A_5=\mathcal{L}(A_1A_5)+(V_{A_1}(1)\otimes V_{A_5}(\lambda_3)),$$

and the second summand is $V_2 \otimes \wedge^3(V_6)$, where V_2, V_6 are the natural modules for A_1, A_5. We check that s has no nonzero fixed points on this tensor product, and it follows that $\mathbf{C}_{E_6}(s) = \mathbf{C}_{A_1A_5}(s)$; hence $\mathbf{C}_G(s) = \mathbf{C}_A(s)$, giving the result.

Now let $G = F_4(q)$. Here we construct our element s in a subsystem subgroup $A = B_4(q) \cong \mathrm{Spin}_9(q)$. It is convenient to define it in the quotient $\Omega_9(q)$ and take a preimage. We follow the proof of Lemma 7.7. Let $\gamma \in \mathbb{F}_{q^2}$ have order $(q^2-1)_2$, and define $s_4 \in \mathrm{GL}_1(q^2) \leq \mathrm{GL}_2(q) \leq SO_4^+(q)$ to be conjugate over $\bar{\mathbb{F}}_q$ to $\mathrm{diag}(\gamma, \gamma^q, \gamma^{-1}, \gamma^{-q})$. Then s_4 has spinor norm -1. Let $q \equiv \epsilon \bmod 4$ with $\epsilon = \pm 1$, and define $s_2 \in SO_2^\epsilon(q)$ to be conjugate to $\mathrm{diag}(\gamma^{q+\epsilon}, \gamma^{-(q+\epsilon)})$. Then s_2 also has spinor norm -1, so $t_1 := \mathrm{diag}(s_4, s_2) \in \Omega_6^\epsilon(q)$. Finally, let $t_2 := \mathrm{diag}(-1,-1,1) \in \Omega_3(q)$ and define $s \in A$ to be the preimage of $\mathrm{diag}(t_1, t_2) \in \Omega_9(q)$. Then $|\mathbf{C}_A(s)| = (q^2-1)(q-\epsilon)^2$. Now

$$\mathcal{L}(F_4) \downarrow B_4 = \mathcal{L}(B_4) \oplus V_{B_4}(\lambda_4).$$

The second summand is the spin module for $B_4(q)$, which restricts to the preimage of $\Omega_6^\epsilon(q) \times \Omega_3(q)$ as $(V_4 \otimes V_2) \oplus (V_4^* \otimes V_2^*)$, where each summand is a tensor product of natural modules for the isomorphic group $\mathrm{SL}_4^\epsilon(q) \times \mathrm{SL}_2(q)$. Elements of $\mathrm{SL}_4^\epsilon(q)$, $\mathrm{SL}_2(q)$ inducing t_1, t_2 are $x_1 := \mathrm{diag}(1, \gamma, \gamma^{\epsilon q}, \gamma^{-\epsilon q-1})$, $x_2 := \mathrm{diag}(\gamma^{(q-\epsilon)/2}, \gamma^{-(q-\epsilon)/2})$, respectively. The tensor product of x_1 and x_2 has fixed point space of dimension at most 1, and it follows that $\dim \mathbf{C}_{\mathcal{L}(F_4)}(s) = 4$ or 6. If it is 4 then $\mathbf{C}_G(s) = \mathbf{C}_A(s)$, while if it is 6, then $\mathbf{C}_{F_4}(s) = A_1T_3$, whence $|\mathbf{C}_G(s)| \leq |A_1(q)|(q+1)^3$, as in the conclusion.

For $G = G_2(q)$ or ${}^3D_4(q)$, we pick our element s in a subgroup $A = \mathrm{SL}_3(q)$: let $\gamma \in \mathbb{F}_{q^2}$ have order $(q^2-1)_2$ and take s to be conjugate over $\bar{\mathbb{F}}_q$ to $\mathrm{diag}(\gamma, \gamma^q, \alpha)$ where $\alpha = \gamma^{-(q+1)}$. Now $\mathcal{L}(G_2) \downarrow A_2 = \mathcal{L}(A_2) + V_3 + V_3^*$ and $\mathcal{L}(D_4) \downarrow A_2 = \mathcal{L}(A_2) + V_3^3 + (V_3^*)^3 + V_1^2$, where V_3 is the natural 3-dimensional module and V_1 is trivial. It follows that $\mathbf{C}_{\mathcal{L}(G_2)}(s)$ and $\mathbf{C}_{\mathcal{L}(D_4)}(s)$ have dimensions 2 and 4 respectively, so $\mathbf{C}_G(s)$ is a maximal torus, as in the conclusion.

Finally, for $G = {}^2G_2(q)$, an element s of order 4 has centralizer of order $q+1$ (see [66]). This completes the proof. ∎

Lemma 7.17. *Theorem* 7.14 *holds for* $E_8(q)$, $E_7(q)$, $G_2(q)$, ${}^2G_2(q)$, *and also for* $E_6^\epsilon(q)$ *with* $q \equiv \epsilon \bmod 4$.

Proof. Let G be one of these groups, and let s be the 2-element of G produced in Lemma 7.16. As in the proof of Proposition 7.9, it is sufficient to establish that for every $g \in G$,

$$\sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(s)^3 \bar{\chi}(g)}{\chi(1)^2} \neq 0, \tag{7.3}$$

and to prove this it suffices to show

$$\sum_{1 \neq \chi \in \mathrm{Irr}(G)} \frac{|\chi(s)|^3}{\chi(1)} < 1.$$

Lemma 7.15 implies that $\chi(1) \geq N$ for all nontrivial irreducible characters χ, where N is as in Table 4. Hence

$$\sum_{1 \neq \chi \in Irr(G)} \frac{|\chi(s)|^3}{\chi(1)} < \frac{|\mathbf{C}_G(s)|^{1/2}}{N} \sum_{\chi \in Irr(G)} |\chi(s)|^2 = \frac{|\mathbf{C}_G(s)|^{3/2}}{N} \leq \frac{C^{3/2}}{N},$$

where C is as in Table 4. One checks that $C^{3/2}/N < 1$ for the groups in the hypothesis, so the lemma follows. ∎

Lemma 7.18. *Theorem* 7.14 *holds for* $E_6^\epsilon(q)$ *with* $q \equiv -\epsilon \bmod 4$, $F_4(q)$ *and* ${}^3D_4(q)$.

Proof. Let G be one of these groups, let s be the 2-element of G from Lemma 7.16, and let $g \in G$. As in the previous proof,

$$\sum_{1\neq\chi\in\mathrm{Irr}(G)} \frac{|\chi(s)|^3|\chi(g)|}{\chi(1)^2} < \frac{|\mathbf{C}_G(s)|^{3/2}|\mathbf{C}_G(g)|^{1/2}}{N^2} \leq \frac{C^{3/2}|\mathbf{C}_G(g)|^{1/2}}{N^2},$$

where C, N are as in Table 4. The result is proved if the above sum is less than 1, so we may assume that

$$|\mathbf{C}_G(g)| \geq \frac{N^4}{C^3}. \tag{7.4}$$

Our strategy is to show that an element g satisfying this bound must lie in a subgroup of G that is a commuting product of quasisimple classical groups. (A similar strategy was carried out in Section 7 of [34].) The conclusion then follows immediately from the results in Section 7.3, where Theorem 7.14 is established for classical groups.

Consider $G = F_4(q)$. Here (7.4) gives

$$|\mathbf{C}_G(g)| \geq \frac{(q^8+q^4+1)^4}{(q+1)^9q^9}. \tag{7.5}$$

Assume first that g is a unipotent element. The classes and centralizers of unipotent elements in G are given in [39, Table 22.2.4], and every centralizer satisfying the above bound has even order. Hence there is an involution t such that $g \in \mathbf{C}_G(t)$. Now $\mathbf{C}_G(t)$ is either a quasisimple group $B_4(q)$, or a group of the form $(\mathrm{SL}_2(q)\circ\mathrm{Sp}_6(q)).2$, with the unipotent element g lying in the subgroup $\mathrm{SL}_2(q)\circ\mathrm{Sp}_6(q)$. Hence g is in a product of quasisimple classical groups, except possibly in the case where $q = 3$ and $g \in \mathbf{C}_G(t) = (\mathrm{SL}_2(3)\circ\mathrm{Sp}_6(3)).2$. In the latter case, a computation shows that every element of $\mathbf{C}_G(t)$ is a product of three 2-elements.

Now assume g is not unipotent; say $g = xu$ has semisimple part $x \neq 1$ and unipotent part $u \in \mathbf{C}_G(x)$. Now $\mathbf{C}_G(x)$ is a subsystem subgroup of G, and the bound (7.5) forces this to have a normal subgroup $D = B_4(q)$, $D_4^\epsilon(q)$, $B_3(q)$, $C_3(q)$, $A_3^\epsilon(q)$, $B_2(q)$ or $A_2^\epsilon(q)$. Then $x \in \mathbf{C}_G(D)$, and the unipotent elements of $\mathbf{N}_G(D)$ generate a subgroup of $D\mathbf{C}_G(D)$, which is contained in a subsystem subgroup $S := B_4(q)$, $A_1(q)C_3(q)$ or $A_2^\epsilon(q)A_2^\epsilon(q)$. Hence $g = xu \in S$. Observe that S is a product of quasisimple classical groups, except for $A_1(q)C_3(q)$ when $q = 3$; however, we already noted that every element of this subgroup is a product of three 2-elements in its normalizer. This completes the proof for $G = F_4(q)$.

The proof for $G = E_6^\epsilon(q)$ is similar. If g is unipotent then the bound (7.4) and [39, Table 22.2.3] imply that $\mathbf{C}_G(g)$ has even order, so $g \in \mathbf{C}_G(t)$ for some involution t. This centralizer is either $(q-\epsilon)\circ D_5^\epsilon(q)$ or $(\mathrm{SL}_2(q)\circ\mathrm{SL}_6^\epsilon(q)).2$. Hence the unipotent element g lies in $D_5^\epsilon(q)$ or $\mathrm{SL}_2(q)\circ\mathrm{SL}_6^\epsilon(q)$, and this is a product of quasisimple groups, apart from the latter when $q = 3$, in which case a computation shows that every element of $\mathbf{C}_G(t)$ is a product of three 2-elements. When g is not unipotent, the bound (7.4) is actually stronger than the bound used in the proof of [34, Theorem 7.1] for non-unipotent elements of $E_6^\epsilon(q)$, and this proof shows that such elements lie in a product of quasisimple classical subgroups. Alternatively, an argument similar to that for $F_4(q)$ gives the result in this case.

