Character degrees and random walks in finite groups of Lie type

Martin W. Liebeck
Department of Mathematics
Imperial College
London SW7 2BZ
England

Aner Shalev
Institute of Mathematics
Hebrew University
Jerusalem 91904
Israel

Abstract

For a finite group H, let $Irr(H)$ denote the set of irreducible characters of H, and define the 'zeta function' $\zeta^H(t) = \sum_{\chi \in Irr(H)} \chi(1)^{-t}$ for real $t > 0$. We study the asymptotic behaviour of $\zeta^H(t)$ for finite simple groups H of Lie type, and also of a corresponding zeta function defined in terms of conjugacy classes. Applications are given to the study of random walks on simple groups, and on base sizes of primitive permutation groups.

1 Introduction

In this paper we prove some mainly asymptotic results concerning the irreducible character degrees of finite groups of Lie type. Applications are given to the study of the mixing time of random walks on these groups, with certain conjugacy classes as generating sets. In various situations we show that the mixing time is 2; this seems to be the first determination of an exact bounded mixing time for random walks in groups of Lie type.

We also prove some 'dual' results concerning conjugacy class sizes in simple groups of Lie type, with an application concerning base sizes of primitive actions of simple groups. More specifically, we show that, with some prescribed exceptions, the base size is at most 3, thus providing a best possible bound in a conjecture of Cameron.

One of our main focuses is on a 'zeta function' encoding the character degrees, defined as follows. For a finite group H, let $Irr(H)$ denote the set of irreducible complex characters of H, and for real $t > 0$, define

$$\zeta^H(t) = \sum_{\chi \in Irr(H)} \chi(1)^{-t}.$$

The second author acknowledges the support of an EPSRC grant and a Bi-National Science Foundation United States-Israel grant 2000-053

This function, occurs naturally in several contexts. For example, $\zeta^H(t)$ is studied for H simple in [31, 32], and used there in the proofs of various results on Fuchsian groups, coverings of Riemann surfaces, subgroup growth, random walks and representation varieties. The study of the so-called representation growth of certain infinite groups K involves the same zeta function. More specifically, for a positive integer n define $r_n(K)$ to be the number of irreducible characters of K of degree n; then $\zeta^K(t) = \sum_{n\geq 1} r_n(K)n^{-t}$. See [1, 33, 23] for some recent results on $r_n(K)$ and ζ^K. We remark also that for K a compact Lie group, the zeta function ζ^K plays a major role in various geometric questions, as shown for example by Witten in [44, (4.72)].

Here we take this study further, proving various results concerning the asymptotic behaviour of $\zeta^H(t)$ for H a finite group of Lie type. It is shown in [32] that, if $t > 1$ and H is a finite simple group, then $\zeta^H(t) \to 1$ as $|H| \to \infty$. Here we prove more refined results, depending on the type of H, which are essential for various applications.

We begin with the case where the rank of H is bounded. Recall that the *Coxeter number* h of a simple algebraic group G is defined by $h + 1 = \dim G/\mathrm{rank}(G)$.

Theorem 1.1 *Fix a (possibly twisted) Lie type L, and let h be the Coxeter number of the corresponding simple algebraic group. Denote by $L(q)$ a finite quasisimple group of type L over $\mathbb{F}_q$. Then for any fixed real number $t > \frac{2}{h}$, we have*

$$\zeta^{L(q)}(t) \to 1 \text{ as } q \to \infty.$$

Moroever, for $t < \frac{2}{h}$, we have $\zeta^{L(q)}(t) \to \infty$.

When $t = \frac{2}{h}$, it can be shown that $\zeta^{L(q)}(t)$ is bounded away from 1 and ∞.

For unbounded ranks, we prove the following.

Theorem 1.2 *Fix a real number $t > 0$. Then there is an integer $r(t)$ such that for quasisimple groups $L = L(q)$ of rank $r \geq r(t)$, we have*

$$\zeta^L(t) \to 1 \text{ as } |L| \to \infty.$$

A similar result for alternating and symmetric groups was proved in [31], following earlier work of Lulov [36] for the case $t = 1$. Combining this with Theorem 1.1, we obtain

Corollary 1.3 *Let H be a finite simple group different from $L_2(q), L_3(q)$ or $U_3(q)$. Then for $t > \frac{1}{2}$, we have*

$$\zeta^H(t) \to 1 \text{ as } |H| \to \infty.$$

Another immediate application of the above results (and their proofs) concerns the representation growth of finite simple groups, that is, the growth of the function $r_n(H)$.

Corollary 1.4 (i) *For a fixed Lie type L, with Coxeter number h, there is a constant $c = c(L)$ such that*

$$r_n(L(q)) < cn^{\frac{2}{h}} \text{ for all } q.$$

Moreover, the exponent $\frac{2}{h}$ is best possible.

(ii) *Given any $\epsilon > 0$, there exists $r = r(\epsilon)$, such that if H is either an alternating group of degree at least r, or a classical group of rank at least r, then*

$$r_n(H) < n^{\epsilon} \text{ for all } n.$$

(iii) *There is an absolute constant c such that for any finite simple group H different from $L_2(q), L_3(q)$ or $U_3(q)$, we have $r_n(H) < c\sqrt{n}$.*

For a finite group H, define

$$Deg(H) = \{\chi(1) \,:\, \chi \in Irr(H)\},$$

the set of degrees of irreducible characters of H. This set has been much studied, see for example [22, Chap. 12]. We make the following contributions for simple groups H of Lie type, regarding the cardinality and structure of the set $Deg(H)$.

For a (possibly twisted) Lie type L, not ${}^2B_2$, ${}^2G_2$ or ${}^2F_4$, define the rank $r = r(L)$ to be the untwisted Lie rank of L (that is, the rank of the ambient simple algebraic group); and for L of type ${}^2B_2$, ${}^2G_2$ or ${}^2F_4$, define $r(L) = 1, 1, 2$ respectively.

Theorem 1.5 *Fix a Lie type L of rank r, and for each q let $L(q)$ denote a quasisimple group of type L over $\mathbb{F}_q$. There is a function $d(r)$ of r alone such that*

$$|Deg(L(q))| < d(r) \text{ for all } q.$$

Moreover, the function $d(r) = c^{r^{5/6}(\log r)^{1/3}}$ will do, where c is an absolute constant.

We remark that the fact that $|Deg(L(q))|$ is bounded by a function of r alone follows quickly from Deligne-Lusztig theory - specifically, from Lemmas 2.1 and 2.2 below, which easily yield $|Deg(L(q)| < c^{r\log r}$. However more work is required to provide the subexponential bound in Theorem 1.5.

It is known that the number of irreducible characters of $L(q)$ is $k(L(q)) \sim q^r$ (see Proposition 3.1). On the other hand Theorem 1.5 shows that the number of irreducible character degrees of $L(q)$ is at most $c^{r^{5/6}(\log r)^{1/3}}$. Thus

$$\frac{k(L(q))}{|Deg(L(q))|} \to \infty \text{ as } |L(q)| \to \infty,$$

and so the pigeonhole principle shows that as $|L(q)| \to \infty$ we obtain unboundedly many characters of the same degree. In other words we have

Corollary 1.6 *There is a function g such that if H is a finite simple group of Lie type such that $r_n(H) \leq b$ for all n, then $|H| \leq g(b)$.*

It would be interesting to know whether the same result holds for alternating groups.

For finite soluble groups H, the conclusion of Corollary 1.6 was proved by Jaikin [24].

Our next result deals with the structure of the set $Deg(L(q))$ when L is a fixed Lie type and q varies; it shows, roughly speaking, that the character degrees, as well as the multiplicity of each degree, are given by polynomials in q.

Theorem 1.7 *Fix a Lie type L of rank r, and for each q let $L(q)$ denote a quasisimple group of type L over $\mathbb{F}_q$. There are functions $d = d(r)$, $e = e(r)$ of r such that the following hold.*

(i) *There are polynomials $f_1(x), \dots, f_d(x) \in \mathbb{Q}[x]$ such that for all q,*

$$Deg(L(q)) \subseteq \{f_1(q), \dots, f_d(q)\}.$$

(ii) *For $1 \leq i \leq d$, there are polynomials $g_{i1}(x), \dots, g_{ie}(x) \in \mathbb{Q}[x]$ such that for all q,*

$$|\{\chi \in Irr(L(q)) \,:\, \chi(1) = f_i(q)\}| \in \{g_{i1}(q), \dots, g_{ie}(q)\}.$$

(iii) *For each q, there exist $j_i \in \{1, \dots, e\}$ for $1 \leq i \leq d$, such that*

$$\zeta^{L(q)}(t) = \sum_{1 \leq i \leq d} f_i(q)^{-t} g_{ij_i}(q)$$

for any real t. Hence $\zeta^{L(q)}$ is given by boundedly many such "rational" expressions in q.

The conclusions hold for the functions $d(r) = c^{r^{5/6}(\log r)^{1/3}}$ and $e(r) = 2^{c\sqrt{r \log r}}$, where c is an absolute constant.

Theorems 1.1 and 1.2 can be applied to the study of random walks on simple groups of Lie type. Let S be a generating set of a finite group G with $S = S^{-1}$, and consider the random walk on the corresponding Cayley graph $\Gamma(G, S)$ starting at the identity, and at each step moving from a vertex $g \in G$ to a neighbour gs, where $s \in S$ is chosen at random. Let $P^t(g)$ be the probability of reaching the vertex g after t steps.

In recent years there has been much work on understanding the distribution P^t as t gets larger, and its relation to the uniform distribution on G. See Diaconis [10, 11] for background. The *mixing time* of the random walk is the smallest integer t such that

$$||P^t - U||_1 < \frac{1}{e}$$

where $||f||_1 = \sum |f(x)|$ is the l_1-norm. Much attention has focussed on the mixing time in the case where $G = S_n$ and S is a conjugacy class of G. For example, [12] deals with transpositions, [36] with cycle-shapes (m^a) for fixed m, and [37] with arbitrary classes of permutations having at least ϵn fixed points (ϵ a positive constant).

Less in known about random walks on simple groups of Lie type, though some results have been obtained, see [17, 20, 29]. Here we focus on the case $G = L$, a simple group of Lie type, and $S = x^L \cup (x^{-1})^L$, a union of one or two conjugacy classes of L. In this case we denote the mixing time for the random walk on $\Gamma(L, S)$ by $T(L, x)$.

Recall that an element x of a group of Lie type is called regular if its centralizer in the corresponding simple algebraic group G is of minimal dimension, namely rank(G). For example, the regular elements of SL_n are those which have a single Jordan block for each eigenvalue. See [40, Chapter III] for a detailed discussion.

Theorem 1.8 *Let $L \neq L_2(q)$ be a simple group of Lie type and let x be a regular element of L. Then for $|L|$ sufficiently large, the mixing time $T(L, x) = 2$.*

For $L = L_2(q)$, our proof shows that $T(L, x) = 2$ unless q is odd and $x \in L$ is a transvection, in which case $T(L, x)$ is at most 3.

Our methods also yield results on mixing times for more general classes. One such result is the following.

