INVARIABLE GENERATION AND THE CHEBOTAREV INVARIANT OF A FINITE GROUP

W. M. KANTOR, A. LUBOTZKY, AND A. SHALEV

Abstract. A subset S of a finite group G *invariably generates* G if $G = \langle s^{g(s)} \mid s \in S \rangle$ for each choice of $g(s) \in G, s \in S$. We give a tight upper bound on the minimal size of an invariable generating set for an arbitrary finite group G. In response to a question in [KZ] we also bound the size of a randomly chosen set of elements of G that is likely to generate G invariably. Along the way we prove that every finite simple group is invariably generated by two elements.

Dedicated to Bob Guralnick in honor of his 60th birthday

1. Introduction

For many years there has been a rapidly growing literature concerning the generation of finite groups. This has involved the number $d(G)$ of generators of a group G, or the expected number $E(G)$ of random choices of elements in order to probably generate G, among other group-theoretic invariants. In this paper we will study further invariants.

Dixon [Di1] began the probabilistic direction for generation of (almost) simple groups, and later he also introduced yet another direction based on the goal of determining Galois groups [Di2]. This has led to the following notions:

Definition. Let G be a finite group.

(a) A subset S of G *invariably generates* G if $G = \langle s^{g(s)} \mid s \in S \rangle$ for each choice of $g(s) \in G, s \in S$ [Di2].

(b) Let $d_I(G) := \min \{ |S| \bigm| S \text{ invariably generates } G \}$.

(c) The *Chebotarev invariant* $C(G)$ of G is the expected value of the random variable n that is minimal subject to the requirement that n randomly chosen elements of G invariably generate G [KZ].

There have been several papers discussing (a) for specific groups (such as finite simple groups) [LuP, NP, Sh, FG1, KZ], but not for finite groups in general. Concerning (c), recall Chebotarev's Theorem that provides elements of a suitable Galois group G, where the elements are obtained only up to conjugacy in G; the interest in (c) comes from computational group theory, where there is a need to know how long one should expect to wait in order to ensure that choices of representatives from the conjugacy classes provided by Chebotarev's Theorem will generate G. This is discussed more carefully in [Di2, KZ].

The authors acknowledge partial support from NSF grant DMS 0753640 (W.M.K.), ERC Advanced Grants 226135 (A.L.) and 247034 (A.S.), and ISF grant 754/08 (A.L. and A.S.). The first author is grateful for the warm hospitality of the Hebrew University while this paper was being written.

Our main results are the next two theorems, which depend on the classification of the finite simple groups.

Theorem 1.1. *Every finite group G is invariably generated by at most $\log_2 |G|$ elements.*

This bound is best possible: we show that $d_I(G) = \log_2 |G|$ if and only if G is an elementary abelian 2-group. It is trivial that $d(G) \leq \log_2 |G|$ using Lagrange's Theorem. However, $d_I(G)$ may be much larger than $d(G)$: Proposition 2.5 states that, *for every $k \geq 1$, there is a finite group G such that $d(G) = 2$ but $d_I(G) \geq k$.* Theorem 3.1 contains a more precise statement of Theorem 1.1 involving the length and structure of a chief series of G.

Theorem 1.2. *There exists an absolute constant c such that*

$$C(G) \leq c|G|^{1/2}(\log |G|)^{1/2},$$

for all finite groups G.

This bound is close to best possible: it is easy to see that sharply 2-transitive groups provide an infinite family of groups G for which $C(G) \sim |G|^{1//2}$ (compare [KZ, Sec. 4]). In fact [KZ, Sec. 9] asks whether $C(G) = O(|G|^{1/2})$ for all finite groups G (which we view as rather likely).

For an arbitrary finite group it is interesting to compare $d_I(G)$ with $d(G)$, and $C(G)$ with $E(G)$. The upper bounds for $d_I(G)$ and $d(G)$ are identical, although (as stated above) these quantities may be very different. On the other hand, $E(G) \leq ed(G) + 2e \log\log |G| + 11 = O(\log |G|)$ [Lu], which is far smaller than the bound in Theorem 1.2.

We will need the following result of independent interest.

Theorem 1.3. *Every nonabelian finite simple group is invariably generated by* 2 *elements.*

In fact, for proofs of Theorems 1.1 and 1.2 we will need slightly stronger results on simple groups involving automorphisms as well (cf. Theorem 5.1 and 5.5). The same week that we proved these results about simple groups essentially the same result with a roughly similar proof was posted in [GM2].

Dealing with simple groups uses the rather large literature of known properties of those groups. The fact that, for finite simple groups G, $d_I(G)$ and $C(G)$ are bounded by some (unspecified) constant c follows for alternating groups from [LuP] (cf. [KZ]), and for Lie type groups from results announced in [FG1] related to "Shalev's ϵ-Conjecture", which concerns the number of fixed-point-free elements in simple permutation groups (cf. Section 4).

The proof of Theorem 1.2 uses bounds in [CC] and [FG1] on the number of fixed-point-free elements of a transitive permutation group, together with a recent bound on the number of maximal subgroups of a finite group [LPS]. We note that an explicit formula for $C(G)$ is given in [KZ, Proposition 2.7], but we have not been able to use it since it appears to be too difficult to evaluate its terms for most groups G.

The proofs of Theorems 1.1, 1.2 and 1.3 are given in Sections 3, 4 and 5, respectively. Section 2 contains the aforementioned result on the non-relationship of $d(G)$ and $d_I(G)$, as well as a characterization of nilpotent groups as those finite groups all of whose generating sets invariably generate.

This paper is dedicated to Bob Guralnick, who has made fundamental contributions in the various areas involved in this or other papers of ours.

2. Preliminary results and examples

Unless otherwise stated, we assume that the group G is finite. If $X, Y \subseteq G$, we say that Y is *similar* to X if there is a function $f\colon X \to Y$ such that $f(X) = Y$ and, for each $x \in X$, $f(x)$ is conjugate in G to x. Thus X invariably generates G if and only if $\langle Y \rangle = G$ for each $Y \subseteq G$ that is similar to X.

Let $\mathrm{Max}(G)$ denote the set of maximal subgroups of G. Let $\mathcal{M} = \mathcal{M}(G)$ be a set of representatives of conjugacy classes of maximal subgroups of G.

If $M \in \mathrm{Max}(G)$, write

$$\widetilde{M} = \bigcup_{g \in G} M^g \quad \text{and} \quad v(M) = \frac{|\widetilde{M}|}{|G|}.$$

Clearly $\widetilde{M_1} = \widetilde{M_2}$ if the maximal subgroups M_1, M_2 are conjugate in G. Also, $\widetilde{M}$ is the set of elements of G having at least one fixed point in the primitive permutation representation of G on the set G/M of (left) cosets of M in G.