Finally, let $G = {}^3D_4(q)$. The unipotent classes and centralizers can be found in [57], and the unipotent case is handled exactly as for $F_4(q)$. For $g = xu$ non-unipotent as above, (7.4) implies that $\mathbf{C}_G(x)$ has a normal subgroup $D = A_1(q^3)$ or $A_2^\epsilon(q)$. In the first case we argue as before that $g = xu$ lies in $D\mathbf{C}_G(D) = A_1(q^3)\circ A_1(q)$. In the second case $\mathbf{C}_G(s) = ((q^2+\epsilon q+1)\circ D).(3, q-\epsilon)$, and we can assume that $u \neq 1$ (otherwise $g = x$ is real, and the result follows from Lemma 2.7. The group generated by the unipotent elements of $\mathbf{C}_G(s)$ is just D, so $u \in D$. But the centralizer of a nontrivial unipotent

element of $D = A_2^\epsilon(q)$ has order at most $(q+1)q^3$ (see [39, Chapter 3]), so this gives $|\mathbf{C}_G(g)| \leq (q^2+\epsilon q+1)(q+1)q^3$, which contradicts (7.4). ∎

8. Asymptotic surjectivity: Proofs of Theorems 4, 5, and 6

Lemma 8.1. *Let $k, Q \geq 2$ be integers. There is an explicit integer $D = D(k,Q)$, depending on k and Q and divisible by 8, such that, for every integer N with $\mathbf{\Omega}(N) \leq k$ and for every $q < Q$, every central element of $G \in \{\mathrm{SL}_m(q), \mathrm{SU}_m(q), \mathrm{Sp}_{2m}(q), \Omega^+_{2m}(q)\}$ is an Nth power in G whenever $D|m$.*

Proof. We define $D = 2(Q!)^{k+1}$ in the case $G = \mathrm{SL}$ or SU, and $D = 2^{k+1}$ in the case $G = \mathrm{Sp}$ or Ω^+. It suffices to prove the claim for nontrivial $z \in \mathbf{Z}(G)$.

Consider the case $G = \mathrm{SL}_m(q)$ or $\mathrm{SU}_m(q)$, and set $\epsilon = +$, respectively $\epsilon = -$. Since $2|m$,

$$\mathrm{GL}^\epsilon_m(q) > \mathrm{GL}_{m/2}(q^2) \geq T := C_{q^m-1}.$$

Furthermore, $T_1 := T \cap G$ has index dividing $q-\epsilon$ and contains $\mathbf{Z}(G)$; in particular, $z \in T_1$. If p is a prime dividing $|z|$, then $p|(q-\epsilon)$, whence $p|(q^2-1)$ and $p \leq q+1 \leq Q$. Thus

$$\left(\frac{q^m-1}{q^2-1}\right)_p = \left(\frac{m}{2}\right)_p \geq ((q-\epsilon)_p)^{k+1},$$

so

$$\left(\frac{|T_1|}{|z|}\right)_p \geq ((q-\epsilon)_p)^k \geq p^k.$$

Write $N = N_1N_2$, where all prime divisors of N_1 divide $|z|$ and $\gcd(N_2,|z|) = 1$. Since $\mathbf{\Omega}(N) \leq k$, we have shown that N_1 divides $|T_1|/|z|$. As T_1 is cyclic, we can find $t \in T_1$ such that all prime divisors of $|t|$ divide $|z|$ and $t^{N_1} = z$. Since $\gcd(N_2,|t|) = 1$, $t = h^{N_2}$ for some $h \in T_1$. It follows that $z = h^N$, as desired.

If G is $\mathrm{Sp}_{2m}(q)$ or $\Omega^+_{2m}(q)$, then $|z| = 2$ and q is odd. We can use the same argument as above, taking T_1 to be a cyclic maximal torus of order q^m-1 in $\mathrm{Sp}_{2m}(q)$, respectively $\mathrm{SO}^+_{2m}(q)$. ∎

Let $q = p^f$ be a prime power, let $n \geq 13$ be an integer, and let $\epsilon = \pm$. If $\epsilon = +$, then we use $\ell^*(q^n-\epsilon)$ to denote a primitive prime divisor $\ell(p,nf)$ if $2 \nmid n$, and $\ell(p,nf)\ell(p,nf/2)$ if $2|n$. If $\epsilon = -$, then we use $\ell^*(q^n-\epsilon)$ to denote a primitive prime divisor $\ell(p,2nf)$. Recall the set $\mathcal{R}(G)$ for a classical group was defined after Theorem 2.1. It is convenient to also include $\ell(p,nf/2)$ in $\mathcal{R}(\mathrm{SL}_n(p^f))$ when $2|n$.

Lemma 8.2. *Let q be a prime power, let $n \geq m \geq 13$ be integers, and let $\alpha, \beta = \pm$. Suppose that $\gcd(\ell^*(q^n-\alpha), \ell^*(q^m-\beta)) > 1$. Then either $(n,\alpha) = (m,\beta)$, or $\alpha = +$ and $n \in \{2m, 4m\}$.*

Proof. If $n = m$, then $\gcd(\ell^*(q^n-\alpha), \ell^*(q^m-\beta)) > 1$ certainly implies $\alpha = \beta$. Suppose $n > m$. If $\alpha = -$, then $\ell^*(q^n-\alpha) = \ell(q,2n)$ does not divide $\prod_{i=1}^{2n-1}(q^i-1)$, so it cannot be non-coprime to $\ell^*(q^m-\beta)$. So $\alpha = +$, and $\gcd(\ell^*(q^n-1), \ell^*(q^m-\beta)) > 1$ implies that $n = 2m$ or $n = 4m$. ∎

Now we prove an analogue of [31, Proposition 3.4.1] for groups of type A and C:

Proposition 8.3. *For every integer $a \geq 1$, there are explicit positive integers $N_1(a)$ and $V_1(a)$ such that the following statements hold. Let $n > 2a+2$ be any integer and q be any prime power. Let s and t be regular semisimple elements of $G := \mathrm{Sp}_{2n}(q)$ belonging to maximal tori T_1 and T_2 of type $T^{\epsilon_1,\epsilon_2}_{n-a,a}$ and $T^{\epsilon_3,\epsilon_4}_{a+1,n-a-1}$ respectively, where $\epsilon_i = \pm$ and $\epsilon_1\epsilon_2 = -\epsilon_3\epsilon_4$. Then the number of distinct irreducible characters of G which vanish neither*

on s nor on t is at most $N_1(a)$. Likewise, the absolute values of these characters on s and t is at most $V_1(a)$.

Proof. (i) First we show that the maximal tori T_1 and T_2 are *weakly orthogonal* in the sense of [31, Definition 2.2.1] whenever $\epsilon_1\epsilon_2 = -\epsilon_3\epsilon_4$. We follow the proof of [31, Proposition 2.6.1]. The dual group G^* is $\mathrm{SO}(V) \cong \mathrm{SO}_{2n+1}(q)$, where $V = \mathbb{F}_q^{2n+1}$ is endowed with a suitable quadratic form Q. Consider the tori dual to T_1 and T_2, and assume g is an element belonging to both of them. We need to show that $g = 1$. We consider the spectrum S of the semisimple element g on V as a multiset. Then S can be represented as the joins of multisets $X \sqcup Y \sqcup \{1\}$ and $Z \sqcup T \sqcup \{1\}$, where

$$\begin{aligned} X &:= \{x, x^q, \dots, x^{q^{n-a-1}}, x^{-1}, x^{-q}, \dots, x^{-q^{n-a-1}}\},\\ Y &:= \{y, y^q, \dots, y^{q^{a-1}}, y^{-1}, y^{-q}, \dots, y^{-q^{a-1}}\},\\ Z &:= \{z, z^q, \dots, z^{q^{n-a-2}}, z^{-1}, z^{-q}, \dots, z^{-q^a}\},\\ T &:= \{t, t^q, \dots, t^{q^a}, t^{-1}, t^{-q}, \dots, t^{-q^a}\}, \end{aligned}$$

for some $x, y, z, t \in \bar{\mathbb{F}}_q^\times$. Furthermore,

$$x^{q^{n-a}-\epsilon_1} = y^{q^a-\epsilon_2} = z^{q^{n-a-1}-\epsilon_3} = t^{q^{a+1}-\epsilon_4} = 1.$$

Let A be a multiset of elements of $\bar{\mathbb{F}}_q$, where $1 \in A$, the multiplicity of each element of A is $2n+1$, and with the property that if $u \in A$ then $u^q, u^{-1} \in A$. We claim that if $|A \cap S| > 1$ then $A \supseteq S$. Indeed, since the multiplicity of every $u \in S$ is at most $2n+1$, if $A \cap (X \sqcup \{1\}) > 1$ then $A \supseteq X$, and if $|A \cap (X \sqcup \{1\})|, |A \cap (Y \sqcup \{1\})| > 1$ then $A \supseteq S$; and similarly for Y, Z, T. Now if $|A \cap S| > 1$ but $A \not\supseteq S$, then $S = X \sqcup Y \sqcup \{1\}$ implies that $|A \cap S| \in \{2a+1, 2(n-a)+1\}$. But $S = Z \sqcup T \sqcup \{1\}$ also, so $|A \cap S| \in \{2a+3, 2(n-a)-1\}$, which is a contradiction as $n \geq 2a+3$.

Applying the claim to the multiset A consisting of those $u \in \bar{\mathbb{F}}_q$ such that $u^{q^{n-a}-\epsilon_1} = 1$, each with multiplicity $2n+1$, and noting that $A \supseteq X \sqcup \{1\}$, we deduce that $u^{q^{n-a}-\epsilon_1} = 1$ for all $u \in S$. Arguing similarly, we obtain

$$u^{q^{n-a}-\epsilon_1} = u^{q^a-\epsilon_2} = u^{q^{n-a-1}-\epsilon_3} = u^{q^{a+1}-\epsilon_4} = 1$$

for all $u \in S$.