Theorem 1.9 *Let $L = L(q)$ be a simple group of Lie type over $\mathbb{F}_q$ and fix $\epsilon > 0$ and an integer $k \geq 2$. Then there is a function $r = r(\epsilon)$ such that if L has rank at least r, and $x \in L$ satisfies $|C_L(x)| < cq^{4r(1-\frac{1}{k}-\epsilon)}$, then the mixing time $T(L, x)$ is at most k.*

In particular, if $|C_L(x)| < cq^{(2-\epsilon)r}$ and r is sufficiently large, then the mixing time $T(L, x) = 2$.

This greatly improves Theorem 1.13 in [29], which shows only that there exists a function f such that $|C_L(x)| < q^{(2-\epsilon)r}$ implies $T(L,x) \leq f(\epsilon)$.

Another such result for exceptional groups is given in Proposition 6.3.

These appear to be the first results giving exact bounded mixing times for random walks on finite groups of Lie type.

Though our main focus is the character theoretic function $\zeta^H(t)$ and its application above, it is also of interest to consider a corresponding function defined in terms of conjugacy classes. For a finite group H, let $\mathcal{C}(H)$ be the set of conjugacy classes of H, and for real t define

$$\eta^H(t) = \sum_{C \in \mathcal{C}(H)} |C|^{-t}.$$

If $c_n(H)$ denotes the number of conjugacy classes of H of size n, then $\eta^H(t) = \sum_{n \geq 1} c_n(H) n^{-t}$. We shall establish analogues of some of the above results for η^H in the case where H is simple. See Section 5 for statements. One such result is the following analogue of Theorems 1.1 and 1.2.

Theorem 1.10 *Fix a Lie type L, and let h_L be the Coxeter number of the corresponding simple algebraic group. For each q denote by $L(q)$ the finite simple group of type L over $\mathbb{F}_q$, and let $H(q)$ be an almost simple group lying between $L(q)$ and* $\mathrm{Inndiag}(L(q))$*, the group generated by all inner and diagonal automorphisms of $L(q)$.*

(i) *For a fixed Lie type L, and for any fixed real number $t > \frac{1}{h_L}$, we have*

$$\eta^{H(q)}(t) \to 1 \text{ as } q \to \infty.$$

Moroever, for $t < \frac{1}{h_L}$, we have $\eta^{L(q)}(t) \to \infty$.

(ii) *Fix a real number $t > 0$. Then there is an integer $r(t)$ such that for almost simple groups $H = H(q)$ of rank $r \geq r(t)$, we have*

$$\eta^H(t) \to 1 \text{ as } |H| \to \infty.$$

Combining this result with a theorem of Burness [2], we shall prove a sharp form of a conjecture of Cameron and Kantor concerning bases of almost simple primitive permutation groups. Recall that given a permutation group H on a set Ω, a *base* for H is a sequence of points $\omega_1, \ldots, \omega_b \in \Omega$ such that only the identity element of H fixes $\omega_1, \ldots, \omega_b$. The *base size* $b(H)$ of H is defined to be the minimal size of a base for H. This notion has been studied for more than a century, in various contexts, such as bounding the size of primitive groups, computational group theory, and others. See [30] and the references therein for more background.

In 1990 Cameron [4] conjectured that, with some obvious prescribed exceptions, primitive almost simple groups H have bounded base size. Cameron and Kantor [5] then made an even stronger conjecture, that for some absolute constant c, a random choice of c points in the permutation domain provides a base for such a group H with probability tending to 1 as $|H| \to \infty$, and proved it for $H = A_n, S_n$ with $c = 2$. The Cameron-Kantor conjecture has been proved in [28] with an unspecified constant c. Excluding certain low-rank groups, we can now prove the conjecture for groups of Lie type with the best possible bound, namely 3:

Theorem 1.11 *Let H be a finite almost simple group having socle a classical group with natural module of dimension greater than* 15*. Suppose H acts primitively on a set Ω in a non-subspace action. Then the probability that three randomly chosen points in Ω form a base for H tends to* 1 *as $|H| \to \infty$. In particular, for H sufficiently large we have $b(H) \leq 3$.*

See Section 7 for the exact definition of a subspace action. Since there are infinitely many non-subspace actions for which $|H_\alpha| > |H|^{1/2}$ (e.g. $Sp_{2n}(q)$ acting on the cosets of $Sp_n(q) \wr C_2$), the number 3 in this result is indeed best possible.

More detailed results about base sizes for primitive actions of groups of Lie type, including the low rank cases excluded in Theorem 1.11, will appear in a forthcoming paper [3].

The layout of this paper is as follows. In Section 2 we prove Theorem 1.1, and Theorem 1.2 is proved in Section 3. Section 4 is devoted to the proof of Theorems 1.5 and 1.7. In Section 5 we study conjugacy class sizes and prove various results including Theorem 1.10. Section 6 then deals with applications to random walks, providing proofs of Theorems 1.8 and 1.9. Section 7 is devoted to applications to base size and the proof of Theorem 1.11.

2 Groups of bounded rank

In this section we prove Theorem 1.1. In the proof we may assume that $L(q)$ is of universal type - that is, $L(q) = G_\sigma$ where G is a simply connected simple algebraic group over $\bar{\mathbb{F}}_p$, and σ is a Frobenius morphism of G. Write r for the rank of $L(q)$, and set $W = W(G)$, the Weyl group of G.

We shall make extensive use of the Deligne-Lusztig theory of irreducible characters of $L(q)$, as expounded in [13, 34, 35]. We summarise the main points very briefly. For convenience we exclude the cases where G_σ is a Suzuki or Ree group (of type ${}^2B_2$, ${}^2G_2$ or ${}^2F_4$) from the discussion for the time being, and prove the theorem for these cases separately. Let (G^*, σ^*) be dual to (G, σ), as defined in [13, 13.10]; so in particular, G^* is adjoint, and of the same type as G, except that if $G = B_n$ then $G^* = C_n$ and vice versa. The irreducible characters of G_σ are partitioned into Lusztig series $\mathcal{E}(G_\sigma,(s))$, where (s) ranges over the conjugacy classes of semisimple elements s of $G^*_{\sigma^*}$. The characters in $\mathcal{E}(G_\sigma,(s))$ are the irreducible characters which occur as a constituent of some Deligne-Lusztig character $R_T^G(\theta)$, where (T,θ) corresponds to (s) via the correspondence given by [13, 13.12].

The characters in $\mathcal{E}(G_\sigma,(1))$ are called unipotent characters. There is a bijection ψ_s from $\mathcal{E}(G_\sigma,(s))$ to the set of unipotent characters of the centralizer $C_{G^*}(s)_{\sigma^*}$, and the degree of any character $\chi\in\mathcal{E}(G_\sigma,(s))$ is given by the formula

$$\chi(1)=|G^*_{\sigma^*}\,:\,C_{G^*}(s)_{\sigma^*}|_{p'}\cdot(\psi_s(\chi))(1). \qquad (1)$$

Lemma 2.1 *For any class (s) as above, we have*

$$|\mathcal{E}(G_\sigma,(s))|\le|W|^2.$$

Proof By [13, 13.13], the number of pairs (T,θ) corresponding to (s), as in the definition of $\mathcal{E}(G_\sigma,(s))$ above, is bounded above by the number of $G^*_{\sigma^*}$-classes of σ^*-stable maximal tori in $C_{G^*}(s)$, hence by $|W|$ (see [13, 3.23]). Also, by [13, 11.15], the number of irreducible constituents of a Deligne-Lusztig character $R_T^G(\theta)$ is at most $|W|$. The conclusion follows. ∎

Lemma 2.2 (i) *If $s\in G^*_{\sigma^*}$ is a semisimple element, then $C_{G^*}(s)$ is a reductive σ^*-stable subgroup of G^* of maximal rank.*

(ii) *If C is a connected reductive σ^*-stable subgroup of G^* of maximal rank, then $|N_{G^*}(C)/C|$ is bounded above by a function of r.*

(iii) *The number of $G^*_{\sigma^*}$-classes of reductive σ^*-stable subgroups of maximal rank is bounded above by a function of r.*

Proof This is well known. Part (i) follows from [40, II,4.1]. To prove (ii), write $N=N_{G^*}(C)$ and let T be a maximal torus in C. If $n\in N$ then T^n is another maximal torus in C, hence $T^n=T^c$ for some $c\in C$. Therefore $nc^{-1}\in N_N(T)$, and it follows that $N=CN_N(T)$, whence N/C is isomorphic to a section of W, establishing (ii). Finally, there are boundedly many G^*-classes of connected reductive maximal rank subgroups (they correspond to W-orbits of subsystems of the root system of G^*); if C lies in such a class, then the number of G_{σ^*}-orbits on the σ^*-stable members of this class is at most N/C, by [40, 2.7]. ∎

Lemma 2.3 *The number of classes (s) (with $s\in G^*_{\sigma^*}$ semisimple), such that $C_{G^*}(s)^0$ has finite centre, is bounded above by a function of r.*

Proof By Lemma 2.2, G^* has boundedly many classes of connected subgroups of maximal rank. Those with finite centre are semisimple, and have centres of order bounded in terms of r. The conclusion follows. ∎

Lemma 2.4 *Fix a reductive σ^*-stable subgroup C of maximal rank in G^*, let $Z = Z(C^0)$, and suppose Z^0 is a torus of rank $k \geq 1$. Write $L = C_{G^*}(Z^0)$, a Levi subgroup of G^*, and denote by N_L (resp. N_G) the number of positive roots in the root system of L' (resp. G). Then there is a constant c depending only on r such that the following hold:*

(i) *the number of semisimple elements $s \in G^*_{\sigma^*}$, such that $C_{G^*}(s) = C$, is at most cq^k;*

(ii) $|G^*_{\sigma^*} : C_{\sigma^*}|_{p'} \geq cq^{N_G - N_L}$.

Proof (i) If $C_{G^*}(s) = C$ then $s \in C^0$, so the number in question is at most $|Z_{\sigma^*}|$. Since $|Z/Z^0|$ is bounded by a function of r, and $|Z^0_{\sigma^*}| \leq (q+1)^k$ (see [38, 2.4]), the conclusion of (i) follows.

(ii) Since $C \leq N_{G^*}(L)$ and $|N_{G^*}(L)/L|$ is bounded, it is enough to bound $|G^*_{\sigma^*} : L_{\sigma^*}|_{p'}$ from below. Denote by Q_L the unipotent radical of the parabolic subgroup with Levi factor L. Then

$$|G^*_{\sigma^*} : L_{\sigma^*}| \sim q^{2 \dim Q_L} = q^{2(N_G - N_L)}$$

(where $\sim$ denotes equality up to a constant depending only on r). Hence

$$|G^*_{\sigma^*} : L_{\sigma^*}|_{p'} \sim |G^*_{\sigma^*} : L_{\sigma^*}| \cdot q^{-(N_G - N_L)} \sim q^{N_G - N_L},$$

as required. ∎

Lemma 2.5 *Denote by $\mathcal{L}_k$ the set of Levi subgroups of G of semisimple rank $r - k$. Then*

$$\max\{\frac{k}{N_G - N_L} : L \in \mathcal{L}_k, 1 \leq k \leq r\} = \frac{r}{N_G}.$$

Proof This amounts to proving that

$$\frac{N_L}{N_G} \leq \frac{k}{r} \text{ for all } L \in \mathcal{L}_{r-k}. \tag{2}$$

For G of exceptional type, verifying (2) is a matter of routine inspection. So assume that G is classical.

