Fuchsian groups, finite simple groups and representation varieties

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

Aner Shalev
Institute of Mathematics
Hebrew University
Jerusalem 91904
Israel

Abstract

Let Γ be a Fuchsian group of genus at least 2 (at least 3 if Γ is non-oriented). We study the spaces of homomorphisms from Γ to finite simple groups G, and derive a number of applications concerning random generation and representation varieties.

Precise asymptotic estimates for $|\mathrm{Hom}(\Gamma, G)|$ are given, implying in particular that as the rank of G tends to infinity, this is of the form $|G|^{\mu(\Gamma)+1+o(1)}$, where $\mu(\Gamma)$ is the measure of Γ. We then prove that a randomly chosen homomorphism from Γ to G is surjective with probability tending to 1 as $|G| \to \infty$. Combining our results with Lang-Weil estimates from algebraic geometry, we obtain the dimensions of the representation varieties $\mathrm{Hom}(\Gamma, \bar{G})$, where $\bar{G}$ is $GL_n(K)$ or a simple algebraic group over K, an algebraically closed field of arbitrary characteristic.

A key ingredient of our approach is character theory, involving the study of the 'zeta function' $\zeta^G(s) = \sum \chi(1)^{-s}$, where the sum is over all irreducible complex characters χ of G.

The second author thanks EPSRC for its support and Imperial College for its hospitality while this work was carried out

Contents

1 Introduction

Results on random generation of finite simple groups often amount to saying that randomly chosen homomorphisms from certain infinite groups Γ to finite simple groups G are surjective with probability tending to 1 as $|G| \to \infty$. For example, if Γ is the free group of rank two this is Dixon's conjecture on random generation of simple groups by two elements, which was proved in [6, 16, 27]; if $\Gamma = Z_2 * \mathbb{Z}$ this is the Kantor-Lubotzky conjecture on random generation by an involution and another element proved in [29]; for $\Gamma = \mathrm{PSL}_2(\mathbb{Z})$ this is random $(2,3)$-generation obtained in [28, 14] (assuming G is not of type B_2 or ${}^2B_2$); and for $\Gamma = Z_r * Z_s$ this is random (r,s)-generation, proved in [31] for G classical of large rank and r, s primes (not both 2).

All the groups Γ above are Fuchsian, and it is natural to ask whether results of this type can be obtained in the much more general context of Fuchsian groups. Some positive evidence is provided in [32], where various results on random Fuchsian generation of alternating and symmetric groups are established. In particular, we show in [32, 1.12] that if Γ is a Fuchsian group of genus at least 2 (3 if Γ is non-oriented), and G is an alternating group, then a random homomorphism from Γ to G is surjective with probability tending to 1 as $|G| \to \infty$. One main goal of this paper is to extend this result to all finite simple groups G (see Theorem 1.6 below).

To prove such a result one needs good estimates on $|\mathrm{Hom}(\Gamma, G)|$ and $|\mathrm{Hom}(\Gamma, M)|$ for finite simple groups G and their maximal subgroups M.

Bounds for these numbers are given in terms of a character-theoretic 'zeta function' (see Lemma 3.3), and much of the proof involves analysis of these functions using character theory of finite groups of Lie type. Another ingredient is an estimate for the number of solutions to the equation $x^m = 1$ in finite simple groups (see Section 4). These results seem to have some independent interest.

When $G = G(q)$, a group of Lie type over $\mathbb{F}_q$, the space $\mathrm{Hom}(\Gamma, G(q))$ can essentially be regarded as the set of q-rational points of the representation variety $\mathrm{Hom}(\Gamma, \bar{G})$, where $\bar{G}$ is the simple algebraic group of the same type as G over the algebraic closure of $\mathbb{F}_q$. Combining our results on $|\mathrm{Hom}(\Gamma, G(q))|$ with Lang-Weil estimates for the number of q-rational points in algebraic varieties ([19]), we obtain the dimensions of these representation varieties, solving some open problems initiated in [42] (see 1.8 - 1.11 below).

Recall that a Fuchsian group is a finitely generated non-elementary discrete group of isometries of the hyperbolic plane $\mathbb{H}^2$. By classical work of Fricke and Klein, the orientation-preserving such groups Γ have a presentation of the following form:

(1.1) generators: $a_1, b_1, \ldots, a_g, b_g$ (hyperbolic)
$x_1, \ldots, x_d$ (elliptic)
$y_1, \ldots, y_s$ (parabolic)
$z_1, \ldots, z_t$ (hyperbolic boundary elements)

relations: $x_1^{m_1} = \cdots = x_d^{m_d} = 1,$
$x_1 \cdots x_d\, y_1 \cdots y_s\, z_1 \cdots z_t\, [a_1, b_1] \cdots [a_g, b_g] = 1,$

where $g, d, s, t \geq 0$ and $m_i \geq 2$ for all i. The number g is referred to as the *genus* of Γ. The *measure* $\mu(\Gamma)$ of an orientation-preserving Fuchsian group Γ is defined by

$$\mu(\Gamma) = 2g - 2 + \sum_{i=1}^{d} (1 - \frac{1}{m_i}) + s + t.$$

It is well known that $\mu(\Gamma) > 0$.

We shall also study non-orientation-preserving Fuchsian groups; these have presentations as follows, with $g > 0$:

(1.2) generators: $a_1, \ldots, a_g$
$x_1, \ldots, x_d$
$y_1, \ldots, y_s$
$z_1, \ldots, z_t$

relations: $x_1^{m_1} = \cdots = x_d^{m_d} = 1,$
$x_1 \cdots x_d\, y_1 \cdots y_s\, z_1 \cdots z_t\, a_1^2 \cdots a_g^2 = 1.$

In this case the measure $\mu(\Gamma)$ is defined by

$$\mu(\Gamma) = g - 2 + \sum_{i=1}^{d}(1 - \frac{1}{m_i}) + s + t,$$

and again, $\mu(\Gamma) > 0$.

Note that Γ is a lattice in $PSL_2(\mathbb{R})$, and $\mu(\Gamma) = -\chi(\Gamma)$, where $\chi(\Gamma)$ is the Euler characteristic.

We call Fuchsian groups as in (1.1) *oriented*, and those as in (1.2) *non-oriented*. Define $v = v(\Gamma)$ to be 2 if Γ is oriented and 1 otherwise. Define also $d^* = d^*(\Gamma)$ to be the number of i such that m_i is even.

If $s + t > 0$ then Γ is just a free product of cyclic groups. The most interesting Fuchsian groups are those with $s = t = 0$; these are co-compact (also termed *proper* in [32]) and are the main focus of this paper. Examples include surface groups (where $d = 0$) of genus $g \geq 2$ ($g \geq 3$ in the non-oriented case); note that surface groups of smaller genus are not Fuchsian, and are in fact virtually abelian.

Many of our proofs will depend on the above-mentioned 'zeta function', which seems to have some independent interest. For a finite group G, let $Irr(G)$ denote the set of irreducible complex characters of G, and for real $s > 0$, define

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

For example, $\zeta^G(-2) = |G|$, and $\zeta^G(0) = k(G)$, the number of conjugacy classes of G. The behaviour of $\zeta^G(s)$ for $s > 0$ is significant for many applications: for instance, when G is a symmetric group, this was studied in [36, 41, 32], with applications to random walks, subgroup growth and coverings of Riemann surfaces.

Note that, if $c_n = c_n(G)$ denotes the number of characters of degree n of G, then $\zeta^G(s) = \sum_{n \geq 1} c_n n^{-s}$. A similar function can be defined for certain infinite groups, for which c_n are all finite, and polynomially bounded, in which case $\zeta^G(s)$ converges for all large enough s. For example, this is the case when G is a compact connected semisimple Lie group and we count Lie group representations, as can be quickly deduced from the Weyl dimension formula. In this case the zeta function has great geometric significance, as shown for instance by Witten (see [53, (4.72)]). Note that, for $G = SU(2)$ we have $c_n = 1$ for all n, and so in this case ζ^G coincides with the classical Riemann zeta function.

For our purpose here it is important to understand the asymptotic behaviour of $\zeta^G(s)$ where G is a finite quasisimple group whose order tends to infinity. Recall that G quasisimple means that G is perfect and $G/Z(G)$ is simple. Note that with finitely many exceptions, quasisimple groups are

central factor groups of either double covers of alternating groups, or of finite Chevalley groups of simply connected types (see [10, 6.1.4]).

We show the following.

Theorem 1.1 *Let G be a finite quasisimple group.*

(i) *If $s > 1$, then $\zeta^G(s) \to 1$ as $|G| \to \infty$.*

(ii) *If $s > \frac{2}{3}$ and $G \neq L_2(q)$ or $SL_2(q)$, then $\zeta^G(s) \to 1$ as $|G| \to \infty$.*

The condition $s > 1$ in (i) is sharp: indeed, inspection of the character table of $SL_2(q)$ (see [7, p.228]) shows that $\zeta^{SL_2(q)}(1) \to 2$ and for q odd, $\zeta^{L_2(q)}(1) \to \frac{3}{2}$ as $q \to \infty$, while $\zeta^G(s) \to \infty$ for $s < 1$ for these groups (see Lemma 2.2). Likewise, the condition on s in (ii) is also sharp, since $\zeta^G(2/3) \not\to 1$ for $G = L_3(q)$ or $U_3(q)$. Excluding the latter groups, even sharper results can be obtained. These will appear in [33].

For G alternating, a stronger result holds, namely $\zeta^G(s) \to 1$ as $|G| \to \infty$ for any $s > 0$ (see [32, 2.7]). We show in [33] that this also holds for classical groups of rank tending to infinity.

Note that since the limit points of $\{\zeta^G(1) : G \text{ finite simple}\}$ are 1, $\frac{3}{2}$ and 2, it follows that with the above notation, $c_n(G) < Cn$ for all finite simple groups G, where C is an absolute constant, and sharper results follow for $G \neq L_2(q)$ - see Corollary 2.7.

Theorem 1.1 can be extended to the case where G is a nearly simple group - that is, $F^*(G)$ is quasisimple (see Theorem 2.8).

We shall apply Theorem 1.1 in the study of the space of homomorphisms from Fuchsian groups to finite quasisimple groups. In [41], the authors obtain good estimates for $|\mathrm{Hom}(\Gamma, G)|$ where Γ is a surface group and $G = S_n$. This is extended in [32] to the case where Γ is an arbitrary Fuchsian group and $G = S_n$ or A_n. Hence our focus here is on the case where G is a quasisimple group of Lie type.

For a finite group G and a positive integer m, denote by $j_m(G)$ the number of solutions in G of the equation $x^m = 1$. If Γ is a non co-compact Fuchsian group, then Γ decomposes as a free product of $vg + s + t - 1$ copies of $\mathbb{Z}$ and cyclic groups of orders $m_1, \ldots, m_d$, and hence for any finite group G, we have $|\mathrm{Hom}(\Gamma, G)| = |G|^{vg+s+t-1} \cdot \prod_{i=1}^{d} j_{m_i}(G)$. The following result shows that if G is a finite quasisimple group, a rather similar estimate holds also for co-compact groups (i.e. when $s + t = 0$), provided the genus is not too small. In the statements below, $o(1)$ refers to a quantity which tends to 0 as $|G| \to \infty$.

Theorem 1.2 *Let Γ be a co-compact Fuchsian group as in* (1.1) *or* (1.2)*, and let G be a finite quasisimple group.*

(i) *If* Γ *is oriented of genus* $g \geq 2$*, we have*

$$|\mathrm{Hom}(\Gamma, G)| = (1 + o(1)) \cdot |G|^{2g-1} \cdot \prod_{i=1}^{d} j_{m_i}(G).$$

(ii) *Assume* Γ *is non-oriented of genus* $g \geq 3$*, and* $(G/Z(G), g) \neq (L_2(q), 3)$*. Then*

$$|\mathrm{Hom}(\Gamma, G)| = (1 + o(1)) \cdot |G|^{g-1} \cdot \prod_{i=1}^{d} j_{m_i}(G).$$

(iii) *Assume* Γ *is non-oriented of genus* $g = 3$ *and* $G = L_2(q)$*. Then*

$$|\mathrm{Hom}(\Gamma, G)| = (h + o(1)) \cdot |G|^{2} \cdot \prod_{i=1}^{d} j_{m_i}(G),$$

where $h = 1$ *unless* $(m_i, |G|) = 1$ *for all* i*, in which case* $h = \frac{3}{2}$ *for* q *odd and* $h = 2$ *for* q *even.*

(iv) *Assume* Γ *is non-oriented of genus* $g = 3$ *and* $G = SL_2(q)$ *with* q *odd. Then*

$$|\mathrm{Hom}(\Gamma, G)| = (h + o(1)) \cdot |G|^{2} \cdot \prod_{i=1}^{d} j_{m_i}(G),$$

where $h = 1$ *unless* $d^* > 0$ *and* $(m_i, |G|)$ *is* 1 *or* 2 *for all* i*, in which case* $h = 3 \cdot 2^{d^*-1}$*.*

The anomaly of $L_2(q)$ and $SL_2(q)$ in the theorem is related to their exceptional behaviour in Theorem 1.1 and the remark following. This anomaly is also reflected in subsequent results on representation varieties (see 1.8, 1.11). Note also that in part (iii) we have $h \neq 1$ if and only if all homomorphisms from Γ to $G = L_2(q)$ factor through a non-oriented surface group of genus 3.

Theorem 1.2 takes a particularly simple form when $d = 0$, that is, Γ is a surface group:

Corollary 1.3 *Let* Γ *be a surface group which is not virtually abelian, let* g *be the genus of* Γ*, let* $v = v(\Gamma)$*, and let* G *be a finite quasisimple group. Then*

$$|\mathrm{Hom}(\Gamma, G)| = (h + o(1)) \cdot |G|^{vg-1}$$

where $h = 1$ *unless* $v = 1$*,* $g = 3$ *and* $G = L_2(q)$*, in which case* $h = \frac{3}{2}$ *for* q *odd, and* $h = 2$ *for* q *even.*

In order to use Theorem 1.2 one requires information on the values of $j_m(G)$ for G quasisimple. Such information can be found in [32, 52] for $G = A_n$, in [28, 31] for G classical and m prime, and in [15] for G exceptional and $m \leq 5$. Recently, Lawther [20] has obtained tight estimates for the dimension of the variety $J_m(X) = \{x \in X : x^m = 1\}$, where X is any connected simple algebraic group. Using this we prove the following.

Theorem 1.4 *Let $G = G(q)$ be a finite quasisimple group of Lie type over $\mathbb{F}_q$ of rank r, and let $m \geq 2$ be an integer. Then*

$$j_m(G) = |G|^{1-\frac{1}{m}+\epsilon(r)},$$

where $|\epsilon(r)| = O(r^{-1})$.

We also obtain a number of more detailed estimates of $j_m(G)$ for G of Lie type, including $GL_n(q)$ (see Section 4).

Combining Theorems 1.2 and 1.4 gives the following.

Theorem 1.5 *Let Γ be a Fuchsian group of genus $g \geq 2$ ($g \geq 3$ if G is non-oriented), and let G be a finite classical quasisimple group of rank r. Then*

$$|\mathrm{Hom}(\Gamma, G)| = |G|^{\mu(\Gamma)+1+\delta(r)},$$

where $|\delta(r)| = O(r^{-1})$.

Hence, if G_n is a sequence of finite quasisimple classical groups whose ranks tend to infinity, then

$$\lim_{n\to\infty} \frac{\log|\mathrm{Hom}(\Gamma, G_n)|}{\log|G_n|} = \mu(\Gamma) + 1.$$

This also holds for alternating groups $G_n = A_n$, as shown in [32].

Our main result concerns random Fuchsian generation of finite simple groups, and uses some of the above theorems, as well as various new results on maximal subgroups of finite simple groups presented in Section 5.

Theorem 1.6 *Let Γ be a Fuchsian group of genus $g \geq 2$ ($g \geq 3$ if G is non-oriented), and let G be a finite simple group. Then the probability that a randomly chosen homomorphism in $\mathrm{Hom}(\Gamma, G)$ is an epimorphism tends to 1 as $|G| \to \infty$.*

We make a few remarks concerning the strategy of the proof of Theorem 1.6. If a homomorphism in $\mathrm{Hom}(\Gamma, G)$ is not an epimorphism, then its image lies in a maximal subgroup M of G, and this happens with probability

$\frac{|\mathrm{Hom}(\Gamma,M)|}{|\mathrm{Hom}(\Gamma,G)|}$. Hence the probability that a randomly chosen homomorphism in $\mathrm{Hom}(\Gamma, G)$ is not an epimorphism is bounded above by

$$Q(\Gamma, G) = \sum_{M \ max \ G} \frac{|\mathrm{Hom}(\Gamma, M)|}{|\mathrm{Hom}(\Gamma, G)|}.$$

It therefore suffices to show that $Q(\Gamma, G) \to 0$ as $|G| \to \infty$.

To prove this we need not only lower bounds on $|\mathrm{Hom}(\Gamma, G)|$ provided by Theorem 1.2, but also upper bounds on $|\mathrm{Hom}(\Gamma, M)|$ for all maximal subgroups M of finite simple groups G. The latter are obtained via the inequality

$$|\mathrm{Hom}(\Gamma, M)| \leq |M|^{vg-1} \cdot \prod_{i=1}^{d} j_{m_i}(M) \cdot \zeta^M(vg-2),$$

where $v = v(\Gamma)$ (see Lemma 3.3). To apply this, a painstaking analysis of the function $\zeta^M(s)$ is required, leading to a bound on $\zeta^M(1)$ in terms of the index of M in G (see Theorem 5.1 below). This bound is combined with recent results on maximal subgroups [26] to complete the proof of Theorem 1.6.

Theorem 1.6 is new even for surface groups, where it takes the following form.

Corollary 1.7 *Let Γ be a surface group which is not virtually abelian, and let G be a finite simple group. Then the probability that a randomly chosen homomorphism in $\mathrm{Hom}(\Gamma, G)$ is an epimorphism tends to 1 as $|G| \to \infty$.*

Theorem 1.6 extends [32, 1.12], which yields the conclusion in the case where $G = A_n$. We note that some assumption on the genus is essential, since there are Fuchsian groups of genus 0 or 1 which do not have all large enough finite simple groups as quotients. Examples include triangle groups of genus 0 such as the Hurwitz $(2, 3, 7)$-group (see for example [4]), and genus 1 groups of the form (1.1) with $d = 1$ and m_1 an odd prime (since there are infinitely many finite simple groups containing no element of order m_1).

Still, it would be interesting to find partial extensions of Theorem 1.6 to Fuchsian groups of genus 0 or 1. We propose the following.

Conjecture *For any Fuchsian group Γ there is an integer $f(\Gamma)$, such that if G is a finite simple classical group of rank at least $f(\Gamma)$, then the probability that a randomly chosen homomorphism from Γ to G is an epimorphism tends to 1 as $|G| \to \infty$.*

We can show that the conjecture holds for non co-compact Fuchsian groups. Since the latter are free products of cyclic groups, some cases are

already covered by results mentioned in the first paragraph of this paper; the proof is completed by establishing that the simple groups in question are also randomly (r, s)-generated when r, s are not both prime. This work will appear elsewhere.

