Annals of Mathematics **174** (2011), 1885–1950
http://dx.doi.org/10.4007/annals.2011.174.3.10

The Waring problem for finite simple groups

By Michael Larsen, Aner Shalev, and Pham Huu Tiep

Abstract

The classical Waring problem deals with expressing every natural number as a sum of $g(k)$ k-th powers. Recently there has been considerable interest in similar questions for non-abelian groups, and simple groups in particular. Here the k-th power word can be replaced by an arbitrary group word $w \neq 1$, and the goal is to express group elements as short products of values of w.

We give a best possible and somewhat surprising solution for this Waring type problem for (non-abelian) finite simple groups of sufficiently high order, showing that a product of length two suffices to express all elements.

Along the way we also obtain new results, possibly of independent interest, on character values in classical groups over finite fields, on regular semisimple elements lying in the image of word maps, and on products of conjugacy classes.

Our methods involve algebraic geometry and representation theory, especially Lusztig's theory of representations of groups of Lie type.

Contents

Michael Larsen was partially supported by NSF Grant DMS-0800705. Aner Shalev was partially supported by ERC Advanced Grant 247034. The first and the second named authors were partially supported by Bi-National Science Foundation United States-Israel Grant 2008194. Pham Huu Tiep was partially supported by NSF Grant DMS-0901241.

1. Introduction

1.1. *Background and main results.* A well-known classical result of Lagrange shows that every positive integer is a sum of four squares. The Waring problem in number theory generalizes this, asking whether every positive integer is a sum of $g(k)$ k-th powers, where g is a suitable function. Positive solutions for small values of k were obtained, and in 1909 Hilbert solved the general problem affirmatively. Hardy and Littlewood provided another solution using the circle method, which also sheds light on the number of representations of numbers as sums of $g(k)$ k-th powers. See [Nat96] for a more detailed background.

In the past 15 years noncommutative analogues of the Waring problem have been considered, and various interesting results have been obtained, with particular emphasis on finite (non-abelian) simple groups. Martinez and Zelmanov [MZ96], and independently Saxl and Wilson [SW97], showed in 1996–1997 that any element of a finite simple group Γ is a product of $f(k)$ k-th powers, provided there are nontrivial k-th powers in Γ. In 1994 Wilson [Wil96] showed that any element of a finite simple group is a product of c commutators, where c is some (unspecified) constant.

Are there extensions of these results to general words w? Recall that a word $w = w(x_1, \dots, x_d)$ is an element of the free group F_d on $x_1, \dots, x_d$. Given a word w and a group Γ we consider the word map $w_\Gamma : \Gamma^d \to \Gamma$ obtained by substituting group elements $g_1, \dots, g_d$ in $x_1, \dots, x_d$, respectively. Let $w(\Gamma) \subseteq \Gamma$ denote the image of this map. For subsets $S, T \subseteq \Gamma$ we set $ST = \{st : s \in S, t \in T\}$; in particular $S^k = \{s_1 \cdots s_k : s \in S\}$.

Extending the aforementioned results on powers and commutators, Liebeck and Shalev [LS01] showed in 2001 that for any word w there exists a positive integer c_w depending on w such that if Γ is a finite simple group and $w(\Gamma) \neq \{1\}$, then $w(\Gamma)^{c_w} = \Gamma$. No explicit bounds on c_w were given.

Later, it turned out that if Γ is large enough (given $w \neq 1$), then c_w does not depend on w and is in fact surprisingly small. Indeed Shalev [Sha09] showed that for any nontrivial word w, there exists a number N_w such that if Γ is a finite simple group of order at least N_w, then

$$w(\Gamma)^3 = \Gamma.$$

A different proof of this theorem using a method of Gowers has subsequently been given by Nikolov and Pyber [NP11].

While this result seems a rather satisfactory solution to this Waring type problem, it was not clear whether it is best possible; indeed, in some cases sharper results were obtained. If $w = [x_1, x_2]$, then a recent paper by Liebeck, O'Brien, Shalev, and Tiep [LOST10] shows that $w(\Gamma) = \Gamma$; namely, every element of a finite non-abelian simple group is a commutator. This proves

a longstanding conjecture of Ore. There were many partial results on this conjecture; most notably, Ellers and Gordeev [EG98] had used entirely different methods to prove the result for all the Chevalley groups over fields of size at least 8 (and in many cases even smaller).

However, various words w are not surjective on all (or even any) finite simple groups (for example consider the word $w = x_1^2$). Hence, if we could show that $w(\Gamma)^2 = \Gamma$ for all words $w \neq 1$ and finite simple groups of sufficiently large order (given w), this would constitute a best possible solution to the Waring type problem we consider.

Positive evidence for this conjecture was provided very recently. It is shown in [Sha09] (see also [Sha08]) that if Γ is a finite simple group of Lie type, then $|w(\Gamma)^2|/|\Gamma| \to 1$ as $|\Gamma| \to \infty$. Larsen and Shalev then showed in [LS09] that if $w \neq 1$ and the simple group Γ is alternating, or of Lie type of bounded rank (excluding Suzuki groups and Ree groups), then there exists a number N_w depending on w (and in the latter case also on the bound on the rank of Γ) such that $|\Gamma| \geq N_w$ implies

$$w(\Gamma)^2 = \Gamma.$$

See also [LS08] for a different proof for alternating groups and for related results on covering numbers and random walks. However, the main case of classical groups of unbounded rank remained very much open.

In this paper we solve this problem. Our main result is as follows.

THEOREM 1.1.1. *Let $w_1, w_2 \in F_d$ be nontrivial words in the free group on d generators. Then there exists a constant $N = N_{w_1,w_2}$ depending on w_1, w_2 such that for all finite non-abelian simple groups Γ of order greater than N, we have*

$$w_1(\Gamma)w_2(\Gamma) = \Gamma.$$

This result confirms Conjecture 1.9 posed in [LS09].

COROLLARY 1.1.2. *Let $w \in F_d$ be a nontrivial word in the free group on d generators. Then there exists a constant $N = N_w$ depending on w such that for all finite non-abelian simple groups Γ of order greater than N, we have*

$$w(\Gamma)^2 = \Gamma.$$

This solves Problem 10.1 in [Sha09].

The particular case $w = x_1^k$ is also novel and leads to the following best possible Waring type result for powers (sharpening [MZ96] and [SW97]):

COROLLARY 1.1.3. *For every positive integer k there exists a constant $N = N_k$ depending on k such that for all finite simple groups Γ of order greater than N, we have*

$$\{x^k y^k \mid x, y \in \Gamma\} = \Gamma.$$

This result is new even for $k = 2$; in fact, it is likely that the word $x_1^2 x_2^2$ is surjective on *all* finite simple groups of order > 2 (see [GS09] for related results).

Finally, our methods may be relevant to a well-known conjecture of J. G. Thompson, stating that any finite simple group Γ has a conjugacy class C such that $C^2 = \Gamma$. We obtain the following variant of Thompson's conjecture:

THEOREM 1.1.4. *There is an explicit constant N such that any finite nonabelian simple group Γ of order larger than N possesses two conjugacy classes C_1, C_2 with $C_1 C_2 \supseteq \Gamma \setminus \{1\}$.*

Here N can be chosen to be 2^{630}.

Results of [EG98], [MSW94], and [LM99] imply Theorem 1.1.4 for all but one infinite family of finite simple groups. Here we handle this remaining case.

It is intriguing that Waring type problems in highly noncommutative objects such as finite simple groups have much sharper solutions than in the classical case of the natural numbers.

1.2. *Strategy of proof.* The proof of our main result is rather long and complex, involving representation theory, geometry, and other tools. Let us now describe the strategy of the proof in some detail (with some unavoidable simplification). We focus on the main case, where Γ is a classical group of large rank.

The rough idea is to construct special conjugacy classes $C_1, C_2 \subset G$ satisfying

$$C_1 \subset w_1(\Gamma),\ C_2 \subset w_2(\Gamma) \tag{1.2.1}$$

and

$$C_1 C_2 \supseteq \Gamma \setminus \{1\}. \tag{1.2.2}$$

Using the machinery of Deligne-Lusztig [DL76] and Lusztig [Lus84], we can usually find many pairs (C_1, C_2) satisfying (1.2.2). Here the methods and results of [MSW94] are useful. The difficult point is to find a pair also satisfying (1.2.1). This requires geometric arguments and will be described later. Since $1 \in w_i(\Gamma)$ anyway, it follows that $w_1(\Gamma) w_2(\Gamma) = \Gamma$. In some cases the structure of the argument is more complex: We show that $C_1 C_2$ contains all elements of large support and that $w_1(\Gamma) w_2(\Gamma)$ contains the remaining elements of bounded support.

The classes C_1, C_2 are of suitable regular semisimple elements $s_1, s_2 \in \Gamma$ lying in maximal tori $T_1, T_2 \subset \Gamma$. The tori T_i are chosen to be *weakly orthogonal* (see §2 for the precise definition), and this ensures that if χ is an irreducible character of Γ such that $\chi(s_1)\chi(s_2) \neq 0$, then χ is unipotent. Moreover, there will be a small (in particular, bounded) number of such unipotent characters.

Now, the number of ways a group element $g \in \Gamma$ can be expressed as $g = x_1x_2$, where $x_i \in C_i$ is given by

$$\frac{|C_1||C_2|}{|\Gamma|} \sum_{\chi \in \mathrm{Irr}(\Gamma)} \frac{\chi(s_1)\chi(s_2)\overline{\chi}(g)}{\chi(1)},$$

and so we need to show that the sum above is nonzero for any nonidentity element $g \in \Gamma$. The choice of s_1, s_2 ensures that the number of nonzero summands is small. However, in order to control these summands we need information on the character ratios $|\chi(g)|/\chi(1)$. Gluck's bounds [Glu93], [Glu95] are useful but they do not suffice, and we have to establish sharper character bounds for elements of large support (see §4 for precise definition). Indeed, we prove in Section 4:

THEOREM 1.2.1. *If Γ is a finite quasi-simple classical group over $\mathbb{F}_q$ and $g \in \Gamma$ is an element of support at least N, then*

$$|\chi(g)|/\chi(1) < q^{-\sqrt{N}/481}$$

for all $1_\Gamma \neq \chi \in \mathrm{Irr}(\Gamma)$.

See Theorem 4.3.6 for more precise bounds. This character theoretic result seems to be of independent interest and may have further applications.

In order to show that $C_i \subset w_i(\Gamma)$, we use geometric tools to establish a Chebotarev Density Theorem for word maps (see results 5.3.2 and 5.3.3 below). We roughly show that for any word $w \neq 1$, if we fix the group type G and let the field size q tend to infinity, then $w(G(\mathbb{F}_q))$ hits all maximal tori $T(\mathbb{F}_q)$ of $G(\mathbb{F}_q)$ the expected number of times. In particular, if q is sufficiently large, there exist regular semisimple elements $s_i \in w_i(G(\mathbb{F}_q))$ lying in any prescribed maximal torus $T(\mathbb{F}_q)$.

This itself is not enough, since our group Γ is classical of unbounded rank. We overcome this obstacle by embedding groups Δ of very small rank (such as SL_2) over large extension fields in Γ so that $s_i \in w_i(\Delta)$ remains regular semisimple in Γ and lies in the required maximal torus T_i of Γ. Clearly $s_i \in w_i(\Gamma)$ so that $w_i(\Gamma)$ contains the conjugacy class $C_i = s_i^\Gamma$. This concludes the outline of the proof for classical groups of large rank.

The proof of the main result for the Suzuki and Ree groups combines methods from [LS09] with a strong version of Deligne conjecture established by Varshavsky [Var07].

Our notations GL, GU, GO, Ω, etc. for different classes of classical groups are as in [KL90]. We consider 1 (resp. -1) to be synonymous with $+$ and $-$ when used as superscripts.

We would like to acknowledge helpful discussions with Frank Lübeck and Yakov Varshavsky. We thank the referee for useful comments.

2. **Weakly orthogonal pairs**

In this section we introduce the notion of *weakly orthogonal pairs* of maximal tori in a simple connected semisimple group over a finite field.

2.1. *Connected reductive groups and maximal tori.* Let G be a connected reductive algebraic group over an algebraically closed field k. Let T be a maximal torus of G defined over k. The pair (G,T) defines a *root datum* $\Psi_G(T) := (X, \Phi, X^\vee, \Phi^\vee)$ in the sense of [Car93]. Here X and $X^\vee$ denote respectively the character group and cocharacter group of T, $\Phi \subset X$ is the system of roots of G with respect to T, and $\Phi^\vee \subset X^\vee$ denotes the coroot system. Let $W_G(T)$ denote the Weyl group of Φ. If T_1 and T_2 are maximal tori, then they are conjugate over $G(k)$, so $\Psi_G(T_1)$ and $\Psi_G(T_2)$ are isomorphic. The isomorphism is unique up to precomposition by the conjugation action of $W_G(T_1)$ or (equivalently) postcomposition by the conjugation action of $W_G(T_2)$. In particular, $W_G(T_1)$ and $W_G(T_2)$ are isomorphic and the isomorphism is well defined up to inner automorphism. To avoid keeping track of extra data, we will ignore the dependence of the root datum $\Psi := \Psi_G := \Psi_G(T)$ and especially the root system Φ and the Weyl group $W := W_G := W_G(T)$ on the choice of torus, which means that we will work throughout up to W-conjugation. We will also suppress G in the notation when there is no possible ambiguity.

We say G^*/k is *dual* to G if

$$\Psi_{G^*} = (X^\vee, \Phi^\vee, X, \Phi).$$

For every connected reductive group, a dual group (also connected and reductive) exists and is unique up to isomorphism.

If G is a connected reductive group over a finite field $\mathbb{F}$, we can choose a maximal torus T of G defined over $\mathbb{F}$. Extending scalars to $k = \overline{\mathbb{F}}$, we get a root datum with Frobenius action. In general, the Frobenius action depends on the choice of $\mathbb{F}$-torus T. We say two maximal tori are of the same *type* if they are conjugate over $G(\mathbb{F})$, so the Frobenius action on the root datum depends only on the type of the maximal torus chosen. By a standard Galois cohomology computation, the isomorphism class of G determines a W-coset of $\mathrm{Aut}(W)$, and the torus types are in one-to-one correspondence with W-orbits in this coset. In particular, if G is split over $\mathbb{F}$, the torus types are in one-to-one correspondence with conjugacy classes in W. We do not carefully distinguish between torus types and individual maximal tori in this paper. This should not cause confusion.

The dual group G^* can be defined over $\mathbb{F}$. Given a maximal torus T of G, there exists a maximal torus T^* of G^*, unique up to conjugation by $G^*(\mathbb{F})$, such that the duality between $\Psi_G(T)$ and $\Psi_{G^*}(T^*)$ respects Galois actions. In particular, T^* is dual to T in the sense that the Frobenius actions on their

character groups are mutually transpose. This duality sets up a one-to-one correspondence between torus types in G and those in G^*.

2.2. *Some consequences of Deligne-Lusztig.* We recall some basic results and definitions of Deligne-Lusztig [DL76] and apply them to give the necessary criteria that $\chi(s_1)\chi(s_2) \neq 0$, where χ is an irreducible character, and s_1 and s_2 are semisimple elements of a reductive group over a finite field $\mathbb{F} := \mathbb{F}_q$.

Fix a rational prime ℓ not dividing q. To each character $\theta \in \mathrm{Hom}(T(\mathbb{F}), \overline{\mathbb{Q}}_\ell^\times)$, one can attach an element R_T^θ in the ring of virtual representations of $G(\mathbb{F})$ over the field $\overline{\mathbb{Q}}_\ell$. By duality, there also exists a corresponding element $\theta^* \in T^*(\mathbb{F})$. Thus, a pair (T, θ) up to $G(\mathbb{F})$-conjugacy defines in a unique way a semisimple element $\theta^* \in G^*(\mathbb{F})$ up to $G^*(\mathbb{F})$-conjugacy. Let $G^*(\mathbb{F})^\natural$ denote the set of conjugacy classes of semisimple elements in $G^*(\mathbb{F})$. Every irreducible representation χ of $G(\mathbb{F})$ is associated to a unique element $C_\chi \in G^*(\mathbb{F})^\natural$ such that χ has nonzero multiplicity in R_T^θ only if $\theta^* \in C_\chi$ [Car95, 9.2]; moreover, every χ has nonzero multiplicity in some R_T^θ [DL76, 7.7]. We say that χ is *unipotent* if $C_\chi = \{e\}$.

Definition 2.2.1. We say that two $\mathbb{F}$-rational maximal tori T_1 and T_2 in a connected reductive group $G/\mathbb{F}$ are *weakly orthogonal* if

$$T_1^*(\mathbb{F}) \cap T_2^*(\mathbb{F}) = \{e\}$$

for every choice of T_1^* and T_2^*. This depends only on types of T_1 and T_2.

This concept was already used in [MSW94] (albeit without a formal definition).

For the remainder of Section 2, we will assume that G is semisimple and simply connected, so G^* is semisimple and adjoint. By Steinberg's theorem, the centralizer of every regular semisimple element in G is a maximal torus of G. If s_1 and s_2 are regular semisimple elements of $G(\mathbb{F})$ and T_i denotes the centralizer $C_G(s_i)$, we say s_1 and s_2 are *weakly orthogonal* if and only if T_1 and T_2 are weakly orthogonal. If s_1 and s_2 fail to be weakly orthogonal, then there exists a nontrivial (and therefore noncentral) semisimple element $g^* \in G^*(\mathbb{F})$ such that T_1^* and T_2^* can both be taken to lie in the connected reductive group $C_{G^*}(g^*)^\circ$.

Proposition 2.2.2. *If s_1 and s_2 are weakly orthogonal regular semisimple elements of $G(\mathbb{F})$ and χ is an irreducible character of $G(\mathbb{F})$ such that $\chi(s_1)\chi(s_2) \neq 0$, then χ is unipotent.*

Proof. By [MM99, 5.1], if $s \in G(\mathbb{F})$ is semisimple, and $\chi(s) \neq 0$, then there exist T and θ such that $\mathrm{Tr}(s, R_T^\theta) \neq 0$, and θ^* belongs to the conjugacy class C_χ. By [DL76, 7.2], this implies that s lies in the $G(\mathbb{F})$-conjugacy class of some element of $T(\mathbb{F})$. If $\chi(s_1)\chi(s_2) \neq 0$, then there exist $G^*(\mathbb{F})$-conjugate

elements θ_1^* and θ_2^* belonging to tori T_1^* and T_2^* which are dual to tori T_1 and T_2 containing s_1 and s_2, respectively. As T_1^* and T_2^* intersect in $\{e\}$, this means $\theta_1^* = \theta_2^* = e$, and χ is indeed unipotent. □

2.3. *Type A_r.* We consider first split groups of type A_r. Let $n = r+1$. The Weyl group of $G := \mathrm{SL}_n$ is isomorphic to S_n. If $a_1 + \cdots + a_k = n$ for positive integers a_i, we denote by $T_{a_1,\dots,a_k}$ the torus type in G associated with the permutation

$$(1\,2\,\cdots\,a_1)(a_1+1\,\cdots\,a_1+a_2)\cdots(n+1-a_k\,\cdots\,n)$$

with cycles of length $a_1,\dots,a_k$.

PROPOSITION 2.3.1. *For $0 \le a \le n$, the maximal tori T_n and $T_{1,a,r-a}$ are weakly orthogonal. If $2 \le a \le r-1$, the maximal tori $T_{1,r}$ and $T_{a,n-a}$ are weakly orthogonal.*

Proof. Suppose T_n^* and $T_{1,a,r-a}^*$ can be chosen to intersect nontrivially. Let s^* denote an element in their intersection, and $Z^\circ(s^*)$ the identity component of the centralizer of s^*. As $Z^\circ(s^*)$ contains T_n^*, it must be of the form

$$P(\mathrm{Res}_{\mathbb{F}_{q^m}/\mathbb{F}_q}\mathrm{GL}_{n/m})$$

for some divisor $m > 1$ of n, where Res denotes restriction of scalars. However, this group is anisotropic and therefore cannot contain a torus of type $T_{1,a,r-a}$. Now suppose $T_{1,r}^*$ and $T_{a,n-a}^*$ intersect in $s^* \in \mathrm{PGL}_n(\mathbb{F}_q)$. As $Z^\circ(s^*)$ contains $T_{1,r}^*$, it must be of the form

$$P(\mathrm{GL}_1 \times \mathrm{Res}_{\mathbb{F}_{q^m}/\mathbb{F}_q}\mathrm{GL}_{r/m}) \cong \mathrm{Res}_{\mathbb{F}_{q^m}/\mathbb{F}_q}\mathrm{GL}_{r/m}, \tag{2.3.1}$$

where $m \ge 1$ divides r. If $m > 1$, then either a or $n-a$ fails to be divisible by m, so $T_{a,n-a}^*$ cannot be contained in $Z^\circ(s^*)$. Thus $m = 1$. However, $T_{a,n-a}^* \subset \mathrm{GL}_r$ if and only if $a \in \{1, r\}$, contrary to hypothesis. □

Maximal torus types in the unitary group $G := \mathrm{SU}_n$ and its dual PGU_n are indexed by S_n-orbits in the the nontrivial S_n coset of $\mathrm{Aut}(\Phi) = \mathsf{S}_n \times \{\pm 1\}$. Such an orbit is given by a conjugacy class in S_n. We let $T_{a_1,\dots,a_k}$ and $T_{a_1,\dots,a_k}^*$ denote representative maximal torus types in G and G^* associated to the Weyl orbit of (2.3.1).

PROPOSITION 2.3.2. *For $0 \le a \le r+1$, the maximal tori T_n and $T_{1,a,r-a}$ are weakly orthogonal. If $2 \le a \le r-1$, the maximal tori $T_{1,r}$ and $T_{a,n-a}$ are weakly orthogonal.*

Proof. The proof is essentially the same except that the descriptions of the centralizers containing specified maximal tori must be slightly modified;

for example, the centralizers containing T_n are of the form

$$\begin{cases} P(\mathrm{Res}_{\mathbb{F}_{q^m}/\mathbb{F}_q}\mathrm{GU}_{n/m}) & \text{if } m|n \text{ is odd,} \\ P(\mathrm{Res}_{\mathbb{F}_{q^m}/\mathbb{F}_q}\mathrm{GL}_{n/m}) & \text{if } m|n \text{ is even.} \end{cases}$$ □

2.4. *Type B_r.* The Weyl group W_r of B_r is isomorphic to the group of permutations of $\Sigma_r := \{1, 2, \ldots, r, 1', 2', \ldots, r'\}$ commuting with the involution $'$ (where $i'' = i$). The map $\Sigma_r \to \{1, \ldots, r\}$ sending i and i' to i induces a surjective homomorphism $\phi\colon \mathsf{W}_r \to \mathsf{S}_r$. If $w \in \mathsf{W}_r$ and $S \subset \{1, \ldots, r\}$ is a single orbit of $\phi(w)$, then we say S is a *positive* (resp. *negative*) cycle of w if $S \setminus w(S)$ has even (resp. odd) cardinality. A conjugacy class of W_r is determined by a partition of r (specifying a conjugacy class in S_r), together with the data specifying how many parts of each size are positive and how many are negative. Equivalently, the data may be regarded as an ordered pair of partitions which total r.

Consider $G = \mathrm{Spin}_{2r+1}$, the simply connected group over $\mathbb{F}_q$ with root system B_r, with dual $G^* = \mathrm{PCSp}_r$. Given positive integers $a_1, \ldots, a_k$ summing to r, we write $T^+_{a_1,\ldots,a_k}$ for a maximal torus of G associated with the partition $r = a_1 + \cdots + a_k$, where all parts are positive and $T^-_{a_1,\ldots,a_k}$ for a maximal torus of G associated with the same partition, where all parts are negative. We will need to work with two pairs of maximal tori. For the first pair, T^+_r and T^-_r, we can appeal to [MSW94, Th. 2.4].

Proposition 2.4.1. *For $1 \le a \le r/2 - 1$ and $(\varepsilon, \varepsilon) \ne ((-1)^a, (-1)^{r-a})$, the maximal tori $T^{\varepsilon}_{a,r-a}$ and $T^{-\varepsilon}_{a+1,r-a-1}$ are weakly orthogonal.*

Proof. Use the same arguments as in the proof of Proposition 2.6.1, replacing $\mathrm{CO}^{\pm}_{2n}(\mathbb{F}_q)^\circ$ by $\mathrm{CSp}_{2n}(\mathbb{F}_q)$. □

2.5. *Type C_r.* Here the fact that we will need is that the tori T^+_r and T^-_r are weakly orthogonal. We again omit the proof since we will be citing a stronger result [MSW94, Th. 2.3] below.

2.6. *Type D_r.* If G is the split group Spin^+_{2r}, the $G(\mathbb{F}_q)$-conjugacy classes of maximal tori of G over $\mathbb{F}_q$ are indexed by conjugacy classes in the Weyl group $\mathsf{W}'_r \triangleleft \mathsf{W}_r$. A conjugacy class in W_r is represented by an element of W'_r if and only if the number of negative parts is even.

If G is the nonsplit group Spin^-_{2r}, the $G(\mathbb{F}_q)$-conjugacy classes of maximal tori of G over $\mathbb{F}_q$ are indexed by W_r-orbits in $\mathsf{W}_r \setminus \mathsf{W}'_r$. A conjugacy class in W_r has a representative in $\mathsf{W}_r \setminus \mathsf{W}'_r$ if and only if the number of negative parts is odd. For both the split and nonsplit spin groups, we write $T^{\varepsilon_1,\ldots,\varepsilon_k}_{a_1,\ldots,a_k}$ for a class where the part of size a_i has sign $\varepsilon_i = \pm$. Furthermore, this class is unique for the types that we will consider.

To prove the next statement, it is convenient to work with (finite) *multisets*, i.e., collections of elements with possible repetitions. The total number of elements in a multiset X, including repeated memberships, is called its *cardinality* $|X|$. Let Y be another multiset. The *join* $X \sqcup Y$, respectively the intersection $X \cap Y$, is the multiset Z, where the multiplicity of any $u \in Z$ is the sum, respectively the minimum, of its multiplicities in X and in Y. Similarly, we say that $X \subseteq Y$ if, for any $u \in X$, the multiplicity of u in X does not exceed its multiplicity in Y.

PROPOSITION 2.6.1. (i) *Let* $1 \leq a < b-1$, $\alpha, \beta \in \{\pm 1\}$ *and* $(\alpha, \beta) \neq ((-1)^a, (-1)^b)$. *Then the maximal tori* $T_{a,b}^{\alpha,\beta}$ *and* $T_{a+1,b-1}^{-\alpha,-\beta}$ *are weakly orthogonal.*

(ii) *Assume that* $\varepsilon \in \{\pm 1\}$ *and, in addition,* r *is odd if* $\varepsilon = 1$. *Then the maximal tori* T_r^{ε} *and* $T_{r-1,1}^{-,-\varepsilon}$ *are weakly orthogonal.*

Proof. (i) In this case, the dual group G^* is $\mathrm{PCO}(V)^\circ$, where $V = \mathbb{F}_q^{2(a+b)}$ is endowed with a suitable quadratic form Q; see [TZ96, Lemma 7.4] for an explicit description of the groups G^* and $H := \mathrm{CO}(V)^\circ$. Consider the complete inverse images in H of the tori dual to $T_{a,b}^{\alpha,\beta}$ and $T_{a+1,b-1}^{-\alpha,-\beta}$, and assume g is an element belonging to both of them. We need to show that $g \in Z(H)$. We will consider the spectrum S of the semisimple element g on V as a multiset. Let $\gamma \in \mathbb{F}_q^\times$ be the *conformal coeficient* of g, i.e., $Q(g(v)) = \gamma Q(v)$ for all $v \in V$. Then S can be represented as the joins of multisets $X \sqcup Y$ and $Z \sqcup T$, where

$$\begin{aligned}
X &:= \{x, x^q, \dots, x^{q^{a-1}}, \gamma x^{-1}, \gamma x^{-q}, \dots, \gamma x^{-q^{a-1}}\},\\
Y &:= \{y, y^q, \dots, y^{q^{b-1}}, \gamma y^{-1}, \gamma y^{-q}, \dots, \gamma y^{-q^{b-1}}\},\\
Z &:= \{z, z^q, \dots, z^{q^a}, \gamma z^{-1}, \gamma z^{-q}, \dots, \gamma z^{-q^a}\},\\
T &:= \{t, t^q, \dots, t^{q^{b-2}}, \gamma t^{-1}, \gamma t^{-q}, \dots, \gamma t^{-q^{b-2}}\},
\end{aligned}$$

for some $x, y, z, t \in \overline{\mathbb{F}}_q^\times$; furthermore, $x^{q^a-\alpha} = 1$ if $\alpha = +$ and $x^{q^a-\alpha} = \gamma$ if $\alpha = -$, and similarly for y, z, t.

Let A be any multiset of elements of $\overline{\mathbb{F}}_q$, where the multiplicity of each element in A is $2(a+b)$, and with the property that if $u \in A$, then $u^q, \gamma u^{-1} \in A$. We claim that if $A \cap S \neq \emptyset$, then $A \supseteq S$. Indeed, since the multiplicity of any $u \in S$ is at most $2(a+b)$, 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 since $S = X \sqcup Y$, we must have $|A \cap S| \in \{2a, 2b\}$. But $S = Z \sqcup T$ as well, so we see that $|A \cap S| \in \{2a+2, 2b-2\}$, which is a contradiction as $a + 1 < b$.

Consider, for instance, the case $b = 2k+1$ and $\beta \neq (-1)^b$, i.e., $\beta = 1$. Applying the claim to the multiset A consisting of elements $u \in \overline{\mathbb{F}}_q$ such that $u^{q^b-\beta} = 1$, each with multiplicity $2(a+b)$, and noting that $A \supseteq Y$, we see

that $u^{q^b-\beta} = 1$ for all $u \in S$. In particular, $t^{q^{2k+1}-1} = t^{(q^{2k}+1)(q-1)} = 1$, whence $t \in \mathbb{F}_q^\times$ and $\gamma = t^{q^{2k}+1} = t^2$, i.e., $\gamma t^{-1} = t$. Now applying the claim to the multiset A consisting of elements $v \in \mathbb{F}_q^\times$ such that $v = \gamma v^{-1}$, each with multiplicity $2(a+b)$, and noting that $A \supseteq T$, we see that $v \in \mathbb{F}_q^\times$ and $v = \gamma v^{-1}$ for all $v \in S$. Thus $g = x \cdot 1_V$, as stated. The same argument applies to the other cases.