If $G = A_r$ then $L' = \prod A_{k_i}$ with $\sum k_i = k$, and

$$N_G = r(r+1)/2, \quad N_L = \sum k_i(k_i+1)/2.$$

Clearly then $N_L \leq k(k+1)/2$, whence $\frac{N_L}{N_G} \leq k(k+1)/r(r+1) \leq k/r$, giving (2).

Likewise, if $G = B_r$ or C_r then $L' = (\prod A_{k_i}) \cdot B_{k_0}$ or $(\prod A_{k_i}) \cdot C_{k_0}$ with $k_0 + \sum k_i = k$. Then $N_L = k_0^2 + \sum k_i(k_i+1)/2 \leq k^2$, so $\frac{N_L}{N_G} \leq k^2/r^2 \leq k/r$. The argument for $G = D_r$ is similar. ∎

Proof of Theorem 1.1

Fix a universal Lie type L, and for a prime power q write $L(q) = G_\sigma$ as above, with G of rank r. Assume $L(q)$ is not of type ${}^2B_2$, ${}^2G_2$ or ${}^2F_4$.

For $0 \le k \le r$ write

$$\mathcal{E}_k = \bigcup \{\mathcal{E}(G_\sigma, (s)) \,:\, Z(C_{G^*}(s)^0)^0 \text{ is a torus of rank } k\},$$

and for $t > 0$ set

$$\Delta_k(t) = \sum_{\chi \in \mathcal{E}_k} \chi(1)^{-t}.$$

Thus

$$\zeta^{L(q)}(t) = \sum_{k=0}^{r} \Delta_k(t). \tag{3}$$

By Lemma 2.3, the number of characters in $\mathcal{E}_0$ is bounded; apart from the trivial character, each has degree at least cq, and it follows that

$$\Delta_0(t) = 1 + O(q^{-t}). \tag{4}$$

For $k \ge 1$, Lemmas 2.1, 2.2 and 2.4(i) show that the number of characters in $\mathcal{E}_k$ is at most $c_1 q^k$, where c_1 depends only on r. By (1) and Lemmas 2.4(ii) and 2.5, these characters have degree at least $cq^{N_G k/r}$. Hence

$$\Delta_k(t) = O(q^{k - \frac{N_G k t}{r}}) = O(q^{k(1 - \frac{N_G t}{r})}).$$

For $t > \frac{r}{N_G}$, it follows that

$$\sum_{k=1}^{r} \Delta_k(t) = O(q^{-\epsilon}) \tag{5}$$

for some $\epsilon > 0$. Finally, observe that $\frac{r}{N_G} = \frac{2}{h-1}$, where h is the Coxeter number of G. Now the conclusion of Theorem 1.1 follows from (3), (4) and (5).

It remains to handle the excluded cases where $L(q)$ is of type ${}^2B_2$, ${}^2G_2$ or ${}^2F_4$. Here the discussion up to and including Lemma 2.1 remains valid. Each of these groups $L(q)$ is self-dual, and a convenient list of their semisimple element classes and centralizers can be found in [9, Section 2]. Hence we obtain the following crude information about the nontrivial irreducible character degrees of these groups, which is easily sufficient for our purposes (c denotes an absolute constant in the table):

$L(q)$	nontrivial irred. character degrees
${}^2B_2(q)$	$\sim q$ of degree $\ge cq^2$
${}^2G_2(q)$	~ 1 of degree $\ge cq^2$, $\sim q$ of degree $\ge cq^3$
${}^2F_4(q)$	~ 1 of degree $\ge cq^9$, $\sim q$ of degree $\ge cq^{11}$, $\sim q^2$ of degree $\ge cq^{12}$

Theorem 1.1 follows for these groups, noting that $\frac{2}{h-1} = \frac{1}{2}, \frac{1}{3}, \frac{1}{6}$ for the respective types.

This completes the proof of Theorem 1.1.

3 Groups of unbounded rank

In this section we prove Theorem 1.2.

We begin with a basic piece of information concerning the number $k(L)$ of conjugacy classes of a group of Lie type L, and also its character degrees. Recall our definition of rank just before the statement of Theorem 1.5.

Proposition 3.1 *There are absolute constants $c, d > 0$ such that for any simple group L of Lie type of rank r over $\mathbb{F}_q$, we have*

(i) *$k(L) < cq^r$, and*

(ii) *$\chi(1) > dq^r$ for any nontrivial irreducible character χ of L.*

Proof Part (i) follows from [26, Theorem 1] for groups of bounded rank, and from [16] for groups of unbounded rank (see also [15, 9.1]). Part (ii) is immediate from [25]. ∎

We now embark on the proof of 1.2. Fix $t > 0$, and let $L = Cl_n(q)$ denote a classical simple group with natural module V of dimension n over $\mathbb{F}_{q^u}$ where $u = 2$ if L is unitary and $u = 1$ otherwise). Let p be the characteristic of $\mathbb{F}_{q^u}$.

We continue to use the Deligne-Lusztig theory outlined in the previous section. As before we can take $L = G_\sigma$ with G a simple algebraic group of simply connected type and σ a Frobenius morphism. Write L^* for the dual group $G^*_{\sigma^*}$.

Lemma 3.2 *Fix a constant $c > 0$. Then there exist $N = N(c)$, and absolute constants d, d', such that for $n \geq N$ the following hold, denoting by (s) a class of semisimple elements in L^*:*

(i) $|\{(s) \,:\, |L^* : C_{L^*}(s)|_{p'} < dq^{cn}\}| < d'q^c$.

(ii) *if s is such that $|L^* : C_{L^*}(s)|_{p'} < dq^{cn}$, then $C_{L^*}(s)$ has a factor of the form $Cl_{n-a}(q)$ with $a \leq 2c$.*

Proof Consider first the case where $L = SL^\epsilon_n(q)$, so $L^* = PGL^\epsilon_n(q)$. Let $s \in L^*$ be semisimple, with preimage $\hat{s} \in GL^\epsilon_n(q)$. Set $K = \bar{\mathbb{F}}_q$, the algebraic closure of $\mathbb{F}_q$, let $\bar{V} = V \otimes K$, and as in [28], define

$$\nu(s) = \min\,\{\dim[\bar{V}, \lambda\hat{s}] \,:\, \lambda \in K^*\}.$$

If $m = \nu(s)$, then

$$C_{GL_n^\epsilon(q)}(\hat{s}) = GL_{n-m}^{\delta}(q^l) \times \prod GL_{n_i}^{\delta_i}(q^{l_i}) \tag{6}$$

for some $l, l_i, n_i, \delta, \delta_i$, where $l(n-m) + \sum l_i n_i = n$ and $n_i \le n - m$ for all i.

Assume now that $|L^* : C_{L^*}(s)|_{p'} < dq^{cn}$, where d is some positive absolute constant. Then it is clear from (6) that for sufficiently large n (in terms of c), we must have $m = \nu(s) < \frac{1}{2}n$. Hence we see that

$$|s^{L^*}|_{p'} = |\hat{s}^{GL_n^\epsilon(q)}|_{p'} \ge |GL_n^\epsilon(q) : GL_{n-m}^\epsilon(q) \times GL_m^\epsilon(q)|_{p'}.$$

The right hand side is at least $d_0 q^{m(n-m)}$ for a suitably chosen constant d_0, and we take the above constant d to be equal to d_0. Hence $q^{m(n-m)} < q^{cn}$, which for sufficiently large n forces $m = \nu(s) \le c$. This means that $\hat{s} = \mathrm{diag}(I_{n-[c]}, s_0)$, where $s_0 \in GL_{[c]}^\epsilon(q)$. Part (ii) follows. Moreover, the number of conjugacy classes of such s is at most $k(GL_{[c]}^\epsilon(q))$, which by Proposition 3.1 is at most $d' q^{[c]}$. This yields the conclusion of (i).

This completes the proof in the case where $L = SL_n^\epsilon(q)$. The proof for symplectic groups is similar, and we give just a sketch. Suppose $L = Sp_n(q)$, so $L^* = SO_{n+1}(q)$. Let $s \in L^*$ be semisimple with $\nu(s) = m$, and assume that $|L^* : C_{L^*}(s)|_{p'} < dq^{cn}$. Here $C_{L^*}(s)$ is of the form $O_a(q) \times O_b(q) \times \prod GL_{m_i}(q^{a_i}) \times \prod GU_{n_i}(q^{b_i})$, where $a + b + 2\sum(a_i m_i + b_i n_i) = n + 1$. Thus for sufficiently large n we have $m < \frac{1}{2}n$ and

$$|L^* : C_{L^*}(s)|_{p'} \ge |L^* : O_{n+1-m}(q) \times O_m(q)|_{p'} > d_0 q^{m(n-m+1)/2}.$$

This forces $m \le 2c$, whence $s = \mathrm{diag}(\pm I_{n-[2c]}, s_0)$ with $s_0 \in O_{[2c]}(q)$. The number of conjugacy classes of such s is at most $d' q^c$, by Proposition 3.1.

The proof for L orthogonal is similar and is left to the reader. ■

Next we prove a refinement of Lemma 2.1, for which we require a preliminary observation.

Lemma 3.3 *There is an absolute constant c_1 such that the number of unipotent characters of L^* is at most $c_1^{\sqrt{n}}$.*

Proof First consider $L^* = PGL_n^\epsilon(q)$. As described in [7, 13.8], the unipotent characters are parametrised by partitions of n, hence their number is $P(n)$, and the conclusion follows. Similarly, for symplectic and orthogonal groups the unipotent characters can be parametrised by certain pairs (α_i), (β_j) of partitions, with $\sum \alpha_i + \sum \beta_j \le n$ (see [7, p.467]), and the conclusion again follows. ■

Lemma 3.4 *Given any $c > 0$, there exist $N = N(c)$, $c_2 = c_2(c)$ and an absolute constant d such that if $n \geq N$ and $s \in L^*$ is a semisimple element satisfying $|L^* : C_{L^*}(s)|_{p'} < dq^{cn}$, then*

$$|\mathcal{E}(G_\sigma, (s))| \leq c_2^{\sqrt{n}}.$$

Proof As explained in Section 2, $|\mathcal{E}(G_\sigma, (s))|$ is equal to the number of unipotent characters of $C_{G^*}(s)_{\sigma^*}$. Write $C = C_{G^*}(s)$. Then $|C/C^0| \leq n$ by [40, II,4.4], and C^0 is connected and reductive. The number of unipotent characters of C_{σ^*} is therefore at most n times the number for $(C^0)_{\sigma^*}$ (see the definition at the top of p.112 of [13]); moreover, by [13, 13.20], $(C^0)_{\sigma^*}$ has the same number of irreducible characters as $((C^0)')_{\sigma^*}$, which is a commuting product of classical groups of dimensions n_i, where $\sum n_i \leq n$. The number of unipotent characters of this product is at most the product of the numbers of unipotent characters of the simple factors (cf. [7, p.380]). Hence by Lemma 3.3, we conclude that

$$|\mathcal{E}(G_\sigma, (s))| \leq \prod_i c_1^{\sqrt{n_i}}.$$

By Lemma 3.2(ii), there exists $N(c)$ such that provided $n \geq N(c)$, some n_i is at least $n - 2c$. Consequently $|\mathcal{E}(G_\sigma, (s))| \leq c_1^{\sqrt{n}} c_1^{2c}$, and the result follows. ∎

Proof of Theorem 1.2

Let $t > 0$, and take $c = 2/t$. Let $N(c)$ and d be as in Lemma 3.4, and take $L = Cl_n(q)$ with $n \geq N(c)$. Define

$$I_1 = \{\chi \in Irr(L), \chi(1) < dq^{cn}\}, \quad I_2 = \{\chi \in Irr(L) \,:\, \chi(1) \geq dq^{cn}\},$$

and write $\zeta^L(t) = \zeta_1(t) + \zeta_2(t)$, where

$$\zeta_1(t) = \sum_{\chi \in I_1} \chi(1)^{-t}, \quad \zeta_2(t) = \sum_{\chi \in I_2} \chi(1)^{-t}.$$

We shall show that $\zeta_1(t) \to 1$ and $\zeta_2(t) \to 0$ as $|L| \to \infty$.