Lemma 2.1. *A subset $X \subseteq G$ generates G invariably if and only if $X \not\subseteq \widetilde{M}$ for all $M \in \mathcal{M}$.*

Proof. If $X \subseteq \widetilde{M}$ for some $M \in \mathcal{M}$ then each element of X is conjugate to an element of M, and hence X does not generate G invariably. Conversely, if X does not generate G invariably, then there exists a set Y similar to X such that $\langle Y \rangle \neq G$. Hence (using the finiteness of G) there exist $M \in \mathcal{M}$ and $g \in G$ such that $\langle Y \rangle \subseteq M^g$, and hence $X \subseteq \widetilde{M}$. □

The "only if" part of the above lemma holds also for infinite groups (as the proof shows). This enables us to show that some infinite groups are not invariably generated by any set of elements. For example, if p is a large prime, and G is a group of exponent p in which all subgroups H with $1 < H < G$ are conjugate (of order p), as constructed by Ol'shanskii [Ol] and Rips, then all such subgroups H satisfy $\widetilde{H} = G$, so even G itself does not generate G invariably.

However, for finite groups there are no anomalies of this kind, since $\widetilde{H} \neq G$ for all proper subgroups H. In fact, if $k(G)$ denotes the number of conjugacy classes of (elements of) the finite group G, then we have

Lemma 2.2. *For any finite group G we have $d_I(G) \leq k(G)$. Moreover, $d_I(G)$ is at most the number of conjugacy classes of cyclic subgroups of G.*

Proof. If H is the subgroup of G generated by a set of cyclic subgroups, one from each conjugacy class, then the union of all conjugates of H is G, and hence $H = G$. □

For $k \geq 1$, let $P_I(G, k)$ be the probability that k randomly chosen elements of G generate G invariably.

Lemma 2.3. *If $M \in \mathcal{M}$ then* $\max_{M \in \mathcal{M}} v(M)^k \leq 1 - P_I(G, k) \leq \sum_{M \in \mathcal{M}} v(M)^k.$

Proof. Let $g_1, \dots, g_k \in G$ be randomly chosen. Given $M \in \mathcal{M}$, the probability that $g_i \in \widetilde{M}$ for all i is $v(M)^k$. Both inequalities now follow easily from Lemma 2.1. □

We next characterize nilpotent groups in terms of invariable generation.

Proposition 2.4. *A finite group G is nilpotent if and only if every generating set of G invariably generates G.*

Proof. Let $\Phi(G)$ denote the Frattini subgroup of G. Then a subset of G generates G if and only if its image in $G/\Phi(G)$ generates $G/\Phi(G)$.

Suppose G is nilpotent. Then $G/\Phi(G)$ is abelian. Suppose $X \subseteq G$ generates G, and let $Y \subseteq G$ be similar to X. Clearly the images of X and Y in the abelian group $G/\Phi(G)$ coincide. Since the image of X generates $G/\Phi(G)$, so does the image of Y. It follows that Y generates G. We conclude that X invariably generates G.

Now suppose G is not nilpotent. We shall construct a generating set X for G that does not generate G invariably using a theorem of Wielandt [Rob, p. 132]: if $G/\Phi(G)$ is abelian then G is nilpotent. Then $G/\Phi(G)$ is not abelian, and hence some maximal subgroup M of G is not normal in G. Let $g \in G$ with $M^g \neq M$. Let $x \in M^g \setminus M$ and $X := M \cup \{x\}$. Then $\langle X \rangle = G$ since M is maximal, so that $M \cup \left\{x^{g^{-1}}\right\} = M$ is similar to X and is proper in G. This implies that X does not generate G invariably. □

In particular, for nilpotent G we have $d_I(G) = d(G)$. For simple groups, by Theorem 1.3 we also have the same equality (with both sides 2). However, our next result shows that, in general, $d_I(G)$ is not bounded above by any function of $d(G)$:

Proposition 2.5. *For every $k \geq 1$ there is a finite group G such that $d(G) = 2$ but $d_I(G) \geq k$.*

This group G will be a power T^k of an alternating group T. For this purpose we recall an elementary criterion in [KL, Proposition 6]:

Proposition 2.6. *Let $G = T^k$ for a nonbelian finite simple group T. Let $S = \{s_1, \dots, s_r\} \subset G$, so that $s_i = (t_1^i, \dots, t_k^i), t_j^i \in T$. Form the matrix*

$$A = \begin{pmatrix} t_1^1 & \dots & t_k^1 \\ & \dots & \\ t_1^r & \dots & t_k^r \end{pmatrix}.$$

Then S generates G if and only if the following both hold:

(a) *If $1 \leq j \leq k$ then $T = \langle t_j^1, \dots, t_j^r \rangle$; and*
(b) *The columns of A are in different* Aut(T)*-orbits for the diagonal action of* Aut(T) *on T^r.*

Proof of Proposition 2.5. Fix n, let $T = A_n$ and let $k = k(n)$ be the largest integer such that $d(G) = 2$, where $G := G_n = T^k$. Then $k \geq n!/8$ ([KL, Example 2], obtained from Proposition 2.6).

Let S be as in Proposition 2.6, and assume that S invariably generates G. Then we can arbitrarily conjugate each t_j^i independently and still generate G. Let $\mathbf{C}(T)$ denote the set of conjugacy classes of T. Project each column β_j of A to $\bar{\beta}_j \in \mathbf{C}(T)^r$. In view of conditions (a) and (b) in Proposition 2.6, the $\bar{\beta}_j$ are in different Aut(T)-orbits of the diagonal action on $\mathbf{C}(T)^r$.

The number of conjugacy classes in T is at most $c^{\sqrt{n}}$, so $|\mathbf{C}(T)|^r \leq c^{r\sqrt{n}}$. The number of projections $\bar{\beta}_j$ is k (since $1 \leq j \leq k$), where $k \geq n!/8$. Then $c^{r\sqrt{n}} \geq n!/8$ by the Pigeon Hole Principle, so that $|S| = r \geq C\sqrt{n}\log n$. □

3. Proof of Theorem 1.1

Let $l(G)$ denote the length of a chief series of G. The following is a stronger version of Theorem 1.1:

Theorem 3.1. *Let G be a finite group having a chief series with a abelian chief factors and b non-abelian chief factors. Then*

$$d_I(G) \leq a + 2b.$$

In particular, $d_I(G) \leq 2l(G)$, and if G is solvable then $d_I(G) \leq l(G)$.

Proof. We use induction on $|G|$ (the case $|G| = 1$ being trivial). Suppose $|G| > 1$ and let $N \lhd G$ be a minimal normal subgroup of G. It suffices to show that

$$d_I(G) \leq d_I(G/N) + c,$$

where $c = 1$ if N is abelian and $c = 2$ if N is non-abelian. In the latter case our proof relies on Theorem 5.1 (proved below).

Let $X \subseteq G$ be a set of size $d_I(G/N)$ whose image in G/N generates G/N invariably.