Consider $u \in S$. Suppose for instance that $\epsilon_3 \neq \epsilon_1$. In particular,

$$u^{q^{n-a-1}+\epsilon_1} = u^{q^{n-a}-\epsilon_1} = 1,$$

whence $u^{q+1} = 1$. The condition $\epsilon_1\epsilon_2 = -\epsilon_3\epsilon_4$ now implies that $\epsilon_2 = \epsilon_4$, so $|u|$ divides $\gcd(q^{a+1} - \epsilon_2, q^a - \epsilon_2) | (q-1)$. It follows that $u^2 = 1$ for all $u \in S$. The same argument applies to the case $\epsilon_3 = \epsilon_1$. We have shown that $u^2 = 1$ for all $u \in S$. Now if 1 has multiplicity at least 2 in S, then applying the claim to the multiset A' consisting only of 1 with multiplicity $2n+1$, we see that $g = 1_V$ as stated. It remains to consider the case $g = \mathrm{diag}(-1, -1, \dots, -1, 1)$. Now $\mathrm{Ker}(g + 1_V)$ is a quadratic subspace of V of type $\epsilon_1\epsilon_2$ and also of type $\epsilon_3\epsilon_4$, a contradiction.

(ii) Now we proceed exactly as in the proof of [31, Proposition 3.4.1], using the main result of [44] which holds for both types B_n and C_n. Also note that the proof of [31, Proposition 3.4.1] uses only the weak orthogonality of the two tori T_1 and T_2 but not the signs ϵ_i in their definitions. ∎

Proposition 8.4. *For every integer $a \geq 1$, there are explicit positive integers $N_2(a)$ and $V_2(a)$ such that the following statements hold. Let $\epsilon = \pm$, q any prime power, and let n be any integer greater than $2a+2$. Let s and t be regular semisimple elements of $G := \mathrm{SL}_n^\epsilon(q)$ belonging to maximal tori T_1 and T_2 of type $T_{n-a,a}$ and $T_{a+1,n-a-1}$. Then the number of distinct irreducible characters of G which vanish neither on s nor on t is at most $N_2(a)$. Likewise, the absolute values of these characters on s and t is at most $V_2(a)$.*

Proof. (i) Again, we show that the maximal tori T_1 and T_2 are weakly orthogonal. Here, the dual group G^* is $\mathrm{PGL}^\epsilon(V) \cong \mathrm{PGL}^\epsilon_n(q)$, where $V = \mathbb{F}_q^n$ for $\epsilon = +$ and $V = \mathbb{F}_{q^2}^n$ for $\epsilon = -$. Consider the complete inverse images $T_{n-a,a}$ and $T_{n-a-1,a+1}$ of the tori dual to T_1 and T_2 in $H := \mathrm{GL}^\epsilon(V)$, and assume g is an element belonging to both of them. We need to show that $g \in \mathbf{Z}(H)$. The multiset S of eigenvalues of the semisimple element g on V can be represented as the joins of multisets $X \sqcup Y \sqcup \{1\}$ and $Z \sqcup T \sqcup \{1\}$, where

$$X := \{x, x^{q\epsilon}, \dots, x^{(q\epsilon)^{n-a-1}}\},\ Y := \{y, y^{q\epsilon}, \dots, y^{(q\epsilon)^{a-1}}\},$$
$$Z := \{z, z^{q\epsilon}, \dots, z^{(q\epsilon)^{n-a-2}}\},\ T := \{t, t^{q\epsilon}, \dots, t^{(q\epsilon)^{a}}\},$$

for some $x, y, z, t \in \bar{\mathbb{F}}_q^\times$; furthermore,

$$x^{(q\epsilon)^{n-a}-1} = y^{(q\epsilon)^a-1} = z^{(q\epsilon)^{n-a-1}-1} = t^{(q\epsilon)^{a+1}-1} = 1.$$

Let A be a multiset of elements of $\bar{\mathbb{F}}_q$, where the multiplicity of each element of A is n, and with the property that if $u \in A$ then $u^{q\epsilon} \in A$. We claim that if $A \cap S \neq \emptyset$ then $A \supseteq S$. Indeed, since the multiplicity of every $u \in S$ is at most n, if $A \cap X \neq \emptyset$ then $A \supseteq X$, and if $A \cap X, A \cap Y \neq \emptyset$ then $A \supseteq S$; and similarly for Y, Z, T. Now if $A \cap S \neq \emptyset$ but $A \not\supseteq S$, then $S = X \sqcup Y$ implies that $|A \cap S| \in \{a, n-a\}$. But $S = Z \sqcup T$ as well, so $|A \cap S| \in \{a+1, n-a-1\}$, which is a contradiction as $n \geq 2a+3$.

Applying the claim to the multiset A consisting of those $u \in \bar{\mathbb{F}}_q$ such that $u^{(q\epsilon)^{n-a}-1} = 1$, each with multiplicity n, and noting that $A \supseteq X$, we see that $u^{(q\epsilon)^{n-a}-1} = 1$ for all $u \in S$. Arguing similarly, we see that $u^{(q\epsilon)^{n-a-1}-1} = 1$, so $u^{q\epsilon-1} = 1$ for all $u \in S$. Now applying the claim to the multiset A' consisting of only x but with multiplicity n, and noting that $A \supseteq X$, we conclude that $A = S$ and $g = x \cdot 1_V$, as stated.

(ii) Now we proceed as in the proof of [31, Proposition 3.1.5]. Assume that $\chi \in \mathrm{Irr}(G)$ and $\chi(s)\chi(t) \neq 0$. By (i) and [31, Proposition 2.2.2], $\chi = \chi_{\mathrm{uni},\alpha}$ is a unipotent character of G labeled by a partition $\alpha \vdash n$. If $\chi_\alpha \in \mathrm{Irr}(\mathsf{S}_n)$ corresponds to α, then

$$\chi_\alpha(s_1) = \chi(s) \neq 0,\ \chi_\alpha(t_1) = \chi(t) \neq 0,$$

where $s_1 \in \mathsf{S}_n$ has cycle type $(n-a, a)$ and $t_1 \in \mathsf{S}_n$ has cycle type $(n-a-1, a+1)$. Arguing as in the proof of [31, Corollary 3.1.3], one can show that there are at most $4a+6$ possibilities for α, and $|\chi_\alpha(s_1)|, |\chi_\alpha(t_1)| \leq 4$. ∎

Proposition 8.5. *For every positive integer k, there are explicit positive integers $A = A(k)$, $B_1 = B_1(k)$, and $B_2 = B_2(k)$, each depending on k, with the following property. For every $n \geq A$ and for every prime power q, every $G \in \{\mathrm{SL}_n(q), \mathrm{SU}_n(q), \mathrm{Sp}_n(q), \mathrm{Spin}_n^\pm(q)\}$ contains $k+1$ pairs (s_i, t_i) of regular semisimple elements, $1 \leq i \leq k+1$, such that:*

(a) *If $i \neq j$, then $\gcd(|s_i| \cdot |t_i|, |s_j| \cdot |t_j|) = 1$;*
(b) *For each i, there are at most B_1 irreducible characters of G that vanish neither on s_i nor on t_i. The absolute values of these characters at s_i and t_i are at most B_2.*

Proof. (i) First we consider the case $G = \mathrm{Spin}^\epsilon_{2n}(q)$ with $n \geq 10k + 65$. For *odd* $a_i = 2i + 11$, $1 \leq i \leq k+1$, there are regular semisimple elements s_i, t_i of G belonging to maximal tori T_i^1 and T_i^2 of type $T^{\epsilon,+}_{n-a_i,a_i}$ (of order $(q^{n-a_i} - \epsilon)(q^{a_i} - 1)$) and $T^{-\epsilon,-}_{n-a_i-1,a_i+1}$ (of order $(q^{n-a_i-1} + \epsilon)(q^{a_i+1} + 1)$) respectively. In fact, we can choose

$$|s_i| = \ell^*(q^{n-a_i} - \epsilon) \cdot \ell^*(q^{a_i} - 1),\ |t_i| = \ell^*(q^{n-a_i-1} + \epsilon) \cdot \ell^*(q^{a_i+1} + 1).$$

By [31, Proposition 3.3.1] the number of distinct irreducible characters of G that vanish neither on s_i nor on t_i is bounded by some explicit integer $B_1(k)$, dependent on k but independent of n, q. Likewise, the absolute values of these characters on s_i and t_i are bounded by some explicit integer $B_2(k)$, dependent on k but independent of n, q.

It remains to check the condition (a). Let $1 \le i < j \le k+1$. By the choice of n, $n/5 \ge a_j + 1 \ge a_i + 3 \ge 16$. It follows that

$$2(n - a_j - 1) > n - a_i > n - a_i - 1 > \max(n - a_j, 4(a_j + 1)).$$

Hence, by Lemma 8.2, each of $\ell^*(q^{n-a_i} - \epsilon)$ and $\ell^*(q^{n-a_i-1} + \epsilon)$ is coprime to $\ell^*(q^{n-a_j} - \epsilon) \cdot \ell^*(q^{n-a_j-1} + \epsilon) \cdot \ell^*(q^{a_j} - 1) \cdot \ell^*(q^{a_j+1} + 1)$. Similarly, as $n - a_j - 1 > 4(a_i + 1)$, each of $\ell^*(q^{a_i} - 1)$ and $\ell^*(q^{a_i+1} + 1)$ is coprime to $\ell^*(q^{n-a_j} - \epsilon) \cdot \ell^*(q^{n-a_j-1} + \epsilon)$. Finally, since a_j and a_i are distinct odd integers, Lemma 8.2 also yields that $\ell^*(q^{a_i} - 1) \cdot \ell^*(q^{a_i+1} + 1)$ is coprime to $\ell^*(q^{a_j} - 1) \cdot \ell^*(q^{a_j+1} + 1)$, and we are done.