First consider $\zeta_1(t)$. By (1), if $\chi \in I_1$ then $\chi \in \mathcal{E}(G_\sigma, (s))$, where $|L^* : C_{L^*}(s)|_{p'} < dq^{cn}$. The number of such classes (s) is less than $d'q^c$ by Lemma 3.2(i), and for each such (s) we have $|\mathcal{E}(G_\sigma, (s))| \leq c_2(c)^{\sqrt{n}}$ by Lemma 3.4. It follows that

$$|I_1| < d'q^c c_2^{\sqrt{n}}.$$

Since by Proposition 3.1 we have $\chi(1) > c_3 q^{(n-1)/2}$ for all nontrivial $\chi \in Irr(L)$, it follows that

$$\zeta_1(t) \leq 1 + c_4 q^c c_2^{\sqrt{n}} \cdot q^{-t(n-1)/2},$$

and hence, provided n is sufficiently large in terms of t, we have $\zeta_1(t) \to 1$ as $|L| \to \infty$.

Now consider $\zeta_2(t)$. By Proposition 3.1, $|I_2| < c_5 q^n$, so

$$\zeta_2(t) < c_5 q^n \cdot (dq^{cn})^{-t} = c_5 d^{-t} q^n q^{-2n},$$

whence $\zeta_2(t) \to 0$ as $|L| \to \infty$.

This completes the proof of Theorem 1.2.

4 Proof of Theorems 1.5 and 1.7

As usual we can take $L(q) = G_\sigma$ with G a simple algebraic group of simply connected type of rank r, and σ a Frobenius morphism. Write $L^*(q)$ for the dual group $G^*_{\sigma^*}$, and let p be the characteristic of the field $\mathbb{F}_q$.

We begin with a refinement of Lemma 2.2(iii).

Lemma 4.1 (i) *The number of conjugacy classes of subgroups of $L^*(q)$ of the form $C_{L^*(q)}(s)$ with $s \in L^*(q)$ semisimple, is at most $d_1 = c_1^{\sqrt{r \log r}}$ for some absolute constant c_1.*

(ii) *Moreover, there are polynomials $h_1(x), \dots, h_{d_1}(x) \in \mathbb{Q}[x]$ such that $|L^*(q) : C_{L^*(q)}(s)|_{p'} \in \{h_i(q) : 1 \le i \le d_1\}$ for all s, q.*

Proof (i) If the rank r is bounded, this follows from Lemma 2.2(iii), so assume r is unbounded, and in particular $L(q)$ is classical.

Consider first the case where $L^*(q) = PGL_n(q)$. For a semisimple element $s \in L^*(q)$, with preimage $\hat{s} \in GL_n(q)$, we have

$$C_s = C_{GL_n(q)}(\hat{s}) = \prod_{b=1}^{n} D_b,$$

where

$$D_b = \prod_{i=1}^{n} GL_i(q^b)^{n_{ib}},$$

with $n_{ib} \ge 0$ and $\sum ibn_{ib} = n$. Moreover, $C_{L^*(q)}(s)$ contains the image of C_s modulo scalars with index dividing n.

For $1 \le b \le n$, define

$$m_b = \sum_{i=1}^{n} in_{ib}, \tag{7}$$

so that $\sum bm_b = n$. Given m_b, the number of choices for $(n_{ib} : 1 \le i \le n)$ satisfying (7) is $P(m_b)$, the number of partitions of m_b. Hence, given the sequence $(m_b : 1 \le b \le n)$, the number of choices for $(n_{ib} : 1 \le i, b \le n)$ is at most

$$\prod_{b=1}^{n} P(m_b) \le \prod_{b=1}^{n} c^{\sqrt{m_b}} = c^{\sum \sqrt{m_b}} \tag{8}$$

for some absolute constant c.

We now claim that

$$\sum \sqrt{m_b} \le \sqrt{n \log n}. \tag{9}$$

To see this, write $x_b = (bm_b)^{1/2}$, so that $\sum x_b^2 = n$. By the Cauchy-Schwarz inequality, it follows that

$$\sum \sqrt{m_b} = \sum x_b \cdot b^{-1/2} \le (\sum x_b^2)^{1/2} \cdot (\sum_{b \le n} b^{-1})^{1/2}.$$

The harmonic sum $\sum_{b \le n} b^{-1}$ is bounded above by $\log n$, and the claim (9) follows.

Combining (8) with (9), we see that given $(m_b : 1 \le b \le n)$, the number of choices for $(n_{ib} : 1 \le i, b \le n)$ is at most $c^{\sqrt{n \log n}}$. Finally, the number of choices for $(m_b : 1 \le b \le n)$ with $\sum bm_b = n$ is $P(n)$, and hence the total number of choices for the n_{ib} is at most

$$P(n) \cdot c^{\sqrt{n \log n}} < c_1^{\sqrt{n \log n}}.$$

The conclusion of (i) follows for the case $L^*(q) = PGL_n(q)$.

The case where $L^*(q) = Cl_n(q)$ is unitary, symplectic or orthogonal is similar: here $C_{L^*(q)}(s)$ has a subgroup of index dividing n which is the image modulo scalars of

$$C_s = Cl_{a_1}(q^{b_1}) \times Cl_{a_2}(q^{b_2}) \times \prod GL_{m_i}(q^{c_i}) \times \prod GU_{n_j}(q^{d_j}), \tag{10}$$

where for the unitary case $a_1 = a_2 = 0$, $\sum m_i c_i + \sum n_j d_j = n$, and for the symplectic and orthogonal cases, $a_1 b_1 + a_2 b_2 + 2(\sum m_i c_i + \sum n_j d_j) = n$ (see for example [6]). The conclusion of (i) follows arguing as above.

(ii) Fix the type of L. There is a polynomial $l(x) \in \mathbb{Z}[x]$ such that $|L^*(q)|_{p'} = l(q)$ for all q. Moreover, for $s \in L^*(q)$ semisimple, the centralizer $C_{L^*(q)}(s)$ is of the form C_{σ^*}, where C^0 is reductive and $|C/C^0| \le r$; as in (i) the number of possibilities for C up to $L^*(q)$-conjugacy is at most d_1. It follows that there are polynomials $k_1(x), \ldots, k_{d_1}(x) \in \mathbb{Z}[x]$ such that for all q we have

$$\{|C_{L^*(q)}(s)|_{p'} \ : \ s \text{ semisimple}\} \subseteq \{vk_i(q) \ : \ 1 \le i \le d_1,\ 1 \le v \le r\},$$

and moreover for each i, $k_i(q)$ divides $l(q)$ for infinitely many values of q. It follows easily that $k_i(x)$ divides $l(x)$ with quotient $h_i(x) \in \mathbb{Q}[x]$. Since $rd_1 < c_2^{\sqrt{r \log r}}$ for a suitable constant c_2, the conclusion follows. ∎

Lemma 4.2 *Let s be a semisimple element of $L^*(q)$. Then the number of degrees of unipotent characters of $C_{L^*(q)}(s)$ is at most $d_2 = c^{r^{5/6}(\log r)^{1/3}}$, where c is an absolute constant. Moreover, there are polynomials $e_1(x), \ldots, e_{d_2}(x) \in \mathbb{Q}[x]$ such that the set of degrees of unipotent characters of $C_{L^*(q)}(s)$ is contained in $\{e_i(q) : 1 \le i \le d_2\}$ for all q.*

Proof Write $C = C_{G^*}(s)$, so $C_{L^*(q)}(s) = C_{\sigma^*}$. We use some of the information in the proof of Lemma 3.4. We have $|C/C^0| \le r$, and C^0 is reductive. The degrees of unipotent characters of C_{σ^*} are therefore products of those of $(C^0)_{\sigma^*}$ by integers at most r. Moreover, by [13, 13.20], the degrees of unipotent characters of $(C^0)_{\sigma^*}$ are the same as those of $((C^0)')_{\sigma^*}$; writing $(C^0)' = C_1 \ldots C_a$, a product of simple factors, these degrees are products of degrees of unipotent characters of the factors $(\prod_{i\in\Delta} C_i)_{\sigma^*}$ for Δ an orbit of σ^* on the C_i.

The unipotent character degrees of groups of Lie type of rank l over $\mathbb{F}_q$ are given in [7, 13.8]: they are rational polynomials in q, and by Lemma 3.3 there are at most $c_1^{\sqrt{l}}$ of them.

The conclusion follows from the above if the rank r of $L^*(q)$ is bounded, so assume it is unbounded. Thus $L^*(q)$ is classical. As in the previous proof, we begin with the case $L^*(q) = PGL_n(q)$. Here $(C^0)_{\sigma^*}$ is the image modulo scalars of a group of the form $D = \prod GL_{n_i}(q^{l_i})$, where $\sum l_i n_i = n$. Rewrite this as

$$D = \prod_{b=1}^{n}\prod_{i=1}^{n}(GL_i(q^b))^{n_{ib}},$$

where $n_{ib} \ge 0$ and moreover, writing $m_b = \sum_i in_{ib}$, we have $\sum_b bm_b = n$. Set $D_b = \prod_{i=1}^{n}(GL_i(q^b))^{n_{ib}}$, and write $N_u(D_b)$ for the number of disctinct degrees of unipotent characters of D_b, with similar notation for other groups. We have $N_u(GL_i(q^b)) \le d_i = c_1^{\sqrt{i}}$.