Suppose first that N is abelian. Let $x \in N$ be any non-identity element of N. We claim that $Y = X \cup \{x\}$ *invariably generates* G. Indeed, suppose $Z \subseteq G$ is similar to Y. Then the image of Z in G/N generates G/N (by the assumption on X). Moreover, Z contains a conjugate $z = x^g$ that is a non-identity element of N. Since G/N acts irreducibly on N, $\langle Z\rangle \geq N$. It follows that $\langle Z\rangle = G$, so Y generates G invariably. Thus $d_I(G) \leq d_I(G/N) + 1$ in this case.

Now suppose N is non-abelian. Then $N = T_1 \times \cdots \times T_k$, where $k \geq 1$ and the T_i are non-abelian finite simple groups such that the conjugation action of G on N induces a transitive action of G/N on the set $\{T_1, \ldots, T_k\}$.

The group $A := N_G(T_1)/C_G(T_1)$ is an almost simple group with socle $T_1^\star := T_1C_G(T_1)/C_G(T_1) \cong T_1$. By Theorem 5.1, there are elements $x_1 \in T_1^\star$, $x_2 \in A$ such that $\langle x_1^{a_1}, x_2^{a_2}\rangle \geq T_1^\star$ for all $a_1, a_2 \in A$. Let $y_1 \in T_1, y_2 \in N_G(T_1)$, be pre-images of x_1, x_2, respectively. We claim that $Y := X \cup \{y_1, y_2\}$ *invariably generates* G.

To see this, let Z be a set similar to Y, so $Z = X' \cup \{y_1^{g_1}, y_2^{g_2}\}$ where X' is similar to X and $g_i \in G$ $(i = 1, 2)$. We need to show that Z generates G. Let $K = \langle Z\rangle$ and $H = \langle X'\rangle$. Since X invariably generates G modulo N we have $HN = G$. Hence H acts transitively (by conjugation) on $\{T_1, \ldots, T_k\}$.

Moreover, $T_1^{g_1} = N_i$ and $T_1^{g_2} = T_j$ for some i, j. By the transitivity of H there are elements $h_1, h_2 \in H$ such that $T_i^{h_1} = T_1$ and $T_j^{h_2} = T_1$. Then $g_1h_1, g_2h_2 \in N_G(T_1)$.

Clearly $y_1^{g_1h_1} \in T_1^{g_1h_1} = T_1$ and $y_2^{g_2h_2} \in N_G(T_1)^{g_2h_2} = N_G(T_1)$. Then $y_1^{g_1h_1}$ and $y_2^{g_2h_2}$ induce automorphisms of T_1 by conjugation. In view of our choice of x_1 and x_2, $\langle y_1^{g_1h_1}, y_2^{g_2h_2}\rangle$ induces all inner automorphisms of T_1. In particular, the conjugates of the element $y_1^{g_1h_1} \in T_1$ under this group generate the simple group T_1. Thus, $K \geq \langle y_1^{g_1h_1}, y_2^{g_2h_2}, H\rangle \geq T_1$, so that $K \geq T_i$ for all i and hence $G = KN = K$, as required.

We see that $d_I(G) \leq d_I(G/N) + 2$ in this case. This completes the proof of the first assertion in the theorem. The last two assertions follow immediately. □

We can now complete the proof of Theorem 1.1. Let G, a, b be as above. Every abelian chief factor of G has order at least 2, while every non-abelian chief factor has order at least 60. This yields $|G| \geq 2^a 60^b$, so that

$$\log_2 |G| \geq a + (\log_2 60)b \geq a + 2b \geq d_I(G),$$

as required. Moreover, if $d_I(G) = \log_2 |G|$ then we must have $b = 0$, and all chief factors of G have order 2. Thus G is a 2-group, so that $d_I(G) = d(G) = \log_2 |G|$ by Proposition 2.4. Now $d(G) = \log_2 |G|$ easily implies that G is an elementary abelian 2-group. □

Note that the bound in Theorem 3.1 is tight both for non-abelian simple groups and for elementary abelian p-groups.

4. Proof of Theorem 1.2

The main result of this section is the following.

Theorem 4.1. *For any $\epsilon > 0$ there exists $c = c(\epsilon)$ such that $P_I(G, k) \geq 1 - \epsilon$ for any finite group G and any $k \geq c|G|^{1/2}(\log |G|)^{1/2}$.*

Proof. By increasing the constant c we may assume that $|G|$ is as large as required in various parts of the proof.

For $M \leq G$ let $M_G = \cap_{g \in G} M^g$ denote the *core* of M in G, the kernel of the permutation action of G on the set of conjugates of M.

Divide the set $\mathcal{M}$ of representatives of conjugacy classes of maximal subgroups of G into three subsets $\mathcal{M}_1, \mathcal{M}_2, \mathcal{M}_3$ as follows. The set $\mathcal{M}_1$ consists of the subgroups $M \in \mathcal{M}$ such that the primitive group G/M_G is not of affine type. The set $\mathcal{M}_2$ consists of the subgroups $M \in \mathcal{M}$ such that the primitive group G/M_G is of affine type and $|G\colon M| \leq |G|^{1/2}/(\log |G|)^{1/2}$. Finally, $\mathcal{M}_3$ consists of the remaining subgroups in $\mathcal{M}$, namely the subgroups M such that G/M_G is affine and $|G\colon M| > |G|^{1/2}/(\log |G|)^{1/2}$.

By [LPS, Theorem 1.3], for any finite group G we have $|\mathrm{Max}(G)| \leq c_1 |G|^{3/2}$, where c_1 is an absolute constant. In particular, for $i = 1, 2, 3$,

$$|\mathcal{M}_i| \leq |\mathcal{M}| \leq c_1 |G|^{3/2}.$$

Fix $k \geq 1$ and let $g_1, \ldots, g_k \in G$ be randomly chosen (we will restrict k in later parts of the proof). By Lemma 2.1,

$$1 - P_I(G, k) \leq P_1 + P_2 + P_3,$$

where P_i is the probability that $g_1, \ldots, g_k \in \widetilde{M}$ for some $M \in \mathcal{M}_i$ $(i = 1, 2, 3)$. It suffices to show that, for k as in the statement of the theorem, $P_i < \epsilon/3$ for $i = 1, 2, 3$.

We bound each of the probabilities P_i separately.

