Annals of Mathematics **173** (2011), 769–814
doi: 10.4007/annals.2011.173.2.4

Random generation of finite and profinite groups and group enumeration

By Andrei Jaikin-Zapirain and László Pyber

Abstract

We obtain a surprisingly explicit formula for the number of random elements needed to generate a finite d-generator group with high probability. As a corollary we prove that if G is a d-generated linear group of dimension n then $cd + \log n$ random generators suffice.

Changing perspective we investigate profinite groups F which can be generated by a bounded number of elements with positive probability. In response to a question of Shalev we characterize such groups in terms of certain finite quotients with a transparent structure. As a consequence we settle several problems of Lucchini, Lubotzky, Mann and Segal.

As a byproduct of our techniques we obtain that the number of r-relator groups of order n is at most n^{cr} as conjectured by Mann.

1. Introduction

Confirming an 1882 conjecture of Netto [40], Dixon [13] proved in 1969 that two randomly chosen elements generate the alternating group $\mathrm{Alt}(n)$ with probability that tends to 1 as $n \to \infty$. This was extended in [21] and [24] to arbitrary sequences of non-abelian finite simple groups. Such results form the basis of applying probabilistic methods to the solution of various problems concerning finite simple groups [50].

Interest in random generation of more general families of finite groups arose when it was realized that randomized algorithms play a critical role in handling matrix groups [4]. Denote by $\nu(G)$ the minimal number k such that G is generated by k random elements with probability $\geq 1/e$. As Pak [44] has observed, up to a small multiplicative constant, $\nu(G)$ is the same as the expected number of random elements generating G. We obtain the following quite unexpected result.

The first author is supported in part by the Spanish Ministry of Science and Innovation, the grant MTM2008-06680. The second author is supported in part by OTKA grant numbers NK 72523 and NK 78439.

For a non-abelian characteristically simple group A denote by $\mathrm{rk}_A(G)$ the maximal number r such that a normal section of G is the product of r chief factors isomorphic to A. Denote by $l(A)$ the minimal degree of a faithful transitive permutation representation of A.

THEOREM 1. *There exist two absolute constants $\alpha > \beta > 0$ such that for any finite group G we have*

$$\alpha\left(d(G) + \max_A\left\{\frac{\log(\mathrm{rk}_A(G))}{\log(l(A))}\right\}\right) < \nu(G) < \beta d(G) + \max_A\left\{\frac{\log(\mathrm{rk}_A(G))}{\log(l(A))}\right\},$$

where A runs through the non-abelian chief factors of G.

COROLLARY 2. (1) *If G is a finite d-generated linear group of dimension n over some field K then $\nu(G) \leq cd + \log n$ for some absolute constant c.*

(2) *If G is a finite d-generated group then $\nu(G) \leq cd + \log \tilde{d}$ for some absolute constant c, where $\tilde{d} = \tilde{d}(G)$ is the maximum size of a minimal generating set.*

(3) *If G is a finite d-generated group then $\nu(G) \leq cd + \log\log|G|$ for some absolute constant c.*

Note that in the first bound the number of random generators does not depend on K and it grows very slowly when the dimension is increased. Our bounds can be used in particular in analyzing the behavior of the famous Product Replacement Algorithm [9], [12], [31]. The parameter $\tilde{d}$ (instead of $\log \tilde{d}$) appears in various results concerning the behaviour of this algorithm [9], [12]. A slightly different version of the third part of Corollary 2 was first proved in [11] and [29]. For more details and more precise bounds see Section 9.

Asymptotic results for finite groups are often best understood by considering their inverse limits, i.e., profinite groups. Motivated in part by Dixon's theorem, in the past 20 years results on random generation were obtained for various profinite groups. Recall that a profinite group G may be viewed as a probability space with respect to the normalised Haar measure.

Let A denote the Cartesian product of all finite alternating groups of degree at least 5. Kantor and Lubotzky [21] showed that A can be generated (as a topological group) by three random elements with positive probability. They used a more precise version of Dixon's theorem due to Babai [3]. The same was shown to hold for profinite groups G obtained as the Cartesian product of any collection of distinct non-abelian simple groups [21], [24].