We claim first that

$$N_u((GL_i(q^b))^{n_{ib}}) \le c^{m^{2/3}(\log m)^{1/3}}, \text{ where } m = in_{ib}. \tag{11}$$

To see this, set $l = n_{ib}$, and observe that $N_u((GL_i(q^b))^l)$ is the number of distinct products $\chi_1(1)\ldots\chi_l(1)$ of degrees in $N_u(GL_i(q^b))$, which is at most the number of monomials in d_i variables of total degree l. Hence

$$N_u((GL_i(q^b))^l) \le \binom{d_i+l-1}{d_i-1} \le d_i^l = c_1^{\sqrt{i}l} = c_1^{m/\sqrt{i}}.$$

If $i \ge (m/\log m)^{2/3}$, then (11) holds, so suppose $i < (m/\log m)^{2/3}$.

At this point we require some detailed information about the degrees of unipotent characters of $GL_i(q^b)$, taken from [7, 13.8]. Set $Q = q^b$. The degrees of unipotent characters of $GL_i(Q)$ have the form

$$Q^{a_0}\prod_{j=1}^{i}(Q^j-1)^{a_j}, \tag{12}$$

where a_j are integers, $0 \le a_0 < i^2$ and $|a_j| < i$ for $j \ge 1$. It follows that the degrees of unipotent characters of $GL_i(q^b))^l$ also take the form (12), with $0 \le a_0 < li^3$ and $|a_j| < li$ for $j \ge 1$. Hence the number of choices for the latter i-tuple $(a_0, \dots, a_i)$ is at most $li^3 \cdot (2li)^i$. Recalling that $m = li$, we therefore have

$$N_u(GL_i(q^b))^l) \le li^3 \cdot (2li)^i = m^{i+1} \cdot 2^i i^2 < c^{i\log m}$$

for some absolute constant c. This is bounded by $c^{m^{2/3}(\log m)^{1/3}}$ since $i < (m/\log m)^{2/3}$. Thus (11) is proved.

Next we establish

$$N_u(D_b) \le c^{m_b^{5/6}(\log m_b)^{1/3}}. \tag{13}$$

To show this, let $\{i : n_{ib} \ne 0\} = \{i_1, \dots, i_k\}$, where $i_1 < \cdots < i_k$, and for $1 \le j \le k$ let $x_j = i_j n_{i_j b}$. Then $\sum_{j=1}^k x_j = \sum_i in_{ib} = m_b$. By (11),

$$N_u(D_b) \le c^{\sum_j x_j^{2/3}(\log x_j)^{1/3}}.$$

Write $\sum_j x_j^{2/3}(\log x_j)^{1/3} = \Sigma_1 + \Sigma_2$, where

$$\Sigma_1 = \sum_{j\,:\,x_j \le m_b^{1/2}} x_j^{2/3}(\log x_j)^{1/3}, \;\; \Sigma_2 = \sum_{j\,:\,x_j > m_b^{1/2}} x_j^{2/3}(\log x_j)^{1/3}.$$

Since $x_j \ge i_j \ge j$, we have

$$\Sigma_1 \le \sum_{j \le m_b^{1/2}} m_b^{1/3}(\log m_b)^{1/3} \le m_b^{5/6}(\log m_b)^{1/3}.$$

Next,

$$\Sigma_2 \le \sum_j \frac{x_j(\log m_b)^{1/3}}{x_j^{1/3}} \le \frac{(\log m_b)^{1/3}}{m_b^{1/6}}\sum_j x_j \le m_b^{5/6}(\log m_b)^{1/3}.$$

Now (13) follows.

Finally, we show that

$$N_u(D) \le c^{n^{5/6}(\log n)^{1/3}}. \tag{14}$$

Indeed, since $D = \prod_b D_b$, we have $N_u(D) \le c^x$ where

$$x = \sum_{b:m_b>0} m_b^{5/6} (\log m_b)^{1/3}.$$

Set $I = \{b : m_b > 0\}$, and for $b \in I$ let $y_b = bm_b$. Then $\sum y_b = n$ and $x \le \sum (y_b b^{-1})^{5/6} (\log n)^{1/3}$. By the Cauchy-Schwarz inequality,

$$\sum (y_b b^{-1})^{5/6} \le (\sum y_b^{5/3})^{1/2} \cdot (\sum b^{-5/3})^{1/2} \le (n^{5/3})^{1/2} \cdot c_2 = c_2 n^{5/6},$$

where c_2 is an absolute constant. Hence $x \le c_2 n^{5/6} (\log n)^{1/3}$, and (14) follows.

This completes the proof for the case where $L^*(q) = PGL_n(q)$. The proof for the other types is similar, using the centralizer structure given in (10). ■

Lemma 4.3 *Let $h(x)$ be one of the polynomials $h_i(x) \in \mathbb{Q}[x]$ in the conclusion of Lemma 4.1. Then there are polynomials $g_1(x), \dots, g_d(x) \in \mathbb{Q}[x]$, where $d \le cr$ for some absolute constant c, such that for all q,*

$$|\{(s) : |L^*(q) : C_{L^*(q)}(s)|_{p'} = h(q)\}| \in \{g_1(q), \dots, g_d(q)\}.$$

Proof This follows quickly from the results and methods in [8, Section 3]. These show that if we fix a maximal rank subgroup C of $L^*(q)$, then the number of $L^*(q)$-classes of semisimple elements having centralizer conjugate to C is equal to $p_C(q)$, where p_C is a polynomial which depends only on the congruence class of q modulo $c_1 r$, for some absolute constant c_1. Moreover, $|C_{L^*(q)}(s)|_{p'}$ is a product of cyclotomic polynomials in q with an integer at most r; for $q > c_2 r$, two such expressions can be equal only if the corrsponding polynomials are identical.

It follows that for $q > cr$ (c an absolute constant), the expression

$$|\{(s) : |L^*(q) : C_{L^*(q)}(s)|_{p'} = h(q)\}|$$

is a sum of the above polynomials p_C over a fixed collection of maximal rank subgroups C. The result follows. ■

Lemma 4.4 *For every class (s), the number of unipotent characters of $C_{L^*(q)}(s)$ is at most c^r, where c is an absolute constant.*

Proof We adopt the notation of the proof of Lemma 4.2. If the rank r is bounded the result is clear by the argument of the first paragraph of that proof, so assume the rank is unbounded. Begin with the case $L^*(q) = PGL_n(q)$, and take $(C^0)_{\sigma^*}$ to be the image modulo scalars of the group

$$D = \prod GL_{n_i}(q^{l_i}),$$

where $\sum l_i n_i = n$. The number of unipotent characters of $C_{L^*(q)}(s)$ is at most n times the number of unipotent characters of D, which by Lemma 3.3 is at most $\prod_i c_1^{\sqrt{n_i}}$. The conclusion follows for $PGL_n(q)$, and for the other classical groups by a similar argument. ∎

Proof of Theorems 1.5 and 1.7

Theorem 1.5 and part (i) of Theorem 1.7 follow from Lemmas 4.1 and 4.2, using the degree formula (1).

To prove part (ii) of 1.7, let $f(x)$ be one of the polynomials $f_i(x)$ in part (i). If $\chi \in Irr(L(q))$ satisfies $\chi(1) = f(q)$, then by (1),

$$f(q) = \chi(1) = |L^*(q) : C_{L^*(q)}(s)|_{p'} \cdot \chi_u(1),$$

where s is a semisimple element of $L^*(q)$ and χ_u is a unipotent character of $C_{L^*(q)}(s)$. By Lemma 4.1 the first factor is of the form $h_i(q)$ for some $i \le d_1$; and given h_i, the second factor is determined as $f(q)/h_i(q)$. Next, Lemma 4.3 shows that the number of (s) such that $|L^*(q) : C_{L^*(q)}(s)|_{p'} = h_i(q)$ is equal to $g_{j_i}(q)$ for some $j_i \le d$, while by Lemma 4.4, if n_i is the number of χ_u such that $\chi_u(1) = f(q)/h_i(q)$ then $n_i \le c^r$. We conclude that

$$|\{\chi \in Irr(L(q)) \,:\, \chi(1) = f(q)\}| = \sum_{i \le d_1} n_i g_{j_i}(q),$$

which is one of at most c^{rdd_1} polynomials in q. This yields the conclusion of (ii).

Finally, part (iii) of Theorem 1.7 follows immediately from the other parts.

5 Conjugacy classes

In this section we prove various results concerning the function

$$\eta^H(t) = \sum_{C \in \mathcal{C}(H)} |C|^{-t},$$

where H is a finite almost simple group, and $\mathcal{C}(H)$ denotes the set of conjugacy classes of H.

We begin with the proof of Theorem 1.10 stated in the Introduction.

Proof of Theorem 1.10

First we prove part (i) of the theorem. This is quite similar to the proof of Theorem 1.1, and we give just a sketch.

As in the hypothesis let L be a fixed Lie type of rank r with Coxeter number $h = h_L$, and let $L(q)$ be the simple group of type L over $\mathbb{F}_q$. Write

$L(q) = G'_\sigma$, where G is a simple algebraic group and σ a Frobenius morphism. Then the group generated by inner and diagonal automorphisms of $L(q)$ is G_σ. Let $H = H(q)$ satisfy $L(q) \le H(q) \le G_\sigma$.

Consider a class x^H with $x \in G_\sigma$. Write $x = su$ where s and u are commuting semisimple and unipotent elements of G_σ. By Lemma 4.1(i), the number of possibilities for $C = C_H(s)$ up to conjugacy is bounded above by a function $f(r)$ of the rank r. Also the number of unipotent classes of C is bounded above by a function $g(r)$. For $0 \le k \le r$, define $\mathcal{C}_k$ to be the set of semisimple classes s^H such that $Z(C_G(s)^0)^0$ is a torus of rank k, and set

$$\eta_k(t) = \sum_{x=su, s\in\mathcal{C}_k} |x^H|^{-t}.$$

Then $\eta^H(t) = \sum_{k=0}^r \eta_k(t)$.

Since the number of classes in $\mathcal{C}_0$ is bounded by a function $h(r)$ (see Lemma 2.3), and all classes have size at least q, we have

$$1 \le \eta_0(t) \le 1 + h(r)g(r)q^{-t}. \tag{15}$$

For $k \ge 1$, the number of classes s^H in $\mathcal{C}_k$ is at most cq^k (see Lemma 2.4(i)); moreover, $C_{G_\sigma}(s)$ lies in a Levi subgroup L_σ of semisimple rank $r-k$, and $|G_\sigma : L_\sigma| \ge c_1 q^{2(N_G - N_L)}$ (see Lemma 2.4(ii)). Hence, using Lemma 2.5 we have

$$\eta_k(t) \le \sum_{L\in\mathcal{L}_k} \frac{cq^k g(r)}{(c_1 q^{2(N_G-N_L)})^t} = O(q^{k - \frac{2N_G kt}{r}}).$$

Therefore for $t > \frac{r}{2N_G}$, we have

$$\sum_{k=1}^r \eta_k(t) = O(q^{-\epsilon}) \tag{16}$$

for some $\epsilon > 0$. Since $\frac{r}{2N_G} = \frac{1}{h-1}$, the conclusion of Theorem 1.10(i) now follows from (15) and (16).