The proof of the conjecture for co-compact Fuchsian groups (of small genus) seems to require strong bounds on character ratios $|\chi(x)/\chi(1)|$ for $\chi \in Irr(G)$ and for elements $x \in G$ of given order (see Lemma 3.1 below). Some bounds on these ratios do exist (see for instance [11]), with many interesting applications, but these bounds are not sufficient to settle our conjecture, and substantial refinements will be required.

Finally, we apply our results on $\mathrm{Hom}(\Gamma, G)$ for G finite of Lie type to the study of representation varieties of Γ in reductive algebraic groups over algebraically closed fields. For a Fuchsian group Γ, an algebraically closed field K, and a positive integer n, define

$$R_{n,K}(\Gamma) = \mathrm{Hom}(\Gamma, GL_n(K)).$$

This has a natural structure as an algebraic variety defined over the prime subfield of K, and has been extensively studied in the case where K has characteristic zero and Γ is a surface group (see [35, 42, 3, 12]). However, not much seems to be known in positive characteristic. We make the following contribution.

Theorem 1.8 *Let Γ be a surface group of genus g which is not virtually abelian, and let K be an algebraically closed field of characteristic $p > 0$.*

(i) *If Γ is oriented, then $\dim R_{n,K}(\Gamma) = (2g-1)n^2 + 1$ and $R_{n,K}(\Gamma)$ has a unique irreducible component of highest dimension.*

(ii) *If Γ is non-oriented, then $\dim R_{n,K}(\Gamma) = (g-1)n^2$ and $R_{n,K}(\Gamma)$ has $(2, p-1)$ irreducible components of highest dimension unless $(n, g) = (2, 3)$, in which case it has $(2, p-1) + 1$ such components.*

These dimensions agree with those given for the characteristic zero case in [42] for oriented groups and in [3] for non-oriented groups. In fact it is well known that the dimension of a variety in characteristic zero coincides with the dimension of its reduction modulo p for all large primes p, and so Theorem 1.8 provides an alternative proof of the characteristic zero dimension results in [42, 3].

Our methods extend to give the values of $\dim R_{n,K}(\Gamma)$ for arbitrary Fuchsian groups. We need some notation. For positive integers n and $m_1, \ldots, m_d$, all at least 2, write $n = k_i m_i + l_i$ with $0 \leq l_i < m_i$, and $\mathbf{m} = (m_1, \ldots, m_d)$, and define

$$c(n, \mathbf{m}) = \sum_{i=1}^{d} l_i(1 - \frac{l_i}{m_i}).$$

Note that $c(n, \mathbf{m})$ is bounded in terms of $\mathbf{m}$ only.

Theorem 1.9 *Let Γ be a co-compact Fuchsian group as in* (1.1) *or* (1.2)*, of genus $g \geq 2$ ($g \geq 3$ if Γ is non-oriented). Set $E = \{i : m_i \text{ even }\}$, $\mu = \mu(\Gamma)$, $v = v(\Gamma)$, let $n \geq 2$, and let K be an algebraically closed field of arbitrary characteristic. Then*

$$\dim R_{n,K}(\Gamma) = (\mu + 1)n^2 - c(n, \mathbf{m}) + v - \delta,$$

where $\delta = 1$ unless $v = 2$, $\mathrm{char}(K) \neq 2$, $m_i | n$ for all $i \in E$, and $\sum_{i \in E} \frac{n}{m_i}(m_i + 1)$ is odd, in which case $\delta = 3$.

It follows from the theorem that $\dim R_{n,K}(\Gamma) = (\mu(\Gamma) + 1)n^2 + O(1)$; in particular,

$$\frac{\dim R_{n,K}(\Gamma)}{n^2} \to \mu(\Gamma) + 1 \text{ as } n \to \infty.$$

As suggested in [42], it is of interest to extend these results to representation varieties $\mathrm{Hom}(\Gamma, \bar{G})$ for other algebraic groups $\bar{G}$, the natural focus being on the case where $\bar{G}$ is a connected simple algebraic group. For a positive integer m, define

$$J_m(\bar{G}) = \{x \in \bar{G} : x^m = 1\},$$

Then $J_m(\bar{G})$ is an algebraic variety. Information about its dimension can be found in Section 4 (see Theorem 4.1).

Theorem 1.10 *Let Γ be a Fuchsian group of genus $g \geq 2$ ($g \geq 3$ if Γ is non-oriented), let $v = v(\Gamma)$, and let $\bar{G}$ be a connected simple algebraic group over an algebraically closed field K of arbitrary characteristic. Then*

(i) $\dim \mathrm{Hom}(\Gamma, \bar{G}) = (vg - 1) \dim \bar{G} + \sum_{i=1}^{d} \dim J_{m_i}(\bar{G})$;

(ii) $\frac{\dim \mathrm{Hom}(\Gamma, \bar{G})}{\dim \bar{G}} \to \mu(\Gamma) + 1$ *as* $\dim \bar{G} \to \infty$.

For surface groups we obtain more detailed information. In the statement below, for a simple algebraic group $\bar{G}$ we denote by $\pi_1(\bar{G})$ the fundamental group of $\bar{G}$, that is, the kernel of the canonical map from the simply connected cover of $\bar{G}$ onto $\bar{G}$; and $\pi_1(\bar{G})^2$ denotes the subgroup generated by all squares in $\pi_1(\bar{G})$.

Corollary 1.11 *Let Γ be a non-virtually abelian surface group of genus g, let $v = v(\Gamma)$, and let $\bar{G}$ be a connected simple algebraic group over an algebraically closed field K of arbitrary characteristic.*

(i) *We have* $\dim \mathrm{Hom}(\Gamma, \bar{G}) = (vg - 1) \cdot \dim \bar{G}$.

(ii) *If* Γ *is oriented, then the number of irreducible components of highest dimension in* $\mathrm{Hom}(\Gamma, \bar{G})$ *is equal to* $|\pi_1(\bar{G})|$*; in particular if* $\bar{G}$ *is simply connected, this number is* 1*.*

(iii) *If* Γ *is non-oriented, then the number of irreducible components of highest dimension in* $\mathrm{Hom}(\Gamma, \bar{G})$ *is equal to* $|\pi_1(\bar{G})/\pi_1(\bar{G})^2|$*, except when* $(g, \bar{G}) = (3, PSL_2)$*, in which case the number is* $1 + |\pi_1(\bar{G})/\pi_1(\bar{G})^2|$*.*

It is interesting to note that while results for finite groups are frequently deduced from corresponding results for algebraic groups, in our case the deductions are in the reverse direction.

Finally, we note that when $\bar{G}$ is a compact Lie group and Γ a surface group, the space $\mathrm{Hom}(\Gamma, \bar{G})$ has geometric significance. For example, in [40] its volume is defined and studied using a representation-theoretic formula; this is closely related to Witten's celebrated volume formula for the moduli space of flat $\bar{G}$-connections on the relevant surface [53].

Notation and layout

We shall freely use the notation already introduced, together with the following. We define $\mathcal{F}$ to be the class of all co-compact Fuchsian groups as in (1.1) with $g \geq 2$, or in (1.2) with $g \geq 3$. For functions f, g, we write $f \sim g$ to mean that there are positive absolute constants c_1, c_2 such that $c_1 f \leq g \leq c_2 f$. Finally, if $m_1, \ldots, m_d$ are positive integers and G is a group, then, setting $\mathbf{m} = (m_1, \ldots, m_d)$, we define

$$I_{\mathbf{m}}(G) = \{(g_1, \ldots, g_d) \ : \ g_i \in G,\, g_i^{m_i} = 1, \prod_1^d g_i \in G'\}.$$

The layout of the paper is as follows. In Section 2 we study the function $\zeta^G(s)$ and prove Theorem 1.1. In Section 3 we recall two character-theoretic formulae, essentially dating back to Hurwitz, giving the size of certain homomorphism spaces from a Fuchsian group to a finite group, and use these, together with Theorem 1.1, to prove Theorem 1.2 and various related results. Section 4 is devoted to counting elements of given order in finite classical groups; this is where Theorems 1.4 and 1.5 are established. In Section 5 we study $\zeta^M(s)$ for maximal subgroups M of finite simple groups. The bound on $\zeta^M(1)$ in Theorem 5.1 is one of the main tools in our proof of Theorem 1.6, given in Section 6. Finally, representation varieties are discussed in Section 7, where the results 1.8 - 1.11 are proved.

2 Character degrees

In this section we prove Theorem 1.1 and various related results. For $G = A_n$, it is shown in [32, 2.7] that $\zeta^G(s) \to 1$ as $n \to \infty$ for any $s > 0$. Moreover, for the double cover $\hat{A}_n$, it follows from [49] that every faithful irreducible character of $\hat{A}_n$ has degree at least c_1^n, where $c_1 > 1$ is an absolute constant. Also $k(\hat{A}_n) < c_2^{\sqrt{n}}$ for some absolute constant c_2. Hence for $s > 0$,

$$\sum_{\chi \in Irr(\hat{A}_n)\ faithful} \chi(1)^{-s} < c_2^{\sqrt{n}} c_1^{-sn} \to 0 \text{ as } n \to \infty.$$

This establishes Theorem 1.1 in the case where $G/Z(G) = A_n$. Hence it remains to deal with simple groups of Lie type.

For a finite group G, let $k(G)$ denote the number of conjugacy classes of elements in G. And for a simple group G of Lie type, not of type ${}^2B_2$, ${}^2G_2$ or ${}^2F_4$, define the rank $r = r(G)$ to be the untwisted Lie rank of G (that is, the rank of the ambient simple algebraic group $\bar{G}$); for G of type ${}^2B_2$, ${}^2G_2$ or ${}^2F_4$, define $r(G) = 1, 1, 2$ respectively.

Lemma 2.1 *Let $G = G(q)$ be a quasisimple group of Lie type of rank $r = r(G)$ over $\mathbb{F}_q$. Then there are positive absolute constants c_1, c_2 such that*

(i) *$k(G) < c_1 q^r$, and*

(ii) *$\chi(1) > c_2 q^r$ for any nontrivial irreducible complex character χ of G.*

Proof Part (i) follows from [23, Theorem 1] for groups of bounded rank, and from [9] for groups of unbounded rank (see also [8, 9.1]). Part (ii) is immediate from [18]. ∎

Proof of Theorem 1.1(i) This now follows quickly. By Lemma 2.1, we have

$$\zeta^G(s) \leq 1 + c_1 q^r \cdot (c_2 q^r)^{-s} = 1 + c_3(s) q^{-(s-1)r},$$

which tends to 1 as $|G| \to \infty$, assuming that $s > 1$. This completes the proof of Theorem 1.1(i).

To see that in general the condition $s > 1$ is necessary, we note the following.

Lemma 2.2 (i) *For q odd, $\zeta^{L_2(q)}(1) \to 3/2$ as $q \to \infty$.*

(ii) *$\zeta^{SL_2(q)}(1) \to 2$ as $q \to \infty$.*

(iii) *For $G = L_2(q)$ or $SL_2(q)$ and $s < 1$, we have $\zeta^G(s) \to \infty$ as $q \to \infty$.*

Proof Suppose first that q is odd. From the character table of $SL_2(q)$ given in [7, 38.1], we see that $L_2(q)$ has $\frac{q}{2} + O(1)$ irreducible characters of

degree $q+1$ or $q-1$, and three other nontrivial irreducible characters, all of degree at least $\frac{1}{2}(q-1)$. This yields part (i).

For (ii), observe that by [7, 38.1] (for q odd) and [7, 38.2] (for q even), $SL_2(q)$ has $q+O(1)$ irreducible characters of degree $q\pm 1$, and at most five other nontrivial irreducible characters, all of degree at least $\frac{1}{2}(q-1)$. Part (ii) follows, and (iii) is immediate from the above information. ■

To prove 1.1(ii), we need more detailed information about irreducible characters of small degree of groups of Lie type. First we handle exceptional groups. The following is taken from [18].

Proposition 2.3 *Let $G = G(q)$ be an exceptional quasisimple group of Lie type over $\mathbb{F}_q$, and define $h = h(G)$ as follows:*

G	E_8	E_7	E_6^ϵ	F_4	${}^2F_4$	${}^3D_4$	G_2	${}^2G_2$	${}^2B_2$
h	29	17	11	8	$\frac{11}{2}$	5	3	2	$\frac{3}{2}$

Then there is an absolute constant $c > 0$ such that every nontrivial irreducible character of G has degree greater than cq^h.

We can now deduce the following.

Corollary 2.4 *If G is an exceptional quasisimple group of Lie type and $s > \frac{6}{11}$, then $\zeta^G(s) \to 1$ as $|G| \to \infty$.*

Proof By Proposition 2.3, we have

$$\zeta^G(s) \leq 1 + c_1 q^r \cdot (cq^h)^{-s} = 1 + c_3(s) q^{r-sh}.$$

Note that $\frac{r}{h} \leq \frac{6}{11}$ for all types except ${}^2B_2$, G_2 and ${}^3D_4$, so the result follows, apart from these cases. The irreducible character degrees and their multiplicities for ${}^2B_2(q)$ and ${}^3D_4(q)$ can be found in [47, 5], and for $G_2(q)$ a summary can be found in [43, Appendix]. Inspection of this data shows that $\zeta^G(s) \to 1$ for $s > s_0$, where $s_0 = \frac{1}{2}, \frac{1}{3}, \frac{1}{3}$ according as $G = {}^2B_2(q)$, $G_2(q)$, ${}^3D_4(q)$ respectively. This completes the proof. ■

For classical groups we shall need the following slightly more refined information than that in [18]. This result is taken from [48]; the case where G is orthogonal is not explicitly stated there, but it follows easily from the proofs of [48, Theorems 6.1, 7.6].

Proposition 2.5 *Let $G = G(q)$ be a classical quasisimple group over $\mathbb{F}_q$, write $H = G/Z(G)$, and let $f = f(G)$ be as in Table 1 below. Then there is an absolute constant $c > 0$ such that G has at most $q+2$ nontrivial irreducible characters of degree less than cq^f.*

Table 1

H	$L_n^\epsilon(q)\,(n \geq 4)$	$L_3^\epsilon(q)$	$PSp_{2n}(q)$	$P\Omega_{2n+1}(q)\,(n \geq 3)$	$P\Omega_{2n}^\epsilon(q)\,(n \geq 4)$
f	$2n-4$	3	$2n-1$	$2n-1$	$2n-2$

Corollary 2.6 *Let $\mathcal{D}$ be a family of classical finite quasisimple groups, not $L_2(q)$ or $SL_2(q)$, and define $s_0 = \limsup_{G\in\mathcal{D}} \frac{r(G)}{f(G)}$. Then for any $s > s_0$, we have $\zeta^G(s) \to 1$ as $|G| \to \infty$ with $G \in \mathcal{D}$.*

In particular, this holds when $s_0 = \frac{2}{3}$ and $\mathcal{D}$ consists of all classical groups apart from $L_2(q)$, $SL_2(q)$.

Proof Using Lemma 2.1 and Proposition 2.5, we have

$$\zeta^G(s) \leq 1+(q+2)\cdot(c_2q^r)^{-s}+(c_1q^r)\cdot(cq^f)^{-s} = 1+c_3(s)\cdot q^{1-rs}+c_4(s)\cdot q^{r-fs}.$$

As $L_2(q)$, $SL_2(q)$ are excluded, we have $r \geq 2$. The first assertion follows, provided $s > \max(s_0, \frac{1}{r})$, which is equal to s_0 (since $\frac{r}{f} \geq \frac{1}{2}$ in all cases).

An easy check shows that $\frac{r}{f} \leq \frac{2}{3}$ in all cases (with equality when $G = L_3^\epsilon(q)$ or $P\Omega_8^\epsilon(q)$), yielding the last part. ∎

Proof of Theorem 1.1(ii) This now follows from Corollaries 2.4 and 2.6.

This completes the proof of Theorem 1.1.

Combining the results 2.1, 2.3 and 2.5 easily yields the following.

Corollary 2.7 *There exists an absolute constant c such that if $G \neq L_2(q)$ is a finite simple group and n is a positive integer, then G has at most $cn^{2/3}$ irreducible characters of degree n.*

Similar methods yield an analogue of Theorem 1.1 for nearly simple groups, that is, finite groups G such that $F^*(G) = G_0$ is quasisimple. For such a group G, the function $\zeta^G(s) - \zeta^{G/G_0}(s)$ is the sum $\sum \chi(1)^{-s}$ over all irreducible characters χ of G with $\ker\chi \leq Z(G_0)$. Moreover, $G/G_0 \leq \mathrm{Out}(G_0/Z(G_0))$ is a soluble group with a transparent structure, and $\zeta^{G/G_0}(s)$ can be easily computed. Note that $\zeta^G(s) \geq |G/G'|$, and also $\zeta^{G/G_0}(s) \geq |G/G'|$, with equality if and only if $G_0 = G'$.

Theorem 2.8 *Let G be a finite nearly simple group with $F^*(G) = G_0$, and fix a real number s.*

(i) *If $s > 1$, then $\zeta^G(s) - \zeta^{G/G_0}(s) \to 0$ as $|G| \to \infty$.*

(ii) *If $s > 2/3$ and $G_0 \neq L_2(q)$ or $SL_2(q)$, then $\zeta^G(s) - \zeta^{G/G_0}(s) \to 0$ as $|G| \to \infty$.*

(iii) *In particular, if G/G_0 is abelian then $\zeta^G(s) = |G/G'| + o(1)$ for $s > 1$, and the same holds for $s > 2/3$ if $G_0 \neq L_2(q)$ or $SL_2(q)$.*

Proof The case where $G_0 = A_n$ is covered by [32, 1.1], and that where $G_0 = \hat{A}_n$ follows easily as at the beginning of this section.

So assume G_0 is of Lie type, of rank r over $\mathbb{F}_q$. By Lemma 2.1 together with Clifford's theorem, every irreducible character of G with kernel contained in $Z(G_0)$ has degree at least $c_2 q^r$. It is well known that $k(G) \leq |G : G_0| \cdot k(G_0)$, so Lemma 2.1 gives $k(G) \leq c_1 q^r \cdot |G : G_0|$. Moreover, $|G : G_0| \leq |\mathrm{Out}(G_0)| \leq c_3 r \log q$. Hence $k(G) \leq c_4 r q^r \log q$. It follows that

$$\zeta^G(s) - \zeta^{G/G_0}(s) \leq c_4 r q^r \log q \cdot (c_2 q^r)^{-s} \leq c_5(s) \cdot r \log q \cdot q^{-r(s-1)}.$$

If $s > 1$, the right hand side tends to zero as q or r tends to infinity, proving part (i).

For part (ii), in the case where G_0 is an exceptional group, Proposition 2.3 shows that any irreducible character of G with kernel contained in $Z(G_0)$ has degree at least cq^h, and hence

$$\zeta^G(s) - \zeta^{G/G_0}(s) \leq c_4 r q^r \log q \cdot (cq^h)^{-s}.$$

Excluding type ${}^3D_4$, we have $\frac{r}{h} \leq \frac{2}{3}$, so the conclusion follows; for G of type ${}^3D_4$ we use [5] as in the proof of 2.4.

Part (ii) in the case where G_0 is classical is handled similarly, as in the proof of Corollary 2.6.