(ii) A similar argument (but much simpler than that in (i)). □

3. **Unipotent characters of classical groups**

3.1. *Unipotent characters of A_r and ${}^2A_r$.* Let $n = r+1$. Let G be a form of SL_n over $\mathbb{F}_q$, i.e., either SL_n or SU_n. The unipotent representations of $G(\mathbb{F}_q)$ are indexed by partitions $\alpha \vdash n$ [Lus84, App.]. We have seen that the types of maximal torus of G naturally correspond to conjugacy classes $O(\sigma)$ in S_n. If $\chi_{\mathrm{uni},\alpha}$ is the unipotent character of $G(\mathbb{F}_q)$ associated to a partition α of n and t is a regular semisimple element of $G(\mathbb{F}_q)$ associated to the conjugacy class $O(\sigma) \subset \mathsf{S}_n$, then $\chi_{\mathrm{uni},\alpha}(t) \neq 0$ implies that $\chi_\alpha(\sigma) \neq 0$, where χ_α denotes the character of S_n associated to α [Car95, 7.1].

To find sufficient conditions for $\chi_\alpha(\sigma) = 0$, we use the Murnaghan-Nakayama rule [Jam78, 21.1]. A box in a Young diagram belongs to the *rim* if the diagram does not contain a box at the crossing of the next row and the next column. By a *rim t-hook* β in a diagram α, we mean a connected subset of the rim containing t nodes, such that $\alpha \backslash \beta$ is a proper diagram. If, moving from right to left, the rim hook β starts in row i and finishes in column j, then the *leg-length* $l(\beta)$ is defined to be the number of nodes below the ij-node in the α-diagram.

Proposition 3.1.1 (The Murnaghan-Nakayama rule; cf. [Jam78, 21.1]). *Let $\tau\pi \in \mathsf{S}_n$, where τ is a t-cycle and π is a permutation of the remaining $n-t$ points. Then*

$$\chi_\alpha(\tau\pi) = \sum_\beta (-1)^{l(\beta)} \chi_{\alpha\backslash\beta}(\pi),$$

where the sum is over all rim t-hooks β in an α-diagram.

The following corollary is immediate:

Corollary 3.1.2. *For all $\alpha \vdash n$,*

$$\chi_\alpha((1\,2\,\cdots\,n)) \in \{-1, 0, 1\},$$

with nonzero value only if α is of the form $(1^{n-k}, k)$ for some integer $k \in [1, n]$. Likewise,

$$\chi_\alpha((1\,2\,\cdots\,n-1)) \in \{-1, 0, 1\},$$

with nonzero value only if α is of the form (n), (1^n), or $(1^{n-2-k},2,k)$ for some $k\in[2,n-2]$.

For future use, we record the following extension of Corollary 3.1.2:

COROLLARY 3.1.3. *Let $1\le k\le n-1$. For all $\alpha\vdash n$,*

$$|\chi_\alpha((12\dots k)(k+1,k+2,\dots,n))|\le 4,$$

with nonzero value only if α is of the form

(Ia) (n) *or* (1^n);
(Ib) $(1^y,k+1,k+x+1)$ (*type* Ib1) *or* $(1^x,2^k,y+2)$ (*type* Ib2), *where* $0\le x,y\le x+y=n-2k-2$;
(Ic) $(1^y,x+1,k)$ *or* $(1^{k-1-x},2^x,y+2)$ *where* $0\le x\le k-1$, $0\le y$, *and* $x+y=n-k-1$;
(IIa) $(1^j,n-j)$, *where* $\min(j+1,n-j)\le\min(k,n-k)$;
(IIb) $(1^{j-1-y},2^y,k-j+1,k-j+x+1)$, *where* $1\le j\le k-1$, $0\le y\le j-1$, $0\le x$, *and* $x+y=n-2k+j-1$;
(IIc) $(1^y,2^j,k-j+1,k-j+x+1)$, *where* $1\le j\le k-1$, $0\le x,y\le x+y=n-2k-2$;
(IId) $(1^{j-1-y},2^y,x+2,k-j)$, *where* $1\le j\le k-1$, $0\le x\le k-j-2$, $0\le y\le j-1$, *and* $x+y=n-k-1$;
(IIe) $(1^y,2^j,x+2,k-j)$, *where* $1\le j\le k-1$, $0\le x\le k-j-2$, $0\le y$, *and* $x+y=n-k-2-j$.

Proof. The bound on character values comes from [LS09, 7.2]. Assume that $\chi_\alpha(\tau\pi)\ne 0$, where $\tau:=(12\cdots k)$ and $\pi:=(k+1,k+2,\dots,n)$. By Proposition 3.1.1 and Corollary 3.1.2, this implies that we can remove a rim $(n-k)$-hook β from the Young diagram of α to get a k-hook. The possible shapes for α are listed explicitly above, where type I has $\alpha\setminus\beta=(k)$ or (1^k) and type II has $\alpha\setminus\beta=(1^j,k-j)$ with $1\le j\le k-1$. □

Corollary 3.1.3 immediately implies the following:

COROLLARY 3.1.4. *For all $\alpha\vdash n$,*

$$\chi_\alpha((12)(3\,4\,\cdots\,n))\in\{-1,0,1\},$$

with nonzero value if only if α is of the form (n), (1^n), $(1^{n-2},2)$, $(1,n-1)$, $(1^{n-4},2^2)$, $(2,n-2)$, $(1^{n-6-k},3,k+3)$, or $(1^{n-6-k},2^2,k+2)$, for some $k\in[0,n-6]$.

We can now prove the following proposition:

PROPOSITION 3.1.5. *Let a be a fixed positive integer. Then there exists an integer $N\ge a+2$ and a constant C such that if $n>N$, t_1 and t_2 are regular semisimple elements of $G(\mathbb{F}_q)$ belonging to tori of type T_n and $T_{1,a,r-a}$,*

respectively, then there are at most three nontrivial irreducible characters χ *such that* $\chi(t_1)\chi(t_2) \neq 0$ *and only one for which*

$$\chi(1)^2 < \frac{C|G(\mathbb{F}_q)|}{q^n}. \tag{3.1.1}$$

Moreover, for all of these characters, $|\chi(t_1)\chi(t_2)| = 1$. *Likewise, if* $a > 1$ *and* $n > N$, *if* t_1 *and* t_2 *are regular semisimple elements of* $G(\mathbb{F}_q)$ *belonging to tori of type* $T_{1,r}$ *and* $T_{a,n-a}$, *respectively, then there are at most three nontrivial irreducible characters* χ *such that* $\chi(t_1)\chi(t_2) \neq 0$ *and only one for which* (3.1.1) *holds. Moreover, for all of these characters,* $|\chi(t_1)\chi(t_2)| = 1$.

Proof. By Propositions 2.2.2, 2.3.1, and 2.3.2, χ must be unipotent. It is therefore of the form $\chi_{\mathrm{uni},\alpha}$ for some partition α of n. For the first claim, t_1 belongs to a maximal torus of type T_n, so α must be of the form $(1^{n-k}, k)$ for some k. By Proposition 3.1.1,

$$\chi_\alpha((2 \cdots a+1)(a+2 \cdots n)) \in \{-1, 0, 1\},$$

with nonzero value only if $k \in \{1, a+1, n-a, n\}$. The dimensions of the corresponding representations are well known (see, e.g., [Ste51]). In the split case,

$$\chi(1) = q^{\frac{(n^2-n)-(k^2-k)}{2}} \prod_{i=1}^{n-k} \frac{1-q^{i-n}}{1-q^{-i}}.$$

Since $\prod_{i=1}^{\infty}(1-q^{-i})$ is bounded away from 0 and ∞ for all prime powers q, we have

$$\log_q \chi(1) = \frac{(n^2-n)-(k^2-k)}{2} + O(1) = \frac{\log_q |G(\mathbb{F}_q)|}{2} - \frac{n}{2} + O(1)$$

if k is bounded and n grows without bound. When $k = n$, χ is trivial, and this leaves only $k = n - a$ for χ to satisfy (3.1.1). A similar estimate holds in the unitary case (see [Lus77, 9.5]). Note that $\prod_{i=1}^{\infty}(1-(-q)^{-i})$ is also bounded away from 0 and ∞. The values of χ_α at $(1\,2 \cdots n)$ and $(2 \cdots a{+}1)(a{+}2 \cdots n)$ are both ± 1, so the same can be said about the values of $\chi_{\mathrm{uni},\alpha}$ at t_1 and t_2.

For the second claim, by Corollary 3.1.2, the partition α must be (n), (1^n), or of the form $(1^{n-2-k}, 2, k)$. We have already seen that (n) gives the trivial representation, while (1^n) gives rise to the Steinberg representation, which violates the degree bound (3.1.1). For $\alpha = (1^{n-2-k}, 2, k)$, by Proposition 3.1.1, $\chi_{\mathrm{uni},\alpha}(t_2) \neq 0$ implies $k \in \{a, n-a\}$. Again, the dimension formula for $k = a$ gives a character χ which violates (3.1.1). The character associated with $k = n - a$ is the only possible nontrivial character, not vanishing on t_1 or t_2, and satisfying (3.1.1). Computing the values of $\chi_{\mathrm{uni},\alpha}$ at t_1 and t_2 by Proposition 3.1.1 as before, we see that they must belong to $\{\pm 1\}$. □

3.2. *Symbols for orthogonal groups.* We recall Lusztig's theory of symbols, originally developed in [Lus77, 3.1]. By a *symbol*, we mean an ordered pair (λ, μ) of strictly increasing finite sequences of nonnegative integers $\lambda_1 < \lambda_2 < \cdots < \lambda_l$ and $\mu_1 < \mu_2 < \cdots < \mu_m$. The *rank* of the symbol (λ, μ) is the nonnegative integer

$$r := \sum_{i=1}^{s} \lambda_i + \sum_{j=1}^{t} \mu_j - \Big\lfloor \frac{(s+t-1)^2}{4} \Big\rfloor.$$

The *defect* of the symbol is $s - t$. We consider the following *shift-equivalence* relation on the set of symbols of fixed rank and defect. The equivalence relation is the transitive closure of the relation

$$\begin{pmatrix} \lambda_1 < \cdots < \lambda_s \\ \mu_1 < \cdots < \mu_t \end{pmatrix} \sim \begin{pmatrix} 0 < \lambda_1 + 1 < \cdots < \lambda_s + 1 \\ 0 < \mu_1 + 1 < \cdots < \mu_t + 1 \end{pmatrix}.$$

Within each shift-equivalence class, there is a minimal pair (λ, μ) for which $\lambda_1 + \mu_1 > 0$. If (λ, μ) and (λ', μ') are minimal pairs, the corresponding classes lie in the same *family* if and only if the multisets $\{\lambda_1, \lambda_2, \dots, \mu_1, \mu_2, \dots\}$ and $\{\lambda'_1, \lambda'_2, \dots, \mu'_1, \mu'_2, \dots\}$ coincide.

The irreducible representations of W_r are indexed by equivalence classes of symbols of rank r and defect 1 [Lus84, 4.5]. There is another, equivalent, way to index irreducible representations of W_r, more obviously related to the parametrization of conjugacy classes of W_r described in Section 2.4. Namely, the representations are in bijective correspondence to ordered pairs of partitions (α, β) such that $|\alpha| + |\beta| = r$. To convert between these notations, given a symbol (λ, μ), we set $\alpha_i = \lambda_i + 1 - i$, $\beta_j = \mu_j + 1 - j$, and omit all zero-parts in the resulting partitions α, β. An explicit construction of the representation labeled by (α, β) can be described as follows; cf. [Lus81, §2.1]. Let τ be the unique character of W_r taking value 1 on W'_r and -1 on $\mathsf{W}_r \setminus \mathsf{W}'_r$. Now if $\alpha \vdash k$ and $\beta \vdash l$, then we can embed $\mathsf{W}_k \times \mathsf{W}_l$ in W_r. Furthermore, there is a unique irreducible representation of S_k labeled by α as in [Jam78], and using the projection $\phi|_{\mathsf{W}_k} \colon \mathsf{W}_k \to \mathsf{S}_k$, we can inflate it to an irreducible representation $[\alpha]$ of W_k. Similarly, β gives rise to an irreducible representation $[\beta]$ of W_l. Then the irreducible representation of W_r labeled by (α, β) is

$$\operatorname{ind}_{\mathsf{W}_k \times \mathsf{W}_l}^{\mathsf{W}_r} \left([\alpha] \otimes ([\beta] \otimes \tau|_{\mathsf{W}_l}) \right). \tag{3.2.1}$$

The unipotent representations of $\mathrm{Spin}_{2r+1}(\mathbb{F}_q)$ are indexed by equivalence classes of symbols of rank r and odd defect, where in addition to shift-equivalence, we consider (λ, μ) and (μ, λ) to be equivalent [Lus77, 8.2].

The correspondence between irreducible representations of W_r and unipotent characters is not bijective. Nevertheless, for each irreducible representation χ of the Weyl group W_r, there is a natural *almost character* R_χ, which is

a virtual character of $\mathrm{Spin}_{2r+1}(\mathbb{F}_q)$, given by the formula

$$R_\chi = \frac{1}{|\mathsf{W}_r|} \sum_{\sigma \in \mathsf{W}_r} \chi(\sigma) R^1_{T_\sigma},$$

where $R^1_{T_\sigma}$ is the Deligne-Lusztig representation associated to the maximal torus T_σ corresponding to σ and the trivial character. By [DL76, Cor. 7.2], the character of $R^1_{T_\sigma}$ at a regular semisimple element s is equal to 0 if s is not conjugate to an element of T_σ and to $|N_{G^F}(T^F_\sigma) : T^F_\sigma|$ if s is conjugate to an element of T_σ. In the latter case, since s is regular, (a conjugate of) T_σ is the unique maximal torus in $C_G(s)$, and so T_σ is the only maximal torus containing T^F_σ. It follows by [BCC$^+$70, E-II.1.8,1.9,1.10(a)] that

$$|N_{G^F}(T^F_\sigma) : T^F_\sigma| = |C_{\mathsf{W}_r}(\sigma)|.$$

Thus, the character of R_χ at a regular semisimple element of $\mathrm{Spin}_{2r+1}(\mathbb{F}_q)$ corresponding to an element $\sigma \in \mathsf{W}_r$ is $\chi(\sigma)$.

The partition of shift-equivalence classes of symbols into families induces a partition of unipotent representations into families and a corresponding partition of irreducible representations of W_r into families. There is, moreover, a "Fourier transform" matrix relating the almost characters in a given family and the unipotent representations in the corresponding family [Lus81, 5.8], [Car95, 7.1]. As the entries of the matrix have absolute value ≤ 1, if χ_{uni} is a unipotent character of $\mathrm{Spin}_{2r+1}(\mathbb{F}_q)$, then

$$|\chi_{\mathrm{uni}}(t)| \leq \sum_\chi |\chi(\sigma)|,$$

where χ ranges over all irreducible characters of W_r in the family $\mathcal{F}(\chi_{\mathrm{uni}})$ corresponding to that of χ_{uni}. In particular, if $\chi(\sigma) = 0$ for all χ in the family, then $\chi_{\mathrm{uni}}(t) = 0$.

There is a parallel theory for W'_r, the Weyl group of D_r. Here, irreducible representations of W'_r are given by shift-equivalence classes of symbols of rank r and defect zero, with two extra provisos: If the symbol is *nondegenerate*, i.e., $\lambda \neq \mu$, then (μ, λ) and (λ, μ) determine the same representation; if the symbol is *degenerate*, i.e., $\lambda = \mu$, there are two irreducible representations attached to (λ, λ), denoted $(\lambda, \lambda)'$ and $(\lambda, \lambda)''$, where λ and μ are related to α and β respectively as above. Again, we can also describe the indexing in terms of pairs of partitions $\{\alpha, \beta\}$, with total sum r. If $\alpha \neq \beta$, then the W_r-representations associated to (α, β) and (β, α) both restrict to the irreducible representation of W'_r associated to $\{\alpha, \beta\}$; if $\alpha = \beta$, then the W_r-representation associated to (α, α) decomposes into the two W'_r-representations denoted $(\lambda, \lambda)'$ and $(\lambda, \lambda)''$ above.

As in the case of $\mathrm{Spin}_{2r+1}(\mathbb{F}_q)$, the unipotent representations of $\mathrm{Spin}^\varepsilon_{2r}(\mathbb{F}_q)$ can also be labeled by equivalence classes of symbols of rank r, and defect

$\equiv 0 (\mathrm{mod}\, 4)$ if $\varepsilon = +$ (the split case), $\equiv 2 (\mathrm{mod}\, 4)$ if $\varepsilon = -$ (the nonsplit case). Again, when $\lambda \neq \mu$, there is a single unipotent representation associated to (λ, μ) and (μ, λ), and when the symbol Λ is degenerate (which can only happen in the split case), there are two unipotent representations corresponding to it; cf. [Lus82, Lemma 3.8].

3.3. *Unipotent characters of D_r and ${}^2D_r$.* We will deal with unipotent characters of even-dimensional orthogonal groups first.

PROPOSITION 3.3.1. *Fix $a \geq 1$, and let r be any integer greater than $2a+2$. Let t_1 and t_2 be regular semisimple elements of $G := \mathrm{Spin}^{\pm}_{2r}(\mathbb{F}_q)$ belonging to tori T_1 and T_2 of type $T^{\alpha,\beta}_{a,r-a}$ and $T^{-\alpha,-\beta}_{a+1,r-a-1}$ respectively, where $\alpha, \beta \in \{\pm 1\}$ and $(\alpha, \beta) \neq ((-1)^a, (-1)^{r-a})$. Then the number of distinct irreducible characters of G which vanish neither on t_1 nor on t_2 is bounded, independent of r, q, and the choices of t_i. Likewise, the absolute values of these characters on t_1 and t_2 are bounded independent of r, q, and the t_i.*

Proof. 1) Consider any $\chi \in \mathrm{Irr}(G)$ with $\chi(t_1)\chi(t_2) \neq 0$. By Proposition 2.6.1, the tori T_1 and T_2 are weakly orthogonal. Hence χ is unipotent by Proposition 2.2.2. Now, by [DL76, 7.9],

$$\chi(t_i) = [\chi, R^1_{T_i}],$$

where, as above, $R^1_{T_i}$ is the generalized Deligne-Lusztig character corresponding to the principal character of the maximal torus T_i. The above inner product has been determined by Lusztig in [Lus82, Cor. 3.16] for q sufficiently large, and Asai [Asa83] shows that the same formula holds for any q. Also note that in a sense, unipotent characters do not depend on the isogeny type of the finite group G; cf. [DL76, 7.10].

Let T_i correspond to the F-conjugacy class of w_i in the Weyl group W'_r. Under the natural projection $\phi\colon \mathsf{W}'_r \to \mathsf{S}_r$, w_1 projects onto π_1 of cycle type $(a, r-a)$ and w_2 projects onto π_2 of cycle type $(a+1, r-a-1)$. Also, let Λ be a symbol corresponding to χ.

2) Observe that Λ must be nondegenerate. Assume the contrary; in particular, Λ has defect 0 and corresponds to two irreducible representations $[\Lambda]'$ and $[\Lambda]''$ of the Weyl group W'_r, G is split, and $2|r$. Also, χ is one of the two unipotent representations $\rho(\Lambda)_b$, $\rho(\Lambda)_{b'}$ labeled by Λ. By [Lus82, Cor. 3.16(i)], we may assume that

$$[\chi, R^1_{T_i}] = [\Lambda]'(w_i).$$

Clearly, one of a, $a+1$ must be odd, and so some w_j is centralized by an element $t \in \mathsf{W}_r \setminus \mathsf{W}'_r$ (if a is odd for instance, then this element t sends k to k' if and only if k belongs to the a-cycle of π_1). Recall that since Λ is degenerate, $\mathrm{ind}_{\mathsf{W}'_r}^{\mathsf{W}_r}([\Lambda]') = \mathrm{ind}_{\mathsf{W}'_r}^{\mathsf{W}_r}([\Lambda]'')$ is just the irreducible representation $[\Lambda]$

of W_r labeled by Λ, and furthermore,

$$[\Lambda]''(x) = [\Lambda]'(txt^{-1})$$

for any $x \in \mathsf{W}'_r$. As $[t, w_j] = 1$, it follows that

$$[\Lambda]'(w_j) = [\Lambda]''(w_j) = [\Lambda](w_j)/2.$$

Next, the degenerate symbol Λ corresponds to the pair (α, α) where $\alpha \vdash r/2$, and by (3.2.1),

$$[\Lambda] = \mathrm{ind}_{\mathsf{W}_{r/2} \times \mathsf{W}_{r/2}}^{\mathsf{W}_r} \left([\alpha] \otimes ([\alpha] \otimes \tau|_{\mathsf{W}_{r/2}}) \right).$$

By our assumption $a + 1 < r - a - 1$, neither w_1 nor w_2 can belong to (a conjugate in W_r of) $\mathsf{W}_{r/2} \times \mathsf{W}_{r/2}$. Hence, $[\Lambda](w_j) = 0$ and so

$$\chi(t_j) = [\chi, R^1_{T_j}] = [\Lambda]'(w_j) = 0.$$

3) Now we may assume that Λ is nondegenerate. The equivalence class of Λ contains a unique representative $\Lambda = (X, Y)$ such that $0 \notin X \cap Y$, and we will always choose Λ to satisfy this condition. Following the notation of [Lus82], let Z_1 be the set of "singles" in Λ; that is, the set of elements in $(X \cup Y) \setminus (X \cap Y)$ and $Z_2 := X \cap Y$. Then $X = Z_2 \cup (Z_1 \setminus N)$ and $Y = Z_2 \cup N$ for some $N \subseteq Z_1$. Since the defect of Λ is even, $|Z_1| = 2d$ for some integer d.

By [Lus82, Cor. 3.16(ii)], the condition $\chi(t_1)\chi(t_2) \neq 0$ implies that there are some $M_1, M_2 \subseteq Z_1$ such that $|M_1| = |M_2| = d$ and

$$[\Lambda_1](w_1) \neq 0, \ [\Lambda_2](w_2) \neq 0 \tag{3.3.1}$$

in the split case, and

$$[\Lambda_1](w_1\varphi) \neq 0, \ [\Lambda_2](w_2\varphi) \neq 0 \tag{3.3.2}$$

in the nonsplit case. Here, $\Lambda_i := (Z_2 \cup (Z_1 \setminus M_i), Z_2 \cup M_i)$ for $i = 1, 2$, and $\varphi \in \mathsf{W}_r$ sends i to i for $1 \leq i \leq r - 1$ and r to r'. We need to show that the number of such Λ is bounded by a function of a only, and that $|\chi(t_1)|$, $|\chi(t_2)|$ are also bounded by a function of a only for all such $\chi = \rho(\Lambda)$.

4) Let the pair (α_i, β_i) of partitions $\alpha_i \vdash k_i$, $\beta_i \vdash l_i$, correspond to the symbol Λ_i, for $i = 1, 2$. Then condition (3.3.1) in the split case, respectively (3.3.2) in the nonsplit case, and formula (3.2.1) imply that the permutation $\pi_i \in \mathsf{S}_r$ preserves a partition of the set $\{1, 2, \ldots, r\}$ into the union of a k_i-set and an l_i-set. It follows that

$$\{k_1, l_1\} = \{r, 0\} \text{ or } \{a, r - a\}$$

and

$$\{k_2, l_2\} = \{r, 0\} \text{ or } \{a + 1, r - a - 1\}.$$

5) Here we consider the case where $\{k_1, l_1\} = \{k_2, l_2\} = \{r, 0\}$. Then without loss, we may assume that β_1, β_2 are empty partitions and $\alpha_1, \alpha_2 \vdash r$. The nonvanishing condition (3.3.1), respectively (3.3.2), now implies that α_1

is one of the partitions listed in Corollary 3.1.3 for $k = a$ and α_2 is one of the partitions listed in Corollary 3.1.3 for $k = a+1$. In particular, $2 \le |Z_1| \le 4$, i.e., $1 \le d \le 2$. Since Z_1 has 2, respectively 6, subsets of cardinality $|Z_1|/2$ for $d = 1$, respectively for $d = 2$, Corollary 3.1.3 and [Lus82, Cor. (3.16)(ii)] imply that

$$|\chi(t_i)| \le 6.$$

Next we count the total number of possibilities for (Z_1, Z_2); each of these possibilities gives rise to at most $2^{2d} \le 16$ possibilities for Λ. Clearly, (Z_1, Z_2) is uniquely determined by α_1 and also by α_2. Observe that each of the types Iac and IIabde in Corollary 3.1.3 contains at most $(a+1)^2$ partitions α_i. So it remains to consider the cases where the type of α_1 and the type of α_2 belong to $\{\text{Ib}, \text{IIc}\}$. In each of the following cases, we will match up the shapes of Z_1 and Z_2 as they come from α_1 and from α_2 to derive a contradiction. Also, to make the arguments symmetric for t_1 and t_2, we may replace $(a, a+1)$ by $(a, a-1)$ and assume π_2 has cycle type $(a', r-a')$ with $a' = a \pm 1$.

Assume, for instance, that $\alpha_1 = (1^y, a+1, a+x+1)$ is of type Ib1. Then $Z_1 = \{0, y+1, a+1+y, r-a\}$ and $Z_2 = \{1, 2, \dots, y\}$. Now if $\alpha_2 = (1^{y'}, a'+1, a'+x'+1)$ is of type Ib1, then the shape of Z_2 forces $y = y'$, but then Z_2 cannot have the indicated shape. If $\alpha_2 = (1^{x'}, 2^{a'}, y'+2)$ (of type Ib2), or $(1^{y'}, 2^j, a'-j+1, a'-j+x'+1)$ (of type IIc), then $Z_2 = \{1, 2, \dots, x'+a'\} \setminus \{x'+1\}$ or $Z_2 = \{1, 2, \dots, y'+j+1\} \setminus \{y'+1\}$. Both possibilities contradict the given shape of Z_2, unless $a' = a-1 = 1$ and $y = x' = r-2a$, which is impossible.

Next, assume that $\alpha_1 = (1^y, 2^j, a-j+1, a-j+x+1)$ is of type IIc. Then $Z_1 = \{0, y+1, a+1+y, r-a\}$ and $Z_2 = \{1, 2, \dots, y+j+1\} \setminus \{y+1\}$. Now if $\alpha_2 = (1^{y'}, 2^{j'}, a'-j'+1, a'-j'+x'+1)$ is also of type IIc, then the shape of Z_2 forces $j' = j$ and $y' = y$. But then $Z_1 = \{0, y+1, a'+1+y, r-a'\}$, whence $y = r-a-a'-1$ and $x = -2$ or $x' = -2$; a contradiction. On the other hand, if $\alpha_2 = (1^{x'}, 2^{a'}, y'+2)$ (of type Ib2), then $Z_2 = \{1, 2, \dots, x'+a'\} \setminus \{x'+1\}$, forcing $x' = y$ and $x'+a' = y+j+1$. This can happen only when $a' = a-1$ and $j = a-2$. Then the shape of Z_1 implies that $y = r-2a$ and $x = -2$; again a contradiction.

Finally, assume that $\alpha_1 = (1^x, 2^a, y+2)$ and $\alpha_2 = (1^{x'}, 2^{a'}, y'+2)$ are both of type Ib2. Then

$$Z_2 = \{1, 2, \dots, x+a\} \setminus \{x+1\} = \{1, 2, \dots, x'+a'\} \setminus \{x'+1\},$$

forcing $x+1 = x'+1$ and $x+a = x'+a'$; again a contradiction.

6) Now we may assume that $k_1 = a$ and $k_2 = r-a$. Clearly, π_1 preserves a unique partition of $\{1, 2, \dots, r\}$ into the union of an a-set and an $(r-a)$-set. Hence formula (3.2.1) yields that

$$|[\Lambda_1](w_1)| = |[\Lambda_1](w_1\varphi)| = |[\alpha_1]((a))| \cdot |[\beta_1]((r-a))|.$$

By Corollary 3.1.2 and the nonvanishing condition (3.3.1), respectively (3.3.2), both α_1 and β_1 must be hook partitions:

$$\alpha_1 = (1^e, a-e),\ \beta_1 = (1^f, r-a-f),$$

where $0 \le e \le a-1$, and $0 \le f \le r-a-1$. In particular, $2 \le |Z_1| \le 4$ and so $1 \le d \le 2$. As in 5), this upper bound on d, together with Corollaries 3.1.2, 3.1.3, and [Lus82, Cor. (3.16)(ii)], implies that

$$|\chi(t_1)| \le 3/2,\ |\chi(t_2)| \le 6.$$

Next we count the total number of possibilities for (Z_1, Z_2); each of these possibilities gives rise to at most $2^{2d} \le 16$ possibilities for Λ. Clearly, (Z_1, Z_2) is uniquely determined by (α_1, β_1) and also by (α_2, β_2). Also, there are at most $a(a+1)$ possibilities for (α_1, β_1) with $0 \le f \le a-1$ or $r-2a = f-e$. So we may assume that $0 \le e \le a-1 < f \le r-a-1$ and $r-2a \ne f-e$. In this case,

$$Z_1 = \{0, f-e, a+f-e, r-a\},\ Z_2 = \{1, 2, \dots, f\} \setminus \{f-e\}.$$

Assume that $\{k_2, l_2\} = \{a+1, r-a-1\}$. Then, arguing as above, we may also assume that $\alpha_2 = (1^{e'}, a+1-e')$ and $\beta_2 = (1^{f'}, r-a-1-f')$, with $0 \le e' \le a < f' \le r-a-2$ and $r-2a-2 \ne f'-e'$. It follows that

$$Z_1 = \{0, f'-e', a+1+f'-e', r-a-1\},\ Z_2 = \{1, 2, \dots, f'\} \setminus \{f'-e'\},$$

whence $f' = f$, $e' = e$, $f = r-2a-1+e$. Since $0 \le e \le a-1$, we get at most a possibilities for (α_1, β_1).