(ii) Suppose $G = \mathrm{Spin}_{2n+1}(q)$ with $n \ge 10k+65$. For *odd* $a_i = 2i+11$, $1 \le i \le k+1$, there are regular semisimple elements s_i, t_i of G belonging to maximal tori T_i^1 and T_i^2 of type $T^{+,+}_{n-a_i,a_i}$ (of order $(q^{n-a_i} - 1)(q^{a_i} - 1)$) and $T^{-,-}_{n-a_i-1,a_i+1}$ (of order $(q^{n-a_i-1} + 1)(q^{a_i+1} + 1)$) respectively. In fact, we can choose

$$|s_i| = \ell^*(q^{n-a_i} - 1) \cdot \ell^*(q^{a_i} - 1),\ |t_i| = \ell^*(q^{n-a_i-1} + 1) \cdot \ell^*(q^{a_i+1} + 1).$$

By [31, Proposition 3.4.1] the number of distinct irreducible characters of G that vanish neither on s_i nor on t_i is bounded by some explicit integer $B_1(k)$, dependent on k but independent of n, q. Likewise, the absolute values of these characters on s_i and t_i are bounded by some explicit integer $B_2(k)$, dependent on k but independent of n, q. Finally, condition (a) is satisfied as shown in (i).

(iii) Consider the case $G = \mathrm{Sp}_{2n}(q)$ with $n \ge 10k + 65$. For *odd* $a_i = 2i + 11$, $1 \le i \le k + 1$, there are regular semisimple elements s_i, t_i of G belonging to maximal tori T_i^1 and T_i^2 of type $T^{+,+}_{n-a_i,a_i}$ (of order $(q^{n-a_i} - 1)(q^{a_i} - 1)$) and $T^{+,-}_{n-a_i-1,a_i+1}$ (of order $(q^{n-a_i-1} - 1)(q^{a_i+1} + 1)$) respectively. In fact, we can choose

$$|s_i| = \ell^*(q^{n-a_i} - 1) \cdot \ell^*(q^{a_i} - 1),\ |t_i| = \ell^*(q^{n-a_i-1} - 1) \cdot \ell^*(q^{a_i+1} + 1).$$

Now we can finish as in (ii) but using Proposition 8.3.

(iv) Consider the case $G = \mathrm{SL}_n^\epsilon(q)$ with $n \ge 4k + 17$. For $a_i = 2i + 5$, $1 \le i \le k + 1$, there are regular semisimple elements s_i, t_i of G belonging to maximal tori T_i^1 and T_i^2 of type T_{n-a_i,a_i} (of order $(q^{n-a_i} - \epsilon^{n-a_i})(q^{a_i} - \epsilon^{a_i})$) and T_{n-a_i-1,a_i+1} (of order $(q^{n-a_i-1} - \epsilon^{n-a_i-1})(q^{a_i+1} - \epsilon^{a_i+1})$) respectively. Next, observe that for every $m \ge 7$, there is a prime $\ell(-q, m)$ that divides $(-q)^m - 1$ but does not divide $\prod_{i=1}^{m-1}((-q)^i - 1$; namely, we can take $\ell(-q, m) = \ell(q, 2m)$ if $2 \nmid m$, $\ell(-q, m) = \ell(q, m)$ if $4|m$, and $\ell(-q, m) = \ell(q, m/2)$ if $4|(m - 2)$. In particular, if $m \ge m' \ge 7$ and $\ell(q\epsilon, m) = \ell(q\epsilon, m')$, then $m = m'$. Now we can choose

$$|s_i| = \ell(q\epsilon, n - a_i) \cdot \ell(q\epsilon, a_i),\ |t_i| = \ell(q\epsilon, n - a_i - 1) \cdot \ell(q\epsilon, a_i + 1).$$

Condition (b) follows from Proposition 8.4. By the choice of n, $n/2 \ge a_j \ge a_i + 2 \ge 9$ if $1 \le i < j \le k + 1$. It follows that

$$n - a_i - 1 > n - a_j > n - a_j - 1 > a_j + 1 > a_j > a_i + 1,$$

so condition (a) is satisfied. ∎

Lemma 8.6. *Let q be an odd prime power and let $g \in G := \mathrm{SO}(V) = \mathrm{SO}_n^\pm(q)$ be a non-semisimple element with $\det(g + 1_V) \ne 0$. Then there exists a g-invariant, nonzero, totally singular subspace $W \subset V$ such that $\det(g|_W) = 1$. Furthermore, if $\dim W = n/2$ for all such W, then V is of type $+$ and $4|n$.*

Proof. (i) Let s, respectively u, denote the semisimple, respectively unipotent, part of g, and let $(\cdot, \cdot)$ denote the bilinear form on V. It suffices to consider the case where the g-module V is orthogonally indecomposable. Suppose first that $\det(g - 1_V) = 0$, which implies that $s = 1_V$. Since $u \ne 1_V$, there are $0 \ne e, f \in V$ such that $u(e) = e$ and

$u(f) = e + f$. It follows that $(e, e) = 0$, and we can take $W = \langle e \rangle_{\mathbb{F}_q}$. Note that the case $\dim W = n/2$ is impossible here, as $\mathrm{SO}_2^\epsilon(q)$ does not contain non-semisimple elements.

(ii) Next we consider the case where g has an eigenvalue $\lambda \in \mathbb{F}_q^\times \setminus \{\pm 1\}$. The indecomposability of g implies that $\mathbf{C}_G(s) = \mathrm{GL}_{n/2}(q)$; furthermore, $V_\epsilon := \mathrm{Ker}(s - \lambda^\epsilon \cdot 1_V)$ is a maximal totally singular subspace of V for $\epsilon = \pm$. Pick $0 \neq v_\epsilon \in \mathrm{Ker}(u - 1_V) \cap V_\epsilon$. If $(v_+, v_-) \neq 0$, then $\langle v_+, v_- \rangle_{\mathbb{F}_q}$ is a g-invariant non-degenerate subspace of V, and so $V = \langle v_+, v_- \rangle_{\mathbb{F}_q}$, implying that $g = s$ is semisimple, a contradiction. So $(v_+, v_-) = 0$, and we can take $W = \langle v_+, v_- \rangle_{\mathbb{F}_q}$.

Suppose now that g has an eigenvalue $\lambda \neq \pm 1$ with $\lambda^{q+1} = 1$. The indecomposability of g then implies that $\mathbf{C}_G(s) = \mathrm{GU}_{n/2}(q)$ and $(\cdot, \cdot)$ comes from a g-invariant Hermitian structure on $U := \mathbb{F}_{q^2}^{n/2}$. Now s acts on U as $\lambda \cdot 1_U$, and again since $u \neq 1_U$ we can find $0 \neq e, f \in U$ such that $u(e) = e$ and $u(f) = e + f$. It follows that e is totally singular in U, and we can take $W = \langle e \rangle_{\mathbb{F}_{q^2}}$.

The existence of W in the more general case where $\mathbf{C}_G(s) = \mathrm{GL}_a^\epsilon(q^b)$ follows from the previous two cases, by base changing to $\mathbb{F}_{q^b}$ if $\epsilon = +$ and $\mathbb{F}_{q^{2b}}$ if $\epsilon = -$. In each of these cases, $\dim V = 2ab$ and $\dim W = 2b$. Hence the equality $\dim W = (\dim V)/2$ implies that V is of type $+$ and $\dim V = 4b$. ∎

Let $G = \mathrm{Cl}(V) \in \{\mathrm{SL}_n(q), \mathrm{SU}_n(q), \mathrm{Sp}_n(q), \Omega_n^\pm(q)\}$. In what follows, by a *primary eigenvalue* of $g \in G$ we mean an eigenvalue λ of g with $\dim \mathrm{Ker}(g - 1_V) > n/2$. It then follows that $\lambda^{q-\epsilon} = 1$ in the SL^ϵ-case and $\lambda^2 = 1$ in the Sp/SO-case. Also, recall the support $\mathsf{supp}(g)$ was defined in [31, Definition 4.1.1]. We use the convention that in the case $G = \mathrm{SU}(V)$, the relevant subspaces are considered as vector spaces over $\mathbb{F}_{q^2}$.

Proposition 8.7. *Given any positive integers k, C, Q, and $D = D(k, Q)$ as defined in Lemma 8.1. Then there is an explicit positive integer $N = N(k, C, D, Q)$ such that the following statement holds. Let $q < Q$ be a prime power, and let $G = \mathrm{Cl}(V) \in \{\mathrm{SL}_n(q), \mathrm{SU}_n(q), \mathrm{Sp}_n(q), \Omega_n^\pm(q)\}$ with $n \geq N$. Let g be any element of G with $\mathsf{supp}(g) < C$.*

(i) *g has a primary eigenvalue λ.*

(ii) *There exist $2k + 1$ g-stable, orthogonal if $\mathrm{Cl} \neq \mathrm{SL}$, decompositions $V = U_j \oplus W_j$, $1 \leq j \leq 2k + 1$, such that $g \in \mathrm{Cl}(U_j) \times \mathrm{Cl}(W_j)$, $5D | \dim U_j$, $\dim W_j \geq 13$, $U_j \subseteq \mathrm{Ker}(g - \lambda \cdot 1_V)$, and the $4k + 2$ sets $\mathcal{R}(\mathrm{Cl}(U_j))$, $\mathcal{R}(\mathrm{Cl}(W_j))$ are pairwise disjoint.*

(iii) *Assume in addition that $2 \nmid q$, $G = \Omega(V)$, g is not semisimple, and $\lambda = -1$. Then at least one of the following statements holds.*

  (a) *$-1_V \in \Omega(V)$.*

  (b) *There exist $2k + 1$ g-stable orthogonal decompositions $V = U_j \oplus W_j$, $1 \leq j \leq 2k + 1$, such that $g \in \Omega(U_j) \times \Omega(W_j)$, $20C | \dim U_j$, $\dim W_j \geq 13$, the components of g in $\Omega(U_j)$ and $\Omega(W_j)$ are both non-central, and the $4k + 2$ sets $\mathcal{R}(\Omega(U_j))$, $\mathcal{R}(\Omega(W_j))$ are pairwise disjoint.*

  (c) *There exist $2k+1$ g-stable totally singular subspaces $W_j \subseteq V$, $1 \leq j \leq 2k+1$, such that $\mathrm{Stab}_{\mathrm{SO}(V)}(W_j)$ has a Levi subgroup $\mathrm{SO}(U_j) \times \mathrm{GL}(W_j)$, $\dim W_j \geq 10$, $\dim U_j \geq 13$, g projects onto a non-central element in each of $\Omega(U_j)$ and $\mathrm{SL}(W_j)$, and the $4k + 2$ sets $\mathcal{R}(\Omega(U_j))$, $\mathcal{R}(\mathrm{SL}(W_j))$ are pairwise disjoint.*

Proof. We choose

$$n \geq N = N(k, C, D, Q) := 9 \cdot 5^{2k+1}(4C + D). \tag{8.1}$$

(i) Since $\mathsf{supp}(g) < C < n/2$, by [31, Proposition 4.1.2] we see that g has a primary eigenvalue λ. Moreover, arguing as in the proof of [31, Lemma 6.3.4], we deduce that g

fixes an (orthogonal if Cl $\neq$ SL) decomposition $V = U \oplus W$, where $\dim U \geq n - 2C$ and $U \subseteq \mathrm{Ker}(g - \lambda \cdot 1_V)$.