Finally, part (iii) follows immediately from (i) and (ii). ■

Sometimes we shall also need to study certain variants of ζ^G involving only the real irreducible characters of G. For a finite group G, and a real number s, define

$$\zeta_R^G(s) = \sum_{\chi \in Irr(G),\, \chi \text{ real}} \chi(1)^{-s};$$

and for an integer k, define

$$\zeta_r^G(k) = \sum_{\chi \in Irr(G)} \iota(\chi)^k \chi(1)^{-k},$$

where $\iota(\chi) \in \{0, 1, -1\}$ is the Schur indicator of χ. Note that a finite group G has $|G/G^2|$ real linear characters, where G^2 is the group generated by the squares in G. Hence

$$\zeta_R^G(k) \geq |G/G^2|.$$

Lemma 2.9 *Let G be a finite nearly simple group with $F^*(G) = G_0$. Suppose that either $s > 1$, or $G_0 \neq L_2(q)$, $SL_2(q)$ and $s > 2/3$. Then*

$$\zeta_R^G(s) = \zeta_R^{G/G_0}(s) + o(1), \text{ and } \zeta_r^G(s) = \zeta_r^{G/G_0}(s) + o(1).$$

If moreover G/G_0 is abelian, then both $\zeta_R^G(s)$ and $\zeta_r^G(s)$ have the form $|G/G^2| + o(1)$.

Proof Note that $\zeta_R^G(s) - \zeta_R^{G/G_0}(s) = \sum \chi(1)^{-s}$, the sum running over irreducible real $\chi \in Irr(G)$ such that $\ker \chi \leq Z(G_0)$. This sum is bounded above by the sum $\sum \chi(1)^{-s}$ over all $\chi \in Irr(G)$ such that $\ker \chi \leq Z(G_0)$, which is of the form $o(1)$ by Theorem 2.8. If G/G_0 is abelian, then $\zeta_R^{G/G_0}(s) = |G/G^2|$. This completes the proof for ζ_R^G, and a similar argument gives the conclusion for ζ_r^G. ■

We conclude this section with a result on ζ^G and ζ_r^G for $G = GL_n(q)$ which is important for later applications. In the statement we fix n and let $q \to \infty$.

Proposition 2.10 *Fix $n \geq 2$, and let $G = GL_n(q)$.*

(i) *For $n \geq 3$ and $s \geq 2$, we have $\zeta^G(s) = q - 1 + o(1)$.*

(ii) *For $n \geq 3$ and $k \geq 1$, we have $\zeta_r^G(k) = (q-1, 2) + o(1)$.*

(iii) *For $n = 2$, we have $\zeta^G(2) = q + o(1)$, and $\zeta^G(s) = q - 1 + o(1)$ for $s > 2$.*

(iv) *For $n = 2$, we have $\zeta_r^G(1) = (q-1, 2) + 1 + o(1)$, and $\zeta_r^G(k) = (q-1, 2) + o(1)$ for $k > 1$.*

Proof (i) First note that G has at most $c_1 q^n$ irreducible characters, by Lemma 2.1. There are $q - 1$ linear characters, contributing $q - 1$ to $\zeta^G(s)$. The remaining characters have degree at least $c_2 q^{n-1}$. Hence for $s \geq 2$,

$$q - 1 \leq \zeta^G(s) \leq q - 1 + O(q^n \cdot q^{-2(n-1)}),$$

giving the conclusion since $n \geq 3$.

(ii) The linear characters contribute $(q-1, 2)$ to $\zeta_r^G(k)$ for any $k \geq 1$. Of the remaining irreducible characters, Proposition 2.5 shows that there are at most $c_3 q^2$ of degree less than $c_4 q^{2n-4}$, and these have degree at least $c_5 q^{n-1}$. Hence for $k \geq 1$,

$$(q-1, 2) \leq \zeta_r^G(k) \leq (q-1, 2) + O(q^2 \cdot q^{-(n-1)}) + O(q^n \cdot q^{-(2n-4)}).$$

This gives the conclusion for $n \geq 5$.

For $n = 3$ or 4, we use the information in [46]. Analysis of the character tables there shows that there are just $O(q^2)$ real irreducible characters of $GL_3(q)$ in all, and $O(q)$ of these have degree less than $c_6 q^3$, which yields

$$\zeta_r^G(1) = (q-1,2) + O(q.q^{-2}) + O(q^2.q^{-3}) = (q-1,2) + o(1).$$

For $n = 4$, the number of irreducible characters of $GL_4(q)$ of degree less than $c_7 q^5$ is $O(q^2)$, and hence

$$\zeta_r^G(1) = (q-1,2) + O(q^2.q^{-3}) + O(q^4.q^{-5}) = (q-1,2) + o(1).$$

(iii) As follows from [46], $GL_2(q)$ has $(1+o(1))q^2$ non-linear characters, and their degrees are $q-1, q, q+1$. The conclusion follows.

(iv) Again from [46], it can be checked that $GL_2(q)$ has $q + O(1)$ real non-linear characters; their degrees are $q, q-1, q+1$, and Schur indicators are $+1$. The conclusion follows easily. ■

Proposition 2.10 and its proof yield the following.

Corollary 2.11 *Fix $n \geq 2$, and let $G = GL_n(q)$. Then for any integer $k \geq 1$, we have $\zeta_R^G(k) - \zeta_r^G(k) = o(1)$ (as $q \to \infty$). Consequently*

$$\zeta_R^G(k) = (q-1,2) + \delta + o(1),$$

where $\delta = 0$ unless $n = 2$ and $k = 1$, in which case $\delta = 1$.

3 Counting homomorphisms

In this section we prove Theorem 1.2 and related results. We shall use a well known formula expressing the sizes of certain spaces of homomorphisms in terms of characters. At this point the results of the previous section will come into play.

Throughout the section we assume that Γ is a Fuchsian group as in (1.1),(1.2) with $s = t = 0$.

Let G be a finite group, and $\mathbf{C} = (C_1, \ldots, C_d)$ be a d-tuple of conjugacy classes C_i of G with representatives g_i. Set

$$\mathrm{Hom}_{\mathbf{C}}(\Gamma, G) = \{\phi \in \mathrm{Hom}(\Gamma, G) : \phi(x_i) \in C_i \text{ for } i = 1, \ldots, d\}.$$

The next result, essentially dating back to Hurwitz, plays a key role in this paper; for a proof, see for example [32, 3.2].

Lemma 3.1 *Let Γ be a co-compact Fuchsian group and G a finite group.*

(i) *If Γ is oriented, then*

$$|\mathrm{Hom}_{\mathbf{C}}(\Gamma, G)| = |G|^{2g-1}|C_1|\cdots|C_d| \sum_{\chi \in Irr(G)} \frac{\chi(g_1)\cdots\chi(g_d)}{\chi(1)^{d-2+2g}}.$$

(ii) *If Γ is non-oriented, then*

$$|\mathrm{Hom}_{\mathbf{C}}(\Gamma, G)| = |G|^{g-1}|C_1|\cdots|C_d| \sum_{\chi \in Irr(G)} \iota(\chi)^g \frac{\chi(g_1)\cdots\chi(g_d)}{\chi(1)^{d-2+g}},$$

where $\iota(\chi) \in \{0, 1, -1\}$ is the Schur indicator of χ.

We now estimate $|\mathrm{Hom}(\Gamma, G)|$ in terms of the functions ζ^G, ζ_r^G studied above. We start with the case of surface groups, which is already known [39], and follows from Lemma 3.1 by substituting $d = 0$.

Corollary 3.2 *Let Γ be a surface group of genus g and let G be a finite group.*

(i) *If Γ is oriented, then $|\mathrm{Hom}(\Gamma, G)| = |G|^{2g-1}\zeta^G(2g-2)$.*

(ii) *If Γ is non-oriented, then $|\mathrm{Hom}(\Gamma, G)| = |G|^{g-1}\zeta_r^G(g-2)$.*

In order to deal with general Fuchsian groups, recall that we define $j_m(G)$ to be the number of solutions to the equation $x^m = 1$ in G; also $v = v(\Gamma)$ is 2 if Γ is oriented and 1 if not.

Lemma 3.3 *For any finite group G, we have*

$$2 - \zeta^G(vg-2) \leq \frac{|\mathrm{Hom}(\Gamma, G)|}{|G|^{vg-1} \cdot \prod_{i=1}^d j_{m_i}(G)} \leq \zeta^G(vg-2).$$

Proof First assume that Γ is oriented. Observe that for $\chi \in Irr(G)$,

$$\frac{|\chi(g_1)\cdots\chi(g_d)|}{\chi(1)^{d-2+2g}} \leq \chi(1)^{-(2g-2)}.$$

Hence

$$\Big|\sum_{1 \neq \chi \in Irr(G)} \frac{\chi(g_1)\cdots\chi(g_d)}{\chi(1)^{d-2+2g}}\Big| \leq \zeta^G(2g-2) - 1,$$

which yields

$$2 - \zeta^G(2g-2) \leq \sum_{\chi \in Irr(G)} \frac{\chi(g_1)\cdots\chi(g_d)}{\chi(1)^{d-2+2g}} \leq \zeta^G(2g-2). \qquad (1)$$

Now

$$|\mathrm{Hom}(\Gamma, G)| = \sum_{\mathbf{C}} |\mathrm{Hom}_{\mathbf{C}}(\Gamma, G)|,$$

where the sum ranges over d-tuples $\mathbf{C}$ of classes C_i of elements of order dividing m_i. Also $\sum_{\mathbf{C}} |C_1| \cdots |C_d| = \prod_{i=1}^{d} j_{m_i}(G)$. Applying Lemma 3.1(i) and (1), we obtain

$$(2-\zeta^G(2g-2))|G|^{2g-1} \prod_{i=1}^{d} j_{m_i}(G) \leq |\mathrm{Hom}(\Gamma, G)| \leq \zeta^G(2g-2)|G|^{2g-1} \prod_{i=1}^{d} j_{m_i}(G).$$

This completes the case where Γ is oriented.

Now assume Γ is non-oriented. We use 3.1(ii). Observe that for $\chi \in Irr(G)$, we have

$$|\iota(\chi)^g \frac{\chi(g_1) \cdots \chi(g_d)}{\chi(1)^{d-2+g}}| \leq \chi(1)^{-(g-2)}.$$

The proof now follows as in the oriented case above. ■

Lemma 3.3 is particularly useful when $\zeta^G(vg-2)$ is close to 1, since the upper and lower bounds are then both close to 1.

Proof of Theorem 1.2 Let Γ be a Fuchsian group in $\mathcal{F}$ (recall that this means Γ has genus $g \geq 2$ ($g \geq 3$ in the non-oriented case)), and let G be a finite quasisimple group.

(i) Suppose Γ is oriented. Since $2g-2 \geq 2$, we have $\zeta^G(2g-2) = 1+o(1)$ by Theorem 1.1(i), and so Theorem 1.2(i) follows from Lemma 3.3.

(ii) Suppose now that Γ is non-oriented, and either $G/Z(G) \neq L_2(q)$ or $g > 3$. Then using both parts of Theorem 1.1, we have $\zeta^G(g-2) = 1+o(1)$, and Theorem 1.2(ii) follows again from Lemma 3.3.

(iii) Assume now Γ is non-oriented with $g = 3$ and $G = L_2(q)$. Write $h = 3/2$ if q is odd, and $h = 2$ if q is even. Let C_i be classes of elements of order dividing m_i in G ($1 \leq i \leq d$). We claim that

$$|\mathrm{Hom}_{\mathbf{C}}(\Gamma, G)| = (k + o(1)) \cdot |G|^2 \cdot |C_1| \cdots |C_d|, \tag{2}$$

where $k = 1$ unless $C_i = \{1\}$ for all i, in which case $k = h$.

To prove the claim, suppose first that $C_i \neq \{1\}$ for some i, and let $g_i \in C_i$. Inspection of the character table of $G = L_2(q)$ in [7, Section 38] shows that $|\chi(g_i)/\chi(1)| \leq 2q^{-1/2}$ for all nontrivial $\chi \in Irr(G)$, and hence

$$|\sum_{1 \neq \chi \in Irr(G)} \iota(\chi)^g \frac{\chi(g_1) \cdots \chi(g_d)}{\chi(1)^{d-2+g}}| \leq 2q^{-1/2} \sum_{1 \neq \chi \in Irr(G)} \chi(1)^{-1} = 2q^{-1/2}(\zeta^G(1)-1).$$

Since $\zeta^G(1)$ is bounded (see Lemma 2.2), this shows that

$$\sum_{\chi \in Irr(G)} \iota(\chi)^g \frac{\chi(g_1)\cdots\chi(g_d)}{\chi(1)^{d-2+g}} = 1 + 2q^{-1/2}\cdot O(1) = 1 + o(1).$$

Hence by Lemma 3.1(ii), we have

$$|\mathrm{Hom}_{\mathbf{C}}(\Gamma, G)| = (1+o(1))\cdot |G|^2 \cdot |C_1|\cdots|C_d|,$$

proving the claim (2) under the assumption that $C_i \neq \{1\}$ for some i.

Next, suppose $C_i = \{1\}$ for all i. Then Lemma 3.1(ii) gives

$$|\mathrm{Hom}_{\mathbf{C}}(\Gamma, G)| = |G|^2 \cdot \sum_{\chi \in Irr(G)} \iota(\chi)\chi(1)^{-1} = |G|^2 \cdot \zeta_r^G(1).$$

It is easily checked from the character table that $\iota(\chi) = +1$ for all but at most two irreducible characters χ of $G = L_2(q)$. Hence from Lemma 2.2 we have

$$\zeta_r^G(1) = (1+o(1))\cdot \zeta^G(1) = h + o(1),$$

which completes the proof of (2).

Applying (2) and summing over all d-tuples $C_1, \ldots, C_d$ of classes of elements of orders dividing $m_1, \ldots, m_d$ respectively, we obtain

$$|\mathrm{Hom}(\Gamma, G)| = (1+o(1))|G|^2(j_{m_1}(G)\cdots j_{m_d}(G) - 1) + (h+o(1))|G|^2.$$

If $(m_i, |G|) \neq 1$ for some i the right hand side has the form

$$(1+o(1))|G|^2 j_{m_1}(G)\cdots j_{m_d}(G),$$

while if $(m_i, |G|) = 1$ for all i, then it has the form $(h+o(1))|G|^2$.

This completes the proof of Theorem 1.2(iii).

(iv) Suppose Γ is non-oriented with $g = 3$, and $G = SL_2(q)$ with q odd. The proof is similar to the previous case, but a few modifications are necessary. Let C_i be classes of elements of order dividing m_i in G $(1 \leq i \leq d)$, and $g_i \in C_i$. Let $z = -I$ be the non-identity central element of G. Recall that $d^* = d^*(\Gamma)$ is the number of i such that m_i is even. Denote by $n(\mathbf{C})$ the number of i such that $C_i = \{z\}$. Note that $n(\mathbf{C}) \leq d^*$.

We claim that

$$|\mathrm{Hom}_{\mathbf{C}}(\Gamma, G)| = (k+o(1))\cdot |G|^2 \cdot |C_1|\cdots|C_d|, \tag{3}$$

where $k = 1$ unless $|C_i| = 1$ for all i and $n(\mathbf{C})$ is odd , in which case $k = 2$.

The proof of (3) in the case where $|C_i| \neq 1$ for some i is essentially identical to the analogous proof for $G = L_2(q)$, so it will be omitted.

Assume then that the classes C_i are all central, and let $n = n(\mathbf{C})$. Note that for an irreducible character χ of G we have $\chi(g_i)/\chi(1) = 1$ unless χ is faithful and $g_i = z$, in which case $\chi(g_i) = -1$. Combining this with part (ii) of Lemma 3.1 we obtain

$$|\mathrm{Hom}_{\mathbf{C}}(\Gamma, G)| = |G|^2(\Sigma_1 + \Sigma_2), \tag{4}$$

where

$$\Sigma_1 = \sum_{\chi \in Irr(G)\ nonfaithful} \iota(\chi)\chi(1)^{-1}, \ \ \Sigma_2 = \sum_{\chi \in Irr(G)\ faithful} \iota(\chi)(-1)^n\chi(1)^{-1}.$$

Clearly $\Sigma_1 = \zeta_r^{L_2(q)}(1)$, so as seen above,

$$\Sigma_1 = 3/2 + o(1).$$

It is easily checked from the character table that $\iota(\chi) = -1$ for all but two of the faithful irreducible characters χ of G, of which there are $\frac{q}{2} + O(1)$ of degree $q \pm 1$. We conclude that

$$\Sigma_2 = (-1)^{n+1}(\frac{1}{2} + o(1)).$$

Hence $\Sigma_1 + \Sigma_2 = k + o(1)$, where k is as in (3). Now (3) follows using (4).

Let Y (respectively Z) be the set of d-tuples $(C_1, \ldots, C_d)$ such that $|C_i| \neq 1$ for some i (respectively $|C_i| = 1$ for all i). Note that $|Z| = 2^{d^*}$. Write

$$|\mathrm{Hom}(\Gamma, G)| = A + B,$$

where

$$A = \sum_{\mathbf{C} \in Y} |\mathrm{Hom}_{\mathbf{C}}(\Gamma, G)|, \ \ B = \sum_{\mathbf{C} \in Z} |\mathrm{Hom}_{\mathbf{C}}(\Gamma, G)|.$$

By (3), we have

$$A = (1+o(1))|G|^2(\prod_{i=1}^{d} j_{m_i}(G) - \prod_{i=1}^{d} j_{m_i}(Z(G)) = (1+o(1))|G|^2(\prod_{i=1}^{d} j_{m_i}(G) - 2^{d^*}).$$

Also for $d^* > 0$, (3) yields

$$B = |G|^2 \cdot (\sum_{\mathbf{C} \in Z,\, n(\mathbf{C})\ even} 1+o(1) + \sum_{\mathbf{C} \in Z,\, n(\mathbf{C})\ odd} 2+o(1)) = |G|^2 \cdot (3 \cdot 2^{d^*-1} + o(1)),$$

while $B = |G|^2(1 + o(1))$ if $d^* = 0$. In the latter case we have $A + B = (1 + o(1))|G|^2 \prod_{i=1}^{d} j_{m_i}(G)$. Assume now that $d^* > 0$. If $(m_i, |G|) > 2$ for some i, then A is the dominant term and $A+B = (1+o(1))|G|^2 \prod_{i=1}^{d} j_{m_i}(G)$. Finally, if $(m_i, |G|) = 1$ or 2 for all i, then $A = 0$. Thus Theorem 1.2(iv) is proved in all cases.

This completes the proof of Theorem 1.2.

Our methods also enable us to estimate $|\mathrm{Hom}(\Gamma, G)|$, where G is nearly simple, which is important for our applications to representation varieties.

We first formulate the case where Γ is a surface group:

Proposition 3.4 *Let Γ be a surface group of genus g, and let G be a finite nearly simple group with $F^*(G) = G_0$, a quasisimple group.*

(i) *If Γ is oriented with $g \geq 2$, then*

$$|\mathrm{Hom}(\Gamma, G)| = |G|^{2g-1} \cdot (\zeta^{G/G_0}(2g-2) + o(1)).$$

In particular, if $G_0 = G'$ then $|\mathrm{Hom}(\Gamma, G)| = |G|^{2g-1} \cdot (|G/G'| + o(1))$.

(ii) *If Γ is non-oriented with $g \geq 3$, and $(g, G_0/Z(G_0)) \neq (3, L_2(q))$, then*

$$|\mathrm{Hom}(\Gamma, G)| = |G|^{g-1} \cdot (\zeta_r^{G/G_0}(g-2) + o(1)).$$

In particular, if $G_0 = G'$ then $|\mathrm{Hom}(\Gamma, G)| = |G|^{g-1} \cdot (|G/G^2| + o(1))$.