Now we prove part (ii) of Theorem 1.10. This closely follows the proof of Theorem 1.2, and we give a brief sketch. Write $L = L(q) = Cl_n(q)$, a classical group of dimension n. First, using the argument of Lemma 3.2, we show that the number of semisimple classes s^L of size less than dq^{cn} is at most $d'q^c$, and for every such class, $C_L(s)$ has a factor $Cl_{n-a}(q)$ with $a \le 2c$. Next observe that the number of unipotent classes of L is at most $c^{\sqrt{n}}$ (see [26, 1.4]). Using this we show as in Lemma 3.4 that if $s \in L$ satisfies $|s^L| < dq^{cn}$, then the number of unipotent classes of $C_L(s)$ is at most $c^{\sqrt{n}}$. Now the proof of Theorem 1.10(ii) goes through just as in the argument for 1.2 given after 3.4.

The following two results are obvious consequences of Theorem 1.10.

Corollary 5.1 *Let H be a finite simple group different from $L_2(q), L_3(q)$ or $U_3(q)$. Then for $t > \frac{1}{4}$, we have*

$$\eta^H(t) \to 1 \text{ as } |H| \to \infty.$$

Recall that $c_n(H)$ denotes the number of conjugacy classes of H of size n.

Corollary 5.2 (i) *For a fixed Lie type L, with Coxeter number h, there is a constant $c = c(L)$ such that*

$$c_n(L(q)) < cn^{\frac{1}{h}} \text{ for all } q.$$

Moreover, the exponent $\frac{1}{h}$ is best possible.

(ii) *Given any $\epsilon > 0$, there exists $r = r(\epsilon)$, such that if H is either an alternating group of degree at least r, or a classical group of rank at least r, then*

$$c_n(H) < n^\epsilon \text{ for all } n.$$

(iii) *There is an absolute constant c such that for any finite simple group H different from $L_2(q), L_3(q)$ or $U_3(q)$, we have $c_n(H) < cn^{1/4}$.*

We conclude this section with an analogue for η^H of Theorems 1.5 and 1.7. Denote by $CS(H)$ the set of conjugacy class sizes of a finite group H.

Theorem 5.3 *Fix a Lie type L of rank r, and for each q let $L(q)$ denote a quasisimple group of type L over $\mathbb{F}_q$. There are functions $d = d(r)$, $e = e(r)$ of r alone such that the following hold.*

(i) *$|CS(L(q))| < d(r)$ for all q.*

(ii) *There are polynomials $f_1(x), \ldots, f_d(x) \in \mathbb{Q}[x]$ such that for all q,*

$$CS(L(q)) \subseteq \{f_1(q), \ldots, f_d(q)\}.$$

(iii) *For $1 \le i \le e$, there are polynomials $g_{i1}(x), \ldots, g_{ie}(x) \in \mathbb{Q}[x]$ such that for all q,*

$$|C \in \mathcal{C}(H) \,:\, |C| = f_i(q)\}| \in \{g_{i1}(q), \ldots, g_{ie}(q)\}.$$

(iv) *For each q, there exist $j_i \in \{1, \ldots, e\}$ for $1 \le i \le e$, such that*

$$\eta^{L(q)}(t) = \sum_{1 \le i \le e} f_i(q)^{-t} g_{ij_i}(q)$$

for any real t. Hence $\eta^{L(q)}$ is given by boundedly many such "rational" expressions in q.

The conclusions hold for the functions $d(r) = c^{r^{5/6}(\log r)^{1/3}}$ and $e(r) = 2^{c\sqrt{r \log r}}$, where c is an absolute constant.

Proof The proof follows along the lines of that of Theorem 1.7 given in Section 4. The only changes are as follows. Instead of Lemma 4.2 we need the analogue for classes, stating that the number of unipotent class sizes of $C_{L^*(q)}(s)$ is at most $d_2 = c^{r^{5/6}(\log r)^{1/3}}$, and they are given by at most d_2 polynomials in q; the proof of this is exactly the same as that of 4.2, noting that the unipotent class sizes of $GL_i(Q)$ are of the form (12) with $0 \le a_0 < i^2$ and $|a_j| < i$ for $j \ge 1$. Next, we need a version of Lemma 4.3 of the form

$$|\{(s) : |L^*(q) : C_{L^*(q)}(s)| = h(q)\}| \in \{g_1(q), \ldots, g_d(q)\}.$$

This follows from the proof of 4.3. Finally, instead of 4.4 we need the fact that the number of unipotent classes of $C_{L^*(q)}(s)$ is at most c^r. ■

6 Applications I: Random walks

In this section we prove Theorems 1.8 and 1.9. Consider a random walk on $\Gamma(L, x^L \cup (x^{-1})^L)$ as described in the Introduction, and for $y \in L$ let $P^k(y)$ be the probability of arriving at y after k steps. Let U denote the uniform distribution on L, and let $|| \; ||$ be the l_1 norm. Then the upper bound lemma of Diaconis and Shashahani [12] shows that

$$||P^k - U||^2 \le \sum_{\chi \in Irr(L), \chi \ne 1} |\frac{\chi(x)}{\chi(1)}|^{2k} \chi(1)^2. \tag{17}$$

We shall require information on irreducible characters of small degree of classical groups, taken mainly from [41]. First we identify a collection of irreducible *Weil characters* of certain classical groups.

The group $SL_n(q)$ $(n \ge 3)$ has $q-1$ irreducible Weil characters, denoted $\tau_i \, (0 \le i \le q-2)$. The character τ_0 has degree $(q^n - q)/(q-1)$ and is equal to $\pi - 1$, where π is the permutation character of $SL_n(q)$ on the set of 1-spaces of the natural module. For $i \ge 1$, the character τ_i has degree $(q^n - 1)/(q-1)$ and takes values specified as follows. Let δ be a primitive $(q-1)^{th}$ root of 1 (in $\mathbb{F}_q$ and in $\mathbb{C}$). Then for $g \in SL_n(q)$,

$$\tau_i(g) = \frac{1}{q-1} \sum_{j=0}^{q-2} (\delta^{ij} q^{\dim Ker(g - \delta^j)}),$$

where $Ker(x)$ denotes the kernel of x on the natural module for $SL_n(q)$. This formula is well known, and can be found, for example, as formula (1) in [19].

Next, $SU_n(q)$ $(n \ge 3)$ has $q+1$ irreducible Weil characters ξ_i $(0 \le i \le q)$, with ξ_0 of degree $(q^n + (-1)^n q)/(q+1)$ and ξ_i of degree $(q^n - (-1)^n)/(q+1)$

for $i \geq 1$. If ω denotes a primitive $(q+1)^{th}$ root of 1 (in $\mathbb{F}_{q^2}$ and in $\mathbb{C}$), then for any $g \in SU_n(q)$ and any $i \geq 0$ we have (see [42, 4.1])

$$\xi_i(g) = \frac{(-1)^n}{q+1} \sum_{k=0}^{q} \omega^{ik} (-q)^{\dim Ker(g-\omega^k)}.$$

Finally, the symplectic group $Sp_{2n}(q)$ ($n \geq 2$, q odd) has four irreducible Weil characters $\alpha_1, \alpha_2, \beta_1, \beta_2$, with α_i of degree $(q^n-1)/2$ and β_i of degree $(q^n+1)/2$. We can label the subscripts so that $\alpha_1 + \beta_1 = \rho$, the (Weil) representation of degree q^n that arises from the action of $Sp_{2n}(q)$ on a group of symplectic type of order q^{2n+1} (see [21]). For $g \in Sp_{2n}(q)$, we have $|\rho(g)| = q^{\frac{1}{2}\dim Ker(g-1)}$, $|\rho(gz)| = q^{\frac{1}{2}\dim Ker(g+1)}$, where the kernels are taken on the natural $2n$-dimensional module and z denotes the central involution. It follows that

$$\begin{aligned}\alpha_1(g) &= \tfrac{1}{2}(a.q^{\frac{1}{2}\dim Ker(g-1)} + b.q^{\frac{1}{2}\dim Ker(g+1)}),\\ \beta_1(g) &= \tfrac{1}{2}(a.q^{\frac{1}{2}\dim Ker(g-1)} - b.q^{\frac{1}{2}\dim Ker(g+1)}),\end{aligned}$$

for some complex numbers a, b of modulus 1. Similar formulae hold for the values of α_2, β_2.

Write $\mathcal{W}$ for the collection of all the irreducible Weil characters $\tau_i, \xi_i, \alpha_i, \beta_i$ introduced above.

Lemma 6.1 *Let $L = SL_n^\epsilon(q)$ ($n \geq 3$) or $Sp_{2n}(q)$ ($n \geq 2, q$ odd), and let $\chi \in \mathcal{W}$.*

(i) *Suppose $x \in L$ is a regular element. Then $|\chi(x)| \leq \min(n,q)$ if $L = SL_n^\epsilon(q)$, and $|\chi(x)| \leq q^{1/2}$ if $L = Sp_{2n}(q)$.*

(ii) *There is an absolute constant d such that, if $x \in L$ satisfies $C_L(x) \leq q^{cn}$, then $|\chi(x)| < q^{\sqrt{cn+d}}$.*

Proof (i) First consider x a regular element in $L = SL_n(q)$. Write $x = su$ with s, u commuting semisimple and unipotent elements. For $\lambda \in \mathbb{F}_q^*$ denote by V_λ the λ-eigenspace of s on $V = V_n(q)$. Then u acts as a single Jordan block on each V_λ, and hence $\dim Ker(x-\lambda) \leq 1$ for all $\lambda \in \mathbb{F}_q^*$. Hence $|\tau_i(x)| \leq q$ for all i by the above formulae for the values of τ_i. Moreover, since there are at most n eigen values for s, the same formulae (and the equation $\sum_{j=0}^{q-2} \delta^{ij} = 0$ for $i \neq 0$) easily imply $|\tau_i(x)| \leq n$. A similar argument applies for $L = SU_n(q)$.

For $L = Sp_{2n}(q)$, observe with the above notation that u acts as a single Jordan block on the eigenspaces V_1 and V_{-1}, so $\dim Ker(x \pm 1) \leq 1$ and the conclusion follows from the above formula for the values of α_i, β_i.

(ii) Consider first $L = SL_n(q)$, assume $|C_L(x)| \leq q^{cn}$, and write $x = su$ as above. For $\lambda \in \mathbb{F}_q^*$ again let V_λ be the λ-eigenspace of s on V, and write

$n_\lambda = \dim V_\lambda$. Fix λ and let u act on V_λ with $n_{i\lambda}$ Jordan blocks of size i for $1 \le i \le n_\lambda$. Then

$$\sum_i i n_{i\lambda} = n_\lambda, \quad \sum_i n_{i\lambda} = \dim Ker(x - \lambda) = k_\lambda.$$

By [43, p.34], we have

$$|C_{GL(V_\lambda)}(u)| \sim q^{2\sum_{i<j} i n_{i\lambda} n_{j\lambda} + \sum_i i n_{i\lambda}^2}.$$

Writing f_λ for the exponent of q in the previous line, we have

$$f_\lambda = (\sum_i n_{i\lambda})^2 + \sum_i (i-1) n_{i\lambda}^2 + 2\sum_{i<j} (i-1) n_{i\lambda} n_{j\lambda} \ge (\sum_i n_{i\lambda})^2 = k_\lambda^2.$$

It follows that for some absolute constant $c_1 > 0$ and for all $\lambda \in \mathbb{F}_q^*$ we have

$$q^{cn+1} > |C_L(x)|(q-1) \ge |C_{GL(V_\lambda)}(u)| \ge c_1 q^{k_\lambda^2}.$$

We conclude that there is an absolute constant d such that $cn + d > k_\lambda^2$ for all $\lambda \in \mathbb{F}_q^*$. From the formula for $\chi(x)$, we therefore obtain

$$|\chi(x)| \le \frac{1}{q-1} \sum_{\lambda \in \mathbb{F}_q^*} q^{k_\lambda} < q^{\sqrt{cn+d}},$$

as required.