Now we may assume that $\alpha_2 \vdash r$ and $\beta_2 = \emptyset$. As in 5), we see that α_2 is one of the partitions listed in Corollary 3.1.3 for $k = a' = a \pm 1$; and moreover, we may assume that α_2 is of type Ib or IIc. Assume for instance that $\alpha_2 = (1^y, a'+1, a'+x+1)$ is of type Ib1. Then $Z_1 = \{0, y+1, a'+1+y, r-a'\}$ and $Z_2 = \{1, 2, \dots, y\}$, forcing $f = y+1$, $e = 0$, and $y = r-a-a'-1$. Thus we get at most one choice for (α_1, β_1) in this case. Next assume that $\alpha_2 = (1^y, 2^j, a'-j+1, a'-j+x+1)$ is of type IIc. Then $Z_1 = \{0, y+1, a'+1+y, r-a'\}$ and $Z_2 = \{1, 2, \dots, y+j+1\} \setminus \{y+1\}$, forcing $f = y+j+1$, $e = j$, and $y = r-a-a'-1$. Since $1 \le j \le a$, this leads to at most a choices for (α_1, β_1). Finally, assume that $\alpha_2 = (1^x, 2^{a'}, y+2)$ is of type Ib2. Then $Z_1 = \{0, x+1, x+a'+1, r-a'\}$ and $Z_2 = \{1, 2, \dots, x+a'\} \setminus \{x+1\}$, forcing $f = x+a'$, $e = a'-1 = a-2$, $x = r-2a$, and $y = -2$, a contradiction. □

3.4. *Unipotent characters of B_r.* Now let $G = \mathrm{Spin}_{2r+1}$. By [MSW94, Th. 2.4], if $t_1, t_2 \in G(\mathbb{F}_q)$ are regular semisimple elements belonging to tori of type T_r^+ and T_r^- respectively, then every noncentral element of $G(\mathbb{F}_q)$ is a product of a conjugate of t_1 and a conjugate of t_2. For most values of r, this will be enough for the intended application, but depending on the word w and the value of r, we may not be able to guarantee that $w(G(\mathbb{F}_q))$ contains regular

semisimple elements of these two types. To deal with these cases, we have the following result:

PROPOSITION 3.4.1. *Fix $a \geq 1$, and let r be any integer greater than $2a+2$, and $\varepsilon \in \{\pm 1\}$ with $(\varepsilon,\varepsilon) \neq ((-1)^a,(-1)^{r-a})$. If t_1 and t_2 are regular semisimple elements of $\mathrm{Spin}_{2r+1}(\mathbb{F}_q)$ belonging to tori of type $T^{\varepsilon}_{a,r-a}$ and $T^{-\varepsilon}_{a+1,r-a-1}$ respectively, then the number of distinct irreducible characters of $\mathrm{Spin}_{2r+1}(\mathbb{F}_q)$ which vanish neither on t_1 nor on t_2 is bounded, independent of r, q, and the choices of t_i. Likewise, the absolute values of these characters on t_1 and t_2 are bounded independent of r, q, and the t_i.*

Proof. 1) By Proposition 2.4.1, the two tori are weakly orthogonal. We will proceed in parallel with the proof of Proposition 3.3.1 and use the same notation set up in part 1) of that proof. In particular, Λ is a symbol corresponding to a unipotent character χ with $\chi(t_1)\chi(t_2) \neq 0$ so that $\chi = \rho(\Lambda)$; the difference is that now Λ has odd defect. Again, the equivalence class of Λ contains a unique representative $\Lambda = (X,Y)$ such that $0 \notin X \cap Y$, and we will always choose Λ to satisfy this condition. Next, let Z_1 be the set of "singles" and $Z_2 = X \cap Y$, so that $X = Z_2 \cup (Z_1 \setminus N)$ and $Y = Z_2 \cup N$ for some $N \subseteq Z_1$. Since Λ has odd defect, $|Z_1| = 2d+1$ for some integer $d \geq 0$. Then the family $\mathcal{F}(\chi)$ consists of all irreducible characters $[\Lambda']$ of W_r labeled by symbols $\Lambda' = (X',Y')$ of defect 1 which contain the same entries (with the same multiplicities) as Λ does; cf. [Lus81, Cor. (5.9)]. Hence the condition $\chi(t_1)\chi(t_2) \neq 0$ implies that there are some $M_1, M_2 \subseteq Z_1$ such that $|M_1| = |M_2| = d$ and

$$[\Lambda_1](w_1) \neq 0,\ [\Lambda_2](w_2) \neq 0, \tag{3.4.1}$$

where $\Lambda_i := (Z_2 \cup (Z_1 \setminus M_i), Z_2 \cup M_i)$ for $i = 1,2$. We need to show that the number of such Λ is bounded by a function of a only and that $|\chi(t_1)|$, $|\chi(t_2)|$ are also bounded by a function of a only for all such $\chi = \rho(\Lambda)$.

Let the pair (α_i,β_i) of partitions $\alpha_i \vdash k_i$, $\beta_i \vdash l_i$, correspond to the symbol Λ_i for $i = 1,2$. Then condition (3.4.1) and formula (3.2.1) imply that the permutation $\pi_i \in \mathsf{S}_r$ preserves a partition of the set $\{1,2,\dots,r\}$ into the union of a k_i-set and an l_i-set. It follows that

$$\{k_1,l_1\} = \{r,0\} \text{ or } \{a,r-a\}$$

and

$$\{k_2,l_2\} = \{r,0\} \text{ or } \{a+1,r-a-1\}.$$

Also, to make the arguments symmetric for t_1 and t_2, we may replace $(a,a+1)$ by $(a,a-1)$ and assume π_2 has cycle type $(a',r-a')$ with $a' = a \pm 1$.

2) Here we consider the case where $\{k_1,l_1\} = \{k_2,l_2\} = \{r,0\}$. Interchanging α_i with β_i and considering symbols of defect -1 in addition to the ones of defect 1, we may assume that β_1,β_2 are empty partitions and $\alpha_1,\alpha_2 \vdash r$.

The nonvanishing condition (3.4.1) now implies that α_1 is one of the partitions listed in Corollary 3.1.3 for $k = a$, and that α_2 is one of the partitions listed in Corollary 3.1.3 for $k = a + 1$. In particular, $1 \le |Z_1| \le 5$, i.e., $0 \le d \le 2$. Since Z_1 has 3, respectively 10, subsets of cardinality d for $d = 1$, respectively for $d = 2$, Corollary 3.1.3 and [Lus81, Cor. (5.9)] imply that

$$|\chi(t_i)| \le 10.$$

Next we count the total number of possibilities for (Z_1, Z_2); each of these possibilities gives rise to at most $2^{2d+1} \le 32$ possibilities for Λ. Clearly, (Z_1, Z_2) is uniquely determined by α_1 and also by α_2. Observe that each of the types Iac and IIabde in Corollary 3.1.3 contains at most $(a+1)^2$ partitions α_i. So it remains to consider the cases where the type of α_1 and the type of α_2 belong to $\{\mathrm{Ib}, \mathrm{IIc}\}$. In each of the following cases, we will match up the shapes of Z_1 and Z_2 as they come from α_1 and from α_2 to derive a contradiction.

Assume for instance that $\alpha_1 = (1^y, a+1, a+x+1)$ is of type Ib1. Then either

$$Z_1 = \{0, a{+}1{+}y, r{-}a\} \text{ or } \{0, y{+}1, y{+}2, a{+}1{+}y, r{-}a\}, \text{ and } Z_2 = \{1, 2, \dots, y\},$$

or

$$a = 1,\ Z_1 = \{0, y+1, r-a\}, \text{ and } Z_2 = \{1, 2, \dots, y, y+2\}.$$

Now if $\alpha_2 = (1^{y'}, a'+1, a'+x'+1)$ is of type Ib1, then matching up the shapes of Z_1 and Z_2 we see that $y = y' = n - a - a' - 1$, and so either x or x' is negative; a contradiction. The same contradiction occurs if $\alpha_2 = (1^{y'}, 2^j, a'-j+1, a'-j+x'+1)$ is of type IIc. Similarly, the shapes of Z_1 and Z_2 for α_1 and α_2 cannot match if α_2 is of type Ib2.

Next assume that $\alpha_1 = (1^y, 2^j, a-j+1, a-j+x+1)$ is of type IIc. Then one of the following holds:

$$\begin{aligned}
&Z_1 = \{0, y+1, y+j+1, a+y+1, r-a\},\ Z_2 = \{1, 2, \dots, y+j\} \setminus \{y+1\},\\
&Z_1 = \{0, y+1, y+j+2, a+y+1, r-a\},\ Z_2 = \{1, 2, \dots, y+j+1\} \setminus \{y+1\},\\
&j = a-1,\ Z_1 = \{0, y+1, r-a\},\ Z_2 = \{1, 2, \dots, y+j+2\} \setminus \{y+1\}.
\end{aligned}$$

Suppose, in addition, that $\alpha_2 = (1^{y'}, 2^{j'}, a'-j'+1, a'-j'+x'+1)$ is also of type IIc. By symmetry, we may assume that $j \ge j'$. In the case $|Z_1| = 3$ we get $y = y'$, $j = j'$, and $a = a'$; a contradiction. If $|Z_1| = 5$, then $y = y' = r - a - a' - 1$ and so either x or x' is negative; a contradiction. On the other hand, let $\alpha_2 = (1^{x'}, 2^{a'}, y'+2)$ be of type Ib2. Then one can check that the case $|Z_1| = 3$ is impossible, and in the case $|Z_1| = 5$ we must have $y = x' = r - a - a' - 1$, which is also a contradiction.

Finally, consider the case that $\alpha_1 = (1^x, 2^a, y+2)$ and $\alpha_2 = (1^{x'}, 2^{a'}, y'+2)$ are both of type Ib2. Then one of the following holds:

$$Z_1 = \{0, x+1, a+x, a+x+1, r-a\},\ Z_2 = \{1, 2, \dots, x+a-1\} \setminus \{x+1\},$$
$$Z_1 = \{0, x+1, r-a\},\ Z_2 = \{1, 2, \dots, x+a+1\} \setminus \{x+1\},$$
$$a = 1,\ Z_1 = \{0, a+y+1, r-a\},\ Z_2 = \{1, 2, \dots, y\}.$$

Matching up the shapes of Z_1 and Z_2, we see that either $a = a'$ or $a = 0$ or $a' = 0$; a contradiction.

3) Now we may assume that $\{k_1, k_2\} = \{a, r-a\}$. Again by considering symbols of defect -1, we may assume furthermore that $\alpha_1 \vdash a$ and $\beta_1 \vdash r-a$. Clearly, π_1 preserves a unique partition of $\{1, 2, \dots, r\}$ into the union of an a-set and an $(r-a)$-set. Hence formula (3.2.1) yields that

$$|[\Lambda_1](w_1)| = |[\alpha_1]((a))| \cdot |[\beta_1]((r-a))|.$$

By Corollary 3.1.2 and the nonvanishing condition (3.4.1), both α_1 and β_1 must be hook partitions:

$$\alpha_1 = (1^e, a-e),\ \beta_1 = (1^f, r-a-f),$$

where $0 \le e \le a-1$, and $0 \le f \le r-a-1$. In particular, $1 \le |Z_1| \le 5$ and so $0 \le d \le 2$. As in 2), this upper bound on d, together with Corollaries 3.1.2, 3.1.3, and [Lus81, Cor. (5.9)], implies that

$$|\chi(t_1)| \le 5/2,\ |\chi(t_2)| \le 10.$$

Next we count the total number of possibilities for (Z_1, Z_2); each of these possibilities gives rise to at most $2^{2d+1} \le 32$ possibilities for Λ. Clearly, (Z_1, Z_2) is uniquely determined by (α_1, β_1) and also by (α_2, β_2). Also, there are at most $a(a+4)$ possibilities for (α_1, β_1) with $0 \le f \le a$ or $f = r-a-1$ or $r-2a \pm 1 = f-e$. So we may assume that $0 \le e < a < f < r-a-1$ and $r-2a \pm 1 \ne f-e$. In this case, one of the following holds:

(IVa): $Z_1 = \{0, f-e-1, f, a+f-e-1, r-a\}$, $Z_2 = \{1, 2, \dots, f-1\} \setminus \{f-e-1\}$;

(IVb): $Z_1 = \{0, f-e+1, f+1, a+f-e+1, r-a\}$, $Z_2 = \{1, 2, \dots, f\} \setminus \{f-e+1\}$;

(IVc): $e = 1$, $Z_1 = \{0, f, f+1, a+f, r-a\}$, $Z_2 = \{1, 2, \dots, f-1\}$;

(IVd): $e = a-1$, $Z_1 = \{0, f-a+2, r-a\}$, $Z_2 = \{1, 2, \dots, f\} \setminus \{f-a+2\}$.

Assume in addition that $\{k_2, l_2\} = \{a', r-a'\}$ with $a' = a \pm 1$. Then, arguing as above, we may also assume that $\alpha_2 = (1^{e'}, a'-e')$ and $\beta_2 = (1^{f'}, r-a'-f')$, with $0 \le e' < a' < f' < r-a'-1$ and $r-2a' \pm 1 \ne f'-e'$. Suppose the case (IVa) happens for (Z_1, Z_2). Then $|Z_1| = 5$, and by matching up the shapes of Z_1 and Z_2 as they come from (α_1, β_1) and from (α_2, β_2), we see that $f = r-a-a'+e+1$. Since $0 \le e \le a-1$, we get at most a possibilities for (α_1, β_1). Similarly, in the case (IVb) or (IVc), we get $f = r-a-a'+e-1$,

which lead to at most a possibilities for (α_1, β_1). In the case of (IVd), we must have $f = f'$, $a = a'$; a contradiction.

Now we may assume that $\alpha_2 \vdash r$ and $\beta_2 = \emptyset$. As in 2), we see that α_2 is one of the partitions listed in Corollary 3.1.3 for $k = a' = a \pm 1$; and moreover, we may assume that α_2 is of type Ib or IIc. Suppose the case (IVa) happens for (Z_1, Z_2). Then $|Z_1| = 5$, and by matching up the shapes of Z_1 and Z_2 as they come from (α_1, β_1) and from (α_2, β_2), we see that $f = r - a - a' + e + 1$. Since $0 \le e \le a - 1$, we get at most a possibilities for (α_1, β_1). Similarly, in the case (IVb) or (IVc), we get $f = r - a - a' + e - 1$, which lead to at most a possibilities for (α_1, β_1). One can show that the case of (IVd) cannot occur. □

4. **Character estimates for elements of large support**

4.1. *Classical groups and support.* A theorem of Gluck [Glu95] asserts that if G is a finite connected reductive group over $\mathbb{F}_q$ whose commutator subgroup is quasi-simple and simply connected, $g \in G$ is a noncentral element, and χ is a nontrivial irreducible character of G, then

$$\frac{|\chi(g)|}{\chi(1)} \le \gamma_q := \begin{cases} 19/20, & 2 \le q < 43, \\ 1/(\sqrt{q} - 1), & q \ge 43. \end{cases} \tag{4.1.1}$$

While this bound can probably be improved, it cannot be improved beyond $1/\sqrt{3}$ even in the large $|G(\mathbb{F}_q)|$ limit. This can be seen by considering the value of an irreducible *Weil character* of degree $(3^n \pm 1)/2$ at a transvection in $\mathrm{Sp}_{2n}(\mathbb{F}_3)$; cf. [TZ96].

For the intended application, we need a stronger upper bound, which can only be achieved by excluding certain special elements which are in a suitable sense nearly scalar. This leads us to the notion of *support*. We define the support of a matrix as follows:

Definition 4.1.1. The *support* $\mathrm{supp}\,(g)$ of an element $g \in \mathrm{GL}_n(\mathbb{F}) \subset \mathrm{GL}_n(\overline{\mathbb{F}})$ is the codimension of the largest eigenspace of g:

$$\mathrm{supp}\,(g) = \inf_{\lambda \in \overline{\mathbb{F}}} \mathrm{codim}\ \ker(g - \lambda).$$

The *support* of any element in a classical group $G(\mathbb{F})$ is the support of its image under the natural representation $\rho\colon G(\overline{\mathbb{F}}) \to \mathrm{GL}_n(\overline{\mathbb{F}})$.

See also [LS99, p. 509] for an equivalent definition and some properties. If $g \in \mathrm{GL}_n(\mathbb{F})$ with $\mathrm{supp}\,(g) < n/2$, there is a unique eigenvalue λ such that $\mathrm{codim}\ \ker(g - \lambda) = \mathrm{supp}\,(g)$. We call λ the *primary eigenvalue* of g.

Proposition 4.1.2. *If G is GL_n or a simply connected classical group with n-dimensional natural representation, and $g \in G(\mathbb{F}_q)$ has support less than*

$n/2$ with primary eigenvalue λ, then

$$\lambda \in \begin{cases} \mathbb{F}_q^\times & \text{if } G = \mathrm{SL}_n \text{ or } G = \mathrm{GL}_n, \\ \{x \in \mathbb{F}_{q^2} \mid x^{q+1} = 1\} & \text{if } G = \mathrm{SU}_n, \\ \{-1, 1\} & \text{if } n \text{ is even and } G = \mathrm{Sp}_n, \\ \{-1, 1\} & \text{if } n \text{ is odd and } G = \mathrm{Spin}_n, \\ \{-1, 1\} & \text{if } n \text{ is even and } G = \mathrm{Spin}_n^\pm. \end{cases}$$

Proof. As $n - \operatorname{supp}(g)$ is less than or equal to the dimension of the λ generalized eigenspace V_λ of $\rho(g)$, it suffices to prove that the above conditions hold whenever $\dim V_\lambda > n/2$.

For $\rho(g) \in \mathrm{GL}_n(\mathbb{F}_q)$, we have $\dim V_\lambda = \dim V_{\lambda^q}$, so $\lambda \in \mathbb{F}_q^\times$. For $\rho(g) \in \mathrm{SU}_n(\mathbb{F}_q)$, we have $\dim V_\lambda = \dim V_{\lambda^{-q}}$, so $\lambda^{q+1} = 1$. For $\rho(g) \in \mathrm{Sp}_n(\mathbb{F}_q)$, $\rho(g) \in \mathrm{Spin}_n(\mathbb{F}_q)$, $\rho(g) \in \mathrm{Spin}_n^+(\mathbb{F}_q)$, or $\rho(g) \in \mathrm{Spin}_n^-(\mathbb{F}_q)$, we have $\dim V_\lambda = \dim V_{\lambda^{-1}}$, so $\lambda^2 = 1$. □

4.2. *Branching rules and invariants.* Throughout this section, all representations are finite-dimensional complex representations; furthermore, $d(H)$ will denote the minimal degree of a nontrivial representation of the finite group H, and V^H the fixed point subspace of H on a representation space V.

First we record the following obvious observation:

LEMMA 4.2.1. *If $K < H$ is not contained in any proper normal subgroup of H, then*

$$d(H) \geq d(K).$$

LEMMA 4.2.2. *If $K < H$ is not contained in any proper normal subgroup and V is the representation space of an H-representation, then*

$$\frac{\dim V^K}{\dim V} \leq \frac{\dim V^H}{\dim V} + \frac{\sqrt{|K\backslash H/K| - 1}}{d(H)}.$$

Proof. It suffices to show that if $\dim W^H = 0$ for an H-module W, then

$$\frac{\dim W^K}{\dim W} \leq \frac{\sqrt{|K\backslash H/K| - 1}}{d(H)}.$$

It therefore suffices to prove

$$\dim W^K \leq \sqrt{|K\backslash H/K| - 1}$$

for nontrivial irreducible representations W of H with $W^K \neq 0$. By Frobenius' reciprocity, W embeds in $\mathrm{ind}_K^H(1_K)$ with multiplicity $\dim W^K$. Hence $(\dim W^K)^2 < |K\backslash H/K|$, since the latter is the dimension of the fixed point subspace of K on the representation space of $\mathrm{ind}_K^H(1_K)$. □

Let $G(\mathbb{F}_q)$ be a simply connected classical group and W the representation space of the natural representation ρ. (Thus W is a vector space over $\mathbb{F}_q$ except when G is unitary, when it is a vector space over $\mathbb{F}_{q^2}$.) Let W_1 and W_2 be complementary subspaces of W. In the unitary, orthogonal, and symplectic cases, we further assume that W_1 and W_2 are mutually orthogonal with respect to the Hermitian, symmetric, or symplectic form, respectively, which G preserves. The subgroup

$$G_{W_1,W_2}(\mathbb{F}_q) := \{g \in G(\mathbb{F}_q) \mid \rho(g)(W_1) = W_1, (\rho(g) - 1)(W_2) = 0\}$$

is again a simply connected classical group of the same type (but of smaller rank), of which W_1 is the natural representation space. By a *restriction map*, we mean an inclusion of simply connected classical groups which arises in this way.

PROPOSITION 4.2.3. *For all $\varepsilon > 0$, there exists $B = B(\varepsilon)$ such that if G_1 and G_2 are simply connected classical groups over $\mathbb{F}_q$ and $G_1(\mathbb{F}_q) \to G_2(\mathbb{F}_q)$ is a restriction map, V is the representation space of a nontrivial irreducible complex representation of $G_2(\mathbb{F}_q)$, and $|G_1(\mathbb{F}_q)| > B$, then*

$$\dim V^{G_1(\mathbb{F}_q)} \le \varepsilon \dim V.$$

In fact, if the dimension of the natural module of G_1 is $N \ge 8$, then

$$\dim V^{G_1(\mathbb{F}_q)} < q^{\frac{8}{3} - \frac{N}{2}} \dim V.$$

Proof. 1) Define $s := 2$ if G is of type C_r, or D_r and ${}^2D_r$ with even q, and $s := 1$ otherwise. We will find positive numbers $a_{n,q}$ for each positive integer n and each prime power q such that

$$\dim V^{G_{W_1,W_2}(\mathbb{F}_q)} \le a_{\dim W,q} \dim V$$

whenever $\dim W_2 = s$. Given that the dimension of the natural module of G_1 is N, this will imply that

$$\frac{\dim V^{G_1(\mathbb{F}_q)}}{\dim V} < b_{N,q,s} := \sum_{j=1}^{\infty} a_{N+js,q}.$$

Then the first statement follows from the facts that $\sum_{n=1}^{\infty} a_{n,q}$ converges for each q and the sum b_q of this series tends to zero as $q \to \infty$. The second statement follows from upper bounds for $b_{N,q,s}$ when $N \ge 8$.

We begin with the orthogonal case in odd characteristic, since it is the simplest. Here $s = 1$, $W_2 = \mathbb{F}_q w$ for some nonzero vector w, and w cannot be isotropic since $w^{\perp} = W_1$. In this case,

$$G_{W_1,W_2}(\mathbb{F}_q) = \mathrm{Stab}_{G(\mathbb{F}_q)} w. \tag{4.2.1}$$

The double cosets of $G(\mathbb{F}_q)$ with respect to $G_{W_1,W_2}(\mathbb{F}_q)$ are in one-to-one correspondence with $G_{W_1,W_2}(\mathbb{F}_q)$-orbits contained in the $G(\mathbb{F}_q)$-orbit $O_{G(\mathbb{F}_q)}(w)$

of w. Since $G(\mathbb{F}_q)$ acts transitively on all pairs of linearly independent vectors (w', w'') in W with specified values of $\langle w', w'\rangle$, $\langle w', w''\rangle$, and $\langle w'', w''\rangle$, two elements $w_1', w_2' \in O_{G(\mathbb{F}_q)}(w) \setminus \{\pm w\}$ lie in the same $G_{W_1,W_2}(\mathbb{F}_q)$-orbit if and only if $\langle w, w_1'\rangle = \langle w, w_2'\rangle$. We conclude that there are at most $q+2$ double cosets, so by Lemma 4.2.2,

$$\dim V^{G_{W_1,W_2}(\mathbb{F}_q)} \leq \frac{\sqrt{q+1}}{d(G(\mathbb{F}_q))} \dim V.$$

By the Landazuri-Seitz bounds [LS74],

$$\frac{\sqrt{q+1}}{d(G(\mathbb{F}_q))} = O(q^{\min(-1/2, 7/2-\dim W)}),$$

where the implied constant is absolute. Moreover, when $n = \dim W \geq 7$ we can take $a_{n,q} = q^{15/4-n}$.

2) Next we consider the case SU_n, so $s = 1$. We may assume $n \geq 3$ since G_1 is a classical group. Now $W_2 = \mathbb{F}_{q^2} w$, $w^\perp = W_1$, and (4.2.1) holds. Since $\mathrm{SU}_n(\mathbb{F}_q)$ acts transitively on all pairs of linearly independent vectors (w', w'') in W with specified values of the hermitian inner product $\langle w', w'\rangle$, $\langle w', w''\rangle$, and $\langle w'', w''\rangle$, two elements

$$w_1', w_2' \in O_{G(\mathbb{F}_q)}(w) \setminus \{cw \mid c^{q+1} = 1\}$$

lie in the same $G_{W_1,W_2}(\mathbb{F}_q)$-orbit if and only if $\langle w, w_1'\rangle = \langle w, w_2'\rangle$. We conclude that there are at most q^2+q+1 double cosets, so

$$\dim V^{G_{W_1,W_2}(\mathbb{F}_q)} \leq \frac{\sqrt{q^2+q}}{d(G(\mathbb{F}_q))} \dim V.$$

By [LS74],

$$\frac{\sqrt{q^2+q}}{d(G(\mathbb{F}_q))} = O(q^{2-n}).$$

Moreover, when $n \geq 5$ we can take $a_{n,q} = q^{3-n}$.

3) Next we consider the case SL_n, where again $n \geq 3$ and $s = 1$. Let w be a nonzero element of the 1-dimensional space W_2. Now $\mathrm{SL}_n(\mathbb{F}_q)$ acts transitively on all pairs of linearly independent vectors. In particular, the orbit of w under $\mathrm{SL}_n(\mathbb{F}_q)$ is $W \setminus \{0\}$. The $\mathrm{Stab}(w)$-orbits on $W \setminus \{0\}$ are the $q-1$ 1-element sets consisting of a nonzero element of W_2 and the set $W \setminus W_2$. Thus,

$$\frac{\dim V^{\mathrm{Stab}(w)}}{\dim V} \leq \frac{\sqrt{q-1}}{d(\mathrm{SL}_n(\mathbb{F}_q))}.$$

We can write

$$\mathrm{Stab}(w) \cong \mathrm{Hom}(W_1, W_2) \rtimes \mathrm{SL}(W_1).$$

As $\mathrm{SL}(W_1)$ acts transitively on the nonzero vectors of $\mathrm{Hom}(W_1, W_2)$,

$$|\mathrm{SL}(W_1) \backslash \mathrm{Stab}(w) / \mathrm{SL}(W_1)| = 2.$$

On the other hand, as the conjugates of $\mathrm{SL}(W_1)$ in $\mathrm{Stab}(w)$ generate $\mathrm{Stab}(w)$, the restriction of a nontrivial representation of $\mathrm{Stab}(w)$ to $\mathrm{SL}(W_1)$ must be nontrivial and must therefore have dimension at least $d(\mathrm{SL}(W_1))$. Thus,

$$\frac{\dim V^{\mathrm{SL}(W_1)}}{\dim V} \le \frac{\dim V^{\mathrm{Stab}(w)}}{\dim V} + \frac{1}{d(\mathrm{Stab}(w))} \le \frac{\sqrt{q-1}}{d(\mathrm{SL}_n(\mathbb{F}_q))} + \frac{1}{d(\mathrm{SL}(W_1))}.$$

By [LS74], this is $O(q^{2-n})$. In fact, when $n \ge 5$ we can take $a_{n,q} = q^{3-n}$.

4) Here we consider $\mathrm{Sp}_{2r}(\mathbb{F}_q)$ where $r \ge 2$, and so $s = 2$. Let w be a nonzero vector in W_2. The $\mathrm{Sp}_{2r}(\mathbb{F}_q)$-orbit of w is $W \setminus \{0\}$. As $\mathrm{Sp}_{2r}(\mathbb{F}_q)$ acts transitively on all pairs of linearly independent vectors with given pairing, $\mathrm{Stab}(w)$ acts on $W \setminus \{0\}$ with $2q-1$ orbits: $q-1$ singletons consisting of nonzero scalar multiples of w and q orbits consisting of vectors $w' \in W \setminus \mathbb{F}_q w$ with specified values of $\langle w, w' \rangle$. Thus,

$$\frac{\dim V^{\mathrm{Stab}(w)}}{\dim V} \le \frac{\sqrt{2q-2}}{d(\mathrm{Sp}_{2r}(\mathbb{F}_q))}.$$

Now, $\mathrm{Stab}(w) \cong H_{2r-1} \rtimes \mathrm{Sp}_{2r-2}(\mathbb{F}_q)$, where H_{2r-1} is a central extension of $\mathrm{Hom}(w^\perp/\mathbb{F}_q w, \mathbb{F}_q)$, by $\mathbb{F}_q$ (it is the Heisenberg group if q is odd, and abelian if $2|q$). As there is no nontrivial proper subgroup of $\mathbb{F}_q^{2r-2}$ invariant under the action of $\mathrm{Sp}_{2r-2}(\mathbb{F}_q)$, there is no nontrivial subgroup of H_{2r-1} invariant under this action except for the ones contained in $\mathbb{F}_q$. It follows that $\mathrm{Stab}(w)$ is generated by conjugates of $\mathrm{Sp}_{2r-2}(\mathbb{F}_q)$, so $d(\mathrm{Stab}(w)) \ge d(\mathrm{Sp}_{2r-2}(\mathbb{F}_q))$. The number of orbits of $\mathrm{Stab}(w)$ acting on H_{2r-1} is certainly no more than $2q$ since there are only two orbits of $\mathrm{Stab}(w)$ acting on $\mathbb{F}_q^{2r-2}$. Therefore,

$$\frac{\dim V^{\mathrm{Sp}_{2r-2}(\mathbb{F}_q)}}{\dim V} \le \frac{\dim V^{\mathrm{Stab}(w)}}{\dim V} + \frac{\sqrt{2q-1}}{d(\mathrm{Stab}(w))} \le \frac{\sqrt{2q-2}}{d(\mathrm{Sp}_{2r}(\mathbb{F}_q))} + \frac{\sqrt{2q-1}}{d(\mathrm{Sp}_{2r-2}(\mathbb{F}_q))}.$$

By [LS74], this is $O(q^{3/2-r})$. In fact, when $n = 2r \ge 10$, we can take $a_{n,q} = q^{8/3-n/2}$.