Proof Part (i) follows from Theorem 2.8 and Corollary 3.2(i). Similarly part (ii) follows from Lemma 2.9 and Corollary 3.2(ii). ∎

We next extend this result to general Fuchsian groups, assuming that G/G_0 is abelian. This requires some preparation.

Recall from the Introduction that for a d-tuple $\mathbf{m} = (m_1, \ldots, m_d)$ of integers $m_i \geq 2$, we define

$$I_{\mathbf{m}}(G) = \{(g_1, \ldots, g_d) \ : \ g_i \in G,\, g_i^{m_i} = 1, \prod_1^d g_i \in G'\}.$$

Also, letting G^2 denote the group generated by the squares in G, define

$$I_{\mathbf{m}}^r(G) = \{(g_1, \ldots, g_d); : \ g_i \in G,\, g_i^{m_i} = 1, \prod_1^d g_i \in G^2\}.$$

The following result is a variant of Lemma 3.3 which is useful in the case where G is not a perfect group.

Lemma 3.5 *Let Γ be a Fuchsian group as in (1.1), (1.2), and let G be a finite group.*

(i) *If Γ is oriented, then*

$$2|G/G'| - \zeta^G(2g-2) \leq \frac{|\mathrm{Hom}(\Gamma, G)|}{|G|^{2g-1} \cdot |I_{\mathbf{m}}(G)|} \leq \zeta^G(2g-2).$$

(ii) *If* Γ *is non-oriented, then*

$$2|G/G^2| - \zeta_R^G(g-2) \leq \frac{|\mathrm{Hom}(\Gamma, G)|}{|G|^{g-1} \cdot |I_{\mathbf{m}}^r(G)|} \leq \zeta_R^G(g-2).$$

Proof The proof of this extends that of Lemma 3.3. For $1 \leq i \leq d$ let $C_i = g_i^G$ be a conjugacy class of G with $g_i^{m_i} = 1$. Write

$$\sum_{\chi \in Irr(G)} \frac{\chi(g_1) \cdots \chi(g_d)}{\chi(1)^{d-2+2g}} = \Sigma_1 + \Sigma_2,$$

where Σ_1 and Σ_2 are the sums over the linear and non-linear irreducible characters, respectively. Suppose $\mathrm{Hom}_{\mathbf{C}}(\Gamma, G) \neq \emptyset$. Then the relation $x_1 \dots x_d\, [a_1, b_1] \dots [a_g, b_g]$ of Γ implies that $g_1 \dots g_d \in G'$. Hence for every linear character χ of G we have $\chi(g_1) \cdots \chi(g_d) = 1$. This shows that $\Sigma_1 = |G/G'|$. We also have $|\Sigma_2| \leq \zeta^G(2g-2) - |G/G'|$. Now by Lemma 3.1 we have

$$|\mathrm{Hom}_{\mathbf{C}}(\Gamma, G)| = |G|^{2g-1} |C_1| \dots |C_d| \cdot (|G/G'| + \Sigma_2),$$

and so

$$|G|^{2g-1} \prod_{i=1}^{d} |C_i| (2|G/G'| - \zeta^G(2g-2)) \leq |\mathrm{Hom}_{\mathbf{C}}(\Gamma, G)| \leq |G|^{2g-1} \prod_{i=1}^{d} |C_i| \zeta^G(2g-2).$$

Summing over all $C_1, \dots, C_d$ such that $\prod_1^d C_i \subseteq G'$, and observing that $\sum_{\prod C_i \subseteq G'} |C_1| \dots |C_d| = |I_{\mathbf{m}}(G)|$, this yields (i).

The proof of (ii) is similar. For $i \leq i \leq d$ let $C_i = g_i^G$ be a conjugacy class of G with $g_i^{m_i} = 1$. Write

$$\sum_{\chi \in Irr(G)} \iota(\chi)^g \frac{\chi(g_1) \cdots \chi(g_d)}{\chi(1)^{d-2+g}} = \Delta_1 + \Delta_2,$$

where Δ_1 and Δ_2 are the sums over the linear and non-linear irreducible characters, respectively. Suppose $\mathrm{Hom}_{\mathbf{C}}(\Gamma, G) \neq \emptyset$. Then the relation $x_1 \dots x_d\, a_1^2 \dots a_g^2$ of Γ implies that $g_1 \dots g_d \in G^2$. Hence for every real linear character χ of G we have $\chi(g_1) \cdots \chi(g_d) = 1$. This shows that $\Delta_1 = |G/G^2|$. We also have $|\Delta_2| \leq \zeta_R^G(g-2) - |G/G^2|$. Now by Lemma 3.1 we have

$$|\mathrm{Hom}_{\mathbf{C}}(\Gamma, G)| = |G|^{g-1} |C_1| \dots |C_d| \cdot (|G/G^2| + \Delta_2). \tag{5}$$

Summing over all $C_1, \dots, C_d$ such that $\prod_1^d C_i \subseteq G^2$, this yields the required conclusion. ∎

Theorem 3.6 *Let Γ be a Fuchsian group in $\mathcal{F}$, and let G be a finite nearly simple group with $F^*(G) = G_0$. Assume that G/G_0 is abelian.*

(i) *If Γ is oriented, then*

$$|\mathrm{Hom}(\Gamma, G)| = |G|^{2g-1}|I_{\mathbf{m}}(G)| \cdot (|G/G'| + o(1)).$$

(ii) *If Γ is non-oriented, and $(g, G_0/Z(G_0)) \neq (3, L_2(q))$, then*

$$|\mathrm{Hom}(\Gamma, G)| = |G|^{g-1}|I^r_{\mathbf{m}}(G)| \cdot (|G/G^2| + o(1)).$$

Proof (i) By Theorem 2.8(iii) we have $\zeta^G(2g-2) = |G/G'| + o(1)$. Substituting this in Lemma 3.5(i) gives the conclusion.

(ii) By Lemma 3.5(ii),

$$|\frac{|\mathrm{Hom}(\Gamma, G)|}{|G|^{g-1} \cdot |I^r_{\mathbf{m}}(G)|} - |G/G^2|| \leq \zeta^G_R(g-2) - |G/G^2|.$$

The right hand side is of the form $o(1)$ by Lemma 2.9, and the conclusion follows. ∎

In view of Theorem 3.6 it is important to estimate the sizes of the subsets $I_{\mathbf{m}}(G)$ and $I^r_{\mathbf{m}}(G)$. Trivially, we have

$$\prod_{i=1}^{d} j_{m_i}(G') \leq |I_{\mathbf{m}}(G)| \leq |I^r_{\mathbf{m}}(G)| \leq \prod_{i=1}^{d} j_{m_i}(G). \tag{6}$$

We shall show in Section 4 (see Corollary 4.4) that under some conditions, the upper and lower bounds in (6) are asymptotically the same, which will be crucial in the proof of Theorem 1.10 in Section 7.

For our applications on representation varieties we shall also need to estimate $|\mathrm{Hom}(\Gamma, G)|$ when $G = GL_n(q)$, where n is fixed and $q \to \infty$ (note that $GL_n(q)$ is not nearly simple). Again, we start with the easier case of surface groups.

Proposition 3.7 *Let Γ be a surface group of genus g which is not virtually abelian, and fix $n \geq 2$.*

(i) *If Γ is oriented, then*

$$|\mathrm{Hom}(\Gamma, GL_n(q))| = (q - 1 + \delta + o(1)) \cdot |GL_n(q)|^{2g-1},$$

where $\delta = 0$ unless $n = g = 2$, in which case $\delta = 1$.

(ii) *If Γ is non-oriented, then*

$$|\mathrm{Hom}(\Gamma, GL_n(q))| = ((q-1, 2) + \delta + o(1)) \cdot |GL_n(q)|^{g-1},$$

where $\delta = 0$ unless $n = 2$ and $g = 3$, in which case $\delta = 1$.

Proof This follows by combining Corollary 3.2 with Proposition 2.10. ∎

Theorem 3.8 *Let Γ be a Fuchsian group in $\mathcal{F}$, and fix $n \geq 2$.*

(i) *If Γ is oriented, then*

$$|\mathrm{Hom}(\Gamma, GL_n(q))| = (1+o(1))(q-1) \cdot |GL_n(q)|^{2g-1} \cdot |I_{\mathbf{m}}(GL_n(q))|.$$

(ii) *If Γ is non-oriented, then*

$$|\mathrm{Hom}(\Gamma, GL_n(q))| \sim |GL_n(q)|^{g-1} \cdot |I^r_{\mathbf{m}}(GL_n(q))|.$$

Proof (i) Set $G = GL_n(q)$. Then as $g \geq 2$, Lemma 2.10(i),(iii) shows that $\zeta^G(2g-2) = q - 1 + \delta + o(1)$, where $\delta = 0$ unless $n = g = 2$, in which case $\delta = 1$. Substituting in Lemma 3.5(i), we obtain

$$q - 1 - \delta - o(1) \leq \frac{|\mathrm{Hom}(\Gamma, G)|}{|G|^{2g-1} \cdot |I_{\mathbf{m}}(G)|} \leq q - 1 + \delta + o(1).$$

The conclusion follows.

(ii) By Corollary 2.11, $\zeta^G_R(g-2) = (q-1,2) + \delta + o(1)$, where $\delta = 0$ unless $n = 2, g = 3$, in which case $\delta = 1$. Also $|G/G^2| = (q-1,2)$. Hence Lemma 3.5(ii) gives

$$(q-1,2) - \delta - o(1) \leq \frac{|\mathrm{Hom}(\Gamma, G)|}{|G|^{g-1} \cdot |I^r_{\mathbf{m}}(G)|} \leq (q-1,2) + \delta + o(1).$$

The conclusion follows, unless $n = 2, g = 3$ and q is even. In this case, using the notation of the proof of Lemma 3.5(ii), and inspecting the character table of $G = GL_2(q)$, we see that if some C_i is non-central then $\Delta_2 = O(q^{-1})$, and otherwise $\Delta_2 = q/(q-1)$. In either case, (5) shows that

$$|\mathrm{Hom}_{\mathbf{C}}(\Gamma, G)| \sim |G|^{g-1}|C_1| \ldots |C_d|,$$

and the result follows by summing over all $C_1, \ldots, C_d$ such that $\prod_1^d C_i \subseteq G^2$. ∎

Note that the proof shows that the implied constants in part (ii) are between $1 + o(1)$ and $3 + o(1)$.

To apply Theorem 3.8 we need to estimate the sizes of the subsets $I_{\mathbf{m}}(GL_n(q))$ and $I^r_{\mathbf{m}}(GL_n(q))$. By (6), we have

$$\prod_{i=1}^d j_{m_i}(SL_n(q)) \leq |I_{\mathbf{m}}(GL_n(q))| \leq |I^r_{\mathbf{m}}(GL_n(q))| \leq \prod_{i=1}^d j_{m_i}(GL_n(q)). \quad (7)$$

The next few lemmas show that under some extra conditions, tighter estimates can be obtained in terms of the numbers $j_{m_i}(GL_n(q))$ (which in turn will be studied in Section 4 - see Proposition 4.5).

Lemma 3.9 *Let $\mathbf{m} = (m_1, \ldots, m_d)$, where the $m_i \geq 2$ are integers, let p be a prime, and let m_i' be the p'-part of m_i. Let q be a power of p such that $q \equiv 1$ mod m_i' for all i. Fix $n \geq 2$ such that $(m_i', n) = 1$ for all i. Then as $q \to \infty$, we have*

$$|I_{\mathbf{m}}(GL_n(q))| \sim \prod_{i=1}^{d} j_{m_i}(GL_n(q)).$$

Proof In view of (7), it suffices to show that under the hypotheses of the lemma,

$$j_{m_i}(GL_n(q)) = m_i' \cdot j_{m_i}(SL_n(q)). \tag{8}$$

To see this, let $\omega \in \mathbb{F}_q$ be an element of multiplicative order m_i', and let $z = \omega I \in GL_n(q)$. As $(m_i', n) = 1$, $\det(z)$ also has order m_i' in $\mathbb{F}_q$. Now let $g \in GL_n(q)$ satisfy $g^{m_i} = 1$. Then $\det(g)^{m_i'} = 1$, and so there is a unique power z^j of z such that $gz^j \in SL_n(q)$. Moreover $(gz^j)^{m_i} = 1$, and (8) follows. ∎

Lemma 3.10 *Let $\mathbf{m} = (m_1, \ldots, m_d)$, where the $m_i \geq 2$ are integers, and let q be a prime power. If q is odd, assume $q \equiv 1$ mod 2^{a+1}, where 2^a is the maximal power of 2 dividing some m_i. Then for any $n \geq 2$,*

$$|I^r_{\mathbf{m}}(GL_n(q))| = \prod_{i=1}^{d} j_{m_i}(GL_n(q)).$$

Proof Note first that $GL_n(q)^2$ consists of all elements of $GL_n(q)$ whose determinant is a square in $\mathbb{F}_q$. If q is even then $GL_n(q)^2 = GL_n(q)$ and the result follows trivially from the definition of $I^r_{\mathbf{m}}(GL_n(q))$. So suppose q is odd and $q \equiv 1 \bmod 2^{a+1}$. We claim that for any $g_1, \ldots, g_d \in GL_n(q)$ satisfying $g_i^{m_i} = 1$, we have $(g_1, \ldots, g_d) \in I^r_{\mathbf{m}}(GL_n(q))$. Indeed, for $1 \leq i \leq d$, write $m_i = 2^{a_i} k_i$ with k_i odd and $0 \leq a_i \leq a$. Then $1 = \det(g_i)^{m_i} = \det(g_i)^{2^{a_i} k_i}$. By our assumption on q, it follows that $\det(g_i)^{k_i}$ is a square in $\mathbb{F}_q$, and since k_i is odd, $\det(g_i)$ is therefore also a square. The claim follows, and with it the required conclusion. ∎

We remark that in general, $|I_{\mathbf{m}}(GL_n(q))|$ and $|I^r_{\mathbf{m}}(GL_n(q))|$ can be asymptotically smaller than $\prod_{i=1}^{d} j_{m_i}(GL_n(q))$: for example, suppose $d = 1$, $m_1 = n \equiv 2 \bmod 4$, $q \equiv 1 \bmod n$ and $q \equiv 3 \bmod 4$. Then the largest class of elements of order dividing m_1 in $GL_n(q)$ contains $g_1 = \mathrm{diag}(1, \omega, \omega^2, \ldots, \omega^{m_1 - 1})$, where $\omega \in \mathbb{F}_q$ is a primitive m_1^{th} root of 1; this has determinant -1, a non-square, hence does not lie in $I^r_{\mathbf{m}}(GL_n(q))$. It follows easily that in this example, fixing n and letting $q \to \infty$, we have $j_{m_1}(GL_n(q)) \sim q^{n^2 - n}$, while $|I^r_{\mathbf{m}}(GL_n(q))| \sim |I^r_{\mathbf{m}}(GL_n(q))| \sim q^{n^2 - n - 2}$.

Corollary 3.11 *Let Γ be co-compact non-oriented Fuchsian group as in* (1.2)*, of genus $g \geq 3$, and let q satisfy the assumptions of Lemma* 3.10*. Then for any fixed $n \geq 2$, we have*

$$|\mathrm{Hom}(\Gamma, GL_n(q))| \sim |GL_n(q)|^{g-1} \cdot \prod_{i=1}^{d} j_{m_i}(GL_n(q)).$$

Proof This is immediate from Theorem 3.8(ii) and Lemma 3.10. ∎

4 Counting elements of given order

In this section we obtain bounds on the numbers $j_m(G)$ of elements of order dividing m in G, where G is a quasisimple group of Lie type or a general linear group. We use these bounds to deduce Theorems 1.4 and 1.5.

One of our main tools is the following result of Lawther concerning the dimension of $J_m(X)$, the variety of elements of order dividing m in a simple algebraic group X.

Theorem 4.1 (Lawther [20]) *Let X be a simple algebraic group of rank r over an algebraically closed field, and let m be a positive integer. Then there is a constant $c(m)$ depending only on m such that*

$$(1 - \frac{1}{m}) \dim X - c(m) \leq \dim J_m(X) \leq (1 - \frac{1}{m}) \dim X + \frac{r}{m}.$$

Moreover, for X of adjoint type, $\dim J_m(X)$ is known and is given in [20].

The upper bound in this theorem is immediate from [20, Theorem 1]. The lower bound is an easy consequence of the work in [20] (see also the proof of (12) below).

Corollary 4.2 *With notation as in Theorem* 4.1*, we have*

$$\frac{\dim J_m(X)}{\dim X} \to 1 - \frac{1}{m} \text{ as } r \to \infty.$$

Here is our main result on $j_m(G)$ for finite groups G of Lie type.

Theorem 4.3 *Fix an integer $m \geq 2$, a prime p, let $K = \bar{\mathbb{F}}_p$, and let X be a simple algebraic group of rank r over K. For q a power of p, let $G = G(q)$ be a quasisimple group of Lie type over $\mathbb{F}_q$ of the form X'_σ, where $\sigma = \sigma_q$ is a Frobenius endomorphism of X. Define $t = \frac{1}{2}$ if G is of type ${}^2B_2$, ${}^2G_2$ or ${}^2F_4$, and $t = 1$ otherwise. Then there are positive constants c_1, c_2, c_3, c_4 depending only on m, such that the following hold.*

(i) $j_m(G) \leq j_m(X_\sigma) < c_1 m^r q^{t \dim J_m(X)}$.

(ii) *There exists $q_0 = p^a$ such that if q is any power of q_0, then $j_m(G) > c_2 q^{t \dim J_m(X)}$.*

(iii) *For any power q of p, we have*

$$q^{-c_3} \cdot |G|^{1-\frac{1}{m}} < j_m(G) < c_4 m^r \cdot q^{\frac{r}{m}} \cdot |G|^{1-\frac{1}{m}}.$$

Proof For G of type ${}^2B_2$, ${}^2G_2$ or ${}^2F_4$, all the assertions are readily checked using the complete information on conjugacy classes of these groups found in [47, 51, 44]. So assume from now on that G is not of one of these types.

We first claim that if $n_m(X)$ denotes the number of conjugacy classes of elements of order dividing m in X, then

$$n_m(X) \leq m^r. \tag{9}$$

To see this, write $m = m_1 m_2$ where m_1 is coprime to p and m_2 is a power of p. Any element $x \in X$ of order dividing m is a commuting product $x = x_1 x_2$, where x_i has order dividing m_i for $i = 1, 2$. Here x_1 is semisimple, hence lies in a maximal torus of X, and so there are at most m_1^r possibilities for x_1 up to X-conjugacy. Moreover, x_2 is a unipotent element of $D = C_X(x_1)$; by [45, II,4.4], D/D^0 is a p'-group, and D^0 is reductive. As in the proof of [23, 1.7(iii)], we see that the number of classes of unipotent elements of D is at most 6^r. Hence $n_m(X) \leq (6m_1)^r$. The claim (9) follows unless $m_2 \leq 5$. In these cases we estimate the number of classes of unipotent elements of D^0 of order m_2 a little more carefully using the methods of [23, Section 1], and find that this number is at most m_2^r. This proves (9).