(ii) Now we consider a chain of (non-degenerate if Cl $\neq$ SL) subspaces

$$U_1 \subset U_2 \subset \ldots \subset U_{2k+1} \subset U$$

with $e_j := \dim U_j = 5^j D \geq 40$, and moreover U_j is of type + if Cl $= \Omega$ (this can be achieved since $\dim U \geq n - 2C > 5^{2k+1}D + 4$ by (8.1)). We also define $W_j := U_j^{\perp}$, so that

$$V = U_j \oplus W_j,\ d_j := \dim W_j = n - 5^j D.$$

Write $q = p^f$ for a prime p. If Cl $\neq$ SU, observe that each prime in $\mathcal{R}(\mathrm{Cl}(U_j))$ divides $p^a - 1$ for some $a \leq e_j f$, but cannot divide any $p^b - 1$ with $b \leq e_j f/5$. Similarly, if Cl $=$ SU, then each prime in $\mathcal{R}(\mathrm{Cl}(U_j))$ divides $p^a - 1$ for some $a \leq 2e_j f$, but cannot divide any $p^b - 1$ with $b \leq 2e_j f/5$. It follows that the $2k + 1$ sets $\mathcal{R}(\mathrm{Cl}(U_j))$ are disjoint. For the same reason, the condition

$$d_i \geq n - 5^{2k+1}D > 5^{2k+2}D$$

implies that each $\mathcal{R}_i := \mathcal{R}(\mathrm{Cl}(W_i))$ is disjoint from all $\mathcal{R}(\mathrm{Cl}(U_j))$. We claim that

$$\mathcal{R}_i \cap \mathcal{R}_j = \emptyset \tag{8.2}$$

whenever $1 \leq i \neq j \leq 2k + 1$. Assume the contrary: so $\ell \in \mathcal{R}_i \cap \mathcal{R}_j$ for some $i < j$. By the construction of $\mathcal{R}_i$,

$$\ell | (q^{2d_i} - 1)(q^{2d_i - 2} - 1)(q^{2d_i - 4} - 1),$$

and similarly for j. Note that

$$(5^{2k+1} - 5)D \geq d_i - d_j = (5^j - 5^i)D \geq 20D \geq 160.$$

It follows that $\ell | (q^e - 1)$, where

$$316 \leq 2d_i - 4 - 2d_j \leq e \leq 2d_i - 2d_j + 4 < 2 \cdot 5^{2k+1}D.$$

On the other hand, (8.1) implies that

$$(d_j - 2)/4 \geq (n - 5^{2k+1}D - 2)/4 > 2 \cdot 5^{2k+1}D.$$

We have shown that some $\ell \in \mathcal{R}(\mathrm{Cl}_{d_j}(q))$ divides $p^{ef} - 1$ with $316 \leq e < (d_j - 2)/4$. This contradicts the construction of $\mathcal{R}(\mathrm{Cl}_{d_j}(q))$ in Theorem 2.1, according to which $\ell = \ell(p, af)$ for some $a \geq (d_j - 1)f/4$.

(iii) We may now assume that $2 \nmid q$, $G = \Omega(V)$, g is not semisimple, and $\lambda = -1$. If -1 is the only eigenvalue of g on $V \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q$, then the semisimple part s of g is -1_V, whence we arrive at (a). We will therefore assume that -1 is not the only eigenvalue of g on $V \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q$. Recall the g-stable decomposition $V = U \oplus W$ with $\dim U \geq n - 2C$ and $U \subseteq \mathrm{Ker}(g + 1_V) \subseteq V_0 := \mathrm{Ker}(s + 1_V) \neq V$. Note that $\det(s|_{V_0}) = 1$.

Suppose that $\mathrm{Ker}(g + 1_V) \neq V_0$, and decompose $V_0 = U \oplus U_0$ orthogonally. Note that $\dim U_0 \leq 2C$. Then we consider a chain of non-degenerate subspaces

$$U_0 \subset U_1 \subset U_2 \subset \ldots \subset U_{2k+1} \subset V_0$$

with $\dim U_j = 4 \cdot 5^j C \geq 20$ and moreover U_j is of type + for $1 \leq j \leq 2k + 1$ (this can be achieved since $\dim V_0 > n - 2C > 4 \cdot 5^{2k+1}C + 4$ by (8.1)). We also define $W_j := U_j^{\perp}$ for $j \geq 1$. Now, g has a unique eigenvalue -1 but does not act as a scalar on U_j (as $U_0 \neq 0$), and has at least two eigenvalues on $W_j \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q$ (as $V_0 \neq V$) if $j \geq 1$. Furthermore, $g|_{U_j} \in \Omega(U_j)$ as U_j has type + and $4 | \dim U_j$, whence $g \in \Omega(U_j) \times \Omega(W_j)$. The same arguments as in (ii) using (8.1) shows that the $4k + 2$ sets $\mathcal{R}(\mathrm{Cl}(U_j))$, $\mathcal{R}(\mathrm{Cl}(W_j))$ are pairwise disjoint, and we arrive at (b).

Assume now that $\mathrm{Ker}(g+1_V) = V_0$. Changing the notation, we let $W := V_0^\perp$ so that $V = V_0 \oplus W$. Note that $g|_W \in \mathrm{SO}(W)$ is not semisimple, and $\det(g|_W + 1_W) \neq 0$. Hence by Lemma 8.6, g stabilizes a nonzero, totally singular subspace W_0 of W, with $\det(g|_{W_0}) = 1$. As $\mathsf{supp}(g) < C$, we have $\dim W_0 < C$. Since W is non-degenerate, we can find another s-invariant totally singular subspace W_0' of W such that $\tilde{W}_0 := W_0 \oplus W_0'$ is non-degenerate (of type +). Now we consider a chain of s-invariant non-degenerate subspaces of type +

$$\tilde{W}_0 \subset \tilde{W}_1 \subset \tilde{W}_2 \subset \ldots \subset \tilde{W}_{2k+1} \subset V_0 \oplus \tilde{W}_0$$

with $\dim \tilde{W}_j = 2c \cdot 5^j \geq 20$ for $1 \leq j \leq 2k+1$. In each $\tilde{W}_j$, we can find a totally singular subspace $W_j = W_0 \oplus (V_0 \cap W_j)$ of dimension $c \cdot 5^j \geq 10$ which is then g-invariant. Here, we choose $c \in \{3C-1, 3C\}$ such that

$$c \equiv \dim W_0 (\mathrm{mod}\ 2), \tag{8.3}$$

and so $\det(g|_{W_1}) = \det(g|_{W_j}) = 1$. By the construction of W_j, g has eigenvalue -1 and at least one more eigenvalue $\neq -1$ on $W_j \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q$, so $g|_{W_j}$ is non-central.

Now, $\mathrm{Stab}_{\mathrm{SO}(V)}(W_j)$ has a Levi subgroup $\mathrm{SO}(U_j) \otimes \mathrm{GL}(W_j)$, where $U_j := (\tilde{W}_j)^\perp$. Note that, since $\det(g|_{W_j}) = 1$, by [26, Lemma 2.7.2] there is an $h \in \Omega(\tilde{W}_j)$ that induces the same action on W_j as that of g. But $g \in \Omega(V)$, so we conclude that the projection g' of g onto $\mathrm{SO}(U_j)$ is contained in $\Omega(U_j)$. Note that g' always has -1 as an eigenvalue on $U_j \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q$ as $\tilde{W}_{2k+1} \not\supseteq V_0$, and has at least one more eigenvalue *unless* $W = \tilde{W}_0$, in which case $2|(\dim W_0)$ by Lemma 8.6. Suppose that g' is central in $\Omega(U_j)$. Then $g' = -1_{U_j} \in \Omega(U_j)$. Furthermore, $2|c$ by (8.3), when $4|(\dim \tilde{W}_j)$. But $\tilde{W}_j$ is of type +, so $-1_{\tilde{W}_j} \in \Omega(\tilde{W}_j)$. As $V = U_j \oplus \tilde{W}_j$, we conclude that $-1_V \in \Omega(V)$, i.e. (a) holds. The claim about disjointness of $\mathcal{R}(\Omega(U_j))$ and $\mathcal{R}(\mathrm{SL}(W_i))$ now follows by the same arguments as in (ii) using (8.1). ∎

Proof of Theorems 4 and Theorem 5. Let k be a positive integer and let N be any positive integer with $\boldsymbol{\omega}(N) \leq k$. For Theorem 5(i) we also assume that $\boldsymbol{\Omega}(N) \leq k$. By Proposition 2.6, it suffices to prove the theorems for finite simple classical groups S of sufficiently large rank. So we assume that $S = G/\mathbf{Z}(G)$ and $G = \mathrm{Cl}_n(q)$ with $\mathrm{Cl} \in \{\mathrm{SL}, \mathrm{SU}, \mathrm{Sp}, \Omega^\epsilon\}$ (and $\epsilon = \pm$). Let $V := \mathbb{F}_q^n$ (if $\mathrm{Cl} \neq \mathrm{SU}$) and $V := \mathbb{F}_{q^2}^n$ (for $\mathrm{Cl} = \mathrm{SU}$) denote the natural G-module. Also set $\epsilon = +$ if $\mathrm{Cl} = \mathrm{SL}$ and $\epsilon = -$ when $\mathrm{Cl} = \mathrm{SU}$.