5) Finally we consider the orthogonal groups $G = \Omega^\varepsilon_{2r}(\mathbb{F}_q)$ in characteristic 2 and $n = 2r \ge 8$. Then $s = 2$, and the 2-space W_2 contains an anisotropic vector w, say $Q(w) = 1$ if Q denotes the corresponding quadratic form. Observe that stabilizer $S := \mathrm{Stab}(w)$ is isomorphic to $\mathrm{Sp}_{2r-2}(\mathbb{F}_q)$, and it acts on the $G(\mathbb{F}_q)$-orbit of w with $q+1$ orbits. Hence $\dim V^S / \dim V \le \sqrt{q}/d(G(\mathbb{F}_q))$ by Lemma 4.2.2. Next, for each $\varepsilon = \pm$, S contains a subgroup $K_\varepsilon \simeq \Omega^\varepsilon_{2r-2}(q)$, and one of these two subgroups is $L := G_{W_1,W_2}(\mathbb{F}_q)$. The permutation character $\mathrm{ind}_{K_+}^S(1_{K_+}) + \mathrm{ind}_{K_-}^S(1_{K_-})$ is decomposed into irreducible constituents in the proof of [GT04, Lemma 5.9], from which one can show that

$$|L\backslash S/L| = [\mathrm{ind}_L^S(1_L), \mathrm{ind}_L^S(1_L)] \le 2q+1.$$

Applying Lemma 4.2.2 and [LS74] again, we obtain that

$$\frac{\dim V^L}{\dim V} \le \frac{\sqrt{q}}{d(G(\mathbb{F}_q))} + \frac{\sqrt{2q}}{d(S)}$$

is $O(q^{7/2-2r})$. Moreover, when $n \ge 10$ we can take $a_{n,q} = q^{7.2-n}$.

6) Now assume that $N \ge 8$. If $s = 1$, then $a_{n,q} \le q^{15/4-n}$ for $n \ge 7$, and so

$$b_{N,q,s} \le \sum_{n=N+1}^{\infty} q^{15/4-n} = \frac{q^{15/4-N}}{q-1} \le q^{15/4-N}.$$

Next assume that $s = 2$. If G is of type $C_{N/2}$, then $a_{n,q} \le q^{8/3-n/2}$ for $n \ge 10$, and so

$$b_{N,q,s} \le \sum_{r=N/2+1}^{\infty} q^{8/3-r} = \frac{q^{8/3-N/2}}{q-1} \le q^{8/3-N/2}.$$

If G is of type $D_{N/2}$, then $a_{n,q} \le q^{7.2-n}$ for $n \ge 10$, whence

$$b_{N,q,s} \le \sum_{r=N/2+1}^{\infty} q^{7.2-2r} = \frac{q^{7.2-N}}{q^2-1} \le q^{5.7-N},$$

and so we are done. □

4.3. *Upper bounds for* $|\chi(g)|/\chi(1)$. In this section we prove the basic upper bound for $|\chi(g)|/\chi(1)$ for elements g of sufficiently large support in classical groups over finite fields.

The following lemma is useful, in combination with [LS74], for proving that $|\chi(g)|/\chi(1)$ is small when g is not too far from being regular:

LEMMA 4.3.1. *For every finite group H, every nontrivial irreducible character χ of H, and every $h \in H$,*

$$|\chi(h)| \le \sqrt{|C_H(h)|}.$$

Proof. This follows from the orthogonality relation $\sum_{\rho \in \mathrm{Irr}(H)} |\rho(h)|^2 = |C_H(h)|$. □

Every irreducible representation on a product of finite groups factors into an external tensor product of irreducible representations on the individual factors. This is useful for proving upper bounds on $|\chi(g)|/\chi(1)$ for product groups and, more generally, for elements which belong to subgroups which decompose as products. The following lemma allows us to extend this observation to the slightly more general setting in which we wish to use it:

LEMMA 4.3.2. *Let $G = \langle K, g \rangle$ be a finite group with a normal subgroup $K = K_1 * K_2 * \cdots * K_m$, a central product of subgroups $K_1, \ldots, K_m$ with $g \in \cap_{i=1}^m N_G(K_i)$. For each i, assume that there is a finite extension $H_i =$*

$\langle K_i, g_i\rangle \triangleright K_i$, where g and g_i induce the same action on K_i. Furthermore, for a subset $J \subseteq \{1, 2, \dots, m\}$ and any $i \in J$ assume that there is $\alpha_i > 0$ such that

$$|\rho(g_i)| \leq \alpha_i \rho(1)$$

for any $\rho \in \mathrm{Irr}(H_i)$ which is irreducible but nontrivial over K_i. Then for every character χ of G, such that $\chi|_{K_i}$ has no trivial factors for each $i \in J$, we have

$$|\chi(g)| \leq \left(\prod_{i\in J} \alpha_i\right) \chi(1).$$

Proof. It suffices to prove the lemma for χ irreducible on G. Let Φ be a G-representation affording the character χ. If $\Phi|_K$ is not irreducible, then g permutes the K-irreducible constituents of $\Phi|_K$ transitively and so $\chi(g) = 0$. Hence we may assume that $\Phi|_K$ is irreducible. Then $\chi|_K := \rho_1 \boxtimes \cdots \boxtimes \rho_m$, where $\rho_i \in \mathrm{Irr}(K_i) \setminus \{1_{K_i}\}$. Observe that $\rho_i = (\rho_i(1)/\chi(1))\chi|_{K_i}$ is g-invariant. But g and g_i induce the same action on K_i, hence ρ_i is g_i-invariant. Write $\Phi|_K := \Phi_1 \boxtimes \cdots \boxtimes \Phi_m$, where the K_i-representation Φ_i affords the character ρ_i. As mentioned above, Φ_i is g_i-invariant, hence it extends to an H_i-representation Ψ_i, and $|\mathrm{Tr}\Psi_i(g_i)| \leq \alpha_i\rho_i(1)$ by our assumption (where we define $\alpha_i = 1$ for $i \notin J$). Now we set

$$\Psi(g) = \Psi_1(g_1) \otimes \cdots \otimes \Psi_m(g_m).$$

Then for any $x_i \in K_i$,

$$\begin{aligned}\Psi(g)\,(\otimes_{i=1}^m \Phi_i(x_i))\,\Psi(g)^{-1} &= \otimes_{i=1}^m \Psi_i(g_i)\Phi_i(x_i)\Psi_i(g_i)^{-1} = \otimes_{i=1}^m \Phi_i(g_i x_i g_i^{-1})\\ &= \otimes_{i=1}^m \Phi_i(g x_i g^{-1}) = \Phi(g x_1 \dots x_m g^{-1}) = \Phi(g)\,(\otimes_{i=1}^m \Phi_i(x_i))\,\Phi(g)^{-1}.\end{aligned}$$

Since $\Phi|_K$ is irreducible, by Schur's lemma $\Phi(g) = \lambda\Psi(g)$ for some $\lambda \in \mathbb{C}^\times$. Next, the finiteness of G and H_i implies that there is some integer $N > 0$ such that all the matrices $\Phi(g)^N$ and $\Psi_i(g_i)^N$ are identity matrices. It follows that λ is an N^{th}-root of unity, and so

$$|\chi(g)| = |\mathrm{Tr}\Phi(g)| = |\mathrm{Tr}\Psi(g)| = \prod_{i=1}^m |\mathrm{Tr}\Psi_i(g_i)| \leq \prod_{i=1}^m (\alpha_i\rho_i(1)) = \left(\prod_{i\in J} \alpha_i\right)\chi(1).$$

□

In the next statement, by the classical group $I(W)$ over $\mathbb{F}_q$ we mean one of the following groups: $\mathrm{GL}(W) = \mathrm{GL}_n(q)$ with $W = \mathbb{F}_q^n$ and $n \geq 2$, $\mathrm{GU}(W) = \mathrm{GU}_n(q)$ with $W = \mathbb{F}_{q^2}^n$ and $n \geq 3$, $\mathrm{Sp}(W) = \mathrm{Sp}_{2n}(q)$ with $W = \mathbb{F}_q^{2n}$ and $n \geq 2$, and $\mathrm{GO}(W) = \mathrm{GO}_n^{\pm}(q)$ with $W = \mathbb{F}_q^n$ and $n \geq 7$. Also we let $L(W)$ denote the corresponding finite group of simply connected type; for instance $L(W) = \mathrm{Spin}(W)$ if $I(W) = \mathrm{GO}(W)$. We will assume that it has (untwisted) semisimple rank > 1, i.e., we ignore GL_2.

PROPOSITION 4.3.3. *For all $\varepsilon > 0$, there exists $B = B(\varepsilon)$ such that for every classical group $G = I(W)$ over a finite field $\mathbb{F}_q$, of untwisted semisimple rank > 1, not a symplectic group in odd characteristic nor $\mathrm{Sp}_4(q)$ with $2|q$, and every $g \in G$, if $|G| > B$, then one of the following holds for $L = L(W)$:*

(i) $|C_G(g)| < \varepsilon d(L)^2$.

(ii) *W admits a nontrivial g-stable direct sum decomposition $W = \oplus_{i=1}^m W_i$, where the subspaces W_i are mutually orthogonal with respect to the nondegenerate G-invariant bilinear or Hermitian form on W, if any. Moreover, for each i, $g|_{W_i} \in \Omega(W_i)$ if $G = \mathrm{GO}_n(q)$ with $2|q$ and $g \in \Omega(W)$, and $g|_{W_i} \in \mathrm{SO}(W_i)$ if $G = \mathrm{GO}_n(q)$ with q odd and $g \in \mathrm{SO}(W)$.*

Moreover, either (ii) *holds, or*

$$|\chi(g)/\chi(1)| < q^{4-n/2}$$

for every $\chi \in \mathrm{Irr}(G)$ which is nontrivial over L.

Proof. 1) We will assume that W does not admit any nontrivial g-stable decomposition $W = \oplus_{i=1}^m W_i$ satisfying all the conditions set in (ii) (and say for short that $W|_{\langle g\rangle}$ is indecomposable in this case). Let $g = su$ be the Jordan decomposition of g.

First consider the case $G = \mathrm{GL}_n$. If $s = \lambda \cdot 1_W$ is scalar, then the indecomposability of $W|_{\langle g\rangle}$ implies that the Jordan canonical form of g acting on W is just λJ_n, where J_n denotes the Jordan block of size n and with eigenvalue 1, i.e., u is regular unipotent. In this case $|C_G(g)| = q^{n-1}(q-1)$. Next assume that s is not scalar. The indecomposability of $W|_{\langle g\rangle}$ now implies that $C_G(s) = \mathrm{GL}_a(q^b)$ with $ab = n$, and moreover, u is a regular unipotent element in $\mathrm{GL}_a(q^b)$ (every Jordan block J_k of $u \in \mathrm{GL}_a(q^b)$ gives rise to a g-invariant kb-dimensional subspace in W). It follows that $|C_G(g)| = |C_{GL_a(q^b)}(u)| = q^{b(a-1)}(q^b - 1)$. Thus $|C_G(g)| < q^n$ in either case. Since $d(L) > q^{n-1}$ by [LS74] and $n \geq 3$, we see that (i) holds when $|G| > B$ for a suitable B depending on ε. Note that when applying [LS74] we can ignore all the small exceptions for G by taking B large enough. Moreover, if $n \geq 5$, then Lemma 4.3.1 implies that

$$|\chi(g)/\chi(1)| < q^{n/2-(n-1)} = q^{1-n/2}.$$

Next assume $G = \mathrm{GU}_n$. Then the indecomposability of $W|_{\langle g\rangle}$ implies by [LOST10, Lemma 6.7] that $|C_G(g)| \leq q^{n-1}(q+1)$, and (i) holds as $d(L) \geq (q^n - q)/(q+1)$ by [LS74]. Assuming $n \geq 5$, we obtain

$$|\chi(g)/\chi(1)| \leq \frac{q^{(n-1)/2}\sqrt{q+1}}{(q^n - q)/(q+1)} < q^{2-n/2}.$$

2) Here we assume that $2|q$, and either $G = \mathrm{Sp}_{2r}(q)$ with $n = 2r \geq 6$, or $\mathrm{GO}^{\pm}_{2r}(q)$ with $n = 2r \geq 4$. First we consider the case $s \neq 1$. Then W admits a g-stable decomposition $W = \oplus_{i=0}^m W_i$ into mutually orthogonal subspaces,

where $s_{W_0} = 1_{W_0}$ (and W_0 can possibly be zero), $m > 0$, and $C_{\mathrm{GO}(W_i)}(s) = \mathrm{GL}^{\varepsilon}_{a_i}(q^{b_i})$ with $\dim W_i = 2a_ib_i$ for $1 \le i \le m$, and $\mathrm{GL}^{\varepsilon}$ stands for GL if $\varepsilon = +$ and for GU if $\varepsilon = -$. If, in addition, $G = \mathrm{GO}$, then observe that $g|_{W_i} \in \mathrm{GL}^{\pm}_{a_i}(q^{b_i}) < \Omega(W_i)$ for $i > 0$. So if $m \ge 2$, or if $m = 1$ but $W_0 \ne 0$, then the decomposition $W = (\oplus_{i=0}^{m-1} W_i) \oplus W_m$ satisfies the conditions set in (ii). Hence $m = 1$ and $W_0 = 0$; in particular, $a_1b_1 = r$. Next, every Jordan block J_k of the unipotent element $u \in GL^{\varepsilon}_{a_1}(q^{b_1})$ gives rise to a g-invariant nondegenerate subspace U of dimension $2kb_1$ in W (and again $g|_U \in \Omega(\mathbb{F}^{2k}_{q^{b_1}}) \le \Omega(U)$ if $G = \mathrm{GO}$). So we conclude that $u \in GL^{\varepsilon}_{a_1}(q^{b_1})$ is a regular unipotent element, whence

$$|C_G(g)| = |C_{GL^{\varepsilon}_{a_1}(q^{b_1})}(u)| \le q^{b_1(a_1-1)}(q^{b_1}+1) < 2q^r.$$

Since $d(L) > q^{2r-1}/4$ for symplectic groups and $d(L) > q^{2r-3}/2$ for orthogonal groups by [LS74], (i) holds for g.

So we may now assume that $s = 1$, i.e., $g = u$ is unipotent. According to [LS], $W|_{\langle g\rangle}$ is the orthogonal sum of nondegenerate subspaces W_j, where g acts on each W_j as either J_{2k} (which belongs to $\mathrm{GO}(W_j) \setminus \Omega(W_j)$ in the case $G = \mathrm{GO}$), or $2J_k$ (which belongs to $\Omega(W_j)$ if $G = \mathrm{GO}$).

Assume, in addition, that W cannot be written as a nontrivial orthogonal sum of g-invariant nondegenerate subspaces. Then g must act on W as J_{2r} or $2J_r$. The calculations in [LOST10, §§4, 5] then show that $|C_G(g)| \le 2q^{2r}(q^2-1)$ for Sp and $|C_G(g)| \le 2q^{2r-2}(q^2-1)$ for GO. Since $r \ge 3$ for Sp and $r \ge 4$ for GO, we see that (i) holds for g.

Now we assume that $G = \mathrm{GO}(W)$ and $g \in \Omega(W)$. Then the absence of decompositions desired in (ii) implies that g acts on W as $J_{2a} + J_{2r-2a}$, with $1 \le a \le r-1$. Again as in [LOST10, §5.2], we can check that $|C_G(g)| \le 2q^{2r}$ and so (i) holds for g.

Assuming $r \ge 5$ and (ii) does not hold, we see that

$$|\chi(g)/\chi(1)| \le \frac{q^r\sqrt{2(q^2-1)}}{(q^r-1)(q^r-q)/2(q+1)} < q^{4-r}$$

in the case of Sp, and

$$|\chi(g)/\chi(1)| \le \frac{q^r\sqrt{2}}{(q^{r-1}+1)(q^{r-2}-1)} < q^{4-r}$$

in the case of GO.

3) Finally we consider the case where $G = \mathrm{GO}^{\pm}_n(q)$, $n \ge 7$, and q is odd. Assume, in addition, that $s^2 \ne 1$. In this case, as in 2), notice that W admits a g-stable decomposition $W = \oplus_{i=0}^{m} W_i$ of mutually orthogonal subspaces, where $(s_{W_0})^2 = 1_{W_0}$ (and W_0 can possibly be zero), $m > 0$, and $C_{\mathrm{GO}(W_i)}(s) = \mathrm{GL}^{\pm}_{a_i}(q^{b_i}) < \mathrm{SO}(W_i)$ with $\dim W_i = 2a_ib_i$ for $1 \le i \le m$. In particular, each $g|_{W_i} \in \mathrm{SO}(W_i)$ for $i > 0$. So if $m \ge 2$, or if $m = 1$ but $W_0 \ne 0$, then the

decomposition $W = (\oplus_{i=0}^{m-1} W_i) \oplus W_m$ satisfies the conditions set in (ii). Hence $m = 1$ and $W_0 = 0$; in particular, $a_1 b_1 = n/2$. Next, every Jordan block J_k of the unipotent element $u \in GL_{a_1}^{\varepsilon}(q^{b_1})$ gives rise to a g-invariant nondegenerate subspace U of dimension $2kb_1$ with $g|_U \in \mathrm{SO}(\mathbb{F}_{q^{b_1}}^{2k}) \leq \mathrm{SO}(U)$. So we conclude that $u \in GL_{a_1}^{\varepsilon}(q^{b_1})$ is a regular unipotent element, whence

$$|C_G(g)| \leq q^{b_1(a_1-1)}(q^{b_1}+1) < 2q^{n/2}.$$

Since $d(L) > q^{n-3}/2$ by [LS74], (i) holds for g.

So we may assume that $s^2 = 1$. Then $W = W_+ \oplus W_-$ is the orthogonal sum of the 1- and (-1)-eigenspaces of s. Next, $W_\pm|_{\langle g \rangle}$ is the orthogonal sum of nondegenerate subspaces W_j, where g acts on W_j as either $J_{2k+1} \in \mathrm{SO}(W_j)$, or $2J_{2k} \in \mathrm{SO}(W_j)$. Assume in addition that W cannot be written as a nontrivial orthogonal sum of g-invariant nondegenerate subspaces. Then exactly one of W_+, W_- is nonzero, $\pm g = u$ is unipotent and acts on W as J_n or $2J_{n/2}$. The calculations in [LOST10, §5] then show that $|C_G(g)| < 2q^n$, i.e., (i) holds for g as $n \geq 7$.

Next we consider the case $g \in \mathrm{SO}(W)$. Then the absence of decompositions desired in (ii) implies that $W = W_-$ and u acts on W as $J_{2a+1} + J_{n-2a-1}$, with $0 \leq a \leq n/2 - 1$. As in [LOST10, §5.2], we can now check that $|C_G(g)| < 2q^n$ and so (i) again holds.

Assume now that $n \geq 7$ and (ii) does not hold. Then $|C_G(g)| < 2q^n$ and $d(L) > (8/9)q^{n-3}$, whence $|\chi(g)/\chi(1)| < q^{(7-n)/2}$ by Lemma 4.3.1. □

Since the symplectic groups in odd characteristic are exceptions to Proposition 4.3.3, we deal with them separately:

LEMMA 4.3.4. *For all $\varepsilon > 0$ there exists $B = B(\varepsilon)$ such that for $G = \mathrm{Sp}_{2r}(q)$ with odd q, or with $r = 2$ and $2|q$, if $|G| > B$, $g \in G$ (noncentral if $G = \mathrm{Sp}_2(q)$), then one of the following holds*:

(i) *The natural G-module W admits a direct sum decomposition $W = W_1 \oplus W_2$ into nonzero g-stable mutually orthogonal subspaces.*
(ii) *$|\chi(g)/\chi(1)| < \varepsilon$ if $1_G \neq \chi \in \mathrm{Irr}(G)$.*

Moreover, if q is odd, then either (i) *holds, or*

$$|\chi(g)/\chi(1)| < q^{1-r/2}.$$

Proof. We follow part 2) of the proof of Proposition 4.3.3 and assume that (i) does not hold for g. Write $g = su$ and consider the case where $s \neq \pm 1$. Then the indecomposability of $W|_{\langle g \rangle}$ implies that $C_G(s)$ is of type $\mathrm{GL}_a^{\pm}(q^b)$ with $ab = r$, and moreover, u is a regular unipotent element in $\mathrm{GL}_a^{\varepsilon}(q^b)$. It follows that $|C_G(g)| < 2q^n < \varepsilon^2 d(G)^2$ if $|G| > B$ for some $B = B(\varepsilon)$, since $d(G) = (q^r - 1)/2$ [LS74]. Hence we conclude that $\pm g$ is unipotent.

If $r = 2$ and $2|q$, then $|\chi(g)| \le q^2 + q + 1$ and $\chi(1) \ge q(q-1)^2/2$ for any nonprincipal $\chi \in \mathrm{Irr}(G)$ (cf. [Eno72]), whence (ii) holds.

Consider the case q is odd. Then the indecomposability of $W|_{\langle g\rangle}$ implies that the Jordan canonical form of $\pm g$ acting on W is J_{2r}, or $2J_r$ (and n is odd). The calculations in [LOST10, §4.2] then show that $|C_G(g)| < 2q^r$ in the former case and $|C_G(g)| \le q^{2r-1}(q^2-1)$ in the latter case. Thus $|C_G(g)| < \varepsilon^2 d(G)^2$, unless $\pm g$ acts as $2J_r$ on W.

Now we show that (ii) holds for this exception g. Note that $r > 1$ in this case, as otherwise $g \in Z(G)$. By [TZ96], any nonprincipal $\chi \in \mathrm{Irr}(G)$ is either one of the four *Weil characters* $\xi_{1,2}$ and $\eta_{1,2}$ (of degree $(q^r+1)/2$, respectively $(q^r-1)/2$), or it has degree $\chi(1) \ge q^{r-1}(q^{r-1}-1)(q-1)/2$. In the latter case, Lemma 4.3.1 implies

$$|\chi(g)| \le \sqrt{q^{2r-1}(q^2-1)} < \varepsilon\chi(1)$$

if $|G| > B$. Consider the former case: $\chi \in \{\xi_{1,2}, \eta_{1,2}\}$, and let z be the central involution of G. Without loss we may assume that g acts as $2J_r$ on W; in particular, $|C_W(g)| = q^2$ and $|C_W(zg)| = 1$. By [GT04, Lemma 2.4],

$$|\xi_i(g) + \eta_i(g)| \le q,\ |\xi_i(g) - \eta_i(g)| = |\xi_i(zg) + \eta_i(zg)| \le 1.$$

It follows that $|\chi(g)| \le \sqrt{(q^2+1)/2} < \varepsilon\chi(1)$ when $|G| > B$.

Finally, we assume that $r \ge 3$, q is odd, and (i) does not hold. Then we have shown above that $|C_G(g)| \le q^{2r-1}(q^2-1)$. In particular, if $\chi(1) \ge q^{r-1}(q^{r-1}-1)(q-1)/2$, then Lemma 4.3.1 yields $|\chi(g)/\chi(1)| < q^{5/2-r} \le q^{1-r/2}$. Otherwise χ must be one of the four Weil characters of G. The above arguments then show that $|\chi(g)| \le \max\{\sqrt{2q^r}, \sqrt{(q^2+1)/2}\}$. Since $\chi(1) \ge (q^r-1)/2$, we obtain that $|\chi(g)/\chi(1)| < q^{1-r/2}$. □

Proposition 4.3.3 and Lemma 4.3.4 immediately imply:

COROLLARY 4.3.5. *Let $G = I(W)$ be a finite classical group over a finite field $\mathbb{F}_q$ with $n = \dim(W) \ge 12$. Then for every $g \in G$, one of the following holds*:

(i) *W admits a g-stable direct sum decomposition $W = \oplus_{i=1}^m W_i$ satisfying the conditions in Proposition* 4.3.3(ii).
(ii) *$|\chi(g)/\chi(1)| < q^{1-n/4}$ for every $\chi \in \mathrm{Irr}(G)$ which is nontrivial over $L(W)$.*

We now state the main result of Section 4. Recall that the constant γ_q has been defined in (4.1.1).

THEOREM 4.3.6. *For all $\varepsilon > 0$, there exists $N = N(\varepsilon)$ such that if G is a simple simply connected classical group, $h \in G(\mathbb{F}_q)$ is an element of support*

$\geq N$, and χ is a nontrivial irreducible character of $G(\mathbb{F}_q)$, then

$$\left|\frac{\chi(h)}{\chi(1)}\right| \leq \varepsilon. \tag{4.3.1}$$

More precisely,

$$\left|\frac{\chi(h)}{\chi(1)}\right| < \begin{cases} (\gamma_q)^{\sqrt{N/7}} & \text{if } N \geq 567, \\ (\gamma_q)^{\sqrt{N}/6} & \text{if } N \geq 144, \\ q^{-\sqrt{N}/1.15} & \text{if } N \geq 2225 \text{ and } q \geq 109, \\ q^{-\sqrt{N}/481} & \text{for all } N, q. \end{cases} \tag{4.3.2}$$

Proof. 1) By [Glu93], (4.3.1) holds if q is sufficiently large. We therefore assume throughout the proof of (4.3.1) that $q < C_\varepsilon$. Also, by taking N large enough, we may ignore all classical groups of small rank.

Let V be a representation affording the character χ, and let W be the natural representation of $G(\mathbb{F}_q)$ as usual. Suppose that

$$\begin{gathered} \text{there is an } h\text{-invariant decomposition } W = W_1 \oplus \cdots \oplus W_m \\ \text{that satisfies the conditions described in Proposition 4.3.3(ii).} \end{gathered} \tag{4.3.3}$$

Let G' denote the component-wise stabilizer in G of this decomposition, and set

$$G_i := G_{W_i, W_1 \oplus \cdots \oplus \hat{W}_i \oplus \cdots \oplus W_m},\ K_i := G_i(\mathbb{F}_q),\ K := K_1 * \cdots * K_m,$$

so G_i is the subgroup of G' that acts trivially on every W_j with $j \neq i$. Notice that G_i is a simply connected group of the same type as of G and with natural module W_i.

Assume for the moment that G is not a spin group in odd characteristic. Then the action of $G(\mathbb{F}_q)$ on W is faithful and K is the direct product of $K_1, \ldots, K_m$. In addition, set $G^i := G'/G'_{W_1 \oplus \cdots \oplus \hat{W}_i \oplus \cdots \oplus W_m, W_i}$. Then we can identify K_i with $\mathrm{im}(G_i(\mathbb{F}_q) \to G^i(\mathbb{F}_q))$. Let h_i denote the image of h in $G^i(\mathbb{F}_q)$, and let H_i be the subgroup of $G^i(\mathbb{F}_q)$ generated by K_i and h_i. Now, if $G(\mathbb{F}_q) = \mathrm{SL}(W)$, respectively, $\mathrm{SU}(W)$, or $\mathrm{Sp}(W)$, then $G^i(\mathbb{F}_q) = \mathrm{GL}(W_i)$, $\mathrm{GU}(W_i)$, or $\mathrm{Sp}(W_i)$, respectively. If $G(\mathbb{F}_q) = \Omega(W)$ with $2|q$, then $h_i \in \Omega(W_i)$ according to (4.3.3), whence $H_i = \Omega(W_i)$. Thus in any of these cases, the actions of h and h_i on K_i are the same; moreover, H_i is contained in a finite connected reductive group over $\mathbb{F}_q$ whose commutator subgroup is the quasi-simple simply connected group K_i (if $\dim(W_i)$ is not too small, say at least 5), and H_i is *admissible* in the sense of [Glu95].

Now assume that $G(\mathbb{F}_q) = \mathrm{Spin}(W)$ and q is odd. Then the action of $G(\mathbb{F}_q)$ on W may not be faithful, but K is still a central product of $K_1, \ldots, K_m$ and $K_i = \mathrm{Spin}(W_i)$. Recall (see [TZ05, §6] for instance) that the nondegenerate quadratic space W gives rise to the *special Clifford group* $\Gamma^+(W)$ with

$[\Gamma^+(W),\Gamma^+(W)] = \mathrm{Spin}(W)$ (if $\dim W \geq 5$), $Z(\Gamma^+(W)) = \mathbb{F}_q^\times e$, and the following two sequences are exact:

$$1 \longrightarrow \mathbb{F}_q^\times e \longrightarrow \Gamma^+(W) \longrightarrow SO(W) \longrightarrow 1,$$

$$1 \longrightarrow \langle -e\rangle \longrightarrow \mathrm{Spin}(W) \longrightarrow \Omega(W) \longrightarrow 1.$$

Furthermore, by (4.3.3) we have $h|_{W_i} \in \mathrm{SO}(W_i)$. Now we define $G^i(\mathbb{F}_q)$ to be $\Gamma^+(W_i)$. Also, we choose some inverse image $h_i \in G^i(\mathbb{F}_q)$ of $h|_{W_i}$ and let H_i be the subgroup of $G^i(\mathbb{F}_q)$ generated by K_i and h_i. Then again $G^i(\mathbb{F}_q)$ is a finite connected reductive group whose commutator subgroup is the quasi-simple simply connected group K_i, if $\dim W_i \geq 5$, and H_i is admissible. Also, Lemmas 6.1 and 6.2(i) of [TZ05] (notice that the condition $2|k$ formulated in [TZ05, Lemma 6.2] is not needed for part (i) of it) imply that the actions of h and h_i on K_i are the same.

We have shown that the group $\langle K, h\rangle$ satisfies all of the hypotheses in Lemma 4.3.2, and moreover, if $\dim W_i \geq 5$, then Gluck's bound (4.1.1) of [Glu95] is applicable to the group H_i.

2) Next let $\alpha > 0$ be any constant such that $\alpha\sqrt{N} \geq 2$. We will describe two particularly favorable situations for the decomposition (4.3.3), which would guarantee that

$$|\chi(h)/\chi(1)| < (\gamma_q)^{\alpha\sqrt{N}} \tag{4.3.4}$$

whenever $\mathrm{supp}\,(h) \geq N$.