Now let $x \in X_\sigma$ be an element of order dividing m, and consider the σ-stable class x^X. We bound the size of the fixed point set $(x^X)_\sigma$ in similar fashion to the proof of [31, Lemma 1]. Write $x = x_1 x_2$ as above. Then $C_X(x)$ is the centralizer of the unipotent element x_2 in the reductive group $D = C_X(x_1)$. Each of the following quantities is bounded by a function of m: $|D/D^0|$; the number of simple components of D^0; and the rank of the torus $Z(D^0)$. Hence, writing $C = C_X(x)$, the corresponding statement is true for $C/U = C_D(x_2)/U$, where U is the unipotent radical of C. Moreover, $|U_\sigma| = q^{\dim U}$ by [21, 1.7]. By Lang's theorem [45, 3.4], $(x^X)_\sigma$ is a union of X_σ-classes, the number of which is bounded in terms of $|C/C^0|$, and the sizes of which are of the form $|X_\sigma : (C^g)_\sigma|$ for various σ-stable conjugates

C^g of C. Note also that $\dim(X/C) = \dim x^X$. It follows that

$$c_2(m) \cdot q^{\dim x^X} < |(x^X)_\sigma| < c_1(m) \cdot q^{\dim x^X}, \tag{10}$$

where $c_1(m), c_2(m)$ depend only on m. Part (i) follows; so does (ii), noting that for suitable q_0 we have $X_\sigma \leq X'_{\sigma_{q_0}} = G(q_0)$, hence $x \in G(q_0)$.

By Theorem 4.1, $\dim J_m(X) \leq (1 - \frac{1}{m}) \dim X + \frac{r}{m}$, so in particular, if $x \in X_\sigma$ has order dividing m, then $\dim x^X \leq (1 - \frac{1}{m}) \dim X + \frac{r}{m}$. Since $|G| \sim q^{\dim X}$, the upper bound of part (iii) now follows from (9) and (10).

We complete the proof by establishing the lower bound of part (iii). By taking c_3 large enough, we may assume that the rank r of X is large. Let n be the dimension of the natural module V for G, and write $n = km + t$, where k, t are integers with $k > 0$, $0 \leq t < 2m + 2$ and k even for G unitary, symplectic or orthogonal. Then we may embed the cyclic group $C_m = \langle x \rangle$ in G in such a way that $V \downarrow \langle x \rangle = F \oplus I$, where F is free of dimension km and I is trivial of dimension s. Call such an embedding almost free.

We shall show that

$$|x^G| > q^{-c_3} \cdot |G|^{1 - \frac{1}{m}}, \tag{11}$$

where c_3 depends only on m, which will establish the lower bound in (iii). Write $G = X'_\sigma$ as above, where X is the corresponding classical algebraic group over $\bar{\mathbb{F}}_q$. Arguing as for (10), we see that

$$|(x^X)_\sigma| > c_1(m) \cdot q^{\dim x^X},$$

and hence to prove (11) it is sufficient to show that

$$\dim C_X(x) \leq \frac{\dim X}{m} + c_2(m). \tag{12}$$

Write $m = m_1 m_2$ and $x = x_1 x_2$ as above. Then x_1 is semisimple, and on V has each eigenvalue different from 1 occuring with multiplicity km_2, while the eigenvalue 1 has multiplicity $km_2 + t$. Hence, if m_1 is odd we see that $C_X(x_1)^0$ is the image modulo scalars of

$$\begin{array}{ll} ((GL_{km_2})^{m_1 - 1} \times GL_{km_2 + t}) \cap SL_n, & \text{if } X = PSL_n \\ (GL_{km_2})^{(m_1 - 1)/2} \times Sp_{km_2 + t}, & \text{if } X = PSp_n \\ (GL_{km_2})^{(m_1 - 1)/2} \times SO_{km_2 + t}, & \text{if } X = PSO_n. \end{array}$$

If m_1 is even, the second line changes to $(GL_{km_2})^{(m_1 - 2)/2} \times Sp_{km_2 + t} \times Sp_{km_2}$, and similarly for the third line. A quick calculation with the dimensions of these groups yields

$$\dim C_X(x_1) \leq \frac{\dim X}{m_1} + c_3(m_1). \tag{13}$$

Now x_2 is a unipotent element in the semisimple group $D = (C_X(x_1)^0)'$. We shall show that

$$\dim C_D(x_2) \leq \frac{\dim D}{m_2} + c_4(m). \tag{14}$$

Together with (13), this will establish (12).

Now D is a product of at most $m_1 + 1$ simple factors, with x_2 embedded almost freely in each, so it is sufficient to prove (14) for each simple factor of D. Let E be a simple factor, with natural module of dimension d. On this module the unipotent element x_2 acts as $((J_{m_2})^l, (J_1)^u)$, where J_i is a unipotent Jordan block of size i, and we have $d = lm_2 + u$ with $u \leq t$. The dimension of $C_E(x_2)$ can be read off from [50]: assuming E is not symplectic or orthogonal in characteristic 2, $\dim C_E(x_2)$ is as follows:

$$\begin{array}{ll} m_2l^2 + 2ul + u^2 - 1, & \text{if } E = SL_d \\ \frac{1}{2}(m_2l^2 + 2ul + l + u^2 + u), & \text{if } E = Sp_d \\ \frac{1}{2}(m_2l^2 + 2ul - l + u^2 - u) & \text{if } E = SO_d. \end{array}$$

A check of dimensions now yields (14). Finally, if E is symplectic or orthogonal in characteristic 2, then E has two classes of elements of type $((J_{m_2})^l, (J_1)^u)$; taking x_2 in the larger of these, we have

$$\dim C_E(x_2) = \frac{1}{2}(m_2l^2 + 2ul + u^2 + u) \text{ or } \frac{1}{2}(m_2l^2 + 2ul - l + u^2 - u),$$

according as $E = Sp_d$ or SO_d, respectively. Again, (14) follows.

This completes the proof of the theorem. ∎

Proof of Theorem 1.4

Theorem 1.4 follows immediately from part (iii) of Theorem 4.3.

Proof of Theorem 1.5

Let G be a finite simple classical group of rank r, and let Γ be a Fuchsian group as in (1.1) or (1.2).

Suppose first that Γ is co-compact of genus $g \geq 2$ ($g \geq 3$ if Γ is non-oriented). Recall that we defined $v = v(\Gamma)$ to be 2 if Γ is oriented, and 1 otherwise. By Theorem 1.2, we have

$$|\mathrm{Hom}(\Gamma, G)| \sim |G|^{vg-1} \cdot \prod_{i=1}^{d} j_{m_i}(G).$$

Using Theorem 1.4, this yields

$$|\mathrm{Hom}(\Gamma, G)| = |G|^{vg-1} \cdot |G|^{\sum_1^d 1 - \frac{1}{m_i} + \epsilon_i(r)},$$

where $|\epsilon_i(r)| < c(m_i)r^{-1}$. Since $vg - 1 + \sum_{i=1}^{d}(1 - \frac{1}{m_i}) = \mu(\Gamma) + 1$, the conclusion of Theorem 1.5 follows, with $\delta(r) = \sum_{i=1}^{d} \epsilon_i(r)$.

Finally, if Γ is non co-compact (i.e. $s + t > 0$ in (1.1) or (1.2)), then from the preamble to Theorem 1.2 we have

$$|\mathrm{Hom}(\Gamma, G)| = |G|^{vg+s+t-1} \cdot \prod_{i=1}^{d} j_{m_i}(G),$$

and the same proof works, without any assumption on the genus of Γ.

We conclude the section with a few further results concerning the functions $j_m, J_m, I_{\mathbf{m}}, I^r_{\mathbf{m}}$, which will be required later.

Corollary 4.4 *Let m, K, X, t be as in Theorem 4.3, and write $H = H(q) = X_\sigma$. Then the following hold.*

(i) *There exists $q_0 = p^a$ such that for q a power of q_0, we have $j_m(H') \sim j_m(H) \sim q^{t \dim J_m(X)}$.*

(ii) *Let $\mathbf{m} = (m_1, \ldots, m_d)$ with all $m_i \geq 2$. Then there exists $q_1 = p^b$ such that for q a power of q_1, we have*

$$|I_{\mathbf{m}}(H)| \sim |I^r_{\mathbf{m}}(H)| \sim q^{\sum \dim J_{m_i}(X)}.$$

Proof Part (i) follows from Theorem 4.3(i),(ii), and part (ii) is immediate from (i) together with (6). ∎

In later applications we shall require the following version of Proposition 4.3 for $j_m(GL_n(q))$, which also gives an explicit formula for the dimension of $J_m(GL_n(K))$ and $J_m(SL_n(K))$.

Proposition 4.5 *Fix integers $m, n \geq 2$, a prime p, and let K be an algebraically closed field.*

(i) *The conclusions of Theorem 4.3 hold for $G = GL_n(q)$ and $X = GL_n(\overline{\mathbb{F}}_p)$.*

(ii) *Writing $n = km + l$ with $k, l \in \mathbb{Z}$ and $0 \leq l < m$, we have*

$$\dim J_m(GL_n(K)) = n^2(1 - \frac{1}{m}) - l(1 - \frac{l}{m}).$$

(iii) *If m does not divide n, then given any m^{th} root of unity $\lambda \in K$, there exists $y \in GL_n(K)$ of determinant λ such that $\dim J_m(GL_n(K)) = \dim y^{GL_n(K)}$.*

(iv) *If $m|n$ then there is a unique conjugacy class $C = y^{GL_n(K)}$ such that $\dim J_m(GL_n(K)) = \dim C$; moreover, y has determinant $(-1)^{n(m+1)/m}$.*

(v) *We have* $\dim J_m(SL_n(K)) = \dim J_m(GL_n(K))$*, unless* m *is even,* m *divides* n*,* n/m *is odd and* $\mathrm{char}(K) \neq 2$*, in which case* $\dim J_m(SL_n(K)) = \dim J_m(GL_n(K)) - 2$*.*

Proof (i) This follows from the proof of Theorem 4.3.

(ii) It is proved in [20, Theorem 1] that $\dim J_m(PGL_n(K)) = n^2(1 - \frac{1}{m}) - l(1 - \frac{l}{m})$. If $x \in J_m(PGL_n(K))$, then as K is algebraically closed, x has a preimage in $J_m(GL_n(K))$. It follows that $\dim J_m(GL_n(K)) = \dim J_m(PGL_n(K))$, proving (ii).

(iii,iv) We shall frequently use the following formula which can be found in [45, IV,1.8]: for $\lambda \in K^*$, denote by $J_v(\lambda)$ the $v \times v$ Jordan block matrix with all eigenvalues λ. If $x \in GL_n(K)$ has Jordan form $(J_i(\lambda)^{n_i})$ (i.e. all eigenvalues λ, and n_i is the multiplicity of the block of size i), and $q = \max\{i : n_i > 0\}$, then

$$\dim C_{GL_n(K)}(x) = \sum_{i=1}^{q} (n_i + \ldots + n_q)^2. \tag{15}$$

Note also that $\sum_{i=1}^{q}(n_i + \ldots + n_q) = n$.

Write $m = p^a m_1$, where p is the characteristic of K and m_1 is coprime to p (take $a = 0$ if K has characteristic zero). Let $n = um_1 + t$ with $0 \leq t < m_1$, and write $u = kp^a + s$ with $0 \leq s < p^a$. Then $n = km + sm_1 + t$ and $l = sm_1 + t$. Let $\lambda_1, \ldots, \lambda_{m_1}$ be the m_1^{th} roots of 1 in K, and define

$$y = (\bigoplus_{i=1}^{m_1} J_{p^a}(\lambda_i))^k \oplus (\bigoplus_{i=1}^{t} J_{s+1}(\lambda_i)) \oplus (\bigoplus_{i=t+1}^{m_1} J_s(\lambda_i)).$$

Calculating $\dim C_{GL_n(K)}(y)$ using (15), and using (ii), we see that $\dim y^{GL_n(K)} = \dim J_m(GL_n(K))$. Moreover, since $\prod_{i=1}^{m_1} \lambda_i = (-1)^{m_1+1} = (-1)^{m+1}$, we have

$$\det(y) = (-1)^{u(m+1)} \cdot \lambda_1 \ldots \lambda_t.$$

If $t > 0$ then we can choose $\lambda_1, \ldots, \lambda_t$ with product an arbitrary m_1^{th} root of 1, giving the conclusion of (iii). So now assume that $t = 0$.

If $s > 0$ and $m_1 > 1$, define

$$z = (\bigoplus_{i=1}^{m_1} J_{p^a}(\lambda_i))^k \oplus J_{s+1}(\lambda_1) \oplus J_{s-1}(\lambda_2) \oplus (\bigoplus_{i=3}^{m_1} J_s(\lambda_i)).$$

Using (15) we see that $\dim z^{GL_n(K)} = \dim y^{GL_n(K)}$. Also $\det(z) = \det(y) \cdot \lambda_1\lambda_2^{-1}$, so between them, y and z have determinant an arbitrary m_1^{th} root of 1, and (iii) again holds.

Now assume $s = 0$ - that is, $m|n$ and $n = kp^a m_1 = km$. Here we have $\dim C_{GL_n(K)}(y) = k^2 m$ and $\det(y) = (-1)^{k(m+1)}$. We claim that $y^{GL_n(K)}$ is

the unique class of highest dimension. To see this, let $z \in J_m(GL_n(K))$, and for $1 \leq i \leq m_1$ let r_i be the multiplicity of λ_i as an eigenvalue of z. Write $r_i = k_i p^a + l_i$ with $0 \leq l_i < p^a$. By (15), for the given partition $(r_1, \ldots, r_{m_1})$ of n, the dimension of $C_{GL_n(K)}(z)$ is minimal when $z = z_1 \oplus \ldots \oplus z_{m_1}$, where

$$z_i = (J_{p^a}(\lambda_i)^{k_i}, J_{l_i}(\lambda_i)).$$

For this z we have

$$\dim C_{GL_n(K)}(z) = \sum_{i=1}^{m_1} (p^a k_i^2 + 2k_i l_i + l_i).$$

This is equal to $\frac{1}{p^a}\sum_{i=1}^{m_1} r_i^2 + l_i(1 - \frac{l_i}{p^a})$, which is clearly at least $k^2 p^a m_1$, with equality if and only if $r_i = kp^a$ for all i - that is, if and only if $z \in y^{GL_n(K)}$. This establishes the claim. Part (iv) is now proved.

(v) If m does not divide n then the conclusion follows from (iii). So assume that $m|n$. It follows from (15) that all dimensions $\dim C_{GL_n(K)}(x)$ ($x \in J_m(GL_n(K))$) have constant parity, and moreover, if

$$x = J_{p^a}(\lambda_1))^{k-1} \oplus J_{p^a-1}(\lambda_1) \oplus J_1(\lambda_1) \oplus \bigoplus_{i=2}^{m_1} J_{p^a}(\lambda_i)^k,$$

then $\dim x^{GL_n(K)} = \dim y^{GL_n(K)} - 2$. The conclusion of (v) follows. ∎

Corollary 4.6 *Let* $\mathbf{m} = (m_1, \ldots, m_d)$, *where* $m_i \geq 2$ *for all* i, *let* $E = \{i : m_i$ *even* $\}$, *let* K *be an algebraically closed field, and let* $n \geq 2$.

(i) *Then*

$$\dim I_{\mathbf{m}}(GL_n(K)) = \sum_{i=1}^{d} \dim J_{m_i}(GL_n(K)) - \epsilon,$$

where $\epsilon = 0$ *unless* $\mathrm{char}(K) \neq 2$, $m_i|n$ *for all* $i \in E$ *and* $\sum_{i \in E} \frac{n}{m_i}(m_i + 1)$ *is odd, in which case* $\epsilon = 2$.

(ii) *Writing* $n = k_i m_i + l_i$ *with* $0 \leq l_i < m_i$, *we have*

$$\dim I_{\mathbf{m}}(GL_n(K)) = n^2 \cdot \sum_{i=1}^{d} (1 - \frac{1}{m_i}) - \sum_{i=1}^{d} l_i(1 - \frac{l_i}{m_i}) - \epsilon,$$

where ϵ *is as in part* (i).

Proof (i) By Proposition 4.5, for each i we can choose $y_i \in J_{m_i}(GL_n(K))$ such that $\dim y_i^{GL_n(K)} = \dim J_{m_i}(GL_n(K))$ and $\det(y_i) = \pm 1$. If m_i does not divide n for some $i \in E$, then by 4.5(ii), both 1 and -1 are possible for

$\det(y_i)$, so we can choose the y_j so that $\prod_{j=1}^d \det(y_j) = 1$; then $(y_1, \dots, y_d) \in I_{\mathbf{m}}(GL_n(K))$, and hence

$$\dim I_{\mathbf{m}}(GL_n(K)) = \sum_{i=1}^d \dim J_{m_i}(GL_n(K)). \tag{16}$$

Now suppose $m_i | n$ for all $i \in E$. Then by 4.5(iv), $\det(y_i) = (-1)^{n(m_i+1)/m_i}$ for $i \in E$, while $\det(y_i) = 1$ for $i \notin E$, giving

$$\prod_{i=1}^d \det(y_i) = (-1)^{\sum_{i \in E} n(m_i+1)/m_i}.$$

If this product is 1 then (16) holds again. If it is -1 (and $\mathrm{char}(K) \neq 2$), then $\prod_{i \in E} \det(y_i) = -1$, so since -1 is not a product of m_i^{th} roots of 1 for $i \notin E$, we see that (16) does not hold. In this case, choose $i \in E$ such that $n(m_i + 1)/m_i$ is odd, and using 4.5(v), replace y_i by $z_i \in J_{m_i}(GL_n(K))$ of determinant 1 such that $\dim z_i^{GL_n(K)} = \dim J_{m_i}(SL_n(K)) = \dim J_{m_i}(GL_n(K)) - 2$. Then $(y_1, \dots, z_i, \dots, y_d) \in I_{\mathbf{m}}(GL_n(K))$, and hence we see that in this case

$$\dim I_{\mathbf{m}}(GL_n(K)) = \sum_{i=1}^d \dim J_{m_i}(GL_n(K)) - 2.$$

Part (i) is now proved.

Part (ii) follows from (i) together with the formula in Proposition 4.5(ii). ■

5 Maximal subgroups

Recall that for a finite group M and a real number s, we define

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

In this section we prove the following result, which will be one of the main tools in our proof of Theorem 1.6.

Theorem 5.1 *Let G be a finite simple group of Lie type of rank r over $\mathbb{F}_q$, and let M be a maximal subgroup of G. Then there are absolute constants $c, \epsilon > 0$ such that*

$$\zeta^M(1) \leq \frac{c|G:M|}{q^{\epsilon r}},$$

unless $G = L_2(q)$ and M is a parabolic subgroup, in which case $\zeta^M(1) \sim |G : M| \sim q$.

We prove Theorem 5.1 in a series of lemmas.

Let G be a finite simple group of Lie type of rank r over $\mathbb{F}_q$, and let M be a maximal subgroup of G.

Lemma 5.2 *If M is not a parabolic subgroup of G, then the conclusion of Theorem* 5.1 *holds.*

Proof Obviously $\zeta^M(1) \leq k(M)$, the number of conjugacy classes of M, so we may assume that

$$k(M) \cdot |M| \cdot q^{\epsilon r} > c|G|, \tag{17}$$

where ϵ is an arbitrarily small, and c an arbitrarily large, positive constant.