The set $\mathcal{M}_1$. To bound P_1 we use [FG1, Theorem 8.1]: the proportion of fixed-point-free permutations in a non-affine primitive group of degree n is at least $c_2/\log n$, for some absolute constant $c_2 > 0$. This shows that, for $M \in \mathcal{M}_1$,

$$v(M) \leq 1 - c_2/\log |G\colon M| \leq 1 - c_2/\log |G|.$$

By Lemma 2.3 and its proof,

$$P_1 \leq \sum_{M \in \mathcal{M}_1} v(M)^k \leq |\mathcal{M}_1|(1 - c_2/\log |G|)^k \leq c_1 |G|^{3/2}(1 - c_2/\log |G|)^k.$$

Since $(1-x)^k \leq \exp(-kx)$ for $0 < x < 1$, for any $c_3 > \log c_1 + 3/2$ the right hand side is bounded above by $\exp(c_3 \log|G| - c_2 k/\log|G|)$. If $k > c_4(\log|G|)^2$ for a suitable absolute constant c_4, then the latter expression tends to zero as $|G| \to \infty$, and hence so does P_1. In particular we have $P_1 < \epsilon/3$ for $|G|$ large enough.

The set $\mathcal{M}_2$. We next bound P_2. Here our main tool is the theorem that the proportion of fixed-point-free elements in any transitive permutation group of degree n is at least $1/n$ [CC]. This implies that, if $M \in \mathcal{M}_2$, then

$$v(M) \leq 1 - |G:M|^{-1} \leq 1 - (|G|/\log|G|)^{-1/2}.$$

Therefore

$$P_2 \leq \sum_{M \in \mathcal{M}_2} v(M)^k \leq |\mathcal{M}_2|\big(1-(|G|/\log|G|)^{-1/2}\big)^k \leq c_1|G|^{3/2}\big(1-(|G|/\log|G|)^{-1/2}\big)^k.$$

As before the right side is bounded above by $\exp(c_3 \log|G| - k\big(|G|/\log|G|)^{-1/2}\big))$ for suitable $c_3 > 3/2$. This in turn tends to zero as $|G| \to \infty$ for any $k > c_5|G|^{1/2}(\log|G|)^{1/2}$, for arbitrary $c_5 > c_3$. Therefore $P_2 \to 0$ for such k, and $P_2 < \epsilon/3$ for all sufficiently large $|G|$.

The set $\mathcal{M}_3$. Finally we bound P_3. If $M \in \mathcal{M}_3$ then $G/M_G = V \rtimes H$, where V is an elementary abelian p-group for some prime p, acting regularly on the set of cosets of M in G, and H is a point-stabilizer acting irreducibly on V.

Fix a chief series $\{G_i\}$ of G. Fix $M \in \mathcal{M}_3$, and let $\pi\colon G \to G/M_G$ be the canonical projection. The series $\{\pi(G_i)\}$ of normal subgroups of $\pi(G) = G/M_G$ descends from $G/M_G = V \rtimes H$ to 1. If i is minimal such that $\pi(G_{i+1}) = 1$, then $\pi(G_i)$ is a minimal normal subgroup of G/M_G, and hence is V, the unique minimal normal subgroup of G/M_G. In this situation we shall say that M *uses* G_i/G_{i+1}, in which case $G_i/G_{i+1} \cong V$. (For, since $\pi(G_i) = \pi(G_i)/\pi(G_{i+1})$ is a nontrivial G-homomorphic image of G_i/G_{i+1} it is isomorphic to G_i/G_{i+1}; since $\pi(G_i)$ is a minimal normal subgroup of $\pi(G)$ it is V.) We have seen that every $M \in \mathcal{M}_3$ uses G_i/G_{i+1} for a unique i. Moreover, since $M \in \mathcal{M}_3$,

$$|G_i:G_{i+1}| = |V| = |G:M| > (|G|/\log|G|)^{1/2}.$$

We claim that, *if G is sufficiently large, then it has at most two abelian chief factors used by any maximal subgroups in $\mathcal{M}_3$.* Indeed, if there were (at least) three such chief factors, appearing at places $i > j > l$ in our chief series, then we would obtain the contradiction

$$|G| \geq |G_i:G_{i+1}||G_j:G_{j+1}||G_l:G_{l+1}| > \big((|G|/\log|G|)^{1/2}\big)^3.$$

Fix an abelian chief factor $V = G_i/G_{i+1}$ of G as above. Then each $g \in G_i \setminus G_{i+1}$ acts fixed-point-freely on the cosets of any M that uses G_i/G_{i+1} (since $gM_G \in V \setminus \{1\}$). For each such M we have $\widetilde{M} \subseteq G \setminus (G_i \setminus G_{i+1})$. Since

$$|G:G_i| \leq |G|/|G_i:G_{i+1}| = |G|/|V| \leq (|G|\log|G|)^{1/2}$$

by the definition of $\mathcal{M}_3$, the proportion of elements $g \in G_i \setminus G_{i+1}$ inside G is at least $\frac{1}{2}|G:G_i|^{-1} \geq \frac{1}{2}(|G|\log|G|)^{-1/2}$. Since the union of $\widetilde{M}^k$ over all M using G_i/G_{i+1} is contained in $\big(G \setminus (G_i \setminus G_{i+1})\big)^k$, it follows that the probability that randomly chosen elements $g_1, \ldots, g_k$ of G all lie in $\widetilde{M}$ for some such M is at most

$(1-\frac{1}{2}(|G|\log|G|)^{-1/2})^k$. Although there may be many choices for M in $\mathcal{M}_3$, there are at most two choices for the chief factor G_i/G_{i+1}. Thus,

$$P_3 \le 2\big(1-\frac{1}{2}(|G|\log|G|)^{-1/2}\big)^k \le 2\exp\big(-\frac{k}{2}(|G|\log|G|)^{-1/2}\big),$$

where the right hand side is less than $\epsilon/3$ for $k \ge c(|G|\log|G|)^{1/2}$ for some $c = c(\epsilon)$.

Our bounds on the three probabilities P_i complete the proof. □

Remark. Recall that the *ϵ-conjecture*, posed by the third author of this paper, states that there exists an absolute constant $\epsilon > 0$ such that the proportion of fixed-point-free elements in any finite simple transitive permutation group is at least ϵ. This amounts to saying that $v(M) \le 1-\epsilon$ for any finite simple group G and any $M \in \mathrm{Max}(G)$. This conjecture holds for alternating groups [LuP] and for Lie type groups of bounded rank [FG1, Secs. 3 and 4]. Moreover, in [FG1, Theorem 1.3] it is announced that the ϵ-conjecture holds in general, and proofs in some additional cases appear in [FG2]. When $M \in \mathcal{M}_1$ our proof of Theorem 4.1 uses [FG1, Theorem 8.1], which in turn relies on the ϵ-conjecture. However, we now show that Theorem 5.5 below easily yields a weaker version of [FG1, Theorem 8.1] that still suffices for our purpose.