2a) Set

$$N_1 := \lceil 2\alpha\sqrt{N} + 8\rceil; \tag{4.3.5}$$

in particular, $N_1 < 2\alpha\sqrt{N} + 9$. Assume first that for some j, $M := \dim W_j \geq N_1$ and that W_j does not admit any h_j-invariant decomposition satisfying the conditions set in Proposition 4.3.3(ii). Since $M \geq 12$, we can apply Proposition 4.2.3 and Corollary 4.3.5 to K_j and the element h_j. Furthermore, since $\gamma_q > q^{-1/2}$, we see that

$$q^{8/3-M/2} \leq q^{1-M/4} \leq q^{1-N_1/4} < (1/q)^{1+\alpha\sqrt{N}/2} \leq (1/2)\cdot(\gamma_q)^{\alpha\sqrt{N}}.$$

It follows that

$$\begin{cases} \dim V^{K_j}/\dim V < (1/2)\cdot(\gamma_q)^{\alpha\sqrt{N}}, \\ \quad |\varphi(h_j)/\varphi(1)| < (1/2)\cdot(\gamma_q)^{\alpha\sqrt{N}} \end{cases} \tag{4.3.6}$$

for any H_j-character φ whose restriction to K_j is irreducible and nontrivial. Now, if ρ is any irreducible constituent of the restriction of χ to $\langle K, h\rangle$ which does not have any trivial K_j-factor, then (4.3.6) and Lemma 4.3.2 yield that $|\rho(h)/\rho(1)| < (1/2)\cdot(\gamma_q)^{\alpha\sqrt{N}}$. Hence the bound (4.3.4) holds for h. We call this Case A.

2b) Alternatively, suppose that the number m of summands in the decomposition (4.3.3) equals a fixed

$$m_0 := \lceil 1 + \alpha\sqrt{N} \rceil. \tag{4.3.7}$$

We assume further that each $\dim W_i$ is large enough: $\dim W_i \geq N_2$ for some $N_2 \geq 8$ chosen so that Proposition 4.2.3 implies

$$\dim U^{K_i} < \frac{(\gamma_q)^{\alpha\sqrt{N}}(1-\gamma_q)\dim U}{m_0}$$

for all nontrivial irreducible complex representation spaces U of $G(\mathbb{F}_q)$; in particular for V. This can be achieved by choosing

$$N_2 = \begin{cases} \lceil 1.9\alpha\sqrt{N} + 16/3 \rceil, & \text{if } \alpha\sqrt{N} \geq 9, \\ \lceil 6.52\alpha\sqrt{N} + 16/3 \rceil, & \text{if } 9 > \alpha\sqrt{N} \geq 2. \end{cases} \tag{4.3.8}$$

Indeed, by Proposition 4.2.3 we have

$$\frac{\dim U^{K_i}}{\dim U} < q^{8/3 - N_2/2}.$$

Assume that $q \geq 43$. Then $1/7 \geq \gamma_q > 1/\sqrt{q}$; hence when $\alpha\sqrt{N} \geq 2$, we have

$$\frac{2+\alpha\sqrt{N}}{1-\gamma_q} \leq (7/6)(2+\alpha\sqrt{N}) < 7^{\alpha\sqrt{N}/2} \leq (\gamma_q)^{-\alpha\sqrt{N}/2}.$$

Now (4.3.8) implies that

$$q^{8/3-N_2/2} < q^{-0.95\alpha\sqrt{N}} \leq (\gamma_q)^{1.9\alpha\sqrt{N}} < (\gamma_q)^{\alpha\sqrt{N}} \cdot \frac{(1-\gamma_q)}{2+\alpha\sqrt{N}}.$$

Next suppose that $2 \leq q < 43$, so $\gamma_q = 19/20$ and $\gamma_q^{13.51} > 1/q$. In the case $\alpha\sqrt{N} \geq 9$, we have

$$\frac{2+\alpha\sqrt{N}}{1-\gamma_q} = 20(2+\alpha\sqrt{N}) < (\gamma_q)^{-11.7\alpha\sqrt{N}},$$

which implies by (4.3.8) that

$$q^{8/3-N_2/2} < q^{-1.9\alpha\sqrt{N}} < (\gamma_q)^{12.8\alpha\sqrt{N}} < (\gamma_q)^{\alpha\sqrt{N}} \cdot \frac{(1-\gamma_q)}{2+\alpha\sqrt{N}}.$$

On the other hand, in the case $\alpha\sqrt{N} \geq 2$, we have

$$\frac{2+\alpha\sqrt{N}}{1-\gamma_q} = 20(2+\alpha\sqrt{N}) < (\gamma_q)^{-43\alpha\sqrt{N}},$$

which implies by (4.3.8) that

$$q^{8/3-N_2/2} < q^{-3.26\alpha\sqrt{N}} < (\gamma_q)^{44\alpha\sqrt{N}} < (\gamma_q)^{\alpha\sqrt{N}} \cdot \frac{(1-\gamma_q)}{2+\alpha\sqrt{N}}.$$

Since $m_0 < 2 + \alpha\sqrt{N}$ by (4.3.7), in all cases we have

$$\frac{\dim U^{K_i}}{\dim U} < (\gamma_q)^{\alpha\sqrt{N}} \cdot \frac{(1-\gamma_q)}{2+\alpha\sqrt{N}} < \frac{(\gamma_q)^{\alpha\sqrt{N}}(1-\gamma_q)}{m_0},$$

as desired.

We have shown that the choice (4.3.8) implies that the total dimension of all irreducible K-submodules of V which have a trivial K_i-tensor factor for at least one i is less than $(\gamma_q)^{\alpha\sqrt{N}}(1-\gamma_q)\dim V$. Suppose finally that for $i = 1, 2, \ldots, m_0$, h_i does not lie in $Z(H_i)$. Then, as mentioned above, Gluck's bound (4.1.1) is applicable to the H_i-characters which are irreducible and nontrivial over K_i, and the element $h_i \in H_i$. Now if ρ is any irreducible constituent of the restriction of χ to $\langle K, h\rangle$ which does not have trivial K_i-factors for any i, then Lemma 4.3.2 and (4.1.1) imply that

$$|\rho(h)/\rho(1)| \leq (\gamma_q)^{m_0} \leq (\gamma_q)^{1+\alpha\sqrt{N}}.$$

Altogether, these estimates again yield (4.3.4) for h. We call this Case B.

Now let h be *any* element of sufficiently large support. Our strategy is to show that then we are either in Case A or Case B. This implies the theorem.

3) If W admits a decomposition (4.3.3), then we consider such a decomposition where each W_i cannot be decomposed further into h-invariant orthogonal sums satisfying the conditions set in Proposition 4.3.3(ii). If W admits no such decomposition, then just define $W_1 = W$. Now if $\dim W_i \geq N_1$ for some i, where N_1 is chosen as in (4.3.5), then we are in Case A. Thus we may assume that in the decomposition (4.3.3), all W_i are of bounded dimension $< N_1$. We call any W_i *good* if $h_i \notin Z(H_i)$ and *bad* otherwise.

Next we define the set $C := A \cup B$ as follows. Let μ_k be the set of k^{th}-roots of unity in $\overline{\mathbb{F}}_q$. Then $A = \mu_{q-1}$ and $B = \emptyset$ for $G = \mathrm{SL}$, $A = \mu_{q+1}$ and $B = \emptyset$ for $G = \mathrm{SU}$, $A = \mu_2$ and $B = \emptyset$ for $G = \mathrm{Sp}$. If $G = \mathrm{Spin}$, then $A = \mu_2$, and B is the set of pairs $\{\alpha, \alpha^{-1}\}$, where $\alpha \in (\mu_{q+1} \cup \mu_{q-1}) \setminus \mu_2$. The proof of Proposition 4.3.3 shows that if W_i is bad, then one of the following holds:

(i) $\dim W_i \leq 2$, and $h|_{W_i} = \lambda \cdot 1_{W_i}$ with $\lambda \in A$;
(ii) $G = \mathrm{Spin}$, $\dim W_i = 2$, H_i acts on W_i as a subgroup of $\mathrm{SO}(W_i)$ containing $\Omega(W_i)$, and $h|_{W_i}$ is conjugate to $\mathrm{diag}(\alpha, \alpha^{-1})$ for some $\{\alpha, \alpha^{-1}\} \in B$.

Now relabel the indecomposable summands W_i in such a way that the first t of them are good and all the $k_1 + \cdots + k_c$ remaining ones are bad; furthermore, $|C| = c$, $k_1 \leq k_2 \leq \cdots \leq k_c$, $C = \{\gamma_1, \ldots, \gamma_c\}$, and for $1 \leq j \leq c$, we have exactly k_j bad summands W_i, where the set of eigenvalues of $h|_{W_i}$ (without counting multiplicities) is γ_j (we say that these summands are of γ_j-type).

Next we regroup the bad summands W_i as follows. Pair up each W_i of γ_1-type with some $W_{i'}$ of γ_2-type. Then pair up each of the remaining W_i of γ_2-type with some $W_{i'}$ of γ_3-type. Continuing this process, we will pair up

each of the remaining W_i of γ_{c-1}-type with some $W_{i'}$ of γ_c-type. If in addition $\gamma_c \in B$, then we also pair up any two of the remaining W_i of γ_c-type until it is impossible to do it. When this pairing process terminates, we replace every pair $(W_i, W_{i'})$ by $W_i \oplus W_{i'}$ and call the sum a new W_i. Notice that this new W_i is good and has dimension $\le 4 < N_1$.

Now we show that if

$$\operatorname{supp}(h) \ge (m_0 - 1)(N_1 + N_2 - 2) + N_2 + 2, \tag{4.3.9}$$

where m_0 is chosen subject to (4.3.7), then Case B holds. Indeed, our pairing process leaves out at most 1 summand W_i of γ_c-type if $\gamma_c \in B$ and at most k_c summands W_i of γ_c-type if $\gamma_c \in A$. If Σ_g is the total sum of the dimensions of good summands, then in the former case, we have $\Sigma_g \ge \dim W - 2 \ge \operatorname{supp}(h) - 2$. In the latter case we have $\Sigma_g \ge \operatorname{codim} \ker(h - \gamma_c) \ge \operatorname{supp}(h)$. Thus in either case we have

$$\Sigma_g \ge \operatorname{supp}(h) - 2 \ge (m_0 - 1)(N_1 + N_2 - 2) + N_2. \tag{4.3.10}$$

Now we will define a new decomposition $W = \oplus_{j=1}^{m_0} \widetilde{W}_j$ as follows. First we choose $\widetilde{W}_1$ to be the direct sum of, say m_1, good summands W_i, chosen so that $\dim \widetilde{W}_1 \ge N_2$ and m_1 is as small as possible. Then we define $\widetilde{W}_2$ to be the direct sum of, say m_2, of the remaining good summands W_i, chosen so that $\dim \widetilde{W}_2 \ge N_2$ and m_2 is as small as possible. Then define $\widetilde{W}_j$ for $3 \le j \le m_0 - 1$ in the same manner. Note that $\dim \widetilde{W}_j \le N_1 + N_2 - 2$ for $1 \le j \le m_0 - 1$. (Indeed, if $\dim \widetilde{W}_j \ge N_1 + N_2 - 1$, then, since all W_i inside $\widetilde{W}_j$ have dimensions $\le N_1 - 1$, we could remove one of them from $\widetilde{W}_j$ and the remaining sum still has dimension $\ge N_2$.) Finally, $\widetilde{W}_{m_0}$ is the direct sum of all the remaining good summands plus all the remaining bad summands, if any. The inequality (4.3.10) ensures that we can define all the subspaces $\widetilde{W}_j$ for $1 \le j \le m_0$, and moreover $\dim \widetilde{W}_{m_0} \ge N_2$ as well.

Thus $W = \oplus_{j=1}^{m_0} \widetilde{W}_j$ is an h-stable orthogonal sum of m_0 subspaces of shape (4.3.3), each of dimension $\ge N_2$, and furthermore $\tilde{h}_j \notin Z(\widetilde{H}_j)$ for the corresponding $\widetilde{H}_j$ and $\tilde{h}_j$. Thus Case B holds as stated.

4) It remains to show that if $\operatorname{supp}(h) \ge N$ and N is as in Theorem 4.3.6, then (4.3.9) holds and so (4.3.4) also holds (for the suitably chosen α).

First assume that $N \ge 567$. Then we choose $\alpha = \sqrt{1/7}$; in particular $\alpha\sqrt{N} \ge 9$. In this case, $N_2 + 2 < N_1 < 2\sqrt{N/7} + 9$, $m_0 < 2 + \sqrt{N/7}$, and since $N \ge 567$, we get $N \ge N_1(2m_0 - 1)$, whence (4.3.9) holds. Thus (4.3.2) holds in this case, and so (4.3.1) also follows.

Next we consider the case $N \ge 144$. Then we choose $\alpha = 1/6$; in particular $\alpha\sqrt{N} \ge 2$. In this case, $N_1 < N_2 < (6.52)\alpha\sqrt{N} + 19/3$, $m_0 < 2 + \alpha\sqrt{N}$, and since $N \ge 128$, we get $N > N_2(2m_0 - 1) + 2$, whence (4.3.9) holds.

Now we consider the case that $N \geq 2225$ and $q \geq 109$. Then we choose $\alpha = 1/2.2$; in particular $\alpha\sqrt{N} > 9$. In this case we have $N_1 < \sqrt{N}/1.1 + 9$, $N_2 < 1.9\sqrt{N}/2.2 + 19/3$, $m_0 < 2 + \sqrt{N}/2.2$, and since $N \geq 2225$, (4.3.9) holds. Furthermore, $(1/\gamma_q)^{2.3} = (\sqrt{q} - 1)^{2.3} > q^{1.1}$ since $q \geq 109$, whence $\gamma_q^{1/2.2} < q^{-1.15}$. Thus (4.3.2) holds in this case.

Finally, notice that $\gamma_q < q^{-6/481}$. Hence, if $N \geq 144$, then as shown above, $|\chi(g)/\chi(1)| < \gamma_q^{-\sqrt{N}/6} < q^{-\sqrt{N}/481}$. On the other hand, if $N \leq 143$, then the main result of [Glu95] implies that $|\chi(g)/\chi(1)| < \gamma$ for some constant $\gamma < q^{-1/31.35} < q^{-\sqrt{N}/375}$. We have completed the proof of (4.3.2). □

Remark 4.3.7. The proof of Theorem 4.3.6 shows that its conclusion also holds if we define

$$\operatorname{supp}(g) = \inf_{\lambda \in A} \operatorname{codim} \ker(g - \lambda),$$

where $A = \mu_{q-1}$, respectively, μ_{q+1}, μ_2, μ_2, if $g \in G = \mathrm{SL}_n(q)$, $\mathrm{SU}_n(q)$, $\mathrm{Sp}_n(q)$, $\mathrm{Spin}_n(q)$, respectively.

5. **A Chebotarev density theorem for word maps**

Let $w \in F_d$ denote a nontrivial element in the free group on d elements. For any algebraic group G, we again denote by w the word map $G^d \to G$. It is well known [Bor83] that if G is semisimple, w is dominant. Writing G^{rss} for the open subvariety of regular semisimple elements, it follows easily that if w is fixed, then

$$\lim \frac{|w^{-1}(G^{\mathrm{rss}}(\mathbb{F}_q))|}{|G^d(\mathbb{F}_q)|} = 1, \tag{5.0.11}$$

where the limit is taken over over any sequence of groups $G/\mathbb{F}_q$ such that $\dim G$ is bounded and $|G(\mathbb{F}_q)|$ goes to ∞. For each regular semisimple element $g \in G(\mathbb{F}_q)$, there is a well-defined $G(\mathbb{F}_q)$-conjugacy class of maximal tori, and therefore a well-defined W-orbit in $\mathrm{Aut}(\Phi)$, where W and Φ denote respectively the Weyl group and the root system of G, and W acts by conjugation. We would like to understand the asymptotic distribution (in the large-q limit) of these conjugacy classes for regular semisimple elements $w(g_1, \ldots, g_d)$, as $(g_1, \ldots, g_d)$ ranges over $w^{-1}(G^{\mathrm{rss}}(\mathbb{F}_q))$.

5.1. *Regular homomorphisms and Weyl groups.* Let G and H be simply connected semisimple algebraic groups over an algebraically closed field k. Let H^{rss} denote the open subvariety of regular semisimple elements.

Definition 5.1.1. We say that a homomorphism $\phi\colon G \to H$ with finite kernel is *regular* if and only if $\phi^{-1}(H^{\mathrm{rss}}(k))$ is nonempty.

Suppose that ϕ is regular. Thus $\phi^{-1}(H^{\mathrm{rss}}(k)) \cap G^{\mathrm{rss}}(k)$ is nonempty. Let $t \in G(k)$ be a closed point of this intersection, and let T_G and T_H denote the centralizer of t in G and the centralizer of $\phi(t)$ in H, respectively. Let N_G and N_H denote the normalizer of T_G in G and the normalizer of T_H in H. Obviously, $\phi(T_G) \subset T_H$. It is also true that $\phi(N_G) \subset N_H$, since we can identify N_G (resp. N_H) with the transporter from t to T_G (resp. $\phi(t)$ to T_H). Thus, ϕ induces a homomorphism $\phi_W \colon W_G \to W_H$ of Weyl groups. This homomorphism is injective since $\ker \phi$ is finite. Of course W_G and W_H are well defined only up to inner automorphism, and ϕ_W is likewise defined only up to conjugation (see §1.1).

PROPOSITION 5.1.2. *Suppose that for each semisimple root system Φ we are given a subgroup X_Φ of its Weyl group W_Φ (defined up to conjugation) such that*:

- $X_{\Phi_1 \coprod \Phi_2} = X_{\Phi_1} \times X_{\Phi_2}$.
- *If ϕ is a regular homomorphism from a simply connected group of root system Φ_1 to a simply connected group of root system Φ_2, and up to conjugation, $\phi_W(X_{\Phi_1}) \subset X_{\Phi_2}$.*
- *$X_\Phi = W_\Phi$ for Φ of type A_1, A_2, and $B_2 = C_2$.*

Then $X_\Phi = W_\Phi$ for all root systems Φ.

Proof. There are obvious regular homomorphisms $G \to H$ in each of the tabulated cases in Table 1 below. The comments should be self-explanatory except that the prime powers indicated divide the order of the Weyl group W_G.

We prove the theorem by induction, first on rank, and for given rank, on Weyl group order. Assuming the theorem for all simple root systems of lower rank or of equal rank but smaller Weyl group, it suffices to show that no proper subgroup of W_H contains conjugates of the W_G for all groups G admitting a regular homomorphism to H given in the table.

For A_r, $r \geq 3$, it is well known that the symmetric group S_r is a maximal subgroup of S_{r+1}. Therefore, any subgroup of S_{r+1} containing S_r (via the pair $(G, H) = (A_{r-1}, A_r)$) but also containing a permutation without fixed points (via $(A_1 \times A_{r-2}, A_r)$) is all of S_{r+1}.

For B_r, C_r, and D_r, we have surjective homomorphisms from W_H to S_r, and the map from $X_{A_{r-1}} = \mathsf{S}_r$ to W_H guarantees that X_Φ maps onto S_r. For B_r and C_r, it suffices to find a reflection in X_Φ lying in the kernel of this homomorphism, since the X_Φ-conjugates of such a reflection generate $\ker W_H \to \mathsf{S}_r$. This is guaranteed by (A_1^3, B_3), $(A_1 \times D_{r-1}, B_r)$ (for $r \geq 4$), and by (A_1^r, C_r). For D_r, it suffices to find an element of X_Φ in the kernel of $W_H \to \mathsf{S}_r$ which has a codimension 2 fixed space. Such an element is guaranteed by (A_1^4, D_4) and $(A_1^2 \times D_{r-2}, D_r)$ (for $r \geq 5$).

G	H	Comments
A_{r-1}	A_r	$r \geq 2$
$A_1 \times A_{r-2}$	A_r	$r \geq 3$
$A_1 \times A_1 \times A_1$	B_3	
A_{r-1}	B_r	$r \geq 3$
$A_1 \times D_{r-1}$	B_r	$r \geq 4$
A_1^r	C_r	
A_{r-1}	C_r	$r \geq 3$
A_1^4	D_4	
$A_1 \times A_1 \times D_{r-2}$	D_r	$r \geq 5$
A_{r-1}	D_r	
$A_2 \times A_2 \times A_2$	E_6	27
$A_5 \times A_1$	E_6	
$A_2 \times A_5$	E_7	27
A_7	E_7	
$A_4 \times A_4$	E_8	25
$A_1 \times E_7$	E_8	
$A_2 \times A_2$	F_4	9
D_4	F_4	
$A_1 \times A_1$	G_2	4
A_2	G_2	

Table 1.

It is known that the Weyl groups of A_2, D_4, $A_1 \times A_5$, $A_2 \times A_5$, and $A_1 \times E_7$ are maximal subgroups of the Weyl groups of G_2, F_4, E_6, E_7, and E_8, respectively; in the first two cases this is because the index of the subgroup is prime, and the last three cases appear in the tables of maximal subgroups in [CCN$^+$85]. None of these subgroups has order divisible by the prime power given in the comment field for a different subgroup G of the same H. For example, $X_{G_2} = W_{G_2}$ because X_{G_2} contains W_{A_2} which is of order 6 but also contains the subgroup $W_{A_1 \times A_1}$ whose order is divisible by (in this case equal to) 4. □

5.2. *Estimates of Lang-Weil type.* In this section, we prove two propositions of Lang-Weil type which are needed in the following section. We cannot appeal to Lang-Weil directly because we are interested in uniformity. Instead, we use standard results in étale cohomology. We do not claim novelty for either of the results in this section, but lacking suitable references, we give proofs.

PROPOSITION 5.2.1. *Let $\mathcal{Y}$ be a scheme of finite type over $\mathbb{Z}$ and $\pi\colon \mathcal{X} \to \mathcal{Y}$ a morphism of finite type. For all $\varepsilon > 0$, there exists $\delta > 0$ satisfying the following condition*: *For every finite field $\mathbb{F}_q$, every dominant morphism of*

varieties $\pi_0\colon X_0 \to Y_0$ such that the pull-back of π_0 to $\overline{\mathbb{F}}_q$ and the pull-back of π from to $\overline{\mathbb{F}}_q$ coincide, and for every subset $S \subset Y_0(\mathbb{F}_q)$, either

$$|S| > \delta |Y_0(\mathbb{F}_q)|,$$

or

$$|\pi^{-1}(S)| < \varepsilon |X_0(\mathbb{F}_q)|.$$

Proof. We begin by fixing a prime p and assuming $\mathbb{F}_q$ is an extension of $\mathbb{F}_p$. Let $\phi\colon X \to Y$ denote the $\mathbb{F}_p$-fiber of π. We fix $\ell \neq p$. By the finiteness theorem for étale cohomology over a field [Del77, 1.1], $R^i\phi_!\mathbb{F}_\ell$ is constructible. By the proper base change theorem, $\dim H^i_c(X_{\overline{y}}, \mathbb{F}_\ell)$ is bounded as $\overline{y}$ ranges over geometric points of Y. It follows that the rank of $H^i_c(X_{\overline{y}}, \mathbb{Z}_\ell)$ is bounded and therefore that $\dim H^i_c(X_{\overline{y}}, \mathbb{Q}_\ell)$ is bounded. The geometric fibers of π_0 are the same as those of ϕ, so the ℓ-adic cohomology groups of the fibers of π_0 are likewise bounded, independent of π_0. By [Del80, 3.3.1], the weights of $H^i_c((X_0)_{\overline{y}}, \mathbb{Q}_\ell)$ are $\leq i$. By the Lefschetz trace formula, it follows that the number of $\mathbb{F}_q$-points of any fiber $(X_0)_y$, $y \in Y_0(\mathbb{F}_q)$, satisfies

$$|(X_0)_y(\mathbb{F}_q)| \leq c_1 q^{\dim (X_0)_y}, \tag{5.2.1}$$

where c_1 depends only on ϕ.

As ϕ is dominant, the dimension of its generic fiber is $\dim X - \dim Y$ [Gro65, 5.6.6]. Let $Z \subset Y$ denote the Zariski-closure of the set of points y of Y such that

$$\dim X_y \neq \dim X - \dim Y,$$

and let W denote $\pi^{-1}(Z)$. As fiber dimension is a constructible function [Gro66, 9.5.5], $Z \subsetneq Y$, and so $W \subsetneq X$. We endow W with the structure of (proper) reduced closed subscheme of X. Defining Z_0 and W_0 in the analogous way, W and W_0 are isomorphic over $\overline{\mathbb{F}}_q$, so their compactly supported cohomology dimensions are the same. By the Lefschetz trace formula,

$$|W_0(\mathbb{F}_q)| \leq c_2 q^{\dim W_0} = c_2 q^{\dim W}. \tag{5.2.2}$$

Combining (5.2.1) and (5.2.2), we deduce that

$$|\pi_0^{-1}(S)| \leq c_1 |S| q^{\dim X - \dim Y} + c_2 q^{\dim W} \leq c_1 |S| q^{\dim X - \dim Y} + c_2 q^{\dim X - 1}.$$

Applying the Lefschetz trace formula again, we get Lang-Weil estimates

$$|X_0(\mathbb{F}_q)| \geq q^{\dim X} - c_3 q^{\dim X - 1/2},$$
$$|Y_0(\mathbb{F}_q)| \leq q^{\dim Y} + c_4 q^{\dim Y - 1/2},$$

where c_3 and c_4 depend only on X and Y, respectively. If $|S| \leq \delta |Y_0(\mathbb{F}_q)|$, then

$$\begin{aligned} |\pi_0^{-1}(S)| &\leq q^{\dim X}(c_1 q^{-\dim Y}|S| + c_2 q^{-1}) \\ &\leq q^{\dim X}(c_1 \delta q^{-\dim Y}|Y_0(\mathbb{F}_q)| + c_2 q^{-1}) \\ &\leq q^{\dim X}(c_1 \delta(1 + c_4 q^{-1/2} + c_2 q^{-1}) \\ &\leq \frac{\delta c_1(1 + c_4 q^{-1/2}) + c_2 q^{-1}}{1 - c_3 q^{-1/2}} |X_0(\mathbb{F}_q)|. \end{aligned}$$

Given $\varepsilon > 0$, we can choose N and δ such that

$$\frac{\delta c_1(1 + c_4 q^{-1/2}) + c_2 q^{-1}}{1 - c_3 q^{-1/2}} < \varepsilon \tag{5.2.3}$$

for all $q \geq N$ and

$$\delta < \frac{1}{q^{\dim Y} + c_4 q^{\dim Y - 1/2}} \tag{5.2.4}$$

for all $q < N$. This finishes the proof when $\mathcal{Y}$ lies over Spec $\mathbb{F}_p$ or, more generally, over any proper closed subset of Spec $\mathbb{Z}$.

Suppose therefore that $\mathcal{Y}$ is dominant over $\mathbb{Z}$. By the previous discussion, we may assume p is larger than any desired constant. By [Gro66, 9.7.7], the set of points t of Spec $\mathbb{Z}$ for which $\mathcal{X}_t$ and $\mathcal{Y}_t$ are varieties is constructible, so without loss of generality, we may assume that $\mathcal{X}_{\overline{\mathbb{F}}_p} \to \mathcal{Y}_{\overline{\mathbb{F}}_p}$ is always a morphism of varieties. Also the generic fibers $\mathcal{X}_\eta$ and $\mathcal{Y}_\eta$ are varieties, so we may assume that $\mathcal{X}$ and $\mathcal{Y}$ have each a unique generic point. If $\mathcal{X} \to \mathcal{Y}$ fails to be dominant, then by Chevalley's theorem [Gro64, 1.8.4], the set of primes p for which $\mathcal{X}_{\overline{\mathbb{F}}_p} \to \mathcal{Y}_{\overline{\mathbb{F}}_p}$ is dominant is finite, so we may take it to be empty, in which case there is nothing to prove. Otherwise, the constructible set

$$\{y \in \mathcal{Y} \mid \dim \mathcal{X}_y = \dim \mathcal{X} - \dim \mathcal{Y}\}$$

contains the generic point of the generic fiber of $\mathcal{Y}$ since rings of finite type over $\mathbb{Z}$ are catenary [Gro65, 5.6.4].

Let $\mathcal{Z}$ denote the Zariski-closure of the set of points y of $\mathcal{Y}$ such that $\dim \mathcal{X}_y \neq \dim \mathcal{X} - \dim \mathcal{Y}$. Thus $\mathcal{Z}$ defines a proper reduced closed subscheme of $\mathcal{Y}$, and its inverse $\mathcal{W}$ in $\mathcal{X}$ defines a proper closed subscheme of $\mathcal{X}$. By Chevalley's theorem, the set of primes p for which $\mathcal{W}_{\mathbb{F}_p}$ is all of $\mathcal{X}_{\mathbb{F}_p}$ is finite. We may therefore assume that $\mathcal{W}_{\mathbb{F}_p}$ is always a proper closed subscheme of $\mathcal{X}_{\mathbb{F}_p}$. Fix a prime ℓ, and assume $p > \ell$. The finiteness theorem cited above for higher direct images of constructible sheaves with $\mathbb{F}_\ell$ coefficients applies for all schemes of finite type over $\mathbb{F}_\ell$, so arguing as above, we can find an upper bound, uniform in p, for the dimensions of $H_c^i(\mathcal{W}_{\overline{\mathbb{F}}_p}, \mathbb{Q}_\ell)$, $H_c^i(\mathcal{X}_{\overline{\mathbb{F}}_p}, \mathbb{Q}_\ell)$, and $H_c^i(\mathcal{Y}_{\overline{\mathbb{F}}_p}, \mathbb{Q}_\ell)$, and uniform in p and $\overline{y}$ for $\dim H_c^i(\mathcal{X}_{\overline{y}}, \mathbb{Q}_\ell)$. We can now define N and δ as in (5.2.3) and (5.2.4) and conclude as before. □

Let $\mathbb{F}_q$ be a finite field and n a positive integer. Let Y_0 be a variety over $\mathbb{F}_q$, Y the variety obtained from Y_0 by extending scalars to $\mathbb{F}_{q^n}$, and $\overline{Y}$ the variety obtained by extending scalars to $\overline{\mathbb{F}}_q$. Suppose X is a variety over $\mathbb{F}_{q^n}$ and $\pi\colon X \to Y$ is a finite étale morphism such that $\pi_0\colon X \to Y_0$ is étale with group Γ_0. The homomorphism from $\mathrm{Gal}(X/Y_0)$ to $\mathrm{Gal}(Y/Y_0) = \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is surjective and has kernel $\mathrm{Gal}(X/Y)$, which we denote Γ. Thus, we have a short exact sequence

$$0 \to \Gamma \to \Gamma_0 \to \mathbb{Z}/n\mathbb{Z} \to 0,$$

and we denote the inverse image of $1 \in \mathbb{Z}/n\mathbb{Z}$ by Γ^1. Every element $y \in Y_0(\mathbb{F}_q)$ determines a well-defined Frobenius conjugacy class in Γ_0 which lies in Γ^1. Equivalently, we can regard this class as a single Γ-orbit in $\Gamma^1 \subset \Gamma_0$. We denote this class $\mathrm{Frob}(y)$.