(i) Apply Proposition 8.5 to G and consider $n \geq A$. Since $\boldsymbol{\omega}(N) \leq k$, by 8.5(a) there is some i_0 between 1 and $k+1$ such that the orders of $s := s_{i_0}$ and $t := t_{i_0}$ are coprime to N. Define

$$Q = Q(k) := (B_1 B_2^2)^{481}.$$

We claim that if $q \geq Q$, then every $g \in G \setminus \mathbf{Z}(G)$ belongs to $s^G \cdot t^G$, so it is a product of two Nth powers. Indeed, $\mathsf{supp}(g) \geq 1$ since $g \notin \mathbf{Z}(G)$. It follows by [31, Theorem 4.3.6] and the condition on q that

$$\frac{|\chi(g)|}{\chi(1)} < q^{-1/481} \leq \frac{1}{B_1 B_2^2}$$

for every $1_G \neq \chi \in \mathrm{Irr}(G)$. Now condition 8.5(b) implies that

$$\sum_{1_G \neq \chi \in \mathrm{Irr}(G)} \frac{|\chi(s)\chi(t)\chi(g)|}{\chi(1)} < \frac{B_1 B_2^2}{B_1 B_2^2} = 1,$$

so $g \in s^G \cdot t^G$ and is a product of two Nth powers as desired. Thus we have established Theorems 4–5 for classical groups defined over a sufficiently large field $\mathbb{F}_q$.

(ii) From now on we may assume that $2 \le q < Q$. Suppose that $g \in G$ satisfies

$$\mathsf{supp}(g) \ge C = C(k) := (\log_2 Q)^2.$$

By [31, Theorem 4.3.6],

$$\frac{|\chi(g)|}{\chi(1)} < q^{-\sqrt{\mathsf{supp}(g)}/481} \le 2^{-(\log_2 Q)/481} = \frac{1}{B_1 B_2^2}$$

for every $1_G \ne \chi \in \mathrm{Irr}(G)$. Hence, as in (i), $g \in s^G \cdot t^G$, so g is a product of two Nth powers. We have shown that every element in G, with support $\ge C$ and whenever $n \ge A$, is a product of two Nth powers. Applying Gow's theorem, see e.g. [25, Lemma 5.1], we see that the same conclusion also holds for all non-central semisimple $g \in G$.

(iii) It remains to consider the non-semisimple $g \in G$ with $\mathsf{supp}(g) < C$. Recall the integer $D = D(k, Q)$ defined in the proof of Lemma 8.1, which satisfies

$$8|D,\ (q - \epsilon)|D. \tag{8.4}$$

We choose $n \ge N(k, C, D, Q)$ as defined in Proposition 8.7. Let λ denote the primary eigenvalue of g.

Now we apply Proposition 8.7(ii), and *assume in addition that* $\lambda \cdot 1_V \in \Omega(V)$ *if* $G = \Omega(V)$. Since $\boldsymbol{\omega}(N) \le k$, there is some i_0 such that N is not divisible by any prime in $\mathcal{R}(\mathrm{Cl}(W_{i_0}))$. Hence, by Theorem 2.1, $H := \mathrm{Cl}(W_{i_0})$ admits two regular semisimple elements s' and t' whose orders are coprime to N, and such that $(s')^H \cdot (t')^H \supseteq H \smallsetminus \mathbf{Z}(H)$.

Next, G contains a subgroup $\mathrm{Cl}(U_{i_0}) \times \mathrm{Cl}(W_{i_0})$. Note that g acts on U_{i_0} as the scalar λ. Furthermore, in the case of Theorem 4 and Theorem 5(ii) (recall that we are assuming $\lambda \cdot 1_V \in \Omega(V)$ if $G = \Omega(V)$), the scalar transformation $\lambda \cdot 1_V$ belongs to $\mathbf{Z}(G)$. Replacing g by $(\lambda^{-1} \cdot 1_V)g$, which does not change the coset $g\mathbf{Z}(G)$ of g in S, we obtain $x := g|_{U_{i_0}} = 1_{U_{i_0}}$; in particular, $x = u^N$ for $u := 1_{U_{i_0}}$, and we also set $\lambda_0 := 1$. In the case of Theorem 5(i), $\boldsymbol{\Omega}(N) \le k$. Hence the condition (8.4) implies that $x := g|_{U_{i_0}} \in \mathbf{Z}(\mathrm{Cl}(U_{i_0}))$, whence $x = u^N$ for some $u \in \mathrm{Cl}(U_{i_0})$ by Lemma 8.1; set $\lambda_0 := \lambda$.

Since g fixes W_{i_0}, it follows that $g = xy$ with $y := g|_{W_{i_0}} \in H = \mathrm{Cl}(W_{i_0})$. Note that y has λ_0 as an eigenvalue (as $\dim U_{i_0} < \dim U$) but does not act as the scalar λ_0 (as otherwise $g \in \mathbf{Z}(G)$). It follows that $y \in H \smallsetminus \mathbf{Z}(H) \subseteq (s')^H \cdot (t')^H$, so $y = v^N w^N$ with $v, w \in H$. Note that $u \in \mathrm{Cl}(U_{i_0})$ centralizes $v \in H$. Now the claim follows, since $g = xy = u^N \cdot v^N w^N = (uv)^N w^N$.

(iv) It remains to prove Theorem 4 in the case where $G = \Omega(V)$ but $\lambda \cdot 1_V \notin \Omega(V)$; in particular, $2 \nmid q$ and $\lambda = -1$. Now we apply Proposition 8.7(iii) and note that assertion (a) does not hold. Assume assertion (b) holds. Since $\boldsymbol{\omega}(N) \le k$, there are at least $k + 1$ values of j such that N is coprime to all primes in $\mathcal{R}(\Omega(U_j))$. The condition $\boldsymbol{\omega}(N) \le k$ then implies that there is some j_0 (among these values j) such that N is also coprime to all primes in $\mathcal{R}(\Omega(W_{j_0}))$. Applying Theorem 2.1 to $\Omega(U_{j_0})$ and $\Omega(W_{j_0})$, we see that

$$g = a^N b^N \cdot c^N d^N = a^N c^N \cdot b^N d^N = (ac)^N \cdot (bd)^N$$

for some $a, b \in \Omega(U_{j_0})$ and $c, d \in \Omega(W_{j_0})$.

Assume now that we are in the case of Proposition 8.7(iii)(c). Arguing as above, we can find j_0 such that N is coprime to all primes in $\mathcal{R}(\Omega(U_{j_0})) \cup \mathcal{R}(\mathrm{SL}(W_{j_0}))$. As g is non-central in both projections to $\Omega(U_{j_0}))$ and $\mathrm{SL}(W_{j_0})$, we can apply Theorem 2.1 to get regular semisimple N'-elements $a, b \in \Omega(U_{j_0})$, $c, d \in \Omega(W_{j_0})$ such that

$$g = a^N b^N \cdot c^N d^N \cdot v = a^N c^N \cdot b^N d^N \cdot v = (ac)^N \cdot b^N d^N \cdot v$$

for some $v \in U$ and $|d| = \ell^*(q^r - 1)$ for $r := \dim W_{j_0}$. Here, U is the unipotent radical of $\mathrm{Stab}_{\mathrm{SO}(V)}(W_{j_0}) = UL$, and $L = \mathrm{SO}(U_{j_0}) \times \mathrm{GL}(W_{j_0})$. Our construction of b, d implies

that $\mathbf{C}_G(t) \le L$ for $t := b^N d^N$; in particular, $\mathbf{C}_G(t) \cap U = 1$. As t normalizes U, the map $u \mapsto t^{-1}utu^{-1}$ maps U into U injectively, whence also surjectively. Thus $\{utu^{-1} \mid u \in U\}$ coincides with the coset tU. Hence, tv is G-conjugate to $t = (bd)^N$, and so $tv = h^N$ for some G-conjugate h of bd. Thus $g = (ac)^N h^N$, as desired. ∎

Proof of Theorem 6. Let k and N be any positive integers with $\boldsymbol{\omega}(N) \le k$.

(i) Let $G \in \{\mathrm{SL}_n(q), \mathrm{SU}_n(q), \mathrm{Sp}_{2n}(q), \mathrm{Spin}_n^{\pm}(q)\}$. Apply Proposition 8.5 to G and to $k+1$ instead of k and consider $n \ge A$. Since $\boldsymbol{\omega}(N) \le k$, by 8.5(a) there is some i_0, i_1 between 1 and $k+2$ such that the orders of $s := s_{i_0}$, $t := t_{i_0}$, and $v := s_{i_1}$ are coprime to N. Consider any $1_G \ne \chi \in \mathrm{Irr}(G)$. Note if r is the rank of the algebraic group corresponding to G, then since v is regular semisimple we see that $\mathbf{C}_G(v)$ is a maximal torus and so has order at most $(q+1)^r < q^{1.6r}$, whence $|\chi(v)| < q^{0.8r}$. On the other hand, $\chi(1) > q^r/3$ by [28]. It now follows by Proposition 8.5(b) that

$$\sum_{1_G \ne \chi \in \mathrm{Irr}(G)} \frac{|\chi(s)\chi(t)\chi(v)\chi(g)|}{\chi(1)^2} < \frac{3B_1B_2^2}{2^{r/5}} < 1$$

for all $g \in G$ if $r > 5\log_2(3B_1B_2^2)$. In this case, Frobenius' character sum implies that g is a product $s't'v'$ of G-conjugates of s, t, v, hence a product of three Nth powers.