The proof for $L = SU_n(q)$ is entirely similar. As for $L = Sp_{2n}(q)$, writing $k_\epsilon = \dim Ker(x - \epsilon)$ for $\epsilon = \pm 1$, we can again deduce using [43] that $cn + d > k_1^2, k_{-1}^2$ for some constant d, and the conclusion follows from the above formula for $\chi(x)$. ∎

Proposition 6.2 *Let $L = L(q)$ be a quasisimple group of Lie type over $\mathbb{F}_q$ of rank r and Coxeter number h, and let $1 \ne \chi \in Irr(L)$. Then there is an absolute constant $c > 0$ such that one of the following holds:*

(i) $\chi(1) > max(cq^{3r/2}, cq^{2r-3})$;

(ii) $L/Z(L) = L_{r+1}^\epsilon(q)$ *or* $PSp_{2r}(q)\,(q$ *odd), and* $\chi \in \mathcal{W}$;

(iii) *L, and a lower bound for $\chi(1)$, are as in Table 1 below.*

In particular, assuming that $\chi \notin \mathcal{W}$ and $L/Z(L) \notin \{L_2(q), L_3^\epsilon(q), L_4^\epsilon(q)\}$, we have $\chi(1) > cq^{\alpha r}$, where $\alpha > \frac{h-1}{h-2}$.

Table 1

$L/Z(L)$	$L_2(q)$	$L_3^\epsilon(q)$	$L_4^\epsilon(q)$	$D_4^\epsilon(q)$	$D_5^\epsilon(q)$
$\chi(1) >$	cq	cq^3	cq^4	cq^5	cq^7

Proof For L of exceptional type this follows from [25], and for L classical it follows from the results of [41]. ■

Proof of Theorem 1.8

Let $L = L(q)$ be a simple group of fixed Lie type of rank r over $\mathbb{F}_q$, and let x be a regular element of L. As described above, let P^k denote the probability distribution on L after k steps of the random walk on $\Gamma(L, x^L \cup (x^{-1})^L)$. Then by the upper bound (17),

$$||P^2 - U||^2 \leq \sum_{\chi \in Irr(L), \chi \neq 1} \frac{|\chi(x)|^4}{\chi(1)^2}. \tag{18}$$

Write the sum on the right hand side of (18) as $\Sigma_1 + \Sigma_2$, where

$$\Sigma_1 = \sum_{\chi \in \mathcal{W}} \frac{|\chi(x)|^4}{\chi(1)^2}, \quad \Sigma_2 = \sum_{\chi \notin \mathcal{W}} \frac{|\chi(x)|^4}{\chi(1)^2}$$

(where $\mathcal{W}$ is the empty set for $L \neq L_n^\epsilon(q)$ or $PSp_{2r}(q)$ (q odd)).

If $L = L_n^\epsilon(q)\,(n \geq 3)$ then by Lemma 6.1(i), we have $\Sigma_1 \leq (q+1)n^4/(cq^{n-1})^2$; and if $L = PSp_{2r}(q)\,(r \geq 2)$ with q odd, 6.1(i) gives $\Sigma_1 \leq 4(q^{1/2})^4/(cq^r)^2$. Hence in either case we have

$$\Sigma_1 \to 0 \text{ as } |L| \to \infty. \tag{19}$$

We now consider Σ_2. Assume first that $L \notin \{L_2(q), L_3^\epsilon(q), L_4^\epsilon(q)\}$. As x is a regular element of L, there is a constant c such that $|C_L(x)| < cq^r$. Hence $|\chi(x)| < c_1 q^{r/2}$ for any $\chi \in Irr(L)$, and so

$$\Sigma_2 < c_2 q^{2r} \sum_{\chi \notin \mathcal{W}} \chi(1)^{-2}.$$

By Proposition 6.2, for $\chi \notin \mathcal{W}$ we have $\chi(1) > cq^{\alpha r}$, where $\alpha > \frac{h-1}{h-2}$. Then $q^{2r} < c_3 \chi(1)^{2/\alpha}$, and so

$$\Sigma_2 < c_4 \sum_{\chi \notin \mathcal{W}} \chi(1)^{-2(1-\frac{1}{\alpha})} < c_4 \cdot (\zeta^L(2 - 2/\alpha) - 1).$$

Since $2 - 2/\alpha > 2/(h-1)$, it follows from Theorem 1.1 that

$$\Sigma_2 \to 0 \text{ as } |L| \to \infty. \tag{20}$$

By (19), (20) and (18) we have $||P^2 - U|| \to 0$ as $|L| \to \infty$, and the conclusion of Theorem 1.8 follows for L of fixed Lie type, not $L_n^\epsilon(q)\,(n \leq 4)$.

The case of unbounded rank is covered by Theorem 1.9 proved below, so to complete the proof of 1.8 it only remains to deal with $L = L_n^\epsilon(q)$, $n \leq 4$.

For $L = L_4^\epsilon(q)$, it is easy to see using the Deligne-Lusztig theory described in Section 2 that L has at most cq irreducible characters of degree less than $c'q^4$, and all other irreducible characters have degree at least $c''q^5$. Write $\Sigma_2 = \Sigma_2' + \Sigma_2''$ where

$$\Sigma_2' = \sum_{\chi \notin \mathcal{W}, 1 < \chi(1) < cq^4} \frac{|\chi(x)|^4}{\chi(1)^2}, \;\; \Sigma_2'' = \sum_{\chi(1) > c'q^5} \frac{|\chi(x)|^4}{\chi(1)^2}.$$

As $|\chi(x)| < cq^{3/2}$ and $|Irr(L)| < cq^3$, we have $\Sigma_2' < cq \cdot q^6/q^8$, and $\Sigma_2'' < cq^3 \cdot q^6/q^{10}$. It follows from this and (19) that $||P^2 - U|| \to 0$ as $q \to \infty$.

Next consider $L = L_3^\epsilon(q)$. The full character table of L is given in [39]. From this we deduce that there is a set Δ of at most 9 irreducible characters of L such that $|\chi(x)|$ is bounded for $\chi \in Irr(L) \backslash \Delta$; moreover, for $\chi \in \Delta$ we have $\chi(1) \sim q^3$ and $|\chi(x)| < cq$. It now follows easily from (18) that $||P^2 - U|| \to 0$ as $q \to \infty$.

This completes the proof of Theorem 1.8.

Finally, to justify the remark made after Theorem 1.8 for $L = L_2(q)$, the character table of L is given in [14]. If x is not unipotent, or if q is even, then $|\chi(x)|$ is bounded for all χ, and (18) gives mixing time 2 for large q; and if q is odd and x is unipotent then $|\chi(x)| < cq^{1/2}$ for all χ, and (18) gives mixing time at most 3 for large q.

Proof of Theorem 1.9

Let $L = L(q)$ be a simple classical group of rank r over $\mathbb{F}_q$, fix $\epsilon > 0$ and $k \geq 2$, and let $x \in L$ be such that $|C_L(x)| < cq^{4r(1-\frac{1}{k}-\epsilon)}$. As above, let P^k denote the probability distribution on L after k steps of the random walk on $\Gamma(L, x^L \cup (x^{-1})^L)$. Then by (17),

$$||P^k - U||^2 \leq \Sigma_1 + \Sigma_2, \tag{21}$$

where

$$\Sigma_1 = \sum_{\chi \in \mathcal{W}} \frac{|\chi(x)|^{2k}}{\chi(1)^{2k-2}}, \;\; \Sigma_2 = \sum_{\chi \notin \mathcal{W}} \frac{|\chi(x)|^{2k}}{\chi(1)^{2k-2}}.$$

For $\chi \in \mathcal{W}$, Lemma 6.1 gives $|\chi(x)| < q^{\sqrt{4r+d}}$ for some constant d, while $\chi(1) > cq^r$ by Proposition 3.1. Hence

$$\Sigma_1 < \frac{cq \cdot q^{2k\sqrt{4r+d}}}{q^{r(2k-2)}},$$

which tends to 0 as $|L| \to \infty$ provided r is sufficiently large.

Now consider Σ_2. For a nontrivial irreducible character χ not in $\mathcal{W}$, we have $\chi(1) > c_1 q^{2r-3}$ by Proposition 6.2(i), and hence

$$\chi(1)^{2k-2-\epsilon} > q^{(2r-3)(2k-2-\epsilon)-c_2 k} = q^{4r(k-1)-2r\epsilon-6k+6+3\epsilon-c_2 k} \geq q^{4r(k-1)-2\epsilon r-c_3 k},$$

where c_i are some absolute constants. On the other hand we have

$$|C_L(x)|^k < c^k q^{(4r(1-\frac{1}{k}-\epsilon))k} \leq q^{4k(r-1)-4\epsilon kr+c_4k}.$$

Choose $r \geq (c_3+c_4)/(2\epsilon)$. Then $-4\epsilon kr + c_4k \leq -2\epsilon kr - c_3k \leq -2\epsilon r - c_3k$, and this yields

$$|C_L(x)|^k < \chi(1)^{2k-2-\epsilon}.$$

Since $|\chi(x)|^{2k} \leq |C_L(x)|^k$, it follows that for such r, and for $\chi \notin \mathcal{W}$, we have

$$\frac{|\chi(x)|^{2k}}{\chi(1)^{2k-2}} < \chi(1)^{-\epsilon},$$

and so

$$\Sigma_2 < \sum_{\chi \notin \mathcal{W}} \chi(1)^{-\epsilon} \leq \zeta^L(\epsilon) - 1.$$

We are now in a position to apply Theorem 1.2 and conclude that $\Sigma_2 \to 0$ as $|L| \to \infty$ provided r is sufficiently large. Theorem 1.9 now follows from (21).

We conclude the section with a similar result on mixing times for exceptional groups of Lie type, proved as above using the lower bounds on character degrees given by [25].

Proposition 6.3 *Let $L = L(q)$ be an exceptional simple group of Lie type, and fix $k \geq 2$ and $\epsilon > 0$. Suppose $x \in L$ satisfies $|C_L(x)| < q^{A_k-\epsilon}$, where A_k is defined as follows:*

L	E_8	E_7	E_6^ϵ	F_4	${}^2F_4$	${}^3D_4$	G_2	${}^2G_2$	${}^2B_2$
A_k	$58-\frac{66}{k}$	$34-\frac{41}{k}$	$22-\frac{28}{k}$	$16-\frac{20}{k}$	$11-\frac{13}{k}$	$10-\frac{14}{k}$	$6-\frac{8}{k}$	$4-\frac{5}{k}$	$3-\frac{4}{k}$

Then for sufficiently large q, the mixing time $T(L,x) \leq k$.