We can now state the uniform Chebotarev estimate in the function field case:

PROPOSITION 5.2.2. *Let $\mathcal{Y}$ be a scheme of finite type over $\mathbb{Z}$ and $\mathcal{X} \to \mathcal{Y}$ a finite étale cover with Galois group Γ such that the nonempty geometric fibers of $\mathcal{X}$ over $\mathbb{Z}$ are varieties. There exists a constant C such that for every extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ and every variety $Y_0/\mathbb{F}_q$ such that $Y := Y_0 \times_{\mathbb{F}_q} \mathbb{F}_{q^n}$ is isomorphic to $\mathcal{Y}_{\mathbb{F}_{q^n}}$, and $X := \mathcal{X}_{\mathbb{F}_{q^n}}$ is Galois over Y_0 with group Γ_0, we have*

$$\left| q^{-\dim Y} \left| \{ y \in Y_0(\mathbb{F}_q) \mid \mathrm{Frob}(y) = O \} \right| - \frac{|O|}{|\Gamma_0|} \right| \le C q^{-1/2}$$

for every Γ-orbit O in Γ^1.

Proof. Writing the characteristic function of the orbit O as a linear combination of characters of Γ, it suffices to show that for every irreducible $\overline{\mathbb{Q}}_\ell$-representation (ρ, V) of Γ and for every isomorphism $\iota\colon \overline{\mathbb{Q}}_\ell \to \mathbb{C}$,

$$\left| \iota\Big(\sum_{y \in Y_0(\mathbb{F}_q)} \mathrm{Tr}(\rho(\mathrm{Frob}(y))) \Big) \right| = \frac{q^{\dim Y}}{|\Gamma|} \iota\Big(\sum_{g \in \Gamma^1} \mathrm{Tr}(\rho(g)) \Big) + O(q^{\dim Y - 1/2}),$$

where the implied constant does not depend on q. Let $\mathcal{F}_\rho$ denote the lisse $\overline{\mathbb{Q}}_\ell$-sheaf on Y_0 obtained by composing $\pi_1(Y_0, \overline{y}) \to G_0$ with ρ, and $\overline{\mathcal{F}}_\rho$ the pullback of this sheaf to $\overline{Y}$. In particular, $\mathcal{F}_\rho$ is a direct summand of $(\pi_0)_* \overline{\mathbb{Q}}_\ell$. By the Lefschetz trace formula,

$$\sum_{y \in Y_0(\mathbb{F}_q)} \mathrm{Tr}(\rho(\mathrm{Frob}(y))) = \sum_{i=0}^{2 \dim Y} (-1)^i \mathrm{Tr}(\mathrm{Frob}_q \mid H^i_c(\overline{Y}, \overline{\mathcal{F}}_\rho)).$$

The theorem now follows from the weight formalism. As in Proposition 5.2.1, the dimensions of the $\overline{\mathbb{Q}}_\ell$-spaces $H^i_c(\overline{Y}, \overline{\mathcal{F}}_\rho)$ are uniformly bounded by proper base change and the finiteness theorem for étale cohomology over an excellent 1-dimensional base. The weights of $H^i_c(\overline{Y}, \overline{\mathcal{F}}_\rho))$ are $\le i$. For $i = 2 \dim Y$, we may assume without loss of generality that Y is nonsingular, in which

case, by Poincaré duality, $H_c^i(\overline{Y}, \overline{\mathcal{F}}_\rho)$ is nonzero if and only if ρ is trivial on Γ. Each such ρ is associated with a 1-dimensional representation $\chi\colon \mathbb{Z}/n\mathbb{Z} \to \overline{\mathbb{Q}}_\ell^\times$, and the eigenvalue of Frob_q acting on the 1-dimensional space $H_c^i(\overline{Y}, \overline{\mathcal{F}}_\rho)$ is $\chi(1)q^{\dim Y}$. □

5.3. *Torus types of word map images.* Let W^1 denote the coset of W in $\mathrm{Aut}(\Phi)$ associated to G. The classification of maximal tori up to $G(\mathbb{F}_q)$-conjugacy gives a partition of the regular semisimple elements of $G(\mathbb{F})$ in which the parts are indexed by the W-orbits of W^1 under the conjugation action. This classification does not depend on q but only on W and W^1. Our goal in this section is to estimate the proportion of elements $(g_1, \dots, g_d) \in G(\mathbb{F}_q)^d$ such that $w(g_1, \dots, g_d)$ belongs to a given type and to show that the limit of this proportion as q goes to infinity does not depend on d or w.

Let Φ denote a fixed root system. Let $\mathcal{G}/\mathrm{Spec}\ \mathbb{Z}$ denote the Chevalley scheme associated to the simply connected semisimple root datum attached to Φ. Thus $\mathcal{G}$ is an affine group scheme with coordinate ring A. Let $\mathcal{G}^\natural$ denote the spectrum of $A^{\mathcal{G}}$, the subring of A invariant under the action of $\mathcal{G}$ on itself by conjugation. Let $\mathcal{T} \subset \mathcal{G}$ be a split maximal torus of $\mathcal{G}$. Thus $\mathcal{T} = \mathrm{Spec}\ A/I$ for some ideal I. The composition $\mathcal{T} \hookrightarrow \mathcal{G} \to \mathcal{G}^\natural$ factors through $\mathcal{T}/W$, where W denotes the Weyl group of $\mathcal{G}$ with respect to $\mathcal{T}$. The pull-back of the morphism $\mathcal{T}/W \to \mathcal{G}^\natural$ at any geometric point of $\mathrm{Spec}\ \mathbb{Z}$ is well known to be an isomorphism [Ste65, 6.4]. As A and A/I are torsion-free abelian groups, the same is true of $(A/I)^W$ and $A^{\mathcal{G}}$, and it follows that $A^{\mathcal{G}} \to (A/I)^W$ is injective. The cokernel of this map is killed by tensor product with $\overline{\mathbb{Q}}$ and with $\overline{\mathbb{F}}_p$ for every prime p; it is therefore trivial as well. It follows that $\mathcal{T}/W \to \mathcal{G}^\natural$ is an isomorphism, and we have a natural quotient map $\mathcal{G} \to \mathcal{T}/W$ whose geometric fibers are semisimple conjugacy classes.

Let $\mathcal{G}^{\mathrm{rss}}$ denote the open subscheme of $\mathcal{G}$ consisting of regular semisimple elements, and let $\mathcal{T}^{\mathrm{rss}}$ be the regular semisimple open subscheme of $\mathcal{T}$. Note that W preserves $\mathcal{T}^{\mathrm{rss}}$. The map $\xi\colon \mathcal{G}^{\mathrm{rss}} \to \mathcal{T}/W$ sends $\mathcal{T}^{\mathrm{rss}}$ and therefore all of $\mathcal{G}^{\mathrm{rss}}$ to $\mathcal{T}^{\mathrm{rss}}/W$. Given a word map w, let $(\mathcal{G}^d)^{\mathrm{rss}}$ denote the inverse image in $\mathcal{G}^d$ of $\mathcal{G}^{\mathrm{rss}}$. As w defines a dominant map $G^d \to G$ for every semisimple group over every field, the p-fiber of $(\mathcal{G}^d)^{\mathrm{rss}}$ is dense in the p-fiber of $\mathcal{G}^d$ for every prime p.

Consider the following diagram:

$$\begin{array}{ccc}
(\mathcal{G}^d)^{\mathrm{rss}} & \xleftarrow{\ \phi_X\ } & \mathcal{X} \\
\downarrow{\scriptstyle \pi} \quad \searrow{\scriptstyle w} & & \downarrow{\scriptstyle \pi_X} \\
\mathcal{G}^{\mathrm{rss}} & & \\
\swarrow{\scriptstyle \xi} \quad \nwarrow{\scriptstyle i} & & \\
\mathcal{T}^{\mathrm{rss}}/W & \xleftarrow{\ \phi\ } & \mathcal{T}^{\mathrm{rss}},
\end{array}$$

where

$$\mathcal{X} = (\mathcal{G}^d)^{\mathrm{rss}} \times_{\mathcal{T}^{\mathrm{rss}}/W} \mathcal{T}^{\mathrm{rss}}.$$

As ϕ is finite étale and Galois with group W, so is ϕ_X. Thus, for each prime p, ϕ_X induces a map $\mathcal{X}_{\overline{\mathbb{F}}_p} \to (G^d)^{\mathrm{rss}}_{\overline{\mathbb{F}}_p}$ which is finite étale and Galois with group W.

THEOREM 5.3.1. *For all Φ and for all p, $\mathcal{X}_{\overline{\mathbb{F}}_p}$ is irreducible.*

Proof. It suffices to prove that $\mathcal{X}_{\mathbb{F}_q}$ is irreducible for all finite extensions $\mathbb{F}_q$ of $\mathbb{F}_p$. Assuming the contrary, there exists $\mathbb{F}_q$ such that $X := \mathcal{X}_{\mathbb{F}_q}$ is reducible. Let $H \subsetneq W$ be the stabilizer of a component of X. Let G, G^{rss}, etc. denote $\mathcal{G}_{\mathbb{F}_q}$, $\mathcal{G}^{\mathrm{rss}}_{\mathbb{F}_q}$, etc. If $K \supset \mathbb{F}_q$ and $x \in (G^d)^{\mathrm{rss}}(K)$, there exists a Galois extension L/K such that every $\overline{L}$-point of $\phi_X^{-1}(x)$ is defined over L.

We use induction on the number of roots in Φ. We assume the theorem holds for all systems of less than $|\Phi|$ roots. Suppose Φ is not of type A_1, A_2, or B_2. As H is a proper subgroup of $W = W_G$, by Proposition 5.1.2 there exists a split simply connected group G' over $\mathbb{F}_q$ whose root system Φ' has fewer roots than Φ and a regular homomorphism $\psi\colon G' \to G$ such that the image $\psi(W_{G'})$ is not contained (up to conjugacy) in H. By the induction hypothesis, the function field L' of X' is a $W_{G'}$-extension of the function field K' of $(G')^d$. As ψ is regular, the generic points of X' and $(G')^d$ map to X and $(G^d)^{\mathrm{rss}}$, respectively, which gives a contradiction. Thus it suffices to consider the base cases A_1, A_2, and B_2.

Let $G = \mathrm{SL}_2$, and suppose that the stabilizer H is a proper subgroup of the Weyl group S_2, i.e., H is trivial. Then for every field L containing $\mathbb{F}_q$ and every $x \in \mathrm{SL}_2(L)^d$ such that $w(x)$ is regular semisimple, the eigenvalues of x lie in L.

Let K be a local field containing $\mathbb{F}_q$ and D be the nontrivial quaternion algebra over K. Let $\mathrm{SL}_1(D)$ be the group of elements of norm 1 in D. Let G_1 denote the form of SL_2 over K such that $\mathrm{SL}_1(D) = G_1(K)$. As D is split by every quadratic extension L/K, $G_{1,L} = \mathrm{SL}_{2,L}$ for every such L/K. Let G_1^{rss}, $(G_1^d)^{\mathrm{rss}}$, T_1^{rss}, X_1, ϕ_{X_1}, etc. be defined in the obvious way. Extending scalars for $\phi_{X_1}\colon X_1 \to (G_1^d)^{\mathrm{rss}}$ from K to L, we get the same morphism as we do by extending scalars for $\phi_X\colon X \to (G^d)^{\mathrm{rss}}$ from $\mathbb{F}_q$ to L. As $G_1(K)$ is Zariski dense in G_1, there exists $x \in G_1(K)^d$ such that $w(x)$ is regular semisimple. In particular, regarding $w(x)$ as an element of $\mathrm{SL}_2(\overline{L})$, its eigenvalues lie in L. This is true for every quadratic extension L of K.

Now we use the fact that $\overline{K}$ contains two quadratic subextensions of K whose intersection is K, namely the unramified quadratic extension and any ramified quadratic extension. We conclude that $w(x)$ has eigenvalues $a \neq b$ in K. Regarding $w(x)$ as a norm-1 element γ, we have $(\gamma - a)(\gamma - b) = 0$, which is impossible because $\gamma \notin \{a, b\}$ and D is a division algebra.

The argument for SL_3 is similar. The obvious inclusion morphism $\mathrm{SL}_2 \to \mathrm{SL}_3$ is regular. So the stabilizer H of a component of X contains an element of order 2. Either it is all of $W = \mathsf{S}_3$, or X consists of three components, each a nontrivial finite étale quadratic extension of $(G^d)^{\mathrm{rss}}$. The latter possibility is ruled out by considering a nontrivial division algebra D of degree 3 over a local field $K \supset \mathbb{F}_q$. Indeed, $w(x) \in \mathrm{SL}_1(D)$ regular semisimple implies that for any field L that splits D, in particular, for any cubic extension of K, the characteristic polynomial of $w(x)$ has coefficients in L and splits over a quadratic extension of L. Taking two cubic extensions, one totally ramified and the other unramified, we conclude that the characteristic polynomial has coefficients in K and splits over a quadratic extension of K. This implies that it has a root in K, which is impossible since D is a division algebra.

For Sp_4, we use the regular homomorphism $\mathrm{Res}_{\mathbb{F}_{q^2}/\mathbb{F}_q}\mathrm{SL}_2 \to \mathrm{Sp}_4$, thanks to which, for q sufficiently large, there exist regular semisimple elements in $w(\mathrm{Sp}_4(\mathbb{F}_q))$ which are contained in a nonsplit torus of $\mathrm{SL}_2(\mathbb{F}_{q^2})$. Any such element lies in a maximal torus of Sp_4 associated to a Weyl group element of order 4. On the other hand, thanks to the regular homomorphism $\mathrm{SL}_2^2 \to \mathrm{Sp}_4$, we know that the stabilizer H of a component of X also contains the Weyl group of SL_2^2, which has order 4 but no element of order 4. Thus $H = W$. □

THEOREM 5.3.2. *Let w be a nontrivial fixed word and N a fixed positive integer. For any semisimple algebraic group G of dimension less than N over a finite field $\mathbb{F}_q$ and every maximal torus T of G defined over $\mathbb{F}$,*

$$q^{\dim G - \dim T} \frac{|\{(g_1, \dots, g_d) \in G(\mathbb{F}_q) \mid w(g_1, \dots, g_d) \in T(\mathbb{F}_q)\}|}{|G(\mathbb{F}_q)^d|} = 1 + o(1).$$

We remark that in general it seems to be difficult to prove that closed subvarieties of G have nontrivial inverse image in $G(\mathbb{F}_q)^d$. In particular, we do not know how to show that every regular semisimple conjugacy class is hit, even in the large q limit. Indeed, if w is a k-th power for $k \geq 2$, this is not in general the case. The reason that maximal tori are tractable is that their orbits under the action of G by conjugacy are Zariski-dense.

Proof. Fix n such that $G \times_{\mathbb{F}_q} \mathbb{F}_{q^n}$ is split. Let G_s denote the split form of G over $\mathbb{F}_q$ and let

$$\phi\colon G_s \times_{\mathbb{F}_q} \mathbb{F}_{q^n} \to G \times_{\mathbb{F}_q} \mathbb{F}_{q^n}$$

be an isomorphism. There exists a split maximal torus T_s of G_s and a maximal torus T of G such that

$$\phi(T_s \times_{\mathbb{F}_q} \mathbb{F}_{q^n}) = T \times_{\mathbb{F}_q} \mathbb{F}_{q^n}.$$

We write Frob and Frob_s, respectively, for the q-Frobenius maps on $T \times_{\mathbb{F}_q} \mathbb{F}_{q^n}$ and $T_s \times_{\mathbb{F}_q} \mathbb{F}_{q^n}$.

We claim that the map π obtained by composing

$$T_s \times_{\mathbb{F}_q} \mathbb{F}_{q^n} \xrightarrow{\phi} T \times_{\mathbb{F}_q} \mathbb{F}_{q^n} \to G \times_{\mathbb{F}_q} \mathbb{F}_{q^n} \to G^\natural \times_{\mathbb{F}_q} \mathbb{F}_{q^n} \to G^\natural$$

is Galois. Indeed, π can be written as the composition

$$T_s \times_{\mathbb{F}_q} \mathbb{F}_{q^n} \to (T_s/W) \times_{\mathbb{F}_q} \mathbb{F}_{q^n} \to G^\natural,$$

and the first morphism is obviously Galois. It suffices, therefore, to find an automorphism α of $T_s \times_{\mathbb{F}_q} \mathbb{F}_{q^n}$ such that α is a covering map of π and α induces the q-Frobenius map on $\mathbb{F}_{q^n}$. Setting $\alpha = \phi^{-1} \circ \mathrm{Frob} \circ \phi$, the diagram

$$\begin{array}{ccc}
T_s \times_{\mathbb{F}_q} \mathbb{F}_{q^n} & \xrightarrow{\alpha} & T_s \times_{\mathbb{F}_q} \mathbb{F}_{q^n} \\
\downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi} \\
T \times_{\mathbb{F}_q} \mathbb{F}_{q^n} & \xrightarrow{\mathrm{Frob}} & T \times_{\mathbb{F}_q} \mathbb{F}_{q^n} \\
\downarrow & & \downarrow \\
T & \xrightarrow{\mathrm{id}} & T \\
\downarrow & & \downarrow \\
G^\natural & \xrightarrow{\mathrm{id}} & G^\natural
\end{array}$$

shows that α is a covering map.

Let $Y_0 := (G^d)^{\mathrm{rss}}$. Let Y be the variety obtained from Y_0 by extension of scalars to $\mathbb{F}_{q^n}$ and let

$$X := Y \times_{(G^\natural)^{\mathrm{rss}}} (T_s \times_{\mathbb{F}_q} \mathbb{F}_{q^n})^{\mathrm{rss}}.$$

Clearly X is finite étale over Y, and we have shown that it is Galois with a group Γ which is an extension of $\mathbb{Z}/n\mathbb{Z}$ by the Weyl group W.

Given $\mathbf{g} := (g_1, \dots, g_d) \in Y_0(\mathbb{F}_q)$, let

$$h := w(g_1, \dots, g_d) \in G^{\mathrm{rss}}(\mathbb{F}_q).$$

To fix an element of $X(\overline{\mathbb{F}}_q)$ lying over $\mathbf{g}$ is the same as to pick an element $t \in T_s(\overline{\mathbb{F}}_q) \subset G_s(\overline{\mathbb{F}}_q)$ such that $\phi(t)$ is conjugate to h in $G(\overline{\mathbb{F}}_q)$. As h is regular semisimple, such an h is uniquely defined up to the action of W on T_s. The Frobenius conjugacy class $\mathrm{Frob}(\mathbf{g})$ is the W-orbit in Γ^1 containing the automorphism of $T_s \times_{\mathbb{F}_q} \mathbb{F}_{q^n}$ which sends t to t^q and induces the usual q-Frobenius on $\mathbb{F}_{q^n}$. It is clear that this W-orbit depends only on the conjugacy class of h. If h_1 and h_2 are both regular semisimple elements in the same maximal torus of G, the same element of $G_s(\overline{\mathbb{F}}_q)$ will conjugate $\phi^{-1}(h_1)$ and $\phi^{-1}(h_2)$ into $T_s(\overline{\mathbb{F}}_q)$, so $\mathrm{Frob}(\mathbf{g})$ depends only on the torus type of h. The map from torus types to W-orbits in Γ^1 is the usual one, which is bijective. (See, e.g., [Car93, Prop. 3.3.3], where the W-orbits in Γ^1 are described as F-conjugacy classes in W, which are easily seen to be equivalent.)

By Theorem 5.3.1, for any word map w, $X \to Y_0$ satisfies the hypotheses of Proposition 5.2.2. Therefore, in the large q limit, the proportion of $(g_1, \ldots, g_d)$ which map to any particular torus type depends only on the torus type. In particular, it does not depend on w. Applying Proposition 5.2.2 both to w and to the one variable word x_1, we conclude that in the limit as $q \to \infty$, the proportion of d-tuples $\mathbf{g} \in G(\mathbb{F}_q)^d$ such that $w(\mathbf{g})$ belongs to a particular torus type is the same as the proportion of elements of $G(\mathbb{F}_q)$ belonging to that torus type. Since the cardinality of the preimage $w^{-1}(T^{\mathrm{rss}}(\mathbb{F}_q))$ depends only on the conjugacy class of the maximal torus, i.e., on the torus type of T, it follows that

$$\lim_{q\to\infty} \frac{|w^{-1}(T^{\mathrm{rss}}(\mathbb{F}_q))| \cdot |G(\mathbb{F}_q)|}{|G(\mathbb{F}_q)^d| \cdot |T^{\mathrm{rss}}(\mathbb{F}_q)|} = 1.$$

The theorem now follows from the Lang-Weil estimate. □

COROLLARY 5.3.3. *For every fixed nontrivial word w and fixed integer N, there exists $\delta > 0$, so that for every semisimple algebraic group G of dimension less than N over a finite field $\mathbb{F}_q$ and every maximal torus T of G defined over $\mathbb{F}$,*

$$|T(\mathbb{F}_q) \cap w(G(\mathbb{F}_q))| \geq \delta |T(\mathbb{F}_q)|.$$

Proof. This is immediate by applying the preceding theorem and Proposition 5.2.1 to the finite set S consisting of all regular semisimple elements of $G(\mathbb{F}_q)$ of torus type T. □

In particular, we obtain the following useful result:

COROLLARY 5.3.4. *For every fixed nontrivial word w and fixed integer N, there exists q_0, so that for every prime power $q > q_0$ and a semisimple algebraic group G of dimension less than N over the finite field $\mathbb{F}_q$, there exists a regular semisimple element $g \in w(G(\mathbb{F}_q))$ which lies in a maximal split torus of $G(\mathbb{F}_q)$.*

Proof. This follows from the previous corollary applied to a split maximal torus T, noting that for large q, the number of regular elements in $T(\mathbb{F}_q)$ exceeds $(1 - \delta)|T(\mathbb{F}_q)|$. □

The result above can be used to obtain a short proof of one of the main results in [LS09]:

THEOREM 5.3.5. *For every nontrivial words w_1, w_2 and a positive integer r there exists an integer N such that if Γ is a finite simple group of Lie type (excluding Suzuki and Ree groups) of rank at most r and order at least N, then $w_1(\Gamma)w_2(\Gamma) = \Gamma$.*

Proof. Using Corollary 5.3.4, we see that if Γ is large enough, then there exist regular semisimple elements $s_i \in w_i(\Gamma)$ $(i = 1, 2)$ lying in split maximal

tori of Γ. Let C_i be the conjugacy class of s_i in Γ. A theorem of Ellers and Gordeev (see for instance Theorem 1 in [EG98] and the references therein) implies that $C_1C_2 \supseteq \Gamma \setminus \{1\}$. The result follows. □

6. **The main theorem**

In this section, we prove Theorem 1.1.1. In [LS09], we treated the cases that Γ is an alternating group as well as the cases where Γ is of Lie type with bounded rank (which are also treated by the theorem above). In particular, we treated the exceptional groups of types ${}^3D_4$, E_6, ${}^2E_6$, E_7, E_8, F_4, and G_2. The sporadic groups can be ignored by assuming that N is larger than the order of the Monster. What remains are the classical groups of Lie type (where we may exclude low rank cases whenever it is convenient to do so) and the Suzuki and Ree groups. The proofs for sufficiently high rank groups of type A, B, C, and D are given as Propositions 6.2.4, 6.3.5, 6.1.1, and 6.3.7, respectively. The Suzuki and Ree groups are treated in Proposition 6.4.1.

6.1. *Symplectic groups.* If V is a finite dimensional vector space over $\mathbb{F}_{q^r}$ and $\langle \cdot, \cdot \rangle$ is a symplectic pairing on V, then

$$(v_1, v_2) := \mathrm{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q} \langle v_1, v_2 \rangle$$

defines a symplectic pairing on V regarded as $\mathbb{F}_q$-vector space. Thus we have a natural inclusion $\mathrm{SL}_2(\mathbb{F}_{q^r}) \to \mathrm{Sp}_{2r}(\mathbb{F}_q)$. If $x \in \mathrm{SL}_2(\mathbb{F}_{q^r})$ is regular semisimple with eigenvalues $\alpha, \alpha^{-1} \in \overline{\mathbb{F}}_{q^r} = \overline{\mathbb{F}}_q$, and $\rho\colon \mathrm{Sp}_{2r} \to \mathrm{GL}_{2r}$ denotes the natural representation, then $\rho(\alpha)$ has eigenvalues

$$\{\alpha^{\pm 1}, \alpha^{\pm q}, \dots, \alpha^{\pm q^{r-1}}\}.$$

This element is regular semisimple as long as $\alpha^{q^i \pm 1} \neq 1$ for $i = 1, \dots, r-1$. Otherwise, if i is the smallest positive integer for which $\alpha^{q^i} \in \{\alpha, \alpha^{-1}\}$, then i divides r. The set of possible α has less than

$$\sum_{1 \le i \le r/2} \{(q^i + 1) + (q^i - 1)\} < 4q^{r/2}$$

elements.

PROPOSITION 6.1.1. *If $w = w_1 w_2$, where w_1 and w_2 are nontrivial disjoint words, then $w(\Gamma) = \Gamma$ for all sufficiently large finite simple groups Γ of symplectic type.*

Proof. Let Γ be the quotient of $\mathrm{Sp}_{2r}(\mathbb{F}_q)$ by its subgroup of scalar matrices. By [LS09], we may assume that r is larger than any desired constant.

We now fix maximal tori T_1 and T_2 of SL_2 over $\mathbb{F}_{q^r}$ such that T_1 is split and T_2 is nonsplit. By Corollary 5.3.3, if r is sufficiently large, there exist $x_1 \in T_1(\mathbb{F}_{q^r}) \cap w_1(\mathrm{SL}_2(\mathbb{F}_{q^r}))$ and $x_2 \in T_2(\mathbb{F}_{q^r}) \cap w_2(\mathrm{SL}_2(\mathbb{F}_{q^r}))$ such that regarded

as elements of $\mathrm{Sp}_{2r}(\mathbb{F}_q)$, x_1 and x_2 are regular semisimple. They belong to maximal tori of type T_r^+ and T_r^-, respectively, and $x_i \in w_i(\mathrm{Sp}_{2r}(\mathbb{F}_q))$. By [MSW94, Th. 2.3], every noncentral element of $\mathrm{Sp}_{2r}(\mathbb{F}_q)$ is the product of a conjugate of x_1 and a conjugate of x_2. Thus, every nonidentity element of the quotient $S_r(q)$ of $\mathrm{Sp}_{2r}(\mathbb{F}_q)$ by its center lies in $w_1(S_r(q))w_2(S_r(q))$. The identity always lies in $w(H)$ for any word w and any group H. This finishes the symplectic case. □

6.2. *Special linear and unitary groups.*

PROPOSITION 6.2.1. *For all $\varepsilon > 0$, there exists N such that if $n \geq N$, G is of the form SL_n or SU_n, q is any prime power, and χ is any irreducible character of $G(\mathbb{F}_q)$ of degree greater than $\varepsilon q^{-n/2}|G(\mathbb{F}_q)|^{1/2}$, then*

$$|\chi(g)| \leq \varepsilon\chi(1)$$

for all noncentral $g \in G(\mathbb{F}_q)$.

Proof. If $G = \mathrm{SL}_n$, the centralizer of g in $G(\mathbb{F}_q)$ is contained in the centralizer of g in $\mathrm{GL}_n(\mathbb{F}_q)$, which consists of the invertible elements in the centralizer algebra $Z(g)$ of g in $M_n(\mathbb{F}_q)$. By a well-known application of rational canonical form, $\dim_{\mathbb{F}_q} Z(g) \leq n^2 - 2n + 2$, and so

$$|C_{\mathrm{SL}_n(\mathbb{F}_q)}(g)| \leq q^{n^2-2n+2} = O(q^{3-2n}|\mathrm{SL}_n(\mathbb{F}_q)|).$$

If $G = \mathrm{SU}_n$, then the index of any proper subgroup in $\mathrm{SU}_n(\mathbb{F}_q)$ is $> q^{2n-4}$, see [KL90, Table 5.2.A]. Thus in either case, $|C_{G(\mathbb{F}_q)}(g)| = O(q^{4-2n}|G(\mathbb{F}_q)|)$, and the statement follows from Lemma 4.3.1. □

PROPOSITION 6.2.2. *Let w_1 and w_2 be nontrivial words. There exists N such that for all $n > N$ and for all finite fields $\mathbb{F}_q$, there exists an integer $a \geq 2$, depending only on w_1 and w_2, such that $w_1(\mathrm{SL}_n(\mathbb{F}_q))$ and $w_2(\mathrm{SL}_n(\mathbb{F}_q))$ contain regular semisimple elements x_1 and x_2, respectively, belonging to tori of type T_n and $T_{1,a,n-1-a}$, respectively, or to tori of type $T_{1,n-1}$ and $T_{a,n-a}$, respectively.*

Proof. By Corollary 5.3.3, for any fixed w_1, w_2, and k, for all l sufficiently large, for all prime powers q, and for all $i \in \{1, 2\}$, the image $w_i(\mathrm{SL}_k(\mathbb{F}_{q^l}))$ contains a regular semisimple element whose eigenvalues generate $\mathbb{F}_{q^{kl}}$ over $\mathbb{F}_q$. Indeed, the number of elements in a torus of type T_k whose eigenvalues generate a smaller field is less than the number of elements in $\mathbb{F}_{q^{kl}}$ which generate a proper subfield, and this is less than $2q^{kl/2}$. Regarding $\mathrm{SL}_k(\mathbb{F}_{q^l})$ as a subgroup of $\mathrm{SL}_{kl}(\mathbb{F}_q)$, it follows that the w_i-image of the latter group contains a regular element in a torus of type T_{kl}, as long as $l \geq L$, where L is a constant depending only on w_1 and w_2. We apply this for $k \in \{2, 3\}$ and choose $l_3 := 2\lfloor L/2 \rfloor + 1$ and $a := 3l_3$.