The set $\mathcal{M}_1$ revisited. Namely, we claim that there exists $c_2 > 0$ such that

$$v(M) \le 1 - c_2(\log|G|)^{-2}|G|^{-1/3},$$

where G is any non-affine primitive permutation group and M is a point-stabilizer. For, if s_1, s_2 generate G invariably, and if $M \in \mathrm{Max}(G)$, then $\widetilde{M} \cap s_i^G = \emptyset$ for $i = 1$ or 2, in which case $v(M) \le 1 - |s_i^G|/|G|$. Then $v(M) \le 1 - \frac{1}{2}|G|^{-1/3}$ for each sufficiently large finite simple group G and each such M, by Theorem 5.5. This implies that, for all finite simple groups G and all $M \in \mathrm{Max}(G)$, we have $v(M) \le 1 - c_3|G|^{-1/3}$ for some constant $c_3 > 0$.

Consequently, if G is an almost simple group with socle T then, since $|\mathrm{Out}(T)| \le c_4 \log|T|$ (cf. [GLS, Sec. 2.5]), we easily obtain

$$v(M) \le 1 - c_5(\log|G|)^{-1}|G|^{-1/3}$$

for all $M \in \mathrm{Max}(G)$ not containing T for some $c_5 > 0$. Our claim follows by combining this inequality with the reduction to almost simple groups given in the proof of [FG1, Theorem 8.1].

Thus, if $M \in \mathcal{M}_1$, then the above claim yields

$$P_1 \le \sum_{M\in\mathcal{M}_1} v(M)^k \le c_1 \log|G|(1 - c_2(\log|G|)^{-2}|G|^{-1/3})^k.$$

The right hand side tends to zero when $k \ge c_6(\log|G|)^3|G|^{1/3}$; but for the proof of Theorem 4.1 we can assume the stronger inequality $k \ge c_7|G|^{1/2}(\log|G|)^{1/2}$. Consequently $P_1 \to 0$, as required.

Completion of proof of Theorem 1.2 . Apply Theorem 4.1 with $\epsilon = 1/2$ and let $c = c(1/2)$. Let $k = \lceil c|G|^{1/2}(\log|G|)^{1/2}\rceil$. Then k randomly chosen elements of G invariably generate G with probability at least 1/2. This implies that

$$C(G) \le 2k \le (2c+1)|G|^{1/2}(\log|G|)^{1/2}. \quad \square$$

Corollary 4.2. (a) *If G is a finite group without abelian composition factors, then $C(G) = O((\log|G|)^2)$.*

(b) *If G is an almost simple group, then $C(G) = O(\log|G| \log\log|G|)$.*

Proof. We have already seen (a) in our first treatment of the non-affine case ($M \in \mathcal{M}_1$) of Theorem 4.1.

To prove (b) we first note that, for some $c > 0$ and all $M \in \mathcal{M}$, we have $v(M) \leq 1 - c/\log|G|$. Indeed, if M has trivial core then this follows from [FG1, Theorem 8.1] (and hence from the correctness of the ϵ-conjecture stated above). Otherwise, M contains the simple socle T of G, and $|G/T| \leq |\mathrm{Out}(T)| \leq c_4 \log|T| \leq c_4 \log|G|$ as noted above. In this situation, if $g \in G$ acts fixed-point-freely on the cosets of M in G, so do all the elements of gT, so that $v(M) \leq 1 - c_4^{-1}/\log|G|$.

By [GLT, Theorem 1.3], $|\mathcal{M}| \leq c_1(\log|G|)^3$ when G is almost simple. This yields

$$\sum_{M\in\mathcal{M}} v(M)^k \leq c_1(\log|G|)^3(1 - c/\log|G|)^k \leq c_1(\log|G|)^3 \exp(-ck/\log|G|).$$

The right hand side tends to zero as $|G| \to \infty$ when $k \geq c_2 \log|G| \log\log|G|$. This proves part (b). □

We observe that *the bound in* (b) *is almost best possible, up to the* $\log\log|G|$ *factor.* To show this we use the following example [FG1, p. 115]. Fix any prime p. Let $G = PSL(2, p^b).b$, the extension of the simple group by the group B of b field automorphisms, where b is a prime not dividing $p(p^2 - 1)$. Let G act on the cosets of the maximal subgroup $N_G(B)$ of G. Then all fixed-point-free elements are contained in the socle of G, so their proportion is less than $1/b$. Therefore $v(M) \geq 1 - 1/b$.

Hence, by Lemma 2.3, $P_I(G, k) \leq 1 - (1 - 1/b)^k$, so that for sufficiently large b we obtain

$$P_I(G, k) \leq 1 - (1 - c_1/\log|G|)^k \leq 1 - \exp(-c_2k/\log|G|),$$

where c_1, c_2 are suitable constants. Thus $P_I(G, k) \leq 1/2$ for all $k \leq c_3 \log|G|$, where $c_3 > 0$ is an absolute constant. The probability that it takes at least $k + 1$ random choices of elements to invariably generate G is $1 - P_I(G, k)$. By the definition of the expectancy $C(G)$ we have $C(G) \geq (k + 1)(1 - P_I(G, k))$. If $k = [c_3 \log|G|]$ then $1 - P_I(G, k) \geq 1/2$ and $k + 1 \geq c_3 \log|G|$. This yields $C(G) \geq (k + 1)(1/2) \geq (c_3/2) \log|G|$.

5. Simple groups

We will prove the following slightly stronger version of Theorem 1.3:

Theorem 5.1. *Let G be a finite simple group.*

(a) *If G is not one of the groups $\mathrm{P}\Omega^+(8, q)$, $q = 2$ or 3, then there are two elements $s_1, s_2 \in G$ such that $G = \langle s_1^{g_1}, s_2^{g_2}\rangle$ for each choice of $g_i \in \mathrm{Aut}(G)$.*

(b) *If G is $\mathrm{P}\Omega^+(8, q)$, $q = 2$ or 3, and if $G \leq G^\star \leq \mathrm{Aut}(G)$, then there are elements $s_1 \in G, s_2 \in G^\star$ such that $G \leq \langle s_1^{g_1}, s_2^{g_2}\rangle$ for each choice of $g_i \in G^\star$.*

We do not know whether the $q = 2, 3$ are actually exceptional in (b), but we conjecture that they are. Of course, Theorem 1.3 is just (a) using inner automorphisms.