Further examples appear in the work of Bhattacharjee [7]. She proved that if W is an inverse limit of iterated wreath products of finite alternating groups (of degree at least 5) then W is generated by two random elements with

positive probability. This result has recently been extended to iterated wreath products of arbitrary sequences of non-abelian finite simple groups [51].

A profinite group G is called *positively finitely generated* (PFG) if for some r a random r-tuple generates G with positive probability. As we saw above non-abelian finite simple groups can be combined in various ways to yield PFG groups.

This concept actually first arose in the context of field arithmetic. Various theorems that are valid for "almost all" r-tuples in the absolute Galois group $G(F)$ of a field F appear in [15]. (For a survey on random elements of profinite groups see [16].)

Answering a question of Fried and Jarden [15], Kantor and Lubotzky [21] have shown that F_d, the free profinite group of rank d is not PFG if $d \geq 2$. On the other hand, Mann [35] has proved that finitely generated prosoluble groups have this property. More generally in [8] it was shown that finitely generated profinite groups which do not have arbitrarily large alternating sections are PFG.

Denote by $m_n(G)$ the number of index n maximal subgroups of G. A group G is said to have polynomial maximal subgroup growth (PMSG) if $m_n(G) \leq n^c$ for all n (for some constant c).

A one-line argument shows that PMSG groups are positively finitely generated. By a very surprising result of Mann and Shalev the converse also holds.

THEOREM 3. ([38]). *A profinite group is* PFG *if and only if it has polynomial maximal subgroup growth.*

This result gives a beautiful characterization of PFG groups. However, it does not make it any easier to prove that the above mentioned examples of profinite groups are PFG.

In his 1998 International Congress of Mathematicians talk [53, p. 131] Shalev stated that "we are still unable to find a structural characterization of such groups, or even to formulate a reasonable conjecture". Similar remarks have been made in [54, p. 386]. We give a semi-structural characterization which really describes which groups are PFG.

Let L be a finite group with a non-abelian unique minimal normal subgroup M. A *crown-based power* $L(k)$ of L is defined as the subdirect product subgroup of the direct power L^k containing M^k such that $L(k)/M^k$ is isomorphic to L/M (here L/M is the diagonal subgroup of $(L/M)^k$).

THEOREM 4. *Let G be a finitely generated profinite group. Then G is* PFG *if and only if for any L as above if $L(k)$ is a quotient of G then $k \leq l(M)^c$ for some constant c.*

An interesting feature of the theorem is that the number of random elements needed to generate a group G depends only on its normal sections H/N which are powers of some non-abelian finite simple groups such that $|G/H|$ is very small compared to $|H/N|$.

For the full statement of our main result see Section 11. The theorem can be used to settle several open problems in the area. For example, it subsumes a conjecture of Lucchini [33] according to which non-PFG groups have quotients which are crown-based powers of unbounded size. We can also answer a question of Lubotzky and Segal [32] proving that finitely generated profinite groups of polynomial index growth are PFG (see §12). Theorem 4 gives an easy proof that all previously known examples of PFG groups are indeed PFG. In fact groups which are not PFG are rather "large".

COROLLARY 5. *Let G be a finitely generated profinite group. Then G is* PFG *if and only if there exists a constant c such that for any almost simple group R, any open subgroup H of G has at most $l(R)^{c|G:H|}$ quotients isomorphic to R.*

Moreover we show that if G is not a PFG group, then for infinitely many open subgroups H, H has at least $2^{|G:H|}$ quotients isomorphic to some non-abelian simple group S.

Corollary 5 immediately implies a positive solution of a well-known open problem of Mann [35].

COROLLARY 6. *Let H be an open subgroup in a* PFG *group. Then H is also a* PFG *group.*

Note that by a recent deep result of Nikolov and Segal [43], if G is a finitely generated profinite group and H is a finite index subgroup then H is an open subgroup of G.