Suppose $n \geq 5L+4$ is even. Then $l_2 = (n-3l_3-1)/2 \geq L$, so

$$\mathrm{SL}_2(\mathbb{F}_{q^{l_2}}) \times \mathrm{SL}_3(\mathbb{F}_{q^{l_3}}) < \mathrm{SL}_{n-1}(\mathbb{F}_q) < \mathrm{SL}_n(\mathbb{F}_q)$$

contains a regular semisimple element of $w_2(\mathrm{SL}_n(\mathbb{F}_q))$ which lies in a maximal torus of type $T_{1,a,n-1-a}$. Similarly,

$$\mathrm{SL}_2(\mathbb{F}_{q^{n/2}}) < \mathrm{SL}_n(\mathbb{F}_q)$$

contains a regular semisimple element in $w_1(\mathrm{SL}_n(\mathbb{F}_q))$ which lies in a maximal torus of type T_n.

Now let $n \geq 5L+3$ be odd. Then $l_2 = (n-3l_3)/2 \geq L$, and so

$$\mathrm{SL}_2(\mathbb{F}_{q^{\frac{n-1}{2}}}) < \mathrm{SL}_{n-1}(\mathbb{F}_q) < \mathrm{SL}_n(\mathbb{F}_q)$$

and

$$\mathrm{SL}_2(\mathbb{F}_{q^{l_2}}) \times \mathrm{SL}_3(\mathbb{F}_{q^{l_3}}) < \mathrm{SL}_n(\mathbb{F}_q)$$

contain regular semisimple elements in $w_1(\mathrm{SL}_n(\mathbb{F}_q))$ and $w_2(\mathrm{SL}_n(\mathbb{F}_q))$ lying in maximal tori of types $T_{1,n-1}$ and $T_{a,n-a}$, respectively. □

PROPOSITION 6.2.3. *Let w_1 and w_2 be nontrivial words. There exists N such that for all $n > N$ and for all finite fields $\mathbb{F}_q$, there exists an integer $a \geq 2$, depending only on w_1 and w_2, such that $w_1(\mathrm{SU}_n(\mathbb{F}_q))$ and $w_2(\mathrm{SU}_n(\mathbb{F}_q))$ contain regular semisimple elements x_1 and x_2, respectively, belonging to tori of type T_n and $T_{1,a,n-1-a}$, respectively, or to tori of type $T_{1,n-1}$ and $T_{a,n-a}$, respectively.*

Proof. The argument is the same as before, replacing SL by SU everywhere. Note that l_3 is odd, so the inclusion $\mathrm{SU}_3(\mathbb{F}_{q^{l_3}}) \to \mathrm{SU}_{3l_3}(\mathbb{F}_q)$ exists. Furthermore,

$$\mathrm{SU}_2(\mathbb{F}_{q^m}) \cong \mathrm{Sp}_2(\mathbb{F}_{q^m}) < \mathrm{Sp}_{2m}(\mathbb{F}_q) < \mathrm{SU}_{2m}(\mathbb{F}_q)$$

for any m. □

PROPOSITION 6.2.4. *If $w = w_1w_2$, where w_1 and w_2 are nontrivial disjoint words, then $w(\Gamma) = \Gamma$ for all sufficiently large finite simple groups Γ of type A.*

Proof. Let Γ denote the quotient of $G(\mathbb{F}_q) := \mathrm{SL}_{r+1}(\mathbb{F}_q)$ or $\mathrm{SU}_{r+1}(\mathbb{F}_q)$ by its center. For r smaller than any given bound, the proposition is implied by [LS09]. We therefore assume that r is sufficiently large.

Applying Proposition 6.2.2 or Proposition 6.2.3 as Γ is of linear or unitary type, there exists a bounded value of a such that if r is sufficiently large, $w_1(G(\mathbb{F}_q))$ and $w_2(G(\mathbb{F}_q))$ contain regular semisimple elements x and y of types T_{r+1} and $T_{1,a,r-a}$, respectively, or alternatively, of types $T_{1,r}$ and $T_{a,r+1-a}$, respectively. We claim that the product of the conjugacy classes of x and y

contains every noncentral element of $G(\mathbb{F}_q)$. The claim obviously implies the proposition.

Let $\chi_1, \chi_2, \ldots, \chi_k$ denote the irreducible characters of $G(\mathbb{F}_q)$ such that $\chi(x)\chi(y) \neq 0$, arranged by increasing degree. By Proposition 3.1.5, $k \leq 4$. It suffices to prove that if r is sufficiently large and $z \in G(\mathbb{F}_q)$ is noncentral, then

$$\Re\left(\sum_{j=1}^{k} \frac{\chi_j(x)\chi_j(y)\overline{\chi}_j(z)}{\chi_j(1)}\right) = \sum_{j=1}^{k} \frac{\Re(\chi_j(x)\chi_j(y)\overline{\chi}_j(z))}{\chi_j(1)} \geq \frac{1}{40}.$$

The contribution of χ_1 to the sum is 1. For the remaining characters, $|\chi_j(x)\chi_j(y)| = 1$. By (4.1.1), the contribution of χ_2 to the sum is at least $-19/20$. By Proposition 6.2.1, the contribution of each of the remaining characters to the sum can be assumed to be at least $-1/80$. The proposition follows. □

6.3. *Orthogonal groups.* If V is a finite dimensional vector space over $\mathbb{F}_{q^l}$ and $\langle \cdot, \cdot \rangle$ is a nondegenerate symmetric pairing on V, then

$$(v_1, v_2) := \mathrm{Tr}_{\mathbb{F}_{q^l}/\mathbb{F}_q} \langle v_1, v_2 \rangle$$

defines a nondegenerate symmetric pairing on V regarded as $\mathbb{F}_q$-vector space. In particular, we have inclusions

$$i^+ \colon \mathrm{Spin}^+_{2k}(\mathbb{F}_{q^l}) \to \mathrm{Spin}^+_{2kl}(\mathbb{F}_q) \text{ and } i^- \colon \mathrm{Spin}^-_{2k}(\mathbb{F}_{q^l}) \to \mathrm{Spin}^-_{2kl}(\mathbb{F}_q)$$

for odd q. The same is true for even q by a similar base change for the corresponding quadratic forms. Let ρ denote the natural representation of any orthogonal group. If $g \in \mathrm{Spin}^{\pm}_{2k}(\mathbb{F}_{q^l})$ is semisimple and $\rho(g)$ has eigenvalues

$$\{\lambda_1, \lambda_1^{-1}, \ldots, \lambda_k, \lambda_k^{-1}\},$$

then $\rho(i^{\pm}(g))$ has eigenvalues

$$\{\lambda_1, \lambda_1^q, \ldots, \lambda_1^{q^{l-1}}, \lambda_1^{-1}, \ldots, \lambda_k^{-q^{l-1}}\}.$$

If g is any element of the maximal torus T_k^+ of $\mathrm{Spin}^+_{2k}(\mathbb{F}_{q^l})$, then we can order the λ_i such that $\lambda_{i+1} = \lambda_1^{q^{il}}$ and $\lambda_1^{q^{kl}} = \lambda_1$. Then $i^+(g)$ fails to be a regular semisimple element in the torus of type T_{kl}^+ of $\mathrm{Spin}^+_{2kl}(\mathbb{F}_q)$ for at most $2\sum_{0 \leq j \leq kl/2} q^j < 4q^{kl/2}$ such elements g. If g is any element of the maximal torus T_k^- of $\mathrm{Spin}^-_{2k}(\mathbb{F}_{q^l})$, then we may assume $\lambda_{i+1} = \lambda_1^{q^{il}}$ and $\lambda_1^{q^{kl}} = \lambda_1^{-1}$, so again $i^-(g)$ fails to be a regular semisimple element of the torus of type T_{kl}^- of $\mathrm{Spin}^-_{2kl}(\mathbb{F}_q)$ for at most $4q^{kl/2}$ such elements g.

Proposition 6.3.1. *Let w_1 and w_2 be nontrivial words and $k \geq 3$ an integer. Then there exists N such that for all $l > N$ and all q,*

$$w_1(\Omega_{2kl+1}(\mathbb{F}_q))w_2(\Omega_{2kl+1}(\mathbb{F}_q)) = \Omega_{2kl+1}(\mathbb{F}_q).$$

Proof. By Corollary 5.3.3 and the above discussion, if k, w_1 and w_2 are fixed, then for l sufficiently large, $w_1(\mathrm{Spin}^+_{2k}(\mathbb{F}_{q^l}))$ contains a regular semisimple element of type T^+_{kl} in $i^+(\mathrm{Spin}^+_{2k}(\mathbb{F}_{q^l}))$, and $w_2(\mathrm{Spin}^-_{2k}(\mathbb{F}_{q^l}))$ contains a regular semisimple element of type T^-_{kl} in $i^-(\mathrm{Spin}^-_{2k}(\mathbb{F}_{q^l}))$. Now the proposition follows by applying [MSW94, Th. 2.4] to (the images under the inclusions $\mathrm{Spin}^\pm_{2kl}(\mathbb{F}_q) \hookrightarrow \mathrm{Spin}_{2kl+1}(\mathbb{F}_q)$ of) the tori T^+_{kl} and T^-_{kl}. □

PROPOSITION 6.3.2. *If $w = w_1w_2$, where w_1 and w_2 are nontrivial disjoint words, there exists an even integer N such that if n is divisible by N, for every odd prime power q, $w(\mathrm{Spin}^+_{2n}(\mathbb{F}_q))$ contains an element lying above $-I \in \Omega^+_{2n}(\mathbb{F}_q)$.*

Proof. Let $\mathcal{G}/\mathrm{Spec}\ \mathbb{Z}$ denote the Chevalley scheme associated to Spin^+_8. For each prime $p > 2$, the fiber $\mathcal{G}_{\mathbb{F}_p}$ is isomorphic to $\mathrm{Spin}^+_{8,\mathbb{F}_p}$, so the center of $\mathcal{G}_{\mathbb{F}_p}(\mathbb{F}_p)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$. In particular, there exists $z_p \in \mathrm{Spin}^+_8(\mathbb{F}_p)$ which lies over $-I \in \mathrm{SO}^+_8(\mathbb{F}_p)$. For each $s \in \mathbb{N}$, the map $i^+\colon \mathrm{Spin}^+_8(\mathbb{F}_{p^s}) \to \mathrm{Spin}^+_{8s}(\mathbb{F}_p)$ maps $z_p \in \mathrm{Spin}^+_8(\mathbb{F}_p) \subset \mathrm{Spin}^+_8(\mathbb{F}_{p^s})$ to an element lying over $-I \in \mathrm{SO}^+_{8s}(\mathbb{F}_p)$. If there exists m such that for every odd prime p, $z_p \in w(\mathrm{Spin}^+_8(\mathbb{F}_{p^m}))$, then

$$z_p \in w(\mathrm{Spin}^+_8(\mathbb{F}_{p^{klm}})) \subset w(\mathrm{Spin}^+_{8lm}(\mathbb{F}_{p^k}))$$

for all k and l. Setting $q = p^k$ and $N = 4m$, we obtain the proposition.

To prove that such an m exists, note that as w_1 and w_2 induce dominant morphisms $(\mathrm{Spin}^+_{8,\mathbb{F}_p})^{d_i} \to \mathrm{Spin}^+_{8,\mathbb{F}_p}$ and as $\mathrm{Spin}^+_{8,\mathbb{F}_p}$ is irreducible, it follows that w induces a surjective homomorphism $(\mathrm{Spin}^+_{8,\mathbb{F}_p})^d \to \mathrm{Spin}^+_{8,\mathbb{F}_p}$. In particular, $w^{-1}(z_p)$ defines a nonempty reduced closed subscheme of $(\mathrm{Spin}^+_{8,\mathbb{F}_p})^d$. We claim that this subscheme has a point over $\mathbb{F}_{p^M}$ for some M which does not depend on p.

By [Gro66, 9.7.9], the number of geometrically irreducible components of any fiber of the morphism $w\colon \mathcal{G}^d \to \mathcal{G}$ is bounded by some integral constant C. The Galois group $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ acts on the set of irreducible geometric components of the fiber $w^{-1}(x)$ for any point $x \in \mathrm{Spin}^+_8(\mathbb{F}_p)$. If M is divisible by $C!$, then $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_{p^M})$ acts trivially on this set of components, so every geometric component of $w^{-1}(z_p)$ is defined over $\mathbb{F}_{p^M}$. By the standard facts about ℓ-adic cohomology discussed in Section 5.2, there exists a bound b such that

$$|\{x \in \mathrm{Spin}^+_8(\mathbb{F}_{p^M}) \mid w(x) = z_p\}| \geq (p^M)^{\dim w^{-1}(z_p)}(1 - bp^{-M/2}).$$

Choosing M so that $3^{M/2} > b$, we obtain the desired result. □

We will need the following simple number-theoretic fact:

LEMMA 6.3.3. *Let the integers $a, b > 1$ be coprime and $L > 1$. Then any integer $n > La + ab$ can be written in the form $xa + yb$ with $x > L$ and $y > 0$ being integers.*

Proof. Clearly, one can write $n - La$ in the form $ua + vb$ for some integers $u > 0$ and v. Among those representations, choose $n - La = ua + vb$ with u smallest possible. Now if $v \le 0$, then $ua = (n - La) - vb \ge n - La > ab$, and so we can write $n - La = (u - b)a + (v + a)b$ with $u - b > 0$, contradicting the choice of u. Thus $v > 0$, and we can write $n = (u + L)a + vb$. □

We will also need the following extension of Proposition 4.1.2:

LEMMA 6.3.4. *Let $\dim V = n > 2B$ and let $g \in \mathrm{GO}(V)$ have support $\le B$. Then g fixes an orthogonal decomposition $V = U \oplus W$ with $\dim U \ge n - 2B$ and $U \subseteq \ker(g - \lambda)$, where λ is the primary eigenvalue of g.*

Proof. By Proposition 4.1.2, $\lambda = \pm 1$. Multiplying g by -1_V if necessary, we may assume $\lambda = 1$. Consider the Jordan decomposition $g = su$, and write $V = V_0 \oplus V_0^{\perp}$, where $V_0 := \ker(s - 1) \supseteq \ker(g - 1)$. It is well known that one can further decompose $V_0 = \oplus_{i>0} V_i$ into an orthogonal sum of u-invariant subspaces V_i, where u acts on V_i as $a_i J_i$ with $a_i \ge 0$. Now

$$\sum_{i>0} a_i = \dim \ker(g - 1) \ge n - B, \ \sum_i i a_i = \dim V_0 \le n.$$

It follows that $a_1 \ge 2\sum_{i>0} a_i - \sum_{i>0} i a_i \ge n - 2B$, and one can just choose $U = V_1$, $W = V_1^{\perp}$. □

PROPOSITION 6.3.5. *If $w = w_1 w_2$, where w_1 and w_2 are nontrivial disjoint words, then $w(\Gamma) = \Gamma$ for all sufficiently large finite simple groups Γ of odd-dimensional orthogonal type.*

Proof. 1) Again, we may assume $r := \mathrm{rank}(G)$ is arbitrarily large. Fix some pairwise coprime odd integers $k_1, k_2, k_3, k_4 \ge 3$, and some $\varepsilon = \pm$. By Corollary 5.3.3 and the discussion before Proposition 6.3.1, there is some L_1 (depending on the words w_1, w_2, and $\max_{1 \le i \le 4} k_i$) such that for $l_1, l_3 \ge L_1$, $w_1(\mathrm{Spin}^+_{2k_1}(\mathbb{F}_{q^{l_1}}))$ contains a regular semisimple element s_1 of type $T^+_{k_1 l_1}$ in $\mathrm{Spin}^+_{2k_1 l_1}(\mathbb{F}_q)$, and $w_2(\mathrm{Spin}^-_{2k_3}(\mathbb{F}_{q^{l_3}}))$ contains a regular semisimple element s_3 of type $T^-_{k_3 l_3}$ in $\mathrm{Spin}^-_{2k_3 l_3}(\mathbb{F}_q)$. Moreover, when l_1, l_3 are bounded, there is some L_2 (depending on w_1, w_2, $\max_{1 \le i \le 4} k_i$, and $\max\{l_1, l_3\}$) such that for $l_2, l_4 \ge L_2$, $w_1(\mathrm{Spin}^{\varepsilon}_{2k_2}(\mathbb{F}_{q^{l_2}}))$ contains a regular semisimple element s_2 of type $T^{\varepsilon}_{k_2 l_2}$ in $\mathrm{Spin}^{\varepsilon}_{2k_2 l_2}(\mathbb{F}_q)$, and $w_2(\mathrm{Spin}^{-\varepsilon}_{2k_4}(\mathbb{F}_{q^{l_4}}))$ contains a regular semisimple element s_4 of type $T^{-\varepsilon}_{k_4 l_4}$ in $\mathrm{Spin}^{-\varepsilon}_{2k_4 l_4}(\mathbb{F}_q)$, and, in addition, no eigenvalue of s_2 and s_4 can belong to $\mathbb{F}_{q^{2k_1 l_1}} \cup \mathbb{F}_{q^{2k_3 l_3}}$. This extra condition guarantees that $s_1 s_2$, respectively $s_3 s_4$, becomes a regular semisimple element of type $T^{+,\varepsilon}_{k_l l_1, k_2 l_2}$ in

$\mathrm{Spin}^{\varepsilon}_{k_1l_1+k_2l_2}(\mathbb{F}_q)$ under the embedding

$$\mathrm{Spin}^{+}_{k_1l_1}(\mathbb{F}_q) * \mathrm{Spin}^{\varepsilon}_{k_2l_2}(\mathbb{F}_q) \hookrightarrow \mathrm{Spin}^{\varepsilon}_{k_1l_1+k_2l_2}(\mathbb{F}_q),$$

respectively of type $T^{-,-\varepsilon}_{k_3l_3,k_4l_4}$ in $\mathrm{Spin}^{\varepsilon}_{k_3l_3+k_4l_4}(\mathbb{F}_q)$ under the embedding

$$\mathrm{Spin}^{-}_{k_3l_3}(\mathbb{F}_q) * \mathrm{Spin}^{-\varepsilon}_{k_4l_4}(\mathbb{F}_q) \hookrightarrow \mathrm{Spin}^{\varepsilon}_{k_3l_3+k_4l_4}(\mathbb{F}_q).$$

Clearly, we can find integers l_1 and l_3 such that $k_1l_1 = k_3l_3 - 1$. Replacing (l_1, l_3) by $(l_1 + k_3, l_3 + k_1)$, we may assume that l_1 is odd. Replacing (l_1, l_3) by $(l_1 + 2bk_3, l_3 + 2bk_1)$ for b sufficiently large, we can achieve that $l_1, l_3 \geq L_1$. Next, we fix a pair of integers (l_2', l_4') such that $k_2l_2' - k_4l_4' = 1$. Then, for any given residue $t(\mathrm{mod}\, k_2k_4)$, we can find j with $0 \leq j \leq k_2k_4 - 1$ such that $k_1(l_1 + 2jk_3) \equiv (t - k_2l_2')(\mathrm{mod}\, k_2k_4)$. Replacing (l_1, l_3) by $(l_1 + 2jk_3, l_3 + 2jk_1)$ for such j, we get that

$$t = k_1l_1 + k_2l_2' + ck_2k_4 = k_1l_1 + k_2(l_2' + ck_4)$$

for some integer c. Fix such a pair (l_1, l_3) and set $a := k_1l_1$; notice that a is odd and bounded in terms of k_1, k_2, k_3, k_4 and w_1, w_2.

Now, assume r is sufficiently large. Then, we can write $r = t + dk_2k_4$ with $0 \leq t < k_2k_4$ and d sufficiently large. Setting $l_2 := l_2' + (c + d)k_4$ and $l_4 := l_4' + (c + d)k_2$, we get

$$r = k_1l_1 + k_2l_2 = k_3l_3 + k_4l_4$$

and $l_2, l_4 \geq L_2$. We have therefore shown that if r is sufficiently large, then $w_1(\mathrm{Spin}^{\varepsilon}_{2r}(\mathbb{F}_q))$ and $w_2(\mathrm{Spin}^{\varepsilon}_{2r}(\mathbb{F}_q))$ contain regular semisimple elements s_1s_2 and s_3s_4 of type $T^{+,\varepsilon}_{a,r-a}$ and $T^{-,-\varepsilon}_{a+1,r-a-1}$, respectively, with a odd and bounded.

2) We may also assume that q is odd, since otherwise we can use Proposition 6.1.1. Embedding $\mathrm{Spin}^{+}_{2r}(\mathbb{F}_q)$ in $\mathrm{Spin}_{2r+1}(\mathbb{F}_q)$, we see that when r is sufficiently large, $w_1(\mathrm{Spin}_{2r+1}(\mathbb{F}_q))$ and $w_2(\mathrm{Spin}_{2r+1}(\mathbb{F}_q))$ contain regular semisimple elements s_1s_2 and s_3s_4 of type $T^{+}_{a,r-a}$ and $T^{-}_{a+1,r-a-1}$, with a odd and bounded. By Proposition 3.4.1, there is some $\delta > 0$ (depending on a), such that the product of conjugacy classes of s_1s_2 and s_3s_4 contains all elements $g \in \mathrm{Spin}_{2r+1}(\mathbb{F}_q)$ with

$$|\chi(g)/\chi(1)| < \delta \tag{6.3.1}$$

for all nontrivial irreducible characters χ of $\mathrm{Spin}_{2r+1}(\mathbb{F}_q)$. By Theorem 4.3.6, there exists a bound $B > 0$, depending only on δ, such that (6.3.1) holds for any $g \in \mathrm{Spin}_{2r+1}(\mathbb{F}_q)$ with $\mathrm{supp}\,(g) > B$. Therefore, it suffices to prove that every element g of $\Gamma = \Omega_{2r+1}(\mathbb{F}_q)$ of support $\leq B$ lies in $w(\Gamma)$.

3) We may assume that $r > 2B$. Hence, by Proposition 4.1.2, the primary eigenvalue λ of g is ± 1. By Lemma 6.3.4, g fixes an orthogonal decomposition $V = U \oplus W$, where $V = \mathbb{F}_q^{2r+1}$ is the natural module for Γ, $g|_U = \lambda \cdot 1_U$, and $\dim U \geq 2r + 1 - 2B$.

3a) First we consider the case $\lambda = 1$. By Proposition 6.3.1, there exists $N \geq B$ (depending on w_1, w_2) such that $w(\Omega_{6l+1}(\mathbb{F}_q)) = \Omega_{6l+1}(\mathbb{F}_q)$ for all $l \geq N$. Now assume that $r \geq 4N$. Then $\dim U \geq 6N+1$. Writing $\dim W = 3x + y$ for some integers x, y with $0 \leq x$ and $0 \leq y \leq 2$, we have $x < B \leq N$. Now we can decompose $U = U' \oplus \widetilde{U}$ into an orthogonal sum with $\dim U' = 3(2N - x) + 1 - y$. Thus g preserves the orthogonal decomposition $V = \widetilde{V} \oplus \widetilde{U}$ with $\widetilde{V} = W \oplus U'$ of dimension $6N+1$ and $g|_{\widetilde{U}} = 1_{\widetilde{U}}$. It follows that

$$g \in \Omega(\widetilde{V}) = \Omega_{6N+1}(\mathbb{F}_q) = w(\Omega_{6N+1}(\mathbb{F}_q)) \subseteq w(\Gamma).$$

3b) Finally, assume that $\lambda = -1$; in particular $\dim U = 2j$ is even. Then write U as an orthogonal sum $\oplus_{i=1}^{j} U_i$, where $\dim U_i = 2$, and the quadratic space U_i has type $+$ for $1 \leq i \leq j-1$. By Proposition 6.3.2, there exists an even M (depending on w_1, w_2) such that $-I \in w(\Omega^+_{2mM}(\mathbb{F}_q))$ for any $m \geq 1$. Fix an integer $k \geq 3$ coprime to $2M$. By Proposition 6.3.1, there exists $N \geq B$ (depending on w_1, w_2) such that $w(\Omega_{2kl+1}(\mathbb{F}_q)) = \Omega_{2kl+1}(\mathbb{F}_q)$ for all $l \geq N$. Now assume that $r > k(N+M)$. By Lemma 6.3.3, there are some integers $x > N$ and $y > 0$ such that $r = xk + yM$. Clearly, $yM < r - 3B < (\dim U)/2 - 1 = j - 1$. Setting $\widetilde{V} := \oplus_{i=1}^{yM} U_i$ and $\widetilde{U} := \oplus_{i=yM+1}^{j} U_i \oplus W$, we see that g preserves the orthogonal decomposition $V = \widetilde{V} \oplus \widetilde{U}$, where $\dim \widetilde{V} = 2yM$, $\widetilde{V}$ is of type $+$, $g|_{\widetilde{V}} = -1_{\widetilde{V}}$, and $\dim \widetilde{U} = 2kx + 1$ with $x > N$. It follows that $g|_{\widetilde{V}} \in w(\Omega(\widetilde{V}))$ and $g|_{\widetilde{U}} \in w(\Omega(\widetilde{U}))$, and so $g \in w(\Gamma)$. □

For the even-dimensional orthogonal case, we need the following analogue of Proposition 6.3.1:

PROPOSITION 6.3.6. *Let w_1 and w_2 be nontrivial words and let $k, l \geq 3$ be two coprime odd integers. Fix an integer $v > 0$ such that $l|(kv-1)$. Then there exists L such that for all $a \geq L$, $\varepsilon = \pm$, and all q,*

$$w_1(\mathrm{Spin}^{\varepsilon}_{2n}(\mathbb{F}_q))w_2(\mathrm{Spin}^{\varepsilon}_{2n}(\mathbb{F}_q)) \supseteq \mathrm{Spin}^{\varepsilon}_{2n}(\mathbb{F}_q) \setminus Z(\mathrm{Spin}^{\varepsilon}_{2n}(\mathbb{F}_q)),$$

provided that $n = k(2al + v)$ and furthermore v is odd if $\varepsilon = +$.

Proof. Note that $l|(n-1)$ for any $n = k(2al+v)$. By Corollary 5.3.3 and the discussion before Proposition 6.3.1, there exists L depending on k, l, and w_1, w_2 such that for all $a > L$ and $n = k(2al+v)$, $w_1(\mathrm{Spin}^{-}_{2l}(\mathbb{F}_{q^{(n-1)/l}}))$ contains a regular semisimple element s_1 of type T^{-}_{n-1} in

$$i^{-}(\mathrm{Spin}^{-}_{2l}(\mathbb{F}_{q^{(n-1)/l}})) < \mathrm{Spin}^{-}_{2n-2}(\mathbb{F}_q),$$

and $w_2(\mathrm{Spin}^{\varepsilon}_{2k}(\mathbb{F}_{q^{n/k}}))$ contains a regular semisimple element s_2 of type T^{ε}_n in

$$i^{\varepsilon}(\mathrm{Spin}^{\varepsilon}_{2k}(\mathbb{F}_{q^{n/k}})) < \mathrm{Spin}^{\varepsilon}_{2n}(\mathbb{F}_q).$$

Note that under the embedding $\mathrm{Spin}^{-}_{2n-2}(\mathbb{F}_q) \hookrightarrow \mathrm{Spin}^{\varepsilon}_{2n}(\mathbb{F}_q)$, s_1 becomes a regular semisimple element of type $T^{-,-\varepsilon}_{n-1,1}$ of $\mathrm{Spin}^{\varepsilon}_{2n}(\mathbb{F}_q)$. Next, the tori T^{ε}_n and

$T^{-,-\varepsilon}_{n-1,1}$ are weakly orthogonal by Proposition 2.6.1. Hence, by Proposition 2.2.2, all irreducible characters χ of $\mathrm{Spin}^{\varepsilon}_{2n}(\mathbb{F}_q)$ that vanish neither on a regular semisimple element t_1 of type T^{ε}_n nor on a regular semisimple element t_2 of type $T^{-,-\varepsilon}_{n-1,1}$ must be unipotent. But then the results of [DL76] imply that $\chi(t_1)$ does not depend on the particular choice of the element t_1 of given type, and similarly for $\chi(t_2)$. Now the proofs of Theorems 2.5 and 2.6 of [MSW94] (for one particular choice of t_1 and t_2, which does not matter) show that such χ must be either the trivial or the Steinberg character of $K := \mathrm{Spin}^{\varepsilon}_{2n}(q)$. Estimating the character ratios, we see that $s_1^K s_2^K$ contains all noncentral elements of K. $\square$

PROPOSITION 6.3.7. *If $w = w_1 w_2$, where w_1 and w_2 are nontrivial disjoint words, then $w(\Gamma) = \Gamma$ for all sufficiently large finite simple groups Γ of even-dimensional orthogonal type.*

Proof. Let $\mathrm{Spin}^{\varepsilon}_{2r}(\mathbb{F}_q)$ denote the universal cover of Γ for some $\varepsilon = \pm$. We have shown in part 1) of the proof of Proposition 6.3.5 that if r is sufficiently large, then $w_1(\mathrm{Spin}^{\varepsilon}_{2r}(\mathbb{F}_q))$ and $w_2(\mathrm{Spin}^{\varepsilon}_{2r}(\mathbb{F}_q))$ contain regular semisimple elements t_1 and t_2 of type $T^{+,\varepsilon}_{a,r-a}$ and $T^{-,-\varepsilon}_{a+1,r-a-1}$, respectively, with a odd and bounded. Arguing as in part 2) of the proof of Proposition 6.3.5 and using Proposition 3.3.1 instead of Proposition 3.4.1, we can reduce to the case of elements g of bounded support $\le B$. Thus it suffices to prove that if g is of bounded support $\le B$ and r is sufficiently large, there exists z in $Z := Z(\mathrm{Spin}^{\varepsilon}_{2r}(\mathbb{F}_q))$ such that $gz \in w(\mathrm{Spin}^{\varepsilon}_{2r}(\mathbb{F}_q))$. Denote the coset gZ by $\overline{g}$.