Suppose G is classical, say $G = Cl_n(q)$, with natural module V of dimension n over $\mathbb{F}_{q^u}$ (where $u = 2$ if G is unitary, $u = 1$ otherwise). By Aschbacher's theorem [1], either M lies in one of the families $\mathcal{C}_i$ $(1 \leq i \leq 8)$ of subgroups of G, or M lies in a family $\mathcal{S}$ of almost simple subgroups acting absolutely irreducibly on V; for explicit descriptions of the families $\mathcal{C}_i$ and full definition of $\mathcal{S}$, see also [17].

If $M \in \mathcal{C}_1$ then as M is not parabolic, it is of the form $Cl_k(q) \times Cl_{n-k}(q)$ (the stabilizer of a non-degenerate subspace of V). Now an easy check using Lemma 2.1(i) shows that (17) is violated: for example if $G = Sp_{2r}(q)$ and $M = Sp_{2m}(q) \times Sp_{2r-2m}(q)$ (so $n = 2r, k = 2m$), then 2.1(i) and (17) give

$$q^{(1+\epsilon)r} \cdot q^{2m^2+m+2(r-m)^2+r-m} > c_1 q^{2r^2+r},$$

leading to $(1+\epsilon)r > 4m(r-m)$, which is impossible.

For $M \in \mathcal{C}_i$ with $2 \leq i \leq 8$, the argument is similar, noting the following rough structure of such subgroups:

$\mathcal{C}_2$: $Cl_m(q) \wr S_k\,(mk = n)$, or $GL_{n/2}(q^u)$
$\mathcal{C}_3$: $Cl_m(q^k)\,(mk = n)$, or $GU_{n/2}(q)$
$\mathcal{C}_5$: $Cl_n(q^{1/k})\,(k \geq 2)$, or $PSp_n(q), PSO_n(q) < G = U_n(q)$
$\mathcal{C}_8$: $PSp_n(q), PSO_n(q), U_n(q^{1/2}) < L_n(q)$, or $O_n(q) < Sp_n(q)\,(q$ even$)$.

(Subgroups in the classes $\mathcal{C}_4, \mathcal{C}_6, \mathcal{C}_7$ are too small to concern us, having orders much less than $|G|^{1/2}$.)

Finally, consider $M \in \mathcal{S}$. Here, for later use we establish the bound

$$k(M) < c|G : M|^{1/2}, \tag{18}$$

which is more than enough to violate (17). Now [22, 4.1] gives either $|M| < q^{3un}$, or $M \in \{A_{n+\delta}, S_{n+\delta}\}$ with $\delta = 1$ or 2. In the latter case (18) clearly holds. Next, observe that Lemma 2.1(i) implies that $k(M) < c|M|^{1/2}$. Hence, in establishing (18) we may assume that $|M|^{1/2} > c|G : M|^{1/2}$, which gives $|G| < c_1|M|^2 < c_1 q^{6un}$. Inspection of the orders of the simple groups $G = Cl_n(q)$ now shows that $n \leq 12$. For $n \leq 12$ we may assume that $F^*(M) \in \mathrm{Lie}(p)$ where $q = p^e$ (otherwise $|M|$ is bounded), and it is simple to list the possible such groups having irreducible representations of dimension $n \leq 12$ (see [34] for example). In all cases (18) holds.

Now suppose that G is of exceptional type. By (17) we may assume that $|M| > |G|^{\frac{1}{2}-\nu}$ for ν arbitrarily small and positive. Hence M is given by [24, Table 1], and inspection of this list, together with Lemma 2.1(i) shows that (17) is violated. ∎

In view of Lemma 5.2, we assume from now on that M is a parabolic subgroup, say $M = QL$, where Q is the unipotent radical and L a Levi subgroup.

We shall need some fairly crude information about $k(M)$, the number of conjugacy classes of the maximal parabolic subgroup M. By [2], there is an L-invariant central series

$$1 = Q_0 \lhd Q_1 \lhd \cdots \lhd Q_l = Q$$

such that each factor Q_i/Q_{i-1} has the structure of an irreducible L-module over $\mathbb{F}_q$ (or possibly an extension field if G is twisted). Write $V_i = Q_i/Q_{i-1}$.

Lemma 5.3 *Let $C(L)$ be a set of conjugacy class representatives of the Levi subgroup L, and denote by $o(L, Q)$ the number of orbits of L on Q. Then*

$$k(M) \leq o(L, Q) + \sum_{1 \neq x \in C(L)} (\prod_{i=1}^{l} |C_{V_i}(x)|).$$

Proof Every element of M is conjugate to an element of a coset Qx with $x \in C(L)$. The number of M-classes in the coset Q is at most $o(L, Q)$. Now consider a coset Qx with $1 \neq x \in C(L)$. For any $u \in Q$ we have

$$|C_Q(ux)| \leq \prod_{i=1}^{k} |C_{V_i}(x)|,$$

and hence $|(ux)^Q| \geq |Q|/(\prod |C_{V_i}(x)|)$. Hence the number of Q-classes in Qx is at most $\prod |C_{V_i}(x)|$. The conclusion follows. ∎

Here are our estimates for conjugacy class numbers of maximal parabolic subgroups.

Proposition 5.4 *There is an absolute constant $c > 0$ such that if G is a classical group of rank r over $\mathbb{F}_q$, and $M = QL$ is a maximal parabolic subgroup of G, then*

$$k(M) < c|Q| \cdot q^{2r/3}.$$

Proposition 5.5 *There are absolute constants $c, \rho > 0$ such that if G is an exceptional group of Lie type over $\mathbb{F}_q$, and $M = QL$ is a maximal parabolic subgroup of G, then*

$$k(M) < c|Q| \cdot q^{-\rho}.$$

Proof of Proposition 5.4

Suppose first that $G = SL_n(q)$, and let $M = P_m$, the stabilizer of an m-space. Then $M = QL$ with $L = (GL_m(q) \times GL_{n-m}(q)) \cap G$ and $Q \cong V_m(q) \otimes V_{n-m}(q)$ as an $\mathbb{F}_q L$-module. Since $P_m \cong P_{n-m}$, we may assume that $m \leq n/2$.

If $n = 2$ then $M = P_1 \cong AGL_1(q)$, and it is trivial to see that $k(M) = q$, giving the conclusion. So assume that $n \geq 3$.

Let $C(L)$ be a set of class representatives for L. Then $|C(L)| < cq^{n-1}$ by Lemma 2.1. Set $C(L)^* = C(L)\backslash\{1\}$, and define

$$\begin{aligned} C_1 &= C(L)^* \cap (1 \otimes GL_{n-m}(q)), \\ C_2 &= C(L)^* \cap (GL_m(q) \otimes 1), \\ C_3 &= C(L)^* \backslash (C_1 \cup C_2), \end{aligned}$$

and for $1 \leq i \leq 3$, let $\Sigma_i = \sum_{x \in C_i} |C_Q(x)|$. By Lemma 5.3, we have

$$k(M) \leq o(L, Q) + \Sigma_1 + \Sigma_2 + \Sigma_3. \tag{19}$$

For $x \in C_2 \cup C_3$ we have $\dim[Q, x] = \dim Q - \dim C_Q(x) \geq n - m$ (see (22) below). Hence

$$\Sigma_2 + \Sigma_3 < cq^{n-1} \cdot |Q| \cdot q^{-(n-m)} = c|Q| \cdot q^{m-1} \leq c|Q| \cdot q^{2r/3}, \tag{20}$$

the last inequality since $r = n - 1$ and $m \leq n/2$.

To estimate Σ_1, subdivide C_1 into the following two subsets:

$$C_1' = \{1 \otimes y \in C_1 \,:\, \dim C_{V_{n-m}}(y) \geq 2(n-m)/3\}, \;\; C_1'' = C_1 \backslash C_1'.$$

For $1 \otimes y \in C_1'$ we have $y \in GL_{[2(n-m)/3]}(q) \oplus 1 < GL_{n-m}(q)$, so by Lemma 2.1,

$$|C_1'| < cq^{[2(n-m)/3]}.$$

Also $|C_1''| < |C_1| < cq^{n-m}$, and for $x = 1 \otimes y \in C_1''$ we have $\dim C_Q(x) \leq 2m(n-m)/3$. Hence, defining $\Sigma_1' = \sum_{x \in C_1'} |C_Q(x)|$, $\Sigma_1'' = \sum_{x \in C_1''} |C_Q(x)|$, we have

$$\Sigma_1 = \Sigma_1' + \Sigma_1'' < cq^{[2(n-m)/3]} \cdot |Q| + cq^{n-m} \cdot q^{2m(n-m)/3}$$

$$\leq c|Q| \cdot (q^{[2(n-m)/3]} + q^{(n-m)(1-\frac{m}{3})}) \leq c|Q| \cdot q^{2r/3} \qquad (21)$$

(recall that the rank $r = n - 1$ here).

Now observe that $o(L, Q) \leq cm$. Hence the conclusion follows from (19), (21) and (20). This completes the proof for $G = L_n(q)$.

Next consider $G = Sp_n(q)$ (with $n = 2r$). Take $M = P_m$, the stabilizer of a totally isotropic m-space. Here $L = GL_m(q) \times Sp_{2r-2m}(q)$ and Q has an L-invariant central series $1 \leq Q_1 \leq Q$, where as L-modules $Q/Q_1 \cong V_m(q) \otimes V_{2r-2m}(q)$ and $Q_1 \cong S^2(V_m(q))$ (with trivial action of the factor $Sp_{2r-2m}(q)$ on Q_1). If $m < r$ we argue as above with the factor $M/Q_1 \cong (V_m(q) \otimes V_{2r-2m}(q)).(GL_m(q) \times Sp_{2r-2m}(q))$, obtaining $k(M/Q_1) < c|Q/Q_1| \cdot q^{2r/3}$. And if $m = r$ then we have $M = P_r = (S^2(V_r(q)).GL_r(q)$. A simple check shows that if $1 \neq x \in L$ then $\dim[Q, x] \geq r/3$, hence $\dim C_Q(x) \leq \dim Q - (r/3)$. Therefore, letting $C(L)$ denote a set of class representatives from L (so that $|C(L)| < cq^r$ by Lemma 2.1), we have

$$\sum_{1 \neq x \in C(L)} |C_Q(x)| < cq^r \cdot |Q| \cdot q^{-r/3} = c \cdot |Q| \cdot q^{2r/3}.$$

The conclusion now follows from Lemma 5.3.

Similar arguments yield a proof for the other classical groups $Cl_n(q)$, noting that $L = GL_m(q^u) \times Cl_{n-2m}(q)$ and Q has an L-invariant series $1 \leq Q_1 \leq Q$, where Q_1 and Q/Q_1 are the following L-modules:

$$\begin{array}{ll} G = SO_n(q): & Q_1 \cong \wedge^2(V_m(q)),\ Q/Q_1 \cong V_m(q) \otimes V_{n-2m}(q) \\ G = SU_n(q): & Q_1 \cong V_m(q^2) \otimes V_m(q^2)^{(q)} \text{ (realised over } \mathbb{F}_q), \\ & Q/Q_1 \cong V_m(q^2) \otimes V_{n-2m}(q^2). \end{array}$$

This completes the proof of Proposition 5.4. ∎

For the proof of Proposition 5.5, we require some results which classify the possibilities for the L-modules $V_i = Q_i/Q_{i-1}$ occurring within Q, and some information about the action of L on such modules. This is given in the next two lemmas. We use the standard notation for irreducible representations of groups of Lie type in the natural characteristic: thus $V(\lambda) = V_G(\lambda)$ denotes the irreducible G-module of high weight λ in characteristic p. We often abbreviate $V(\lambda)$ by writing just λ. Also for groups of small rank we write $ab...$ to represent the weight $a\lambda_1 + b\lambda_2 + ...$, where $a, b, ...$ are non-negative integers and the λ_i are the fundamental dominant weights. Finally, if V is a G-module in characteristic p, we write $V = V(\lambda)/V(\lambda')/\ldots$ or just $\lambda/\lambda'\ldots$ to indicate that the composition factors of V are $V(\lambda), V(\lambda'), \ldots$.

We need a definition, taken from [30]: if K is a field, and V a finite-dimensional vector space over K, set $\bar{V} = V \otimes \bar{K}$ (where $\bar{K}$ is the algebraic closure of K), and for $x \in GL(V)$ define

$$\nu(x) = \nu_V(x) = \min\ \{\dim[\bar{V}, \alpha x]\ :\ \alpha \in \bar{K}^*\}.$$

Table 2

G	λ	$\dim V(\lambda)$	n_λ
$E_7(q)$	λ_7	56	14
$E_6^\epsilon(q)$	λ_1	27	8
$A_n^\epsilon(q)\,(n \geq 3)$	λ_2	$\frac{1}{2}n(n+1)$	n
$A_n^\epsilon(q)\,(n \geq 5)$	λ_3	$\frac{1}{6}n(n^2-1)$	$n+3$
$D_7^\epsilon(q)$	λ_6	64	8
$D_6^\epsilon(q)$	λ_5	32	8
$D_5^\epsilon(q)$	λ_4	16	5
$B_3(q)$	λ_3	8	4
$C_3(q), (q$ odd)	λ_3	14	4

We shall also need the following elementary fact, taken from [30, 3.7]: if V_a, V_b are K-vector spaces of dimensions a, b respectively, and $x = x_1 \otimes x_2 \in GL(V_a) \otimes GL(V_b)$ is an element of prime order (acting in the obvious way on $V_a \otimes V_b$), then

$$\nu_{V_a \otimes V_b}(x) \geq \max\,(a\nu_{V_b}(x_2), b\nu_{V_a}(x_1)). \tag{22}$$

Lemma 5.6 *Let G be a finite group of Lie type over $\mathbb{F}_q$, and let $V = V(\lambda)$ be an irreducible $\bar{\mathbb{F}}_q G$-module of high weight λ as in Table 2. Then for any semisimple element $x \in G \backslash Z(G)$, we have $\nu_V(x) \geq n_\lambda$, where n_λ is as specified in the table.*

Moreover, for the entries in the table for $G = D_5^\epsilon(q)$ or $C_3(q)$, the number of G-classes of semisimple elements x with $\nu_V(x) \leq 6$ is at most c or cq, respectively.

Proof For G of type A_n, we have $V(\lambda) = \wedge^2(W)$ or $\wedge^3(W)$ where W is the natural G-module, and finding a lower bound for $\nu(x)$ with $x \in G$ semisimple is a routine calculation; in all cases the minimum value is attained by a diagonal matrix having an eigenspace on W of codimension 1 or 2. For $G = E_7(q)$ note that if $A_7(q)$ is a subgroup of maximal rank in G, we have $V(\lambda_7) \downarrow A_7(q) = V_{A_7}(\lambda_2) + V_{A_7}(\lambda_6)$ (see [25, 2.3]), and the bound follows from the A_7 bound of 7 on $V_{A_7}(\lambda_2)$ already observed. Likewise, for G of type E_6, the restriction $V(\lambda_1) \downarrow A_1A_5 = (1 \otimes \lambda_1)/(0 \otimes \lambda_4)$ yields the bound 8 for $\nu(x)$. The bounds for spin modules of D_n are obtained similarly by restricting to a Levi subgroup T_1A_{n-1} using [25, 2.6]; the bound for B_3 is clear; and the bound for C_3 follows from the fact that the 14-dimensional module $V(\lambda_3)$ is the wedge-cube of the natural module, factored out by a copy of the natural module. Finally, the last sentence of the lemma follows from the above considerations as well. ■

We now complete the proof of Proposition 5.5 by using Lemma 5.6 together with Proposition 5.3, observing some relevant L-modules which occur as composition factors in Q. Here are the details.

Lemma 5.7 *Let G be exceptional of Lie type over $\mathbb{F}_q$, and let $M = QL$ be a maximal parabolic subgroup of G. Table 3 below lists some of the high weights λ of irreducible L-modules which occur as composition factors within Q. (The λ's are listed only up to duals.)*

Proof This is routine computation. Write $L(G)$ for the adjoint module for G over $\bar{\mathbb{F}}_q$ (so $L(G)$ is the restriction to G of the Lie algebra $L(\bar{G})$, where $\bar{G}$ is the simple algebraic group corresponding to G). The composition factors of the restriction of the adjoint module $L(G) \downarrow L'$ can be read off using [25, 2.1]. Further, if Q^- denotes the unipotent radical of the parabolic opposite to M, then $L(G) = L(Q) + L(L) + L(Q^-)$, all three subspaces fixed by L, and as L-modules, $L(Q^-)$ affords the dual of $L(Q)$. It is therefore straightforward to compute the L'-composition factors of $L(Q)$, giving the conclusion. ■

Proof of Proposition 5.5

Let G be an exceptional group of Lie type of rank $r = r(G)$ over $\mathbb{F}_q$, and let $M = QL$ be a maximal parabolic subgroup. Assume for now that G is not of type ${}^2B_2$, ${}^2G_2$, G_2 or ${}^3D_4$; we handle these cases at the end of the proof.