On the way towards proving Theorem 4 we obtain similar characterizations for groups of exponential subgroup growth. For example, we have the following surprising result.

THEOREM 7. *Let G be a finitely generated profinite group. Assume that there is a constant c such that each open subgroup H has at most $c^{b|G:H|}$ quotients isomorphic to* $\mathrm{Alt}(b)$ *for any $b \geq 5$. Then G has at most exponential subgroup growth.*

The converse is obvious. Comparing these results with the ones obtained for PFG groups we immediately see that PFG groups have at most exponential subgroup growth. This answers a question of Mann and Segal [37].

The proofs of Theorems 1 and 4 are based on a new approach to counting permutation groups and permutation representations. Our main technical result (which was first conjectured in [49]) is the following.

THEOREM 8. *The number of conjugacy classes of d-generated primitive subgroups of* $\mathrm{Sym}(n)$ *is at most n^{cd} for some constant c.*

This estimate unifies and improves several earlier ones. For primitive soluble groups it is an immediate consequence of [47, Lemma 3.4]. More generally in [8] it was shown to hold for groups G with no large alternating sections (in which case the primitive groups have polynomial size [5]). Moreover by a central result of [38], it was known to hold for primitive groups with a given abstract isomorphism type. The main theorem of [49] bounding the number of all primitive groups can also be seen as an easy consequence. Indeed we can improve this bound using Theorem 8 as follows.

COROLLARY 9. *There exists a constant c such that the number of conjugacy classes of primitive groups of degree n is at most $n^{c \log n/\sqrt{\log \log n}}$.*

Most of Sections 2–8 is devoted to the proof of various structural and counting results which are needed to prove Theorem 8. Sections 9–12 contain the proofs of Theorem 1, Theorem 4 and their corollaries.

In recent years probabilistic methods have proved useful in the solution of several problems concerning finite and profinite groups (see e.g. [25], [50] and [43]). We believe that our counting results will have a number of such applications. As an illustration in Section 13 we confirm a conjecture of Mann [36] by a probabilistic argument

THEOREM 10. *There exists a constant c such that the number of groups of order n that can be defined by r relations is at most n^{cr}.*

This may be viewed as a refinement of various results on abstract group enumeration obtained earlier by Klopsch [23], Lubotzky [28] and P. M. Neumann [41].

2. **Preliminaries**

In this section we collect the notation and the principal results which will be needed later.

2.1. *Notation.*

$a_n(G)$	the number of subgroups of index n in G
$s_n(G)$	the number of subgroups of index at most n in G
$m_n(G)$	the number of maximal subgroups of index n in G
$d(G)$	the minimal number of generators for G
$\tilde{d}(G)$	the maximum of the size of a minimal generating set of G

$l(G)$	the minimal degree of a faithful transitive representation of G
$l^*(G)$	the minimal degree of a faithful primitive representation of a primitive group G
$\mathrm{rk}_A(G)$	the maximal number r such that a non-abelian normal section of G is the product of r chief factors of G isomorphic to A
$\mathrm{rk}_n(G)$	the maximum of the numbers $\mathrm{rk}_A(G)$ with $l(A) \leq n$
$\mathrm{Epi}(G,T)$	the set of epimorphisms from G onto T

2.2. *Basic facts.* First we recall Gaschütz's lemma.

LEMMA 2.1 ([16, Lemma 17.7.2]). *Let T be a d-generated group and $\phi\colon T \to L$ an epimorphism. Suppose that $x_1, \dots, x_d$ generate L. Then there exist $y_1, \dots, y_d$ generating T such that $\phi(y_i) = x_i$ for all i.*

COROLLARY 2.2. *Let G be a group, N a normal subgroup of G and $S \leq G/N$. Then the number of d-generated subgroups T of G such that $TN/N = S$ is at most $|N|^d$.*

Proof. If S is not generated by d elements then the number of such subgroups T is equal to 0. Suppose that S can be generated by d elements. Let $x_1, \dots, x_d \in G/N$ generate S. Using Gaschütz's Lemma, we obtain that there are elements $y_1, \dots, y_d$ generating T such that $y_i N = x_i$ for all i. Thus, there are at most $|N|^d$ possibilities for T. □