We begin with the easiest case:

Table 1. Classical groups

quasisimple G	$\|T_1\|$	on V	$\|t_2\|$	on V
SL(n,q) n odd	$(q^n-1)/(q-1)$	n	$(q^{n-1}-1)/(q-1)$	$(n-1)\oplus 1$
SL(n,q) n even	$(q^{n-1}-1)/(q-1)$	$(n-1)\oplus 1$	$(q^n-1)/(q-1)$	n
$\mathrm{Sp}(2m,q)$	q^m+1	$2m$	$\mathrm{lcm}(q^{m-1}+1,q+1)$	$(2m-2)\perp 2$
$\Omega(2m+1,q)$ q odd	$(q^m+1)/2$	$2m^-\perp 1$	$(q^m-1)/2$	$(m\oplus m)\perp 1$
$\Omega^+(4k,q)$ $n=2n'=4k$	$(q^{n'-1}+1)/\delta_1$	$(n-2)^-\perp 2^-$	$\mathrm{lcm}(q^{n'-2}+1,q^2+1)/\delta_2$	$(n-4)^-\perp 4^-$
$\Omega^+(4k+2,q)$ $2n'=4k+2$	$(q^{n'-1}+1)/\delta_1$	$(n-2)^-\perp 2^-$	$(q^{n'}-1)/\delta_2$	$n'\oplus n'$
$\Omega^-(4k,q)$ $n=2n'=4k$	$(q^{n'}+1)/\delta_1$	n^-	$(q^{n'-1}-1)/\delta_2$	$(n-2)^+\perp 2^-$
$\Omega^-(4k+2,q)$	$(q^{2k+1}+1)/\delta_1$	$(4k+2)^-$	$(q^{2k}+1)/\delta_2$	$4k^-\perp 2^+$
$\mathrm{SU}(2m,q)$	$q^{2m-1}+1$	$(2m-1)\perp 1$	$(q^{2m}-1)/(q+1)$	$2m$
$\mathrm{SU}(2m+1,q)$	$(q^n+1)/(q+1)$	n	$q^{n-1}-1$	$n-1\perp 1$

Lemma 5.2. Theorem 5.1 *holds for each alternating group* A_n*,* $n\geq 5$*.*

Proof. For even $n>6$ use the product x of a disjoint 2-cycle and $(n-2)$-cycle, and the product of a disjoint p-cycle and $(n-1-p)$-cycle for a prime $p\leq n-4$ not dividing $n(n-1)$; it is easy to check that such a prime exists if $n\neq 10,14$. These two elements generate a group H that is easily seen to be transitive and even primitive. Since H contains a p-cycle, $H=A_n$ by a classical result of Jordan [Wie, Theorem 13.9]. When n is 10 or 14, the same argument applies when x is replaced by the product of two $\frac{1}{2}n$-cycles.

If n is odd then an n-cycle and a p-cycle can be used in the same manner, for an odd prime $p\leq n-3$ not dividing n.

Finally, A_6 is generated by any elements of order 4 and 5. □

For groups of Lie type we will use the knowledge of all maximal overgroups M of carefully chosen cyclic tori T_1. (There are various lists of maximal tori of groups of Lie type, collected, for example, in [KS].) Then we only need to choose an $\mathrm{Aut}(G)$-conjugacy class of elements that does not meet the union of the sets $\widetilde{M}$. Our arguments differ from those in [GM2] primarily due to that paper using [GM1] whereas we rely on the earlier paper [MSW].

Lemma 5.3. Theorem 5.1 *holds for each classical simple group other than* $\mathrm{P}\Omega^+(8,q)$*.*

Proof. We will consider the corresponding quasisimple linear group G, using cyclic tori T_1 and semisimple elements t_2 listed in Table 1 (where δ_i is 1 or 2, n is the dimension of the underlying vector space V, and $n'=n/2$).

In each case, T_1 is a cyclic torus appearing in [MSW, Theorem 1.1] and decomposing the space as indicated in the table; if there is a 1− or 2−space indicated then it is centralized. For each group, all maximal overgroups of T_1 are listed in [MSW, Theorem 1.1]. On the other hand, t_2 does not necessarily generate a torus of G; once again it acts as indicated in the table. (For the entries involving $\mathrm{lcm}(q^i+1,q^j+1)$

for some i, j, this element induces irreducible elements of order $q^i + 1$ or $q^j + 1$ on the indicated subspaces of dimension $2i$ or $2j$.) Since automorphisms of G act on V, preserving the underlying geometry [GLS, Sec. 2.5], T_1^G is an $\mathrm{Aut}(G)$-conjugacy class, while $\mathrm{Aut}(G)$-conjugates of t_2 act on V in the same manner as t_2.

If G is neither $\mathrm{SL}(2, q)$ nor $\mathrm{Sp}(4, q)$ then T_1 and t_2 invariably generate G by [MSW, Theorem 1.1]: all of the exceptions in that theorem do not arise here due to the behavior of *both* T_1 and t_2 on the vector space.

Case $\mathrm{SL}(2, q)$. When q is $4, 5$ or 9, see Lemma 5.2 (and likewise for $\mathrm{SL}(4, 2) \cong A_8$). When $q = 7$, elements of order 7 and 4 invariably generate G. For all other $q \geq 4$, T_1 and t_2 invariably generate G by [Di, Ch. XII].)

Case $\mathrm{Sp}(4, q)$. We may assume that $q \geq 4$ (since $\mathrm{Sp}(4, 2)$ is not simple and $\mathrm{PSp}(4, 3) \cong \mathrm{PSU}(4, 2)$). We use T_1 and t_2 as in the table, but now t_2 is chosen more carefully: it has order $q + 1$ and $|C_G(t_2)| = (q + 1)^2$. Once again T_1 and t_2 invariably generate G by [MSW, Theorem 1.1]. □

We note that classical groups were considered in [NP, Section 10] from a probabilistic point of view: a large number of pairs of elements was described that invariably generate various classical groups. The group $\mathrm{GL}(n, q)$ was also handled in [Sh] for large n. All groups of Lie type also were dealt with probabilistically, at least for bounded rank, in [FG1, Theorem 5.3].

Lemma 5.4. Theorem 5.1 *holds for* $\mathrm{P}\Omega^+(8, q)$.

Proof. Once again we will consider the corresponding linear group $G = \Omega^+(8, q)$, using the properties of $\mathrm{Aut}(G/Z(G))$ contained in [GLS, Sec. 2.5]. We have $G/Z(G) \leq G^\star \leq \mathrm{Aut}(G/Z(G))$.

(a) Suppose first that $q > 3$. We will use the same T_1 as above (mod $Z(G)$), of order $(q^3 + 1)/(2, q - 1)$. Its G-conjugacy class and $\mathrm{Aut}(G/Z(G))$-conjugacy class coincide mod $Z(G)$. We also use an element $x \in G$ of order $(q^3 - 1)/(2, q - 1)$. Here x decomposes our space as $8^+ = (3 \oplus 3) \perp (1 \oplus 1)$ using totally singular $3-$ and $1-$spaces, inducing an isometry of order $q - 1$ on the subspace $1 \oplus 1$ and $q^3 - 1$ on the subspace $3 \oplus 3$, and acting irreducibly on the indicated $3-$spaces. Then x fixes exactly two singular $1-$spaces, and two totally singular $4-$spaces in each G-orbit of such 4-spaces (each of the latter fixed subspaces has the form $3 \perp 1$). If τ is any triality (or other) automorphism of $G/Z(G)$ then x^τ has the same properties. In particular, neither x nor x^τ fixes any anisotropic $1-$ or $2-$space (this requires that $q > 3$: if $q \leq 3$ then x induces -1 on the 2^+-space $1 \oplus 1$ and hence fixes all of its $1-$spaces). However, by [MSW, Theorem 1.1] each maximal subgroup of $G/Z(G)$ that contains T_1 (mod $Z(G)$) either fixes such a $1-$ or $2-$space or its image under τ behaves that way. Hence, there is no maximal subgroup containing x and T_1 mod $Z(G)$, and we have invariably generated $G/Z(G)$.