Adopt the notation of the preamble to Lemma 5.3: so $1 = Q_0 < Q_1 < \cdots < Q_l = Q$, and $V_i = Q_i/Q_{i-1}$ are the L-composition factors within Q. Let $C(L)$ be a set of conjugacy class representatives of non-identity elements of L, and let $C(L)^\dagger$ consist of those elements of $C(L)$ whose semisimple part lies in $Z(L)$. For $x \in L$ set $\nu_i(x) = \nu_{V_i}(x)$. Then Lemma 5.3 gives

$$k(M) \leq o(L,Q) + \sum_{x \in C(L)^\dagger} |C_Q(x)| + |Q| \cdot \sum_{x \in C(L) \setminus C(L)^\dagger} q^{-\sum_1^l \nu_i(x)}.$$

Now $|Z(L)| < cq$ (except for the cases where $(G, L') = ({}^2E_6(q), {}^2D_4(q))$ or $({}^2E_6(q), A_1(q^2)A_2(q))$, when $|Z(L)| < cq^2$). Also the number of unipotent classes in L is bounded by a constant, and hence $|C(L)^\dagger| < c'q$ (or $c'q^2$ in the exceptional cases). Since every non-identity element of $Z(L)$ acts nontrivially on some composition factor V_i listed in Table 3, it follows that

$$o(L,Q) + \sum_{x \in C(L)^\dagger} |C_Q(x)| \leq c|Q| \cdot q^{-1}.$$

Now we know from Lemma 2.1 that $|C(L)| < cq^r$. Hence it will suffice to show that for $x \in C(L) \setminus C(L)^\dagger$, we have

$$\sum_{i=1}^{l} \nu_i(x) > r(G). \tag{23}$$

Table 3

type of G	type of L'	λ
E_8	E_7	λ_7
	A_7	$\lambda_1, \lambda_2, \lambda_3$
	A_1A_6	$1 \otimes \lambda_1, 1 \otimes \lambda_2, 0 \otimes \lambda_1, 0 \otimes \lambda_3$
	$A_1A_2A_4$	$1 \otimes 10 \otimes \lambda_1, 0 \otimes 01 \otimes \lambda_1, 1 \otimes 00 \otimes \lambda_2, 0 \otimes 10 \otimes \lambda_2$
	A_3A_4	$100 \otimes \lambda_2, 000 \otimes \lambda_2, 100 \otimes \lambda_4, 010 \otimes \lambda_4$
	A_2D_5	$10 \otimes \lambda_4, 00 \otimes \lambda_4, 10 \otimes \lambda_1$
	A_1E_6	$1 \otimes \lambda_1, 0 \otimes \lambda_1$
	D_7	λ_1, λ_6
E_7	D_6	λ_5
	A_6	λ_1, λ_3
	A_1A_5	$1 \otimes \lambda_2, 0 \otimes \lambda_2$
	$A_1A_2A_3$	$1 \otimes 10 \otimes \lambda_1, 0 \otimes 10 \otimes \lambda_2$
	A_2A_4	$10 \otimes \lambda_1, 10 \otimes \lambda_2$
	A_1D_5	$0 \otimes \lambda_1, 1 \otimes \lambda_4$
	E_6	λ_1
E_6^ϵ	$D_5\,(\epsilon = +)$	λ_4
	$D_4^-\,(\epsilon = -)$	$\lambda_1, \lambda_3, \lambda_4$
	A_5^ϵ	λ_3
	$A_1A_4\,(\epsilon = +)$	$0 \otimes \lambda_1, 1 \otimes \lambda_2$
	$A_1(q^2)A_2(q)\,(\epsilon = -)$	$1 \otimes 1 \otimes 10, 0 \otimes 1 \otimes 10, 1 \otimes 0 \otimes 10$
	$A_1A_2A_2\,(\epsilon = +)$	$1 \otimes 10 \otimes 10, 0 \otimes 10 \otimes 10$
	$A_1(q)A_2(q^2)\,(\epsilon = -)$	$1 \otimes 10 \otimes 10^{(q)}, 0 \otimes 10 \otimes 10^{(q)}$
F_4	C_3	$\lambda_3\,(q \text{ odd})$
		$\lambda_3, \lambda_1\,(q \text{ even})$
	$A_1\tilde{A}_2$	$1 \otimes 02, 0 \otimes 02\,(q \text{ odd})$
		$1 \otimes 02, 0 \otimes 02, 1 \otimes 10, 0 \otimes 10\,(q \text{ even})$
	$\tilde{A}_1A_2$	$2 \otimes 10, 1 \otimes 10, 0 \otimes 10\,(q \text{ odd})$
		$2 \otimes 10, 1 \otimes 10, (0 \otimes 10)^2\,(q \text{ even})$
	B_3	λ_1, λ_3
${}^2F_4$	${}^2B_2$	10^2
	A_1	$1, 2^a, 1 \otimes 2^a$
G_2	A_1	1^2
	$\tilde{A}_1$	$3\,(p \neq 3)$
		$3, 1\,(p = 3)$
${}^3D_4$	$A_1(q)$	1^4
	$A_1(q^3)$	$1 \otimes 1^{(q)} \otimes 1^{(q^2)}$

By definition of $C(L)^\dagger$, each element of $C(L)\backslash C(L)^\dagger$ has a power which is a non-identity semisimple element of $L\backslash Z(L)$. Hence (23) follows quickly from Lemmas 5.7 and 5.6 together with (22), except in the following cases: $(G, L') = (E_6^-, D_4^-), (E_6, D_5)$ or (F_4, C_3). In the last two cases the extra refinement in the last sentence of Lemma 5.6 gives the conclusion. And in the first, we have $\nu_{V(\lambda_i)}(x) \geq 2$ for any non-identity semisimple $x \in D_4^-(q)$ (where $i = 1, 3$ or 4); moreover, if $\nu_{V_1}(x) = 2$ then $\nu_{V_i}(x) > 2$ for $i = 3$ or 4, and this yields (23).

We complete the proof by handling the postponed cases where G is of type ${}^2B_2$, ${}^2G_2$, G_2 or ${}^3D_4$. In the first two cases $M = QL$ is a Borel subgroup, with $|Q| = q^2$ or q^3 and L cyclic of order $q - 1$. Moreover, $|Z(Q)| = q$, and L acts faithfully on both $Z(Q)$ and $Q/Z(Q)$. Hence Lemma 5.3 gives $k(M) \leq cq$ or cq^2 respectively, as required. Now consider $G = G_2(q)$. Let T be a maximal torus of order $(q-1)^2$ in L. Then T lies in a maximal rank subgroup of G of type $A_1\tilde{A}_1(q)$, and $(L(G_2)/L(A_1\tilde{A}_1)) \downarrow A_1\tilde{A}_1 = 1 \otimes 3$ (or $1 \otimes (3/1)$ if $p = 3$). Hence we can parametrise T by ordered pairs $(c, d) \in (\mathbb{F}_q^*)^2$, where (c, d) has eigenvalues $c^{\pm 1}, d^{\pm 3}$ on the L-composition factors of Q listed in Table 3. It follows that

$$\sum_{x \in C(L)\backslash C(L)^\dagger} q^{-\sum_1^l \nu_i(x)} < cq^{-1},$$

and now the conclusion follows as above. The argument for $G = {}^3D_4(q)$ is similar, taking T of order $(q-1)(q^3-1)$ in a maximal rank subgroup of type $A_1(q)A_1(q^3)$.

This completes the proof of Proposition 5.5.

Proof of Theorem 5.1

We are now in a position to complete the proof of 5.1. Let G be a finite simple group of Lie type of rank r over $\mathbb{F}_q$, and let M be a maximal subgroup of G. Recall that

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

By Lemma 5.2, we may assume that M is a parabolic subgroup of G.

If G is of exceptional type, the result is immediate from Proposition 5.5, since clearly $\zeta^M(1) \leq k(M)$.

Now assume that G is classical. Write $M = P_m = QL$ as above. Our estimation of $\zeta^M(1)$ requires one further ingredient.

Lemma 5.8 *If χ is an irreducible character of M such that $Q \not\leq \ker\chi$, then $\chi(1) > cq^{r-1}$, where $c > 0$ is an absolute constant; further, in the case where $G = L_n(q)$ we have $\chi(1) > cq^r$.*

Proof First consider $G = L_n(q)$. Here $Q = V_m(q) \otimes V_{n-m}(q)$ and L is the image modulo scalars of $(GL_m(q) \times GL_{n-m}(q)) \cap SL_n(q)$. By Clifford's theorem, $\chi \downarrow Q = e \sum \theta_i$, where e is an integer and the θ_i are L-conjugate linear characters of Q. Consequently, $\chi(1)$ is at least the size of a nontrivial orbit of L on the linear characters of Q, and such an orbit has size at least $(q^m - 1)(q^{n-m} - 1)/(q - 1)$ (see for example [17, 5.2.2]), which is at least $cq^{n-1} = cq^r$, as required.

Next consider $G = PSp_{2r}(q)$. This is a little more complicated. Again let $M = P_m$. As described in the proof of Proposition 5.4, we have $L = GL_m(q) \times Sp_{2r-2m}(q)$ (modulo scalars), and Q has an L-invariant central series $1 < Q_1 < Q$, where as L-modules $Q/Q_1 \cong V_m(q) \otimes V_{2r-2m}(q)$ and $Q_1 \cong S^2(V_m(q))$ (with trivial action of the factor $Sp_{2r-2m}(q)$ on Q_1). Note that $GL_m(q)$ acts irreducibly on Q_1 if q is odd, while if q is even, Q_1 has a unique $GL_m(q)$-submodule $Q_0 \cong \wedge^2(V_m(q))$, and Q_1/Q_0 is irreducible of dimension m.

Let $\chi \in Irr(M)$ with $Q \not\leq \ker \chi$. If $Q_1 \leq \ker \chi$ then $\chi(1)$ is at least the size of a nontrivial orbit of L on Q/Q_1, hence is at least cq^{2r-m-1} (see [17, 5.2.2]), giving the conclusion. So suppose now that $Q_1 \not\leq \ker \chi$. Let S be the factor $Sp_{2r-2m}(q)$ of L, so $QS \lhd M$. By Clifford's theorem, we can write

$$\chi \downarrow QS = e \sum_{i=1}^{t} \chi_i,$$

where e is a positive integer, and the χ_i are distinct, L-conjugate irreducible characters of QS.

Suppose first that $m > 1$ and the factor $SL_m(q)$ of L fixes χ_i for all i. Then $Q \cap \ker \chi_i$ is $SL_m(q)$-invariant for all i. It is also S-invariant, and hence $Q \cap \ker \chi_i = 1, Q_0, Q_1$ or Q. Since $QS/\ker \chi_i$ must have cyclic centre, this forces $Q_1 \leq \ker \chi_i$, a contradiction. Hence either $m = 1$, or the factor $SL_m(q)$ permutes the χ_i nontrivially. In particular, $t > cq^{m-1}$.

One checks (for example by matrix calculations) that the normal closure of S in QS is the whole group QS. Hence $S \not\leq \ker \chi_i$, and so $\chi_i(1) \geq q^{r-m}$ by Lemma 2.1(ii). It follows that

$$\chi(1) = t\chi_i(1) > cq^{m-1} \cdot q^{r-m} = cq^{r-1},$$

as required.

This completes the proof for $G = PSp_{2r}(q)$, and the proof for the other classical groups is similar, using the structure of the maximal parabolic subgroups given in the proof of Proposition 5.4. ∎

We now conclude the proof of Theorem 5.1. Write $\zeta^M(1) = \Sigma_1 + \Sigma_2$, where

$$\Sigma_1 = \sum_{\chi \in Irr(M), Q \leq ker(\chi)} \chi(1)^{-1}, \ \ \Sigma_2 = \sum_{\chi \in Irr(M), Q \not\leq ker(\chi)} \chi(1)^{-1}.$$

Note that $\Sigma_1 = \zeta^L(1)$. Now $|L/L'| < c_1 q^2$, and L' has a characteristic subgroup L_0 of bounded index which is a central product of at most three quasisimple groups. By Theorem 1.1, $\zeta^{L_0}(1)$ is bounded. Using the easy inequality $\zeta^L(1) \leq |L/L_0|\zeta^{L_0}(1)$, it follows that

$$\Sigma_1 < cq^2. \tag{24}$$

Further, by Propositions 5.4 and 5.8, we have

$$\Sigma_2 < \frac{c|Q| \cdot q^{2r/3}}{q^{r-1}} \tag{25}$$

(and the denominator can be improved to q^r for $G = L_n(q)$).

Since $|G : M| \sim |Q|$, the conclusion of Theorem 5.1 follows from (24) and (25), except when $r \leq 3$. For these low rank groups, the conclusion is obtained by improving the bound in Proposition 5.4, tightening the argument slightly. We do this for $G = L_2(q)$, $U_3(q)$ and $PSp_4(q)$ and leave the remaining groups of rank at most 3 (viz. $L_3(q), L_4(q), U_4(q), PSp_6(q)$) to be dealt with in similar fashion by the reader.

Suppose $G = L_2(q)$. Here $M = P_1 = (\mathbb{F}_q).((q-1)/\delta)$, where $\delta = (q-1, 2)$. Here L acts fixed point freely on Q, hence $k(M) \leq q$. Also M has $(q-1)/\delta$ linear characters, and the rest have degree at least cq. Consequently

$$(q-1)/\delta \leq \zeta^M(1) < (q-1)/\delta + q/cq.$$

Thus $\zeta^M(1) \sim |G : M| \sim q$, giving the exceptional case in Theorem 5.1.

Next let $G = U_3(q)$. Here $M = QL$ with $Q = q^{1+2}$ and $L = (q^2-1)/\delta$ where $\delta = (3, q+1)$. Again L is fixed point free on $Q/Z(Q) = q^2$, so $k(M) < cq^3$. Irreducible characters χ of M with $Q \not\leq \ker \chi$ have degree at least q. Hence we get

$$\zeta^M(1) < c(q^2 + q^3/q).$$

Since $|G : M| = q^3 + 1$ this shows that $\zeta^M(1) < c|G : M|q^{-1}$, giving the result.

Finally consider $G = PSp_4(q)$ with $M = P_1 = QL$; here we have $1 < Q_1 < Q$ with $|Q_1| = q$ and $Q/Q_1 \cong \mathbb{F}_q^2$, and $L \cong GL_2(q)/\langle -1 \rangle$, acting naturally on Q/Q_1 and as the determinant on Q_1. Now L has only cq classes having nontrivial centralizer in Q/Q_1, and hence Lemma 5.3 gives $k(M) < cq^3$. Now we complete the argument in the usual way. The proof for $M = P_2$ has no novel features.

This completes the proof of Theorem 5.1.

6 Random homomorphisms

In this section we prove Theorem 1.6. Let Γ be a Fuchsian group in $\mathcal{F}$, let $v = v(\Gamma)$, and let G be a finite simple group.

Theorem 1.6 is established in [32] for G alternating, so we assume that G is a simple group of Lie type of rank r over $\mathbb{F}_q$.

Lemma 6.1 *The probability that a randomly chosen homomorphism in* $\mathrm{Hom}(\Gamma, G)$ *is an epimorphism is at least*

$$1 - (1 + o(1)) \sum_{M \ max \ G} \zeta^M(vg-2) \cdot |G:M|^{-(vg-1)}.$$

Proof Let Q be the complementary probability. Then

$$Q \leq \sum_{M \ max \ G} \frac{|\mathrm{Hom}(\Gamma, M)|}{|\mathrm{Hom}(\Gamma, G)|}.$$

By Theorem 1.2,

$$|\mathrm{Hom}(\Gamma, G)| \geq (1 + o(1))|G|^{vg-1} \cdot \prod_{i=1}^{d} j_{m_i}(G).$$

By Lemma 3.3 we have

$$|\mathrm{Hom}(\Gamma, M)| \leq |M|^{vg-1} \cdot \prod_{i=1}^{d} j_{m_i}(M) \cdot \zeta^M(vg-2).$$

It follows that

$$\frac{|\mathrm{Hom}(\Gamma, M)|}{|\mathrm{Hom}(\Gamma, G)|} \leq (1 + o(1)) \cdot \zeta^M(vg-2) \cdot |G:M|^{-(vg-1)},$$

giving the result. ∎

We shall also use the following result, taken from [27, Section 3] and [28, 2.1].

Lemma 6.2 *Let G be a finite simple group. Then*

(i) $\sum_{M\ max\ G} |G:M|^{-2} \to 0$ *as* $|G| \to \infty$*;*

(ii) *if G is classical and $s > 1$ then* $\sum_{M\ max\ G} |G:M|^{-s} \to 0$ *as* $|G| \to \infty$.

Proof of Theorem 1.6

Note that by our assumptions on Γ we have $vg - 2 \geq 1$, and so $\zeta^M(vg-2) \leq \zeta^M(1)$. In view of Lemma 6.1, it suffices to show that

$$T(G) = \sum_{M\ max\ G} \zeta^M(1) \cdot |G:M|^{-(vg-1)} \to 0 \text{ as } |G| \to \infty. \tag{26}$$

We distinguish between four cases.

Case 1: $(v,g) \neq (1,3)$.

It follows from Theorem 5.1 that $\zeta^M(1) \leq c|G:M|$. This yields

$$T(G) \leq \sum_{M\ max\ G} c|G:M| \cdot |G:M|^{-(vg-1)} = c \sum_{M\ max\ G} |G:M|^{-(vg-2)}.$$

Our assumptions on (v,g) imply $vg - 2 \geq 2$, and so Lemma 6.2(i) yields $T(G) \to 0$ as $|G| \to \infty$.

Case 2: $v = 1, g = 3$, G is classical, and $G \neq L_2(q)$.

Let $\mathcal{C}$ denote the set of maximal subgroups of G belonging to the Aschbacher classes $\mathcal{C}_1, \ldots, \mathcal{C}_8$, and let $\mathcal{S}$ denote the remaining maximal subgroups (see the proof of Lemma 5.2). Note that $vg - 1 = 2$. Set

$$T_1(G) = \sum_{M \in \mathcal{C}} \zeta^M(1) \cdot |G:M|^{-2},$$

and

$$T_2(G) = \sum_{M \in \mathcal{S}} \zeta^M(1) \cdot |G:M|^{-2}.$$

Then $T(G) = T_1(G) + T_2(G)$, so it suffices to show that $T_i(G) \to 0$ as $|G| \to \infty$.

By Theorem 5.1 (noting that $G \neq L_2(q)$ by assumption), we have $\zeta^M(1) \leq cq^{-\epsilon r}|G:M|$ with $\epsilon > 0$, and this yields

$$T_1(G) \leq cq^{-\epsilon r} \sum_{M \in \mathcal{C}} |G:M|^{-1} = cq^{-\epsilon r} k(\mathcal{C}),$$

where $k(\mathcal{C})$ denotes the number of conjugacy classes of subgroups in $\mathcal{C}$. By [13, 2.1], we have $k(\mathcal{C}) \leq c_1(r + \log\log q)$. It follows that

$$T_1(G) \leq c_2 q^{-\epsilon r} \cdot (r + \log\log q) \to 0 \text{ as } |G| \to \infty.$$

Now, for $M \in \mathcal{S}$ we have $\zeta^M(1) \leq k(M) \leq c|G:M|^{1/2}$ by (18), hence

$$T_2(G) \leq c \sum_{M \in \mathcal{S}} |G:M|^{-3/2},$$

which tends to 0 as $|G| \to \infty$ by part (ii) of Lemma 6.2.

Case 3: $v = 1, g = 3$ and $G = L_2(q)$.

Suppose first that $d > 0$ and $(m_i, |G|) \neq 1$ for some i. It is easily checked for $G = L_2(q)$ that $j_{m_i}(M)/j_{m_i}(G) < cq^{-1}$ for all maximal subgroups M of G. Fix a maximal subgroup M. By Lemma 3.3,

$$|\mathrm{Hom}(\Gamma, M)| \leq |M|^2 \cdot \prod_{i=1}^{d} j_{m_i}(M) \cdot \zeta^M(1).$$

Applying Theorem 1.2, this yields

$$\frac{|\mathrm{Hom}(\Gamma, M)|}{|\mathrm{Hom}(\Gamma, G)|} \leq (1 + o(1)) \cdot |G:M|^{-2} \cdot \prod_{i=1}^{d} \frac{j_{m_i}(M)}{j_{m_i}(G)} \cdot \zeta^M(1).$$

Since $\zeta^M(1) < c|G:M|$ by Theorem 5.1, and $j_{m_i}(M)/j_{m_i}(G) < cq^{-1}$ for some i, it follows that

$$\frac{|\mathrm{Hom}(\Gamma, M)|}{|\mathrm{Hom}(\Gamma, G)|} \leq c_1 q^{-1} \cdot |G:M|^{-1}.$$

Therefore

$$\sum_{M \ max \ G} \frac{|\mathrm{Hom}(\Gamma, M)|}{|\mathrm{Hom}(\Gamma, G)|} < c_1 q^{-1} \sum_{M \ max \ G} |G:M|^{-1} < c_2 q^{-1} \cdot \log\log q,$$

which tends to 0 as $q \to \infty$. This establishes Theorem 1.6 in this case.

To complete the proof in Case 3, suppose now that $(m_i, |G|) = 1$ for all i. Then every homomorphism from Γ to G factors through a non-oriented surface group of genus 3, so we may assume that Γ is such a group, i.e. that $d = 0$. As usual, it is enough to show that $\sum_{M \ max \ G} \frac{|\mathrm{Hom}(\Gamma, M)|}{|\mathrm{Hom}(\Gamma, G)|} \to 0$ as $q \to \infty$. This sum over non-parabolic maximal subgroups can be shown to tend to 0 exactly as in Case 2 above, so it remains to show that the sum over parabolic subgroups also tends to 0.