Assuming $r > B$, we see that g has a (unique) primary eigenvalue $\lambda = \pm 1$. Again by Lemma 6.3.4, g fixes an orthogonal decomposition $V = U \oplus W$, where $V = \mathbb{F}_q^{2r}$ is the natural module for $\mathrm{Spin}^{\varepsilon}_{2n}(\mathbb{F}_q)$, $g|_U = \lambda \cdot 1_U$, and $\dim U \ge 2r - 2B$. If $\lambda = 1$, then the same arguments as in part 3a) of the proof of Proposition 6.3.5 yield $\overline{g} \in w(\Gamma)$.

It remains to consider the case $\lambda = -1$; in particular q is odd. Assume that $\varepsilon = +$ and $2|r$. Then there is some $z \in Z$ acting on V as -1_V. Replacing g by gz, we are done by the case $\lambda = 1$. Thus we may assume that r is odd if $\varepsilon = +$. Write U as an orthogonal sum $\oplus_{i=1}^{j} U_i$, where $\dim U_i = 2$ and the quadratic space U_i has type $+$ for $1 \le i \le j-1$. By Proposition 6.3.2, there exists an even M (depending on w_1, w_2) such that $-I \in w(\Omega^{+}_{2mM}(\mathbb{F}_q))$ for any $m \ge 1$. Fix coprime odd integers $k, l \ge 3$ which are coprime to $2M$. Also, fix an integer $v > 0$ such that $l|(kv-1)$ and $2|(r-v)$. Then by Proposition 6.3.6, there exists $L \ge B$ (depending on w_1, w_2) such that

$$w(\mathrm{Spin}^{\varepsilon}_{2n}(\mathbb{F}_q)) \supseteq \mathrm{Spin}^{\varepsilon}_{2n}(\mathbb{F}_q) \setminus Z(\mathrm{Spin}^{\varepsilon}_{2n}(\mathbb{F}_q))$$

for all $n = k(2al + v)$ and $a \ge L$.

Now assume that $r > kl(2L + M) + kv$. By Lemma 6.3.3, there are some integers $x > L$ and $y > 0$ such that $(r - kv)/2 = xkl + yM/2$, and so

$r = k(2xl+v)+yM$. Clearly, $yM < r - 3B < (\dim U)/2 - 1 = j-1$. Setting $\widetilde{V} := \oplus_{i=1}^{yM} U_i$ and $\widetilde{U} := \oplus_{i=yM+1}^{j} U_i \oplus W$, we see that g preserves the orthogonal decomposition $V = \widetilde{V} \oplus \widetilde{U}$, where $\dim \widetilde{V} = 2yM$, $\widetilde{V}$ is of type $+$, $g|_{\widetilde{V}} = -1_{\widetilde{V}}$, and $\dim \widetilde{U} = k(2xl+v)$ with $x > L$. By Proposition 6.3.2, there is some $h \in w(\mathrm{Spin}(\widetilde{V}))$ that lies above $-1_{\widetilde{V}}$. Then gh^{-1} fixes the decomposition $V = \widetilde{V} \oplus \widetilde{U}$ and acts trivially on $\widetilde{V}$. Clearly, gh^{-1} and g have the same action on $\widetilde{U}$, which has at least two eigenvalues -1 as $yM < j$. If $gh^{-1}|_{\widetilde{U}} = -1_{\widetilde{U}}$, then g acts on V as -1_V and so $\overline{g} = 1$, and we are done. So we may assume that $gh^{-1}|_{\widetilde{U}}$ is not scalar. Since $x > L$, by Proposition 6.3.6 there is some $f \in w(\mathrm{Spin}(\widetilde{U}))$ that lies above $gh^{-1}|_{\widetilde{U}}$. Now g and fh have the same action on V and so $fh = gz$ for some $z \in Z$. Finally, since $\mathrm{Spin}(\widetilde{U})$ and $\mathrm{Spin}(\widetilde{V})$ commute, we conclude that $fh \in w(\mathrm{Spin}(\widetilde{U}))w(\mathrm{Spin}(\widetilde{V})) \subseteq w(\mathrm{Spin}(V))$, whence $\overline{g} \in w(\Gamma)$, as stated. □

6.4. *Suzuki and Ree groups.* Let p be either 2 or 3, G a simple algebraic group over $\mathbb{F}_p$, of type B_2 or F_4 if $p = 2$ and of type G_2 if $p = 3$. There exists a (noncentral) isogeny $\Phi\colon G \to G$ such that Φ^2 coincides with the p-Frobenius F, and (with a finite number of small exceptions) $G(\overline{\mathbb{F}}_p)^{\Phi^{2f+1}}$ is a finite simple group, namely a Suzuki or Ree group. The goal of this section is to prove the following proposition:

PROPOSITION 6.4.1. *If $w = w_1 w_2$, where w_1 and w_2 are nontrivial disjoint words, then $w(\Gamma) = \Gamma$ for all sufficiently large finite simple groups Γ of Suzuki or Ree type.*

Proof. We may fix p and G and prove that w is surjective on $\Gamma = G(\overline{\mathbb{F}}_p)^{\Phi^{2f+1}}$ for all sufficiently large f. The proof is essentially that of [LS09, Th. 1.7], but something more is needed because Φ^{2f+1} is not quite a Frobenius map, but rather the square root of a Frobenius map.

By [LS09, Th. 3.3], if $w\colon G^d \to G$ is the word map, then for all $\mathbb{F}_q \subset \overline{\mathbb{F}}_p$ and all nonidentity elements $g \in G(\mathbb{F}_q)$, $w^{-1}(g)$ is a geometrically connected variety X_g over $\mathbb{F}_q = \mathbb{F}_{p^{2f+1}}$. A standard finiteness argument gives a uniform bound, depending only on G and w, for the sum S of dimensions of all the cohomology groups of $\overline{X}_g$. A standard weight argument shows that if $q^{1/4} > S$, then

$$\sum_i (-1)^i \mathrm{tr}(\Phi F^f | H^i(\overline{X}_q, \mathbb{Q}_\ell)) \neq 0. \tag{6.4.1}$$

If we can interpret (6.4.1) as a sum of local terms indexed by fixed points of Φ^{2f+1} acting on $\overline{X}_g$, it would follow that $\overline{X}_g^{\Phi^{2f+1}} \neq \emptyset$, which is what is needed for the proposition. To do this, we use a strong version of the Deligne conjecture due to Yakov Varshavsky [Var07]. Assuming $f \geq 1$, Φ^{2f+1} factors

through Frobenius on G^d, and is therefore contracting for every fixed point in $G(\mathbb{F}_q)^d$ and, *a fortiori*, for every fixed point in $\overline{X}_g^{\Phi^{2f+1}}$. Applying [Var07, Th. 2.1.3] to the graph of Φ^{2f+1}, we conclude that the Lefschetz number is indeed a sum over fixed points, and therefore that $g \in w(\Gamma)$. □

7. **Towards Thompson's conjecture**

7.1. *Preliminaries.* Let Γ be any finite non-abelian simple group. Thompson's conjecture states that Γ has a conjugacy class C such that $C^2 = \Gamma$. Results of Xu and Ellers-Gordeev (cf. [EG98] and the references therein), establish this for alternating groups and finite simple groups of Lie type defined over finite fields of large enough size. More recent related results can be found in [Sha09] and [Sha08]. In this section we prove Theorem 1.1.4, which may be regarded as an asymptotic approximation of Thompson's conjecture.

If Γ is a classical group, this was largely obtained in [MSW94, §2]. Indeed, it is shown there that Γ contains two (semisimple) conjugacy classes C_1, C_2 such that $C_1C_2 \supseteq \Gamma \setminus \{1\}$, except possibly for $\Gamma = P\Omega^+_{4n}(\mathbb{F}_q)$. The same result for exceptional groups was established in [LM99]. Here we use a similar strategy to handle the remaining family $P\Omega^+_{4n}(\mathbb{F}_q)$ for groups of sufficiently high order.

Applying the above results and choosing $N = 2^{630} > |\Omega^+_{36}(\mathbb{F}_2)|$, it suffices to prove Theorem 1.1.4 for all $\Gamma = P\Omega^+_{2n}(\mathbb{F}_q)$ such that $2|n$, $2 \le q \le 4$ and $|\Gamma| > N$. For such a group, the proof of [MSW94, Th. 2.6] implies the existence of regular semisimple elements x, y such that only two nontrivial characters $\chi \in \mathrm{Irr}(\Gamma)$ can be nonzero at both x and y: the Steinberg character St and another one, ρ. Unfortunately, $|\rho(x)\rho(y)| = 2$, making it difficult to show that $x^\Gamma y^\Gamma \supseteq \Gamma \setminus \{1\}$. To overcome this difficulty, we will work with regular semisimple elements t_1, t_2 belonging to maximal tori $T_1 = T^{+,+}_{n-1,1}$ and $T_2 = T^{-,-}_{n-2,2}$ of $G = \mathrm{Spin}^+_{2n}(\mathbb{F}_q)$, respectively.

Proposition 7.1.1. *Keep the above notation and assume that n is even and $n \ge 6$. Then for $i = 1, 2$, T_i contains a regular semisimple element t_i. Furthermore, there are exactly three nontrivial irreducible characters of G which vanish neither on t_1 nor on t_2: the Steinberg character* St *of degree $q^{n(n-1)}$, a character γ of degree $\frac{q^3(q^{n-3}+1)(q^{n-2}-1)(q^{n-1}+1)(q^n-1)}{2(q-1)^2(q^2+1)}$, and a character δ of degree $q^{(n-1)(n-4)}\gamma(1)$. The values of each of these three characters at t_1 and t_2 are ± 1.*

Proof. 1) Note that T_1 contains a central product of the cyclic tori T^+_{n-1} of $\mathrm{Spin}^+_{2n-2}(\mathbb{F}_q)$ and T^+_1 of $\mathrm{Spin}^+_2(\mathbb{F}_q)$, and that Spin_2 is an 1-dimensional torus. Assuming $n \ge 4$ and choosing t_1 appropriately from this product so that its component in T^+_{n-1} generates the torus, we see that t_1 is regular. A

similar argument applies to T_2 when $n \geq 6$. Now we fix such a pair of regular semisimple elements $\{t_1, t_2\}$.

2) Let $\chi \in \mathrm{Irr}(G)$ be such that $\chi(t_1)\chi(t_2) \neq 0$. Since n is even, the tori T_1 and T_2 are weakly orthogonal by Proposition 2.6.1, whence χ is unipotent. Now we will follow the proof of Proposition 3.3.1 (and its notation) closely to identify the symbol Λ labeling χ. In particular, if $w_i \in \mathsf{W}'_n$ corresponds to T_i, then $w_1 \in \mathsf{W}'_{n-1} \times \mathsf{W}'_1$, and $w_2 = w_{21}w_{22}$ with $w_{21} \in \mathsf{W}_{n-2} \setminus \mathsf{W}'_{n-2}$ and $w_{22} \in \mathsf{W}_2 \setminus \mathsf{W}'_2$. Furthermore, w_1 projects onto $\pi_1 = (12\cdots n-1)(n)$ and w_2 projects onto $\pi_2 = (12\cdots n-2)(n-1,n)$. As shown in the proof of Proposition 3.3.1, $\Lambda = (X, Y)$ is nondegenerate, its set Z_1 of singles has even size $2d \leq 4$, and there are subsets $M_1, M_2 \subset Z_1$ of size d such that (3.3.1) holds. In the notation of part 4) of that proof we now have that $\{k_1, l_1\} = \{n, 0\}$ or $\{n-1, 1\}$, and $\{k_2, l_2\} = \{n, 0\}$ or $\{n-2, 2\}$. Consider for instance the case where $\{k_1, l_1\} = \{k_2, l_2\} = \{n, 0\}$, i.e., $\alpha_1, \alpha_2 \vdash n$ and $\beta_1, \beta_2 = \emptyset$. The nonvanishing condition (3.3.1) implies that α_1 is one of the partitions listed in the second claim of Corollary 3.1.2 and α_2 is as listed in Corollary 3.1.4. Matching up the shapes of Z_1 and Z_2 as they come from (α_1, β_1) and from (α_2, β_2), we can show that either $Z_1 = \{0, n\}$ and $Z_2 = \emptyset$ or $\{1, 2, \ldots, n-1\}$, or $Z_1 = \{0, 1, 2, n-1\}$ and $Z_2 = \emptyset$, or $Z_1 = \{0, n-3, n-2, n-1\}$ and $Z_2 = \{1, 2, \ldots, n-4\}$. The same arguments show that this conclusion about Z_1, Z_2 also holds in the other three cases.

Assume $Z_1 = \{0, n\}$. If $Z_2 = \emptyset$, then $\chi = 1_G$. If $Z_2 = \{1, 2, \ldots, n-1\}$, then $\chi = \mathrm{St}$. In both of these cases, $|\chi(t_i)| = 1$.

3) Consider the case where $Z_1 = \{0, 1, 2, n-1\}$ and $Z_2 = \emptyset$. Then $X = Z_1 \setminus M'$ and $Y = M'$ for some $M' \subseteq Z_1$ of *even* size. We will use [Lus82, Cor. (3.16)(ii)] to find $\chi(t_i)$. To this end, we first compute the values of the character $[\Theta]$ of W'_n at w_1 and w_2, for the symbol $\Theta = (Z_1 \setminus M, M)$ and $M \subset Z_1$ of size 2:

$$([\Theta](w_1), [\Theta](w_2)) = \begin{cases} (-1,1) & \text{if } M = \{0,1\} \text{ or } \{2, n-1\}, \\ (-1,0) & \text{if } M = \{0,2\} \text{ or } \{1, n-1\}, \\ (0,1) & \text{if } M = \{1,2\} \text{ or } \{0, n-1\}. \end{cases}$$

Now [Lus82, Cor. (3.16)(ii)] readily implies that $\chi(t_2) = 0$ if $M' = \{0,1\}$ or $\{2, n-1\}$, and $\chi(t_1) = 0$ if $M' = \emptyset$, $\{0, n-1\}$, $\{1,2\}$, or Z_1. In the remaining subcase $M' = \{0,2\}$ or $\{1, n-1\}$, we get $(\chi(t_1), \chi(t_2)) = (-1, 1)$ and

$$\Lambda = \begin{pmatrix} 1 & n-1 \\ 0 & 2 \end{pmatrix},$$

leading to the character γ, whose degree is computed using [Car93, §13.8].

Finally, consider the case where $Z_1 = \{0, n-3, n-2, n-1\}$ and $Z_2 = \{1, 2, \ldots, n-4\}$. Then $X = Z_2 \cup (Z_1 \setminus M')$ and $Y = Z_2 \cup M'$ for some $M' \subseteq Z_1$ of even size. We again compute the values of the character $[\Theta]$ of W'_n at w_1

and w_2, for the symbol $\Theta = (Z_2 \cup (Z_1 \setminus M), Z_2 \cup M)$ and $M \subset Z_1$ of size 2:

$$([\Theta](w_1), [\Theta](w_2)) = \begin{cases} (-1,1) & \text{if } M = \{0, n-3\} \text{ or } \{n-2, n-1\}, \\ (-1,0) & \text{if } M = \{0, n-2\} \text{ or } \{n-3, n-1\}, \\ (0,1) & \text{if } M = \{0, n-1\} \text{ or } \{n-3, n-2\}. \end{cases}$$

Using [Lus82, Cor. (3.16)(ii)], we can show that $\chi(t_2) = 0$ if $M' = \{0, n-3\}$ or $\{n-2, n-1\}$, and $\chi(t_1) = 0$ if $M' = \emptyset$, $\{0, n-1\}$, $\{n-3, n-2\}$, or Z_1. In the remaining subcase $M' = \{0, n-2\}$ or $\{n-3, n-1\}$, we get $(\chi(t_1), \chi(t_2)) = (-1, 1)$ and

$$\Lambda = \begin{pmatrix} 1 & 2 & \cdots & n-4 & n-3 & n-1 \\ 0 & 1 & \cdots & n-5 & n-4 & n-2 \end{pmatrix},$$

leading to the character δ. To compute $\delta(1)$, we look at the Steinberg character St' of $\mathrm{Spin}^+_{2n-6}(\mathbb{F}_q)$ labeled by $\Lambda' := (X \setminus \{n-1\}, Y \setminus \{n-2\})$, of degree $q^{(n-3)(n-4)}$. Using [Car93, §13.8], one can show that

$$\frac{\delta(1)}{\mathrm{St}'(1)} = \frac{q^{2n-5}(q^{n-3}+1)(q^{n-2}-1)(q^{n-1}+1)(q^n-1)}{2(q-1)^2(q^2+1)},$$

and so $\delta(1) = q^{(n-1)(n-4)}\gamma(1)$. □

7.2. *Completion of the proof of Theorem* 1.1.4. Now we assume $|\Gamma| \geq 2^{630}$, which in particular implies that $q^{n/2-4} \geq 64$ since $q \leq 4$. We will show that any noncentral element $g \in G$ belongs to $(t_1)^G \cdot (t_2)^G$. By Proposition 7.1.1, it suffices to show that

$$\left|\frac{\gamma(g)}{\gamma(1)}\right| + \left|\frac{\delta(g)}{\delta(1)}\right| + \left|\frac{\mathrm{St}(g)}{\mathrm{St}(1)}\right| < 1.$$

According to [KL90, Table 5.2.A], the index of any proper subgroup of G is larger than q^{2n-2}, whence

$$|\delta(g)|^2 + |\mathrm{St}(g)|^2 < |C_G(g)| < |G|/q^{2n-2} < q^{2n^2-3n+2}.$$

Also, notice that $\mathrm{St}(1) > \delta(1) > q^{n^2-n-3}/2$. By the Cauchy-Schwarz inequality,

$$\left|\frac{\delta(g)}{\delta(1)}\right| + \left|\frac{\mathrm{St}(g)}{\mathrm{St}(1)}\right| < \frac{\sqrt{2(|\delta(g)|^2 + |\mathrm{St}(g)|^2)}}{\delta(1)} < \frac{\sqrt{8}}{q^{n/2-4}} < \frac{1}{20}$$

as $q^{n/2-4} > 64$. Since $|\gamma(g)/\gamma(1)| < 19/20$ by (4.1.1), we are done. □

References

[Asa83] T. Asai, Unipotent characters of $\mathrm{SO}^{\pm}_{2n}$, Sp_{2n} and SO_{2n+1} over F_q with small q, *Osaka J. Math.* **20** (1983), 631–643. MR 0718968. Zbl 0516.20028. Available at http://projecteuclid.org/euclid.ojm/1200776326.

[Bor83] A. Borel, On free subgroups of semisimple groups, *Enseign. Math.* **29** (1983), 151–164. MR 0702738. Zbl 0533.22009.

[BCC+70] A. Borel, R. Carter, C. W. Curtis, N. Iwahori, T. A. Springer, and R. Steinberg, *Seminar on Algebraic Groups and Related Finite Groups*, *Lecture Notes in Math.* **131**, Springer-Verlag, New York, 1970.

[Car93] R. W. Carter, *Finite Groups of Lie Type*, *Wiley Classics Library*, John Wiley & Sons Ltd., Chichester, 1993. MR 1266626. Zbl 0900.20021.

[Car95] ———, On the representation theory of the finite groups of Lie type over an algebraically closed field of characteristic 0 [MR1170353 (93j:20034)], in *Algebra*, IX, *Encyclopaedia Math. Sci.* **77**, Springer-Verlag, New York, 1995, pp. 1–120, 235–239. MR 1392478. Zbl 0832.20020.

[CCN+85] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *Atlas of Finite Groups. Maximal Subgroups and Ordinary Characters for Simple Groups*, Oxford University Press, Eynsham, 1985. MR 0827219. Zbl 0568.20001.

[Del77] P. Deligne, *Cohomologie Étale*, *Lecture Notes in Math.* **569**, Springer-Verlag, New York, 1977, Séminaire de Géométrie Algébrique du Bois-Marie SGA $\frac{4}{2}$. MR 0463174. Zbl 0345.00010.

[Del80] ———, La conjecture de Weil. II, *Inst. Hautes Études Sci. Publ. Math.* (1980), 137–252. MR 0601520. Zbl 0456.14014. Available at http://www.numdam.org/item?id=PMIHES_1980__52__137_0.

[DL76] P. Deligne and G. Lusztig, Representations of reductive groups over finite fields, *Ann. of Math.* **103** (1976), 103–161. MR 0393266. Zbl 0336.20029. http://dx.doi.org/10.2307/1971021.

[EG98] E. W. Ellers and N. Gordeev, On the conjectures of J. Thompson and O. Ore, *Trans. Amer. Math. Soc.* **350** (1998), 3657–3671. MR 1422600. Zbl 0910.20007. http://dx.doi.org/10.1090/S0002-9947-98-01953-9.

[Eno72] H. Enomoto, The characters of the finite symplectic group Sp(4, q), $q = 2^f$, *Osaka J. Math.* **9** (1972), 75–94. MR 0302750. Zbl 0254.20005. Available at http://projecteuclid.org/euclid.ojm/1200693539.

[GS09] S. Garion and A. Shalev, Commutator maps, measure preservation, and T-systems, *Trans. Amer. Math. Soc.* **361** (2009), 4631–4651. MR 2506422. Zbl 1182.20015. http://dx.doi.org/10.1090/S0002-9947-09-04575-9.

[Glu93] D. Gluck, Character value estimates for non-semisimple elements, *J. Algebra* **155** (1993), 221–237. MR 1206632. Zbl 0771.20009. http://dx.doi.org/10.1006/jabr.1993.1041.

[Glu95] ———, Sharper character value estimates for groups of Lie type, *J. Algebra* **174** (1995), 229–266. MR 1332870. Zbl 0842.20014. http://dx.doi.org/10.1006/jabr.1995.1127.

[Gro64] A. Grothendieck, Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. I, *Inst. Hautes Études Sci. Publ. Math.* (1964), 259. MR 0173675. Zbl 0136.15901.

[Gro65] ———, Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. II, *Inst. Hautes Études Sci. Publ. Math.* (1965), 231. MR 0199181. Zbl 0135.39701.

[Gro66] A. Grothendieck, Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. III, *Inst. Hautes Études Sci. Publ. Math.* (1966), 255. MR 0217086. Zbl 0144.19904.

[GT04] R. M. Guralnick and P. H. Tiep, Cross characteristic representations of even characteristic symplectic groups, *Trans. Amer. Math. Soc.* **356** (2004), 4969–5023. MR 2084408. Zbl 1062.20013. http://dx.doi.org/10.1090/S0002-9947-04-03477-4.

[Jam78] G. D. James, *The Representation Theory of the Symmetric Groups*, *Lecture Notes in Math.* **682**, Springer-Verlag, New York, 1978. MR 0513828. Zbl 0393.20009.

[KL90] P. Kleidman and M. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, *London Math. Soc. Lecture Note Ser.* **129**, Cambridge Univ. Press, Cambridge, 1990. MR 1057341. Zbl 0697.20004. http://dx.doi.org/10.1017/CBO9780511629235.

[LS74] V. Landazuri and G. M. Seitz, On the minimal degrees of projective representations of the finite Chevalley groups, *J. Algebra* **32** (1974), 418–443. MR 0360852. Zbl 0325.20008. http://dx.doi.org/10.1016/0021-8693(74)90150-1.

[LS08] M. Larsen and A. Shalev, Characters of symmetric groups: sharp bounds and applications, *Invent. Math.* **174** (2008), 645–687. MR 2453603. Zbl 1166.20009. http://dx.doi.org/10.1007/s00222-008-0145-7.

[LS09] ———, Word maps and Waring type problems, *J. Amer. Math. Soc.* **22** (2009), 437–466. MR 2476780. Zbl 1206.20014. http://dx.doi.org/10.1090/S0894-0347-08-00615-2.

[LOST10] M. W. Liebeck, E. A. O'Brien, A. Shalev, and P. H. Tiep, The Ore conjecture, *J. Eur. Math. Soc.* (*JEMS*) **12** (2010), 939–1008. MR 2654085. Zbl 1205.20011. http://dx.doi.org/10.4171/JEMS/220.

[LS] M. W. Liebeck and G. M. Seitz, Unipotent and nilpotent classes in simple algebraic groups and Lie algebras, preprint.

[LS99] M. W. Liebeck and A. Shalev, Simple groups, permutation groups, and probability, *J. Amer. Math. Soc.* **12** (1999), 497–520. MR 1639620. Zbl 0916.20003. http://dx.doi.org/10.1090/S0894-0347-99-00288-X.

[LS01] ———, Diameters of finite simple groups: sharp bounds and applications, *Ann. of Math.* **154** (2001), 383–406. MR 1865975. Zbl 1003.20014. http://dx.doi.org/10.2307/3062101.

[LM99] F. Lübeck and G. Malle, $(2,3)$-generation of exceptional groups, *J. London Math. Soc.* **59** (1999), 109–122. MR 1688493. Zbl 0935.20021. http://dx.doi.org/10.1112/S002461079800670X.

[Lus77] G. Lusztig, Irreducible representations of finite classical groups, *Invent. Math.* **43** (1977), 125–175. MR 0463275. Zbl 0372.20033. http://dx.doi.org/10.1007/BF01390002.

[Lus81] ———, Unipotent characters of the symplectic and odd orthogonal groups over a finite field, *Invent. Math.* **64** (1981), 263–296. MR 0629472. Zbl 0477.20023. http://dx.doi.org/10.1007/BF01389170.

[Lus82] G. Lusztig, Unipotent characters of the even orthogonal groups over a finite field, *Trans. Amer. Math. Soc.* **272** (1982), 733–751. MR 0662064. Zbl 0491.20034. http://dx.doi.org/10.2307/1998725.

[Lus84] ———, *Characters of Reductive Groups over a Finite Field*, *Ann. of Math. Stud.* **107**, Princeton Univ. Press, Princeton, NJ, 1984. MR 0742472. Zbl 0556.20033.

[MM99] G. Malle and B. H. Matzat, *Inverse Galois Theory*, *Springer Monogr. Math.*, Springer-Verlag, New York, 1999. MR 1711577. Zbl 0940.12001.

[MSW94] G. Malle, J. Saxl, and T. Weigel, Generation of classical groups, *Geom. Dedicata* **49** (1994), 85–116. MR 1261575. Zbl 0832.20029. http://dx.doi.org/10.1007/BF01263536.

[MZ96] C. Martinez and E. Zelmanov, Products of powers in finite simple groups, *Israel J. Math.* **96** (1996), 469–479. MR 1433702. Zbl 0890.20013. http://dx.doi.org/10.1007/BF02937318.

[Nat96] M. B. Nathanson, *Additive Number Theory*: *The Classical Bases*, *Grad. Texts in Math.* **164**, Springer-Verlag, New York, 1996. MR 1395371. Zbl 0859.11003.

[NP11] N. Nikolov and L. Pyber, Product decompositions of quasirandom groups and a Jordan type theorem, *J. Euro. Math. Soc.* **13** (2011), 1063–1077. MR 2115666. Zbl pre05919471. http://dx.doi.org/10.4171/JEMS/275.

[SW97] J. Saxl and J. S. Wilson, A note on powers in simple groups, *Math. Proc. Cambridge Philos. Soc.* **122** (1997), 91–94. MR 1443588. Zbl 0890.20014. http://dx.doi.org/10.1017/S030500419600165X.

[Sha08] A. Shalev, Mixing and generation in simple groups, *J. Algebra* **319** (2008), 3075–3086. MR 2397424. Zbl 1146.20057. http://dx.doi.org/10.1016/j.jalgebra.2007.07.031.

[Sha09] ———, Word maps, conjugacy classes, and a noncommutative Waring-type theorem, *Ann. of Math.* **170** (2009), 1383–1416. MR 2600876. Zbl 1203.20013. http://dx.doi.org/10.4007/annals.2009.170.1383.

[Ste51] R. Steinberg, A geometric approach to the representations of the full linear group over a Galois field, *Trans. Amer. Math. Soc.* **71** (1951), 274–282. MR 0043784. Zbl 0045.30201. http://dx.doi.org/10.2307/1990691.

[Ste65] ———, Regular elements of semisimple algebraic groups, *Inst. Hautes Études Sci. Publ. Math.* (1965), 49–80. MR 0180554. Zbl 0136.30002. Available at http://www.numdam.org/item?id=PMIHES_1965__25__49_0.

[TZ96] P. H. Tiep and A. E. Zalesskii, Minimal characters of the finite classical groups, *Comm. Algebra* **24** (1996), 2093–2167. MR 1386030. Zbl 0901.20031. http://dx.doi.org/10.1080/00927879608825690.

[TZ05] ———, Real conjugacy classes in algebraic groups and finite groups of Lie type, *J. Group Theory* **8** (2005), 291–315. MR 2137972. Zbl 1076.20033. http://dx.doi.org/10.1515/jgth.2005.8.3.291.

[Var07] Y. Varshavsky, Lefschetz-Verdier trace formula and a generalization of a theorem of Fujiwara, *Geom. Funct. Anal.* **17** (2007),

271–319. MR 2306659. Zbl 1131.14019. http://dx.doi.org/10.1007/s00039-007-0596-9.

[Wil96] J. Wilson, First-order group theory, in *Infinite Groups* 1994 (Ravello), de Gruyter, Berlin, 1996, pp. 301–314. MR 1477188. Zbl 0866.20001.

(Received: February 10, 2010)
(Revised: June 21, 2010)

Indiana University, Bloomington, IN
E-mail: larsen@math.indiana.edu

Einstein Institute of Mathematics, Hebrew University, Givat Ram, Jerusalem, Israel
E-mail: shalev@math.huji.ac.il

University of Arizona, Tucson, AZ
E-mail: tiep@math.arizona.edu