(ii) Now we assume (without any loss) that $k \ge 52$ and consider $G = 2\mathsf{A}_n$ with

$$n \ge A = A(k) := (k+3)(\ln(k+3) + \ln\ln(k+3) + 2).$$

By [53, Theorem 29], the interval $[2, A]$ contains at least $k+3$ distinct primes. Since $\boldsymbol{\omega}(N) \le k$, we can find a prime $5 \le p < A \le n$ such that $p \nmid N$. Write $n = \sum_{i=0}^{t} a_i p^i$ p-adically, with $0 \le a_i \le p-1$, $a_t \ge 1$, and consider an N'-element $\sigma \in G$ of odd order, whose image $\bar\sigma$ in A_n has cycle type

$$(p^t)^{a_t}(p^{t-1})^{a_{t-1}} \dots (p)^{a_1}(1)^{a_0}. \tag{8.5}$$

In particular, $\bar\sigma$ has at most $a_0 \le p-1 = n^{o(1)}$ cycles of length $< p$. Here and hereafter, $o(1)$ means a function of n that tends to 0 when n tends to infinity. It follows by [29, Theorem 1.2(ii)] that

$$|\chi(\sigma)| \le \chi(1)^{1/p+o(1)} \le \chi(1)^{1/5+o(1)} \tag{8.6}$$

for all $\chi \in \mathrm{Irr}(\mathsf{S}_n)$. Next, the choice (8.5) implies that

$$\mathbf{C}_{\mathsf{S}_n}(\bar\sigma) = (C_{p^t} \wr \mathsf{S}_{a_t}) \times (C_{p^{t-1}} \wr \mathsf{S}_{a_{t-1}}) \times \dots \times (C_p \wr \mathsf{S}_{a_1}) \times \mathsf{S}_{a_0}.$$

It follows that

$$|\mathbf{C}_{\mathsf{S}_n}(\bar\sigma)| = \prod_{i=0}^{t}(p^{ia_i} \cdot a_i!) \le p^{(t+(t-1)+\dots+1)(p-1)} \cdot ((p-1)!)^{t+1} < p^{(p-1)(t+1)(t+2)/2}.$$

Since $p < A$ and $t \le \log_p n$, we see that there is some $B = B(k) > 0$ such that

$$|\chi(\sigma)| \le \sqrt{|\mathbf{C}_G(\sigma)|} \le e^{B(\ln n)^2} \tag{8.7}$$

for all $\chi \in \mathrm{Irr}(G)$. Now if $\chi \in \mathrm{Irr}(G)$ is faithful, then it is well known that $\chi(1) \ge 2^{(n-2)/2}$. Likewise, arguing as in the proof of [27, Proposition 4.1] and using [18, Theorem 5.1], one can show that $\chi(1) \ge 2^{(n-5)/4}$ if $\chi \in \mathrm{Irr}(\mathsf{A}_n)$ does not extend to S_n. Let $J \subseteq \mathrm{Irr}(G)$ denote the subset of all irreducible characters of G that are either faithful, or trivial at $\mathbf{Z}(G) = C_2$ but do not arise as the restriction to A_n of some irreducible character of S_n. Then we have shown that $\chi(1) > 2^{n/5}$ for all $\chi \in J$, and furthermore

$$|J| \le |\mathrm{Irr}(G)| \le 4|\mathrm{Irr}(\mathsf{S}_n)| = 4p(n) \le e^{C\sqrt{n}}, \tag{8.8}$$

say with $C := \pi\sqrt{2/3}+1$ (where $p(n)$ is the partition function of n). Also consider the *Witten zeta function*

$$\zeta_{\mathsf{A}_n}(s) = \sum_{\alpha\in\mathrm{Irr}(\mathsf{A}_n)} \chi(1)^{-s}$$

of A_n. Combining (8.6)–(8.8) together, we get

$$\sum_{1_G\neq\chi\in\mathrm{Irr}(G)} \frac{|\chi(\sigma)|^3}{\chi(1)} \leq \sum_{\chi\in J} \frac{|\chi(\sigma)|^3}{\chi(1)} + \sum_{1_G\neq\chi\notin J} \frac{|\chi(\sigma)|^3}{\chi(1)} \leq \frac{e^{3B(\ln n)^2+C\sqrt{n}}}{2^{n/5}} + \zeta_{\mathsf{A}_n}(2/5-o(1)) - 1.$$

According to [38, Corollary 2.7], $\lim_{n\to\infty}\zeta_{\mathsf{A}_n}(2/5-o(1)) = 1$. Hence, if we choose $n \geq h(k)$ sufficiently large, then

$$\sum_{1_G\neq\chi\in\mathrm{Irr}(G)} \frac{|\chi(\sigma)|^3}{\chi(1)} < 1.$$

It follows by Frobenius' character sum that $G = \sigma^G\cdot\sigma^G\cdot\sigma^G$, and so we are done since $|\sigma|$ is coprime to N. ∎

We can also prove an analogue of Theorem 5(i) for $2\mathsf{A}_n$:

Proposition 8.8. *For any positive integer k, there is some integer $h(k)$ such that if $\mathbf{\Omega}(N) \leq k$ and $n \geq h(k)$ then the word map $(x,y)\mapsto x^Ny^N$ is surjective on the double cover $2\mathsf{A}_n$.*

Proof. Let $\mathbf{\Omega}(N)\leq k$ and let $G = 2\mathsf{A}_n$. The image of the map $x\mapsto x^N$ on the cyclic group C of order 2^{k+3} contains an element of order 8. Similarly, the image of the map $x\mapsto x^N$ on the cyclic group D of order 3^{k+2} contains an element of order 9. Hence, by [32, Lemma 3.3], when n is sufficiently large (compared to k), there is some $u\in G$ such that $G = (u^N)^G\cdot(u^N)^G$. ∎

Finally, we make some remarks about possible generalizations of the aforementioned results.

Remark 8.9. Some natural generalizations of Theorem 1 are false.

(i) *It is not true that for every $N = p^aq^b$ the word map $(x,y)\mapsto x^Ny^N$ is always surjective on every quasisimple group G, or at least hits all the non-central elements of G.* For instance, if $N = 20$, then this map does not hit any element of order 5 in $G = \mathrm{SL}_2(5)$ (indeed, x^{20} has order 1 or 3 in G, and if $x\in G$ has order 3 then $\{1\}\cup x^G\cup x^G\cdot x^G$ does not contain any element of order 5 of G). It may be that this is the only counterexample.

(ii) *It is not true that for every odd integer N the word map $(x,y)\mapsto x^Ny^N$ is always surjective on every non-abelian simple group G.* For instance, consider a prime power $q>3$ where $q\equiv 3 \bmod 8$ and set $G := \mathrm{PSL}_2(q)$ and $N := q(q^2-1)/8$. Note that x^N has order 1 or 2 for every $x\in G$. It follows that every element of G that is hit by the word map $(x,y)\mapsto x^Ny^N$ is either an involution or a product of two involutions, so it is real. On the other hand, the nontrivial unipotent elements of G are not real. The same arguments show that the word map $(x,y)\mapsto x^Ny^N$ is not surjective on the Ree group $G = {}^2G_2(q)$, if $q = 3^{2a+1} > 3$ and $N = |G|_{2'}$. It is an open question whether these two families of simple groups exhaust all the simple groups G on which the word map $(x,y)\mapsto x^Ny^N$ is not surjective for some odd N.

Example 8.10. None of Theorems 4–6 holds for finite simple groups of Lie type and bounded rank over fields of sufficiently large size. Indeed, according to [1, Corollary 4.2], there are infinitely many primes p such that $\mathbf{\Omega}(p^2-1)\leq 21$. For every such prime p, the

word map $(x,y) \mapsto x^{N_p}y^{N_p}$ with $N_p := p(p^2-1)/2$ cannot be surjective on $\mathrm{PSL}_2(p)$ (its image consists only of the identity element); on the other hand,

$$\boldsymbol{\omega}(N_p) \le \boldsymbol{\Omega}(N_p) \le \boldsymbol{\Omega}(p^2-1) \le 21.$$

This example can be generalized to quasisimple Lie-type groups of bounded rank and word maps of arbitrary length. Indeed, for any given integer $r_0 \ge 15$, every finite quasisimple group G of Lie type of rank $\le r_0$ and defined over $\mathbb{F}_p$ has order dividing $N_p' := p^{r_0^2}\prod_{i=1}^{r_0}(p^{2i}-1)$. By [1, Theorem C], there exist an integer k and infinitely many primes p such that $\boldsymbol{\Omega}(p^{2r_0!}-1) \le k/r_0 - r_0$. For every such prime p, the word map

$$(x_1, x_2, \dots, x_m) \mapsto (x_1)^{N_p'}(x_2)^{N_p'} \cdot \ldots \cdot (x_m)^{N_p'}$$

can never be surjective on G (as its image consists only of the identity element), whereas

$$\boldsymbol{\omega}(N_p') \le \boldsymbol{\Omega}(N_p') \le r_0^2 + r_0\boldsymbol{\Omega}(p^{2r_0!}-1) \le k.$$

Example 8.11. Note that no analogue of Theorems 1, 4, or 5 holds for *quasisimple* classical groups, even of unbounded rank and over fields of unbounded size. Indeed, for any odd integer $n \ge 1$ and any $q \equiv 5 (\mathrm{mod}\ 8)$, the word map $(x,y) \mapsto x^8y^8$ is not surjective on $\mathrm{Sp}_{2n}(q)$; see [32, Theorem 4.6] for this and other examples.

Likewise, for any n, if we choose $N = 2^n$, then for any $x \in H := 2\mathsf{A}_n$ the order of x^N is odd. Hence, if z is the central involution of H, then $x^{-N}z$ has even order and so cannot be y^N for any $y \in H$. Thus the map $(x,y) \mapsto x^Ny^N$ is not surjective on H. This shows that Proposition 8.8 does not hold if we replace $\boldsymbol{\Omega}(N) \le k$ with $\boldsymbol{\omega}(N) \le k$. Certainly, this observation also applies to any finite group G and any prime p dividing $|\mathbf{Z}(G)|$ (by choosing $N = p^a$ to be the p-part of the exponent of G).

References

[1] K. Alladi, R.M. Solomon and A. Turull, Finite simple groups of bounded subgroup chain length, *J. Algebra* **231** (2000), 374–386.

[2] E. Bertram, Even permutations as a product of two conjugate cycles, *J. Comb. Theory Ser. A* **12** (1972), 368–380.

[3] W. Burnside, On groups of order $p^\alpha q^\beta$, *Proc. Lond. Math. Soc.* (1904), S2-1, 388–392.

[4] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system I: The user language, *J. Symbolic Comput.* **24** (1997), 235–265.

[5] J. Brundan and A.S. Kleshchev, Lower bounds for degrees of irreducible Brauer characters of finite general linear groups, *J. Algebra* **223** (2000), 615–629.

[6] R.W. Carter, Conjugacy classes in the Weyl group, Springer Lecture Notes **131** (1970), 297–318.

[7] R.W. Carter, '*Finite Groups of Lie type: Conjugacy Classes and Complex Characters*', Wiley, Chichester, 1985.

[8] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker and R.A. Wilson, '*An ATLAS of Finite Groups*', Clarendon Press, Oxford, 1985.

[9] P. Deligne and G. Lusztig, Representations of reductive groups over finite fields, *Annals of Math.* **103** (1976), 103–161.