(b) From now on $q \leq 3$. First consider the case where $G^\star$ acts (projectively) on V (this includes the situation in Theorem 1.3). We use cyclic tori T_3 and T_4 of $G/Z(G)$ of order $(q^4 - 1)/(4, q^4 - 1)$ arising from a decomposition $8^+ = 4^- \perp 2^- \perp 2^+$ and from a decomposition $8^+ = 4 \oplus 4$ into totally singular $4-$spaces (these tori are conjugate under $\mathrm{Aut}(G/Z(G))$ but not under $G^\star$). Let r be an odd prime dividing $q^2 + 1$. The Sylow r-subgroups of T_3 and T_4 behave differently on the vector space. Hence, by [Kl], any maximal overgroup M of $\langle T_3, T_4\rangle$ in $G/Z(G)$ is inside $H := \mathrm{O}^-(4, q) \wr C_2$, preserving a decomposition $8^+ = 4^- \perp 4^-$. Let R be a Sylow r-subgroup of T_4. Then $C_H(R)$ must contain an element of order $(q^4 - 1)/(4, q^4 - 1)$, so that R is the identity on one of the 4^-−subspaces in view of the structure of H. However, this is not possible for the subgroup R of T_4, since T_4 preserves a decomposition $8^+ = 4 \oplus 4$, acting irreducibly on each factor. Thus, there is no such M, and hence $\langle T_3, T_4\rangle = G$.

If no $\mathrm{Aut}(G/Z(G))$-conjugate of $G^\star$ acts on V then $G^\star$ contains a triality outer automorphism. Then there is a subgroup $\mathbb{Z}_3 \times \mathrm{SL}(3, q)$ of $G^\star$ that contains an element x of order $3(q^2 + q + 1)$, where this 3 arises from a triality automorphism $\tau = x^{q^2+q+1}$, and τ^3 acts as $8^+ = (3 \oplus 3) \perp (1 \oplus 1)$.

By [MSW, Theorem 1.1], $\langle T_1, x^3\rangle$ is either G, $\Omega(7, q)$, $2.\Omega(7, 3)$, or lies in $A_9 < \Omega^+(8, 2)$. Since $\langle T_1, x^3\rangle$ is invariant under τ, only the first of these can occur (for example, $\langle T_1, x^3\rangle$ cannot be $\mathrm{PSL}(2, 8) < A_9$). Thus, x and T_1 (mod $Z(G)$) invariably generate $(G/Z(G))\langle\tau\rangle$. □

Completion of proof. In [GM1, Tables 6 and 9] there are lists of carefully chosen cyclic subgroups of exceptional and sporadic simple groups, as well as all of the maximal overgroups of those subgroups. It is straightforward to use those tables to handle these final cases of Theorem 5.1. See Table 2 below for the exceptional group case, where we have also given t_2, generating most of a maxinal torus and not in any of the listed maximal overgroups of T_1 (there are many choices for t_2). □

In Section 4 we needed a bit more information than in the preceding theorem for an alternative proof of Theorem 4.1 and hence of Theorem 1.2:

Theorem 5.5. *For all sufficiently large G in* Theorem 5.1, *the elements s_i can be chosen so that $|s_i^G| > |G|^{2/3}/2$ for $i = 1, 2$.*

Proof. This is a straightforward matter of examining each part of the proof of Theorem 5.1. In each case we need to check that $|C_G(s_i)| < 2|G|^{1/3}$ for $i = 1, 2$ and all sufficiently large $|G|$.

For alternating groups, when n is even each of the groups $C_G(s)$ is the direct product of two cyclic groups, and hence has order satisfying the required bound. When n is odd the same holds if we replace the p-cycle by the product of a disjoint p-cycle and an $(n - p)$-cycle (a power of which is a p-cycle).

In Lemma 5.3 – excluding $\mathrm{SL}(2, q)$ – we have $|C_G(T_1)| \sim q^r$ and $|C_G(t_2)| \sim q^r$, where r is the rank of the corresponding algebraic group. (For example, for $\mathrm{SL}(n, q)$ we have $|C_G(T_1)| = (q^n - 1)/(q - 1)$ or $q^{n-1} - 1$, for $\mathrm{Sp}(2m, q)$ we have $|C_G(t_2)| \le (q^{m-1} + 1)(q + 1)$, and for $\Omega^+(4k + 2, q)$ we have $|C_G(T_1)| \le (q^{2k} + 1)(q + 1)$.) A straightforward calculation using $|G|$ verifies that these bounds are small enough for our purposes. When $G = \mathrm{SL}(2, q)$ we have $|C_G(T_1)| = q+1$, so that $|s_i^G| > |G|^{2/3}/2$ and a denominator larger than 1 is essential.

For the exceptional groups of Lie type we use [GM1, Proposition 2.11 and Table 6]. We reproduce part of that table below. Here T_1 is a cyclic maximal torus of the exceptional group G, and M runs through the isomorphism types of maximal subgroups of G containing T_1. (Notation: $\epsilon = \pm 1$, $\Phi_n = \Phi_n(q)$ is the nth cyclotomic polynomial evaluated at q, $\Phi'_8 = \Phi'_8(q) = q^2+\sqrt{2}q+1$, $\Phi'_{12} = \Phi'_{12}(q) = q^2+\sqrt{3}q+1$ and $\Phi'_{24} = \Phi'_{24}(q) = q^4+\sqrt{2}q^3+q^2+\sqrt{2}q+1$.) Also, t_2 generates a cyclic subgroup of G that has very small index in a maximal torus. In each case, $C_G(T_1) = T_1$, $C_G(t_2)$ is the aforementioned torus, and t_2 is not contained in any of the listed maximal overgroups. Hence, a generator of T_1 and t_2 behave as required in the theorem. □