Note that A_k is just $2A - (2A+r)/k$ where A is the exponent of q in the bound given by [25].

7 Applications II: Base size

In this section we prove Theorem 1.11. This relies on Theorem 1.10, together with the following result of Burness [2]. To state this we need some notation. Let H be a finite almost simple group with socle H_0, a classical group with natural module V over a field of characteristic p. We say that a maximal subgroup M of H is a *subspace subgroup* if either $M \cap H_0$ is reducible on V, or $M \cap H_0$ is an orthogonal group $SO(V)$ embedded in the symplectic group $H_0 = Sp(V)$ with $p = 2$. A *subspace action* of H is a primitive action of H on a set Ω where a point stabilizer is a subspace subgroup.

Proposition 7.1 ([2]) *Let H be an almost simple classical group as above, with $n = \dim V > 15$, and let M be a maximal subgroup of H which is not a subspace subgroup. Then for any element $x \in H$ of prime order, we have*

$$|x^H \cap M| < |x^H|^{1/2+1/n+1/(n-2)}.$$

This is a consequence of a more general result in [2] which covers all dimensions.

We shall also require the following technical result concerning classes of outer automorphisms of prime order of simple groups of Lie type.

Proposition 7.2 *Let $H = L(q)$ be a simple group of Lie type, and let $x_1, \ldots, x_m$ be a set of representatives of the H-classes of automorphisms of H of prime order not lying in* $\mathrm{Inndiag}(H)$*. Then for any $t > 0$,*

$$\sum_{i=1}^{m} |x_i^H|^{-t} \to 0 \text{ as } |H| \to \infty.$$

Proof Each such automorphism is of one of the following types: field, graph-field and graph automorphisms (see [18, p.60]). The classes of such automorphisms are analysed in detail in [18, Chapter 4]: there are at most $cr \log\log q$ classes (where c is a constant and r is the rank of $L(q)$), and each class has size greater than $c_1 q^r$. Hence

$$\sum_{i=1}^{m} |x_i^H|^{-t} \leq (c_2 r \log\log q) \cdot q^{-rt},$$

which tends to 0 as $|H| \to \infty$. ■

Proof of Theorem 1.11

The argument follows the proof of [28, Theorem 1.3]. Let H be a classical almost simple group of dimension greater than 15 acting primitively on a set Ω in a non-subspace action. For $b \geq 1$, define $Q(H, b)$ to be the probability that a randomly chosen b-tuple of points in Ω is not a base for H. Let P be the set of elements of prime order in H, and x_i ($1 \leq i \leq k$) be representatives of the H-conjugacy classes of elements in P.

The probability that a randomly chosen b-tuple is fixed by an element $x \in H$ is $(\mathrm{fix}(x)/|\Omega|)^b$. This is equal to $(|x^H \cap M|/|x^H|)^b$. Moreover, if a b-tuple is not a base, then it is fixed by some element $x \in P$. Hence

$$Q(H, b) \leq \sum_{x \in P} (|x^H \cap M|/|x^H|)^b = \sum_{i=1}^{k} |x_i^H| \cdot (|x_i^H \cap M|/|x_i^H|)^b.$$

By Proposition 7.1,

$$|x_i^H| \cdot (|x_i^H \cap M|/|x_i^H|)^b \leq |x_i^H|^{1-41b/112}.$$

Together with Proposition 7.2, this yields

$$Q(H,b) \leq \sum_{i=1}^{k} |x_i^H|^{1-41b/112} \leq \eta^H(41b/112 - 1) - 1 + o(1).$$

Thus $Q(H,3) \leq \eta^H(11/112) - 1 + o(1)$. Since $\dim V > 15$ we have $h \geq 14$ (where h is the Coxeter number of H), and so by Theorem 1.10(i), we have $Q(H,3) \to 0$ as $|H| \to \infty$. Theorem 1.11 follows.

References

[1] H. Bass, A. Lubotzky, A.R. Magid and S. Mozes, The proalgebraic completion of rigid groups, *Geom. Ded.* **95** (2002), 19-58.

[2] T.C. Burness, Fixed point ratios in actions of finite classical groups, to appear.

[3] T.C. Burness, M.W. Liebeck and A. Shalev, Base sizes for primitive actions of finite groups of Lie type, to appear.

[4] P.J. Cameron, Some open problems on permutation groups, in *Groups, Combinatorics and Geometry* (eds. M. Liebeck and J. Saxl), LMS Lecture Notes Series **165**, Cambridge University Press, Cambridge, 1992, pp. 340-350.

[5] P.J. Cameron and W.M. Kantor, Random permutations: some group-theoretic aspects, *Combinatorics, Probability and Computing* **2** (1993), 257-262.

[6] R.W. Carter, Centralizers of semisimple elements in the finite classical groups, *Proc. London Math. Soc.* **42** (1981), 1-41.

[7] R.W. Carter, *Finite groups of Lie type: conjugacy classes and complex characters*, Wiley Interscience, 1985.

[8] D.I. Deriziotis, On the number of conjugacy classes in finite groups of Lie type, *Comm. Alg.* **13** (1985), 1019-1045.

[9] D.I. Deriziotis and M.W. Liebeck, Centralizers of semisimple elements in finite twisted groups of Lie type, *J. London Math. Soc.* **31** (1985), 48-54.

[10] P. Diaconis, *Group Representations in Probability and Statistics*, Institute of Mathematical Statistics Lecture Notes - Monograph Series, Vol. 11, 1988.

[11] P. Diaconis, Random walks on groups: characters and geometry, in *Groups St Andrews 2001 in Oxford*, London Math. Soc. Lecture Note Series, Cambridge Univ. Press, to appear.

[12] P. Diaconis and M. Shahshahani, Generating a random permutation with random transpositions, *Z. Wahrscheinlichkeitstheorie Verw. Gebiete* **57** (1981), 159-179.

[13] F. Digne and J. Michel, *Representations of finite gruops of Lie type*, London Math. Soc. Student Texts **21**, Cambridge Univ. Press 1991.

[14] L. Dornhoff, *Group Representation Theory, Part A*, Marcel Dekker, 1971.

[15] J. Fulman and R. Guralnick, Derangements in simple and primitive groups, in *Groups, Combinatorics and Geometry: Durham, 2001* (eds. A. Ivanov, M. Liebeck and J. Saxl), World Scientific, 2003.

[16] J. Fulman and R. Guralnick, The number and sizes of conjugacy classes in finite Chevalley groups with applications to derangements, preprint.

[17] D. Gluck, Characters and random walks on finite classical groups, *Adv. Math.* **129** (1997), 46-72.

[18] D. Gorenstein, R. Lyons and R. Solomon, *The classification of the finite simple groups, Volume 3*, Math. Surveys and Monographs, Vol. 40 , No. 3, American Math. Soc., 1998.

[19] R. Guralnick and P.H. Tiep, Cross characteristic representations of even characteristic symplectic groups, *Trans. Amer. Math. Soc.*, to appear.

[20] M. Hildebrand, Generating random elements in $SL_n(F_q)$ by random transvections, *J. Alg. Combin.* **1** (1992), 133-150.

[21] I.M. Isaacs, Characters of solvable and symplectic groups, *Amer. J. Math.* **95** (1973), 594-635.

[22] I.M. Isaacs, *Character theory of finite groups*, Academic Press, 1976.

[23] A. Jaikin, On the characters of pro-p groups of finite rank, to appear.

[24] A. Jaikin, On some finiteness conditions on characters and conjugacy classes in finite soluble groups, to appear.

[25] V. Landazuri and G.M. Seitz, On the minimal degrees of projective representations of the finite Chevalley groups, *J. Algebra* **32** (1974), 418-443.

[26] M.W. Liebeck and L. Pyber, Upper bounds for the number of conjugacy classes of a finite group, *J. Algebra* **198** (1997), 538-562.

[27] M.W. Liebeck, J. Saxl and G.M. Seitz, Subgroups of maximal rank in finite exceptional groups of Lie type, *Proc. London Math. Soc.* **65** (1992), 297-325.

[28] M.W. Liebeck and A. Shalev, Simple groups, permutation groups, and probability, *J. Amer. Math. Soc.* **12** (1999), 497-520.

[29] M.W. Liebeck and A. Shalev, Diameters of finite simple groups: sharp bounds and applications, *Annals of Math.* **154** (2001), 383–406.

[30] M.W. Liebeck and A. Shalev, Bases of primitive permutation groups, in *Groups, Combinatorics and Geometry: Durham 2001*, eds: Ivanov et al., World Scientific, 2003, pp. 147–154.

[31] M.W. Liebeck and A. Shalev, Fuchsian groups, coverings of Riemann surfaces, subgroup growth, random quotients and random walks, *J. Algebra* **276** (2004), 552-601.

[32] M.W. Liebeck and A. Shalev, Fuchsian groups, finite simple groups and representation varieties, *Invent. Math.*, to appear.

[33] A. Lubotzky and B. Martin, Polynomial representation growth and the congruence subgroup property, to appear.

[34] G. Lusztig, *Characters of reductive groups over a finite field*, Annals of Mathematics Studies **107**, Princeton University Press, 1984.

[35] G. Lusztig, On the representations of reductive groups with disconnected centre. Orbites unipotentes et reprsentations, I, *Astérisque* No. **168** (1988), 10, 157-166.

[36] N. Lulov, Random walks on symmetric groups generated by conjugacy classes, Ph.D. Thesis, Harvard University, 1996.

[37] Y. Roichman, Upper bound on the characters of the symmetric groups, *Invent. Math.* **125** (1996), 451-485.

[38] G.M. Seitz, Root groups for maximal tori in finite groups of Lie type, *Pacific J. Math.* **106** (1983), 153-244.

[39] W.A. Simpson and J.S. Frame, The character tables for $SL(3, q)$, $SU(3, q^2)$, $PSL(3, q)$, $PSU(3, q^2)$, *Canad. J. Math.* **25** (1973), 486-494.

[40] T.A. Springer and R. Steinberg, Conjugacy classes, in: *Seminar on algebraic groups and related topics* (ed. A. Borel et al.), Lecture Notes in Math. 131, Springer, Berlin, 1970, pp. 168-266.

[41] P.H. Tiep and A.E. Zalesskii, Minimal characters of the finite classical groups, *Comm. Algebra* **24** (1996), 2093-2167.

[42] P.H. Tiep and A.E. Zalesskii, Some characterizations of the Weil representations of the symplectic and unitary groups, *J. Algebra* **192** (1997), 130-165.

[43] G. E. Wall, On the conjugacy classes in the unitary, symplectic and orthogonal groups, *J. Austral. Math. Soc.* 3 (1965), 1-62.

[44] E. Witten, On quantum gauge theories in two dimensions, *Comm. Math. Phys.* **141** (1991), 153-209.