Let M be a parabolic subgroup of G. By Corollary 3.2(ii), we have

$$|\mathrm{Hom}(\Gamma, M)| = |M|^2 \cdot \zeta_r^M(1).$$

Now $M = (\mathbb{F}_q).((q-1)/\delta)$, where $\delta = (q-1, 2)$, so M has at most 2 real linear characters. The non-linear characters have degree at least cq, and

$k(M) \leq q$. Hence $\zeta_r^M(1) = \sum_{\chi \in Irr(M)} \iota(\chi)\chi(1)^{-1}$ is bounded independently of q. Consequently

$$\sum_{M \ parabolic} \frac{|\mathrm{Hom}(\Gamma, M)|}{|\mathrm{Hom}(\Gamma, G)|} < c_2 \sum_{M \ parabolic} |G : M|^{-2},$$

which tends to 0 as $q \to \infty$.

Case 4: $v = 1, g = 3$ and G is exceptional.

For this case we require the following recent result on maximal subgroups of G taken from [26].

Lemma 6.3 *Let $G = G(q)$ be an exceptional simple group of Lie type over $\mathbb{F}_q$, and let M be a maximal subgroup of G. Then there are absolute constants c_1, c_2 such that one of the following holds:*

(i) *M is a known subgroup, belonging to one of at most $c_1 \log\log q$ conjugacy classes,*

(ii) *G is of type F_4, E_6^ϵ, E_7 or E_8, M is almost simple, and $|M| < c_2$.*

Proof For G of type ${}^2B_2$, ${}^2G_2$, ${}^3D_4$, G_2, ${}^2F_4$, all the maximal subgroups of G are known. For the remaining types, the result follows from [26, Corollary 4]. Note that the $\log\log q$ term comes from the subfield subgroups $G(q^{1/r})$, where r is a prime divisor of $\log_p q$. ∎

Denote by $\mathcal{M}_1, \mathcal{M}_2$ the sets of maximal subgroups as in parts (i), (ii) of Lemma 6.3 respectively, and for $i = 1, 2$ define

$$T_i(G) = \sum_{M \in \mathcal{M}_i} \zeta^M(1) \cdot |G : M|^{-2}.$$

Then $T(G) = T_1(G) + T_2(G)$, so it suffices to show that $T_i(G) \to 0$ as $|G| \to \infty$.

By Theorem 5.1, $\zeta^M(1) \leq cq^{-\epsilon r}|G : M|$ with $\epsilon > 0$, and this yields

$$T_1(G) \leq cq^{-\epsilon r} \sum_{M \in \mathcal{M}_1} |G : M|^{-1} = cq^{-\epsilon r} c_1 \log\log q$$

using Lemma 6.3(i). Thus $T_1(G) \to 0$ as $|G| \to \infty$.

Finally, since for $M \in \mathcal{M}_2$ we have $\zeta^M(1) \leq |M| < c_2$, we conclude that

$$T_2(G) \leq c_2 \sum_{M \ max \ G} |G : M|^{-2},$$

which tends to 0 as $|G| \to \infty$ by Lemma 6.2(i).

This completes the proof of Theorem 1.6.

7 Representation varieties

In this section we apply results on $\mathrm{Hom}(\Gamma, G)$ for Γ a Fuchsian group and G a finite group of Lie type, and use them to study representation varieties of Γ in algebraic groups over algebraically closed fields.

Our main tool is a basic result from algebraic geometry on the number of q-rational points, which follows from the well known Lang-Weil estimate [19]. Here algebraic varieties are assumed to be affine or projective, but not necessarily irreducible; the dimension is defined to be the maximal dimension of an irreducible component.

Lemma 7.1 *Let p be a prime, and let V be an algebraic variety over $K = \bar{\mathbb{F}}_p$. Suppose $\dim V = f$, and that V has e components of dimension f. For a power q of p, let $V(q)$ denote the set of q-rational points in V. Then there is a power q_0 of p such that*

$$|V(q)| = (e + o(1))q^f$$

for all powers q of q_0.

Proof Write $V = \cup_{i=1}^{h} V_i$ where V_i are the irreducible components. Suppose $\dim V_i = f$ for $i \leq e$ and $\dim V_i \leq f - 1$ for $i > e$. Choose a p-power q_0 such that all the varieties V_i are defined over the field $\mathbb{F}_{q_0}$. Then for $q = q_0^k$ the Lang-Weil estimate [19] yields

$$|V_i(q)| = q^f + O(q^{f-1/2}) \quad (1 \leq i \leq e),$$

and

$$|V_i(q)| = O(q^{f-1}) \quad (e < i \leq h).$$

The conclusion follows. ∎

We shall deduce our results on representation varieties by combining Lemma 7.1 with our results on $|\mathrm{Hom}(\Gamma, G)|$ for finite groups G of Lie type.

Proof of Theorem 1.8

Adopt the notation of the theorem, and write $V = \mathrm{Hom}(\Gamma, GL_n(K)) = R_{n,K}(\Gamma)$. We may assume that $K = \bar{\mathbb{F}}_p$. Choose a power q_0 of p such that

all components of V are defined over $\mathbb{F}_{q_0}$. Let q be a power of q_0, and σ a Frobenius q-power endomorphism of $GL_n(K)$ with fixed point group $GL_n(q)$. Then σ acts on V, with fixed points $V(q) = \mathrm{Hom}(\Gamma, GL_n(q))$. It follows from Proposition 3.7(i) that for Γ oriented, we have

$$|V(q)| = (q - 1 + \delta + o(1)) \cdot |GL_n(q)|^{2g-1} = (1 + o(1))q^{(2g-1)n^2+1}.$$

On the other hand, Lemma 7.1 and the choice of q_0 show that $|V(q)| = (e + o(1))q^f$, where $f = \dim V$ and e is the number of f-dimensional components of V. We see that $e = 1$ and $f = (2g-1)n^2 + 1$, proving part (i) of the theorem.

The proof of part (ii) is similar, using Proposition 3.7(ii).

Proof of Theorem 1.9

We start with the following proposition.

Proposition 7.2 *Let $\Gamma \in \mathcal{F}$ be a Fuchsian group, $n \geq 2$, and K an algebraically closed field.*

(i) *If Γ is oriented, then*

$$\dim R_{n,K}(\Gamma) = 1 + (2g-1)n^2 + \dim I_{\mathbf{m}}(GL_n(K)).$$

(ii) *If Γ is non-oriented, then*

$$\dim R_{n,K}(\Gamma) = (g-1)n^2 + \sum_{i=1}^{d} \dim J_{m_i}(GL_n(K)).$$

Proof It is well known that the dimension of a variety in characteristic zero coincides with the dimension of its reduction modulo p for all large primes p. Hence in the proof we may assume that the algebraically closed field K has characteristic $p > 0$.

Let $V, V(q), K, q_0$ be as in the proof above. Then by Theorem 3.8(i) we have

$$|V(q)| = (1 + o(1))q|GL_n(q)|^{2g-1}|I_{\mathbf{m}}(GL_n(q))|.$$

Replacing q_0 by a suitable power of it if needed, we may assume that all components of the variety $U = I_{\mathbf{m}}(GL_n(K))$ are defined over $\mathbb{F}_{q_0}$. Let $f_1 = \dim U$ and e_1 the number of f_1-dimensional components of U. Then for powers q of q_0 we have

$$|I_{\mathbf{m}}(GL_n(q))| = |U(q)| = (e_1 + o(1))q^{f_1},$$

and this implies

$$|V(q)| = (e_1 + o(1))q^{1+(2g-1)n^2+f_1}.$$

Applying 7.1 again we see that $\dim V = 1 + (2g-1)n^2 + f_1$, proving part (i) of the proposition.

To prove part (ii) we apply Corollary 3.11. We first replace q_0 by a suitable power of it which satisfies $q \equiv 1 \bmod 2^{a+1}$, where a is as in Lemma 3.10. It then follows that, with the above notation we have

$$|V(q)| \sim |GL_n(q)|^{g-1} \cdot \prod_{i=1}^{d} j_{m_i}(GL_n(q)).$$

Modifying q_0 again if needed so that all components of $J_{m_i}(GL_n(K))$ are defined over $\mathbb{F}_{q_0}$, we see that

$$|V(q)| \sim q^{(g-1)n^2 + \sum f_i},$$

where $f_i = \dim J_{m_i}(GL_n(K))$. Part (ii) now follows. ∎

We now complete the proof of Theorem 1.9. Suppose first that Γ is oriented. By Proposition 7.2(i) and Corollary 4.6(ii), we have

$$\begin{aligned} \dim R_{n,K}(\Gamma) &= 1 + (2g-1)n^2 + \dim I_{\mathbf{m}}(GL_n(K)) \\ &= 1 + (2g-1)n^2 + n^2 \cdot \textstyle\sum_{i=1}^{d}(1 - \frac{1}{m_i}) - \sum_{i=1}^{d} l_i(1 - \frac{l_i}{m_i}) - \epsilon \\ &= 1 + (\mu+1)n^2 - c(n, \mathbf{m}) - \epsilon, \end{aligned}$$

where $\epsilon \in \{0, 2\}$ is as in Corollary 4.6. Theorem 1.9 follows in the oriented case.

Finally, the non-oriented case follows by combining Propositions 7.2(ii) and 4.5(ii).

Proof of Theorem 1.10

Let Γ be a Fuchsian group in $\mathcal{F}$, and let $\bar{G}$ be a simple algebraic group over the algebraically closed field K. As above, it suffices to consider the case where K has characteristic $p > 0$. For each power q of p let $\sigma = \sigma_q$ be a field morphism of $\bar{G}$ with fixed point group $G = G(q) = \bar{G}_\sigma$, a nearly simple group with G' quasisimple (of untwisted type). Write $V = \mathrm{Hom}(\Gamma, \bar{G})$, so that σ acts naturally on V with fixed point space $V(q) = \mathrm{Hom}(\Gamma, G)$.

Assume now that Γ is oriented. By Theorem 3.6(i), we have

$$|V(q)| = |G|^{2g-1} |I_{\mathbf{m}}(G)| \cdot (|G/G'| + o(1)). \tag{27}$$

Note that $|G/G'|$ is bounded and $|G| \sim q^{\dim \bar{G}}$. By Corollary 4.4(ii), there exists $q_1 = p^b$ such that for q a power of q_1, we have

$$|I_{\mathbf{m}}(G)| \sim q^{\sum \dim J_{m_i}(\bar{G})}.$$

It follows that for q a power of q_1, we have

$$|V(q)| \sim q^{(2g-1)\dim \bar{G} + \sum \dim J_{m_i}(\bar{G})}.$$

Part (i) of Theorem 1.10 in the oriented case now follows using Lemma 7.1.

The non-oriented case of Theorem 1.10(i) is similar, using part (ii) of Theorem 3.6, except when $g = 3$ and $\bar{G} = SL_2$ or PSL_2. In the first case, $G = SL_2(q)$ and the result follows as above using Theorem 1.2(iv). In the second case, $G = PGL_2(q)$, and we may assume q is odd (otherwise we are back in the first case). Inspection of the character table of G in [46] shows that $\zeta_R^G(1) = 3 + o(1)$. Also $|G/G^2| = 2$. Substituting in Lemma 3.5(ii) now gives

$$1 + o(1) \leq \frac{|\mathrm{Hom}(\Gamma, G)|}{|G|^{g-1} \cdot |I_{\mathbf{m}}^r(G)|} \leq 3 + o(1).$$

The conclusion now follows as before.

This completes the proof of Theorem 1.10(i). Part (ii) now follows from (i) using Corollary 4.2.

Proof of Corollary 1.11

Part (i) of the corollary is immediate from Theorem 1.10(i). To prove the other parts, we can assume as above that K has positive characteristic. Suppose first that Γ is oriented. Adopting the above notation, (27) gives

$$|V(q)| = |G|^{2g-1}(|G/G'| + o(1)).$$

There exists q_0 such that for all powers q of q_0 we have $|G/G'| = |\pi_1(\bar{G})|$. The conclusion of Corollary 1.11(ii) follows using Lemma 7.1.

Now suppose Γ is non-oriented. By Corollary 3.2(ii) we have $|\mathrm{Hom}(\Gamma, G)| = |G|^{g-1}\zeta_r^G(g-2)$. If $g > 3$ or $\bar{G} \neq SL_2, PSL_2$ then Lemma 2.9 gives $\zeta_r^G(g-2) = |G/G^2| + o(1)$, and since $|G/G^2| = |\pi_1(\bar{G})/\pi_1(\bar{G})^2|$ for all powers q of a suitable q_0, the conclusion of Corollary 1.11(iii) follows. So assume now that $g = 3$ and $\bar{G} = SL_2$ or PSL_2. In the first case it is easily checked from the character table of $G = SL_2(q)$ that $\zeta_r^G(1) = 1 + o(1)$; and in the second case $G = PGL_2(q)$ and we have $\zeta_r^G(1) = (q-1, 2) + 1 + o(1)$. The conclusion again follows.

References

[1] M. Aschbacher, On the maximal subgroups of the finite classical groups, *Invent. Math.* **76** (1984), 469-514.

[2] H. Azad, M. Barry and G.M. Seitz, On the structure of parabolic subgroups, *Comm. in Alg.* **18** (1990), 551-562.

[3] V.V. Benyash-Krivets and V.I. Chernousov, Varieties of representations of fundamental groups of compact nonoriented surfaces. (Russian) *Mat. Sb.* **188** (1997), 47-92; translation in *Sb. Math.* **188** (1997), 997-1039.

[4] M.D.E. Conder, Hurwitz groups: a brief survey, *Bull. Amer. Math. Soc.* **23** (1990), 359-370.

[5] D.I. Deriziotis and G.O. Michler, Character table and blocks of finite simple triality groups ${}^3D_4(q)$, *Trans. Amer. Math. Soc.* **303** (1987), 39-70.

[6] J.D. Dixon, The probability of generating the symmetric group, *Math. Z.* **110** (1969), 199-205.

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

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

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

[10] 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.

[11] D. Gluck, Sharper character value estimates for groups of Lie type, *J. Algebra* **174** (1995), 229-266.

[12] W.M. Goldman, Topological components of spaces of representations, *Invent. Math.* **93** (1988), 557-607.

[13] R. Guralnick, W.M. Kantor and J. Saxl, The probability of generating a classical group, *Comm. Alg.* **22** (1994), 1395-1402.

[14] R. Guralnick, F. Lübeck and A. Shalev, Zero-one generation laws for Chevalley groups, to appear.

[15] R. Guralnick, J. Saxl, M.W. Liebeck and A. Shalev, Random generation of finite simple groups, *J. Algebra* **219** (1999), 345-355.

[16] W.M. Kantor and A. Lubotzky, The probability of generating a finite classical group, *Geom. Ded.* **36** (1990), 67-87.

[17] P.B. Kleidman and M.W. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, London Math. Soc. Lecture Note Series **129**, Cambridge University Press, Cambridge, 1990.

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

[19] S. Lang and A. Weil, Number of points of varieties over finite fields, *Amer. J. Math.* **76** (1954), 819-827.

[20] R. Lawther, Elements of specified order in simple algebraic groups, *Trans. Amer. Math. Soc.*, to appear.

[21] R. Lawther, M.W. Liebeck and G.M. Seitz, Fixed point ratios in actions of finite exceptional groups of Lie type, *Pacific J. Math.* **205** (2002), 393-464.

[22] M.W. Liebeck, On the orders of maximal subgroups of the finite classical groups, *Proc. London Math. Soc.* **50** (1985), 426-446.

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

[24] M.W. Liebeck and J. Saxl, On the orders of maximal subgroups of the finite exceptional groups of Lie type, *Proc. London Math. Soc.* **55** (1987), 299-330.

[25] M.W. Liebeck and G.M. Seitz, Reductive subgroups of exceptional algebraic groups, *Mem. Amer. Math. Soc.*, Vol. 121, No. 580, 1996.

[26] M.W. Liebeck and G.M. Seitz, The maximal subgroups of positive dimension in exceptional algebraic groups, *Mem. Amer. Math. Soc.*, to appear.

[27] M.W. Liebeck and A. Shalev, The probability of generating a finite simple group, *Geom. Ded.* **56** (1995), 103-113.

[28] M.W. Liebeck and A. Shalev, Classical groups, probabilistic methods, and the (2,3)-generation problem, *Annals of Math.* **144** (1996), 77-125.

[29] M.W. Liebeck and A. Shalev, Simple groups, probabilistic methods, and a conjecture of Kantor and Lubotzky, *J. Algebra* **184** (1996), 31-57.

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

[31] M.W. Liebeck and A. Shalev, Random (r, s)-generation of finite classical groups, *Bull. London Math. Soc.* **34** (2002), 185-188

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

[33] M.W. Liebeck and A. Shalev, Character degrees of finite Chevalley groups, *Proc. London Math. Soc.*, to appear.

[34] F. Lübeck, Small degree representations of finite Chevalley groups in defining characteristic, *LMS J. Comput. Math.* **4** (2001), 22-63.

[35] A. Lubotzky and A.R. Magid, Varieties of representations of finitely generated groups, *Mem. Amer. Math. Soc.* **58** (1985), no. 336.

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

[37] R.C. Lyndon, The equation $a^2b^2 = c^2$ in free groups, *Michigan Math. J.* **6** (1959), 155-164.

[38] G. Malle, J. Saxl and T. Weigel, Generation of classical groups, *Geom. Ded.* **49** (1994), 85–116.

[39] A.D. Mednykh, On the number of subgroups in the fundamental group of a closed surface, *Commun. in Alg.* **16** (1988), 2137-2148.

[40] M. Mulase and M. Penkava, Volume of representation varieties, preprint.

[41] T.W. Müller and J-C. Puchta, Character theory of symmetric groups and subgroup growth of surface groups, *J. London Math. Soc.* **66** (2002), 623-640.

[42] A.S. Rapinchuk, V.V. Benyash-Krivetz and V.I. Chernousov, Representation varieties of the fundamental groups of compact orientable surfaces, *Israel J. Math.* **93** (1996), 29-71.

[43] J. Shamash, Blocks and Brauer trees for groups of type $G_2(q)$, *Proc. Symp. Pure Math.* **47** (1987), 283-295.

[44] K. Shinoda, The conjugacy classes of the finite Ree groups of type (F_4), *J. Fac. Sci. Univ. Tokyo* **22** (1975), 1-15.

[45] 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.

[46] R. Steinberg, The representations of $GL(3,q)$, $GL(4,q)$, $PGL(3,q)$ and $PGL(4,q)$, *Canad. J. Math.* **3** (1951), 225-235.

[47] M. Suzuki, On a class of doubly transitive groups, *Annals of Math,* **75** (1962), 105-145.

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

[49] A. Wagner, An observation on the degrees of projective representations of the symmetric and alternating groups over an arbitrary field, *Arch. Math.* **29** (1977), 583-389.

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

[51] H.N. Ward, On Ree's series of simple groups, *Trans. Amer. Math. Soc.* **121** (1966), 62-89.

[52] H.S. Wilf, The asymptotics of $e^{P(z)}$ and the number of elements of each order in S_n, *Bull. Amer. Math. Soc.* **15** (1986), 228-232.

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