TABLE 2. Exceptional groups

G	$\lvert T_1\rvert$	$M \geq T_1$	further max.	$\lvert t_2\rvert$
${}^2B_2(q^2), q^2 \geq 8$	Φ'_8	$N_G(T_1)$	–	$\Phi'_8(-q)$
${}^2G_2(q^2), q^2 \geq 27$	Φ'_{12}	$N_G(T_1)$	–	$\Phi'_{12}(-q)$
$G_2(q),\ 3\vert q+\epsilon$	$q^2+\epsilon q+1$	$\mathrm{SL}^\epsilon(3,q).2$	$\mathrm{PSL}(2,13)$ $(q=4)$	$q^2-\epsilon q+1$
$G_2(q),\ 3\vert q$	q^2+q+1	$\mathrm{SL}(3,q).2$	$\mathrm{PSL}(2,13)$ $(q=3)$	q^2-q+1
${}^3D_4(q)$	Φ_{12}	$N_G(T_1)$	–	$(q^3+1)(q-1)/(2,q-1)$
${}^2F_4(q^2), q^2 \geq 8$	Φ'_{24}	$N_G(T_1)$	–	$\Phi'_{24}(-q)$
$F_4(q)$	Φ_{12}	${}^3D_4(q).3$	$\mathrm{PSL}(4,3).2_2$, ${}^2F_4(2)\ (q=2)$	q^4+1
$E_6(q)$	$\Phi_9/(3,q-1)$	$\mathrm{SL}(3,q^3).3$	–	$(q+1)(q^5-1)/(6,q-1)$
${}^2E_6(q)$	$\Phi_{18}/(3,q+1)$	$\mathrm{SU}(3,q^3).3$	–	$(q-1)(q^5+1)/(6,q+1)$
$E_7(q)$	$\Phi_2\Phi_{18}/(2,q-1)$	${}^2E_6(q)_{sc}.D_{q+1}$	–	$\Phi_7/(2,q-1)$
$E_8(q)$	Φ_{30}	$N_G(T_1)$	–	Φ_{24}

Random generation. We conclude with remarks concerning the random generation of finite simple groups. All finite simple groups G are generated by two randomly chosen elements with probability tending to 1 as $|G| \to \infty$ [Di1, KL, LS]. We claim that this does not hold for invariable generation: *the probability that two – or any bounded number of – random elements of a simple group G invariably generate G is bounded away from* 1. To show this we need the following result that is implicit in [FG1].

Lemma 5.6. *There exists an absolute constant $\epsilon > 0$ such that any finite simple group G has a maximal subgroup M for which $v(M) \geq \epsilon$.*

Proof. This is trivial for alternating groups A_n, where we take M to be a point-stabilizer in the natural action, so $v(M) \sim 1 - e^{-1}$. For groups G of Lie type of bounded rank over a field with q elements we may assume q is large, and then the result follows with M a maximal subgroup containing a maximal torus (see the discussion in [FG1, start of Sec. 4]). For classical groups of large rank the result follows from [FG1, Theorem 1.7]. Sporadic simple groups satisfy the conclusion trivially. □

This lemma can be considered as a kind of weak analogue of the ϵ-conjecture (stated above) but in the opposite direction.

We can now deduce

Corollary 5.7. *There is an absolute constant $\epsilon > 0$ such that $P_I(G, k) \leq 1 - \epsilon^k$ for all finite simple groups G and positive integers k.*

Proof. This follows by combining the above lemma with Lemma 2.3. □

In [FG1, p. 114] it is announced that, for any $\epsilon > 0$, there is $c = c(\epsilon)$ such that $P_I(G, k) \geq 1 - \epsilon$ whenever G is a finite simple group of Lie type and $k \geq c$. The case of bounded rank is proved in [FG1, Theorem 4.4], and a similar result for alternating groups was proved earlier in [LuP].

Using these results it follows that, for any function $f : \mathbb{N} \to \mathbb{N}$ such that $f(n) \to \infty$ as $n \to \infty$ (even if arbitrarily slowly), we have $P_I(G, f(|G|)) \to 1$ for finite simple groups G whose orders tend to infinity.

References

[CC] P. J. Cameron and A. M. Cohen, On the number of fixed point free elements in a permutation group, Discrete Math. 106/107 (1992) 135–138.

[Di] L. E. Dickson, Linear groups with an exposition of the Galois field theory, Dover (reprint), New York 1958.

[Di1] J. D. Dixon, The probability of generating the symmetric group. Math. Z. 110 (1969) 199–205.

[Di2] J. D. Dixon, Random sets which invariably generate the symmetric group. Discrete Math. 105 (1992) 25–39.

[FG1] J. Fulman and R. M. Guralnick, Derangements in simple and primitive groups. Groups, combinatorics & geometry (Durham, 2001; Eds. A. A. Ivanov, M. W. Liebeck and J. Saxl), 99–121, World Sci. Publ., River Edge, NJ 2003.

[FG2] J. Fulman and R. M. Guralnick, Bounds on the number and sizes of conjugacy classes in finite Chevalley groups with applications to derangements (preprint arXiv:0902.2238v1).

[GLS] D. Gorenstein, R. Lyons and R. Solomon, The classification of the finite simple groups. Number 3. Part I. Chapter A. Almost simple K-groups. AMS, Providence 1998.

[GLT] R. M. Guralnick, M. Larsen and Ph. Tiep, Representation growth in positive characteristic and conjugacy classes of maximal subgroups (preprint arXiv:1009.2437).

[GM1] R. M. Guralnick and G. Malle, Products of conjugacy classes and fixed point spaces (preprint arXiv:1005.3756v2).

[GM2] R. M. Guralnick and G. Malle, Simple groups admit Beauville structures (preprint arXiv:1009.6183).

[Kl] P. B. Kleidman, The maximal subgroups of the finite 8-dimensional orthogonal groups $P\Omega_8^+(q)$ and of their automorphism groups. J. Algebra 110 (1987) 173–242.

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

[KS] W. M. Kantor and A. Seress, Prime power graphs for groups of Lie type. J. Algebra 247 (2002) 370–434.

[KZ] E. Kowalski and D. Zywina, The Chebotarev invariant of a finite group (preprint arXiv:1008.4909v).

[LPS] M. W. Liebeck, L. Pyber and A. Shalev, On a conjecture of G.E. Wall. J. Algebra 317 (2007) 184–197.

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

[Lu] A. Lubotzky, The expected number of random elements to generate a finite group. J. Algebra 257 (2002) 452–459.

[LuP] T. Łuczak and L. Pyber, On random generation of the symmetric group. Combin. Probab. Comput. 2 (1993) 505–512.

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

[NP] A. Niemeyer and C. E. Praeger, A recognition algorithm for classical groups over finite fields. Proc. London Math. Soc. 77 (1998) 117–169.

[Ol] A.Yu. Ol'shanskii, Groups of bounded period with subgroups of prime order. Algebra and Logic 21 (1982) 369–418.

[Rob] D. J. Robinson, A Course in the Theory of Groups. Springer, New York 1982.

[Sh] A. Shalev, A theorem on random matrices and some applications. J. Algebra 199 (1998) 124–141.

[Wie] H. Wielandt, Finite Permutation Groups. Academic Press, New York and London 1964.

University of Oregon, Eugene, OR 97403
E-mail address: kantor@uoregon.edu

Institute of Mathematics, Hebrew University, Jerusalem 91904
E-mail address: alexlub@math.huji.ac.il

Institute of Mathematics, Hebrew University, Jerusalem 91904
E-mail address: shalev@math.huji.ac.il