[10] F. Digne and J. Michel, '*Representations of Finite Groups of Lie Type*', London Mathematical Society Student Texts **21**, Cambridge University Press, 1991.

[11] E.W. Ellers and N. Gordeev, On the conjectures of J. Thompson and O. Ore, *Trans. Amer. Math. Soc.* **350** (1998), 3657–3671.

[12] H. Enomoto, The characters of the finite symplectic groups $Sp(4,q)$, $q = 2^f$, *Osaka J. Math.* **9** (1972), 75–94.

[13] W. Feit and J.G. Thompson, Solvability of groups of odd order, *Pacific J. Math.* **13** (1963), 775–1029.

[14] The GAP group, '**GAP** - *groups, algorithms, and programming*', Version 4.8.7, 2017, `http://www.gap-system.org`.

[15] M. Geck, G. Hiss, F. Lübeck, G. Malle and G. Pfeiffer, **CHEVIE** – A system for computing and processing generic character tables for finite groups of Lie type, Weyl groups and Hecke algebras, *Appl. Algebra Engrg. Comm. Comput.* **7** (1996), 175–210.

[16] D. Gluck, Sharper character value estimates for groups of Lie type, *J. Algebra* **174** (1995), 229–266.

[17] R. Gow, Commutators in finite simple groups of Lie type, *Bull. London Math. Soc.* **32** (2000), 311–315.

[18] R.M. Guralnick, M. Larsen and Pham Huu Tiep, Representation growth in positive characteristic and conjugacy classes of maximal subgroups, *Duke Math. J.* **161** (2012), 107–137.
[19] R.M. Guralnick and F. Lübeck, On p-singular elements in Chevalley groups in characteristic p, in: '*Groups and Computation, III*' (Columbus, OH, 1999), 169–182, Ohio State Univ. Math. Res. Inst. Publ., **8**, de Gruyter, Berlin, 2001.
[20] R.M. Guralnick and G. Malle, Products of conjugacy classes and fixed point spaces, *J. Amer. Math. Soc.* **25** (2012), 77–121.
[21] R.M. Guralnick, G. Malle and Pham Huu Tiep, Product of conjugacy classes in finite simple classical groups, *Adv. Math.* **234** (2013), 618–652.
[22] R.M. Guralnick and Pham Huu Tiep, Low-dimensional representations of special linear groups in cross characteristics, *Proc. London Math. Soc.* **78** (1999), 116–138.
[23] R.M. Guralnick and Pham Huu Tiep, Cross characteristic representations of even characteristic symplectic groups, *Trans. Amer. Math. Soc.* **356** (2004), 4969–5023.
[24] R.M. Guralnick and Pham Huu Tiep, Effective results on the Waring problem for finite simple groups, *Amer. J. Math.* **137** (2015), 1401–1430.
[25] 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.
[26] P.B. Kleidman and M.W. Liebeck, '*The Subgroup Structure of the Finite Classical Groups*', London Math. Soc. Lecture Note Series **129**, Cambridge University Press, Cambridge, 1990.
[27] A.S. Kleshchev, P. Sin and Pham Huu Tiep, Representations of the alternating group which are irreducible over subgroups. II, *Amer. J. Math.* **138** (2016), 1383–1423.
[28] V. Landazuri and G. Seitz, On the minimal degrees of projective representations of the finite Chevalley groups, *J. Algebra* **32** (1974), 418–443.
[29] M. Larsen and A. Shalev, Characters of symmetric groups: sharp bounds and applications, *Invent. Math.* **174** (2008), 645–687.
[30] M. Larsen and A. Shalev, Word maps and Waring type problems. *J. Amer. Math. Soc.* **22** (2009), 437–466.
[31] M. Larsen, A. Shalev and Pham Huu Tiep, The Waring problem for finite simple groups, *Annals of Math.* **174** (2011), 1885–1950.
[32] M. Larsen, A. Shalev and Pham Huu Tiep, Waring problem for finite quasisimple groups, *Int. Math. Res. Notices* 2013, no. 10, 2323–2348.
[33] H. Lee, '*Triples in Finite Groups and a Conjecture of Guralnick and Tiep*', Ph. D. Thesis, University of Arizona, 2017.
[34] M.W. Liebeck, E.A. O'Brien, A. Shalev and Pham Huu Tiep, The Ore conjecture, *J. Eur. Math. Soc.* **12** (2010), 939–1008.
[35] M.W. Liebeck, E.A. O'Brien, A. Shalev and Pham Huu Tiep, Products of squares in finite simple groups, *Proc. Amer. Math. Soc.* **140** (2012), 21–33.
[36] M.W. Liebeck, J. Saxl and G.M. Seitz, Subgroups of maximal rank in finite exceptional groups of Lie type, *Proc. London Math. Soc.* **65** (1992), 297–325.
[37] M.W. Liebeck and A. Shalev, Diameters of finite simple groups: sharp bounds and applications, *Annals of Math.* **154** (2001), 383–406.
[38] M.W. Liebeck and A. Shalev, Fuchsian groups, coverings of Riemann surfaces, subgroup growth, random quotients and random walks, *J. Algebra* **276** (2004), 552–601.
[39] M.W. Liebeck and G.M. Seitz, '*Unipotent and Nilpotent Classes in Simple Algebraic Groups and Lie Algebras*', Mathematical Surveys and Monographs, Vol. **180**, American Mathematical Society, Providence, RI, 2012.
[40] F. Lübeck, Smallest degrees of representations of exceptional groups of Lie type, *Comm. Algebra* **29** (2001), 2147–2169.
[41] F. Lübeck, Character degrees and their multiplicities for some groups of Lie type of rank < 9, http://www.math.rwth-aachen.de/∼Frank.Luebeck/chev/DegMult/index.html
[42] F. Lübeck, Numbers of conjugacy classes in some series of finite groups of Lie type, http://www.math.rwth-aachen.de/∼Frank.Luebeck/chev/nrclasses/nrcldata.html
[43] F. Lübeck and G. Malle, $(2, 3)$-generation of exceptional groups, *J. London Math. Soc.* **59** (1999), 109–122.
[44] G. Lusztig, Unipotent characters of the symplectic and odd orthogonal groups over a finite field, *Invent. Math.* **64** (1981), 263–296.
[45] K. Magaard and Pham Huu Tiep, Irreducible tensor products of representations of quasi-simple finite groups of Lie type, in: '*Modular Representation Theory of Finite Groups*', M. J. Collins, B. J. Parshall, L. L. Scott, eds., Walter de Gruyter, Berlin et al, 2001, pp. 239–262.
[46] A. Malcolm, The involution width of finite simple groups, *J. Algebra* **493** (2018), 297–340.
[47] G. Malle, J. Saxl and T. Weigel, Generation of classical groups, *Geom. Dedicata* **49** (1994), 85–116.

[48] A. Moretó and Pham Huu Tiep, Prime divisors of character degrees, *J. Group Theory* **11** (2008), 341–356.
[49] G. Navarro and Pham Huu Tiep, Rational irreducible characters and rational conjugacy classes in finite groups, *Trans. Amer. Math. Soc.* **360** (2008), 2443–2465.
[50] H.N. Nguyen, Low-dimensional complex characters of the symplectic and orthogonal groups, *Comm. Algebra* **38** (2010), 1157–1197.
[51] S. Nozawa, On the characters of the finite general unitary group $U(4, q^2)$, *J. Fac. Sci. Univ. Tokyo Sect. IA* **19** (1972), 257–295.
[52] S. Nozawa, Characters of the finite general unitary group $U(5, q^2)$, *J. Fac. Sci. Univ. Tokyo Sect. IA* **23** (1976), 23–74.
[53] B. Rosser, Explicit bounds for some functions of prime numbers, *Amer. J. Math.* **63** (1941), 211–232.
[54] D. Segal, '*Words: Notes on Verbal Width in Groups*', London Math. Soc. Lecture Note Series **361**, Cambridge University Press, Cambridge, 2009.
[55] A. Shalev, Word maps, conjugacy classes, and a noncommutative Waring-type theorem, *Annals of Math.* **170** (2009), 1383–1416.
[56] P. Sin and Pham Huu Tiep, Rank 3 permutation modules for finite classical groups, *J. Algebra* **291** (2005), 551–606.
[57] N. Spaltenstein, Caractères unipotents de ${}^3D_4(F_q)$, *Comment. Math. Helv.* **57** (1982), 676–691.
[58] T.A. Springer and R. Steinberg, Conjugacy classes, '*Seminar on Algebraic Groups and Related Finite Groups*', Lecture Notes Math. **131** (1970), 168–266.
[59] B. Srinivasan, The characters of the finite symplectic group $Sp(4, q)$, *Trans. Amer. Math. Soc.* **131** (1968), 488–525.
[60] R. Steinberg, The representations of $GL(3, q)$, $GL(4, q)$, $PGL(3, q)$, and $PGL(4, q)$, *Canad. J. Math.* **3** (1951), 225–235.
[61] Pham Huu Tiep, Dual pairs and low-dimensional representations of finite classical groups, preprint.
[62] Pham Huu Tiep and A. Zalesskii, Minimal characters of the finite classical groups, *Comm. Algebra* **24** (1996), 2093–2167.
[63] 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.
[64] 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.
[65] W.R. Unger, Computing the character table of a finite group, *J. Symbolic Comput.* **41** (2006), 847–862.
[66] H.N. Ward, On Ree's series of simple groups, *Trans. Amer. Math. Soc.* **121** (1966), 62–89.
[67] K. Zsigmondy, Zur Theorie der Potenzreste, *Monatsh. Math. Phys.* **3** (1892), 265–284.

R.M. Guralnick, Department of Mathematics, University of Southern California, Los Angeles, CA 90089, USA

E-mail address: guralnic@usc.edu

M.W. Liebeck, Department of Mathematics, Imperial College, London SW7 2BZ, UK

E-mail address: m.liebeck@imperial.ac.uk

E.A. O'Brien, University of Auckland, Auckland, New Zealand

E-mail address: e.obrien@auckland.ac.nz

A. Shalev, Hebrew University, Jerusalem 91904, Israel

E-mail address: shalev@math.huji.ac.il

P.H. Tiep, Department of Mathematics, Rutgers University, Piscataway, NJ 08854, USA

E-mail address: tiep@math.rutgers.edu