PROPOSITION 2.3 ([46]). *Let P be a primitive permutation group of degree n and suppose that P does not contain $\mathrm{Alt}(n)$. Then the order of P is at most 4^n.*

PROPOSITION 2.4 ([49]). *There exists an absolute constant c_1 such that, for each n, the group $\mathrm{Sym}(n)$ has at most c_1^n conjugacy classes of primitive subgroups.*

Let $\mathrm{Epi}(G,T)$ denote the set of epimorphism from G onto T. We will often use the following lemma.

LEMMA 2.5. *Let T be a transitive subgroup of $\mathrm{Sym}(n)$. Then the number of T-conjugacy classes of epimorphism from G onto T is at most $\frac{n|\mathrm{Epi}(G,T)|}{|T|}$.*

Proof. It is well-known that $|C_{\mathrm{Sym}(n)}(T)| \leq n$. Hence $|Z(T)| \leq n$. This gives the lemma. □

LEMMA 2.6 ([17, Lemma 8.6]). *Let S be a finite non-abelian simple group. Then $|\mathrm{Out}(S)| \leq l(S)$ and $|\mathrm{Out}(S)| \leq 3\log l(S)$.*

We call H a *subdirect product subgroup* of S^t if it is a subdirect product of $S_1 \times \cdots \times S_t$ where the S_i are all isomorphic to S. Such an H is called a *diagonal subgroup* if it is isomorphic to S.

LEMMA 2.7. *Let S be a non-abelian simple group and H a subdirect product subgroup of $S^t \cong S_1 \times \cdots \times S_t$.*

(1) *Then there are partitions of the set of indices $\{1, \ldots, t\}$ and for each part, say $\{i_{j1}, \ldots, i_{jk}\}$, a diagonal subgroup D_j of $S_{i_{j1}} \times \cdots \times S_{i_{jk}}$ such that H is a direct product of the subgroups D_j.*
(2) *The number of S^t-conjugacy classes of diagonal subgroups of S^t is equal to $|\operatorname{Out}(S)|^{t-1}$.*

Proof. (1) This is a standard result.

(2) Identifying $\operatorname{Inn}(S)$ with S, we consider S^t as a subgroup of $\operatorname{Aut}(S)^t$. Note that $\operatorname{Aut}(S)^t$ acts transitively on diagonal subgroups of S^t and the stabilizer of a subgroup $D = \{(s, \ldots, s) | s \in S\}$ is $\widetilde{D} = \{(\phi, \ldots, \phi) | \phi \in \operatorname{Aut}(S)\}$. Since $S^t \cap \widetilde{D} = D$, we obtain that there are

$$\frac{|\operatorname{Aut}(S)|^t |D|}{|\widetilde{D}||S|^t} = |\operatorname{Out}(S)|^{t-1}.$$

S^t-conjugacy classes of diagonal subgroups of S^t. □

2.3. *The number of epimorphisms.* This subsection is mainly devoted to considering subdirect products of groups with unique minimal normal subgroups.

LEMMA 2.8. *Let H be a subgroup of $\operatorname{Sym}(s)^k$. If a chief-factor of H is isomorphic to S^t , where S is a non-abelian simple group, then $t \leq s/2$.*

Proof. If $k = 1$ then our condition implies that $\operatorname{Sym}(s)$ has an elementary abelian section of order p^t for some prime p and it is well-known that this implies $t \leq s/2$ (see, for example, [39]). The general case follows by an easy induction argument. □

LEMMA 2.9. *Let T_i $(i = 0, \ldots, l)$ be a group with a unique minimal normal subgroup K_i and G a subdirect product of $T_1 \times \cdots \times T_l$. Assume that for all i, $K_i \cong S^s$ where S is a non-abelian finite simple group. Put $N = K_1 \times \cdots \times K_l$ and $L = N \cap G$. Then the following holds*:

(1) *If $\phi\colon G \to T_0$ is an epimorphism, then $\phi(L) = K_0$. Moreover $\operatorname{Ker}\phi = C_G(K_i)$ for some $1 \leq i \leq l$.*
(2) *L is a subdirect product subgroup of N.*
(3) *If $G \cap T_i \neq 1$ for all i, then $L = N$.*

Proof. Denote by $\widetilde{N}$ the intersection of the normalizers in $T_1 \times \cdots \times T_l$ of all simple normal subgroups of N. Put $\tilde{L} = \widetilde{N} \cap G$. It is clear that $G/\tilde{L}$ is a subgroup of $\operatorname{Sym}(s)^l$. Hence by Lemma 2.8, $\tilde{L}$ is not contained in $\operatorname{Ker}\phi$. On the other hand $\tilde{L}/L$ is a subgroup of $\operatorname{Out}(S)^{sl}$, whence it is solvable. This

implies that $M = \operatorname{Ker}\phi \cap L$ is a normal subgroup of G properly contained in L and so $\phi(L) \geq K_0$.

Now, we can apply the previous paragraph in the case when $T_0 \cong T_i$ for some $1 \leq i \leq l$ and ϕ is the projection on T_i. In this case it is clear that actually $\phi(L) = K_i$. Thus, L is a subdirect product of $K_1 \times \cdots \times K_l$. This gives us the second part of the lemma.

The third part is trivial, because $G \cap T_i$ is a normal subgroup of T_i and so it contains K_i.

Now we finish the proof of the first part of the lemma. If $l = 1$ then ϕ is an isomorphism and $\operatorname{Ker}\phi = C_G(K_1) = 1$. Suppose, now, that $l > 1$. If $G \cap T_i$ is trivial for some $1 \leq i \leq l$, then G is a subdirect product of $l-1$ subgroups T_j and we can apply induction. Hence we can assume that $G \cap T_i$ is a nontrivial normal subgroup of T_i for all $1 \leq i \leq l$ and therefore $L = N$. Since $M = \operatorname{Ker}\phi \cap L$ is a normal subgroup of G properly contained in L, it follows that M is the product of all but one of the K_i. Therefore we have $\phi(L) = K_i$ in general.

Assume that $M = K_2 \times \cdots \times K_l$. Then $\phi(K_1) = K_0$. Since $C_{T_0}(K_0) = 1$ we have $\phi(C_G(K_1)) = 1$. On the other hand $\operatorname{Ker}\phi$ and K_1 are disjoint normal subgroups hence $\operatorname{Ker}\phi$ centralizes K_1. Thus we have $\operatorname{Ker}\phi = C_G(K_1)$ as required. □

LEMMA 2.10 ([52, Lemma 1.1]). *Let G be a group with a characteristic subgroup H such that $C_G(H) = 1$. Then G is naturally embedded in $\operatorname{Aut}(H)$ by means of conjugation of H by the elements of G, and there is a natural isomorphism between $\operatorname{Aut}(G)$ and $N_{\operatorname{Aut}(H)}(G)$.*

COROLLARY 2.11. *Let T be a group with a unique minimal normal subgroup K. Suppose that K is isomorphic to S^s where S is a non-abelian simple group. Then $|\operatorname{Aut}(T)| \leq (5|\operatorname{Out}(S)|)^s|T|$.*

Proof. Note that $\operatorname{Aut}(K)$ is isomorphic to $\operatorname{Aut}(S) \wr \operatorname{Sym}(s)$. Denote by B the base group of this wreath product. T is a subgroup of $\operatorname{Aut}(K)$ containing S^s and by Lemma 2.10, $\operatorname{Aut}(T)$ is also a subgroup of $\operatorname{Aut}(K)$ normalising T. Let $\overline{T} = TB/B$ be the natural image of T in $\operatorname{Sym}(s)$ and $\bar{A} = \operatorname{Aut}(T)B/B$ the image of $\operatorname{Aut}(T)$. $\overline{T}$ is a transitive group and $\bar{A}$ is contained in its normalizer in $\operatorname{Sym}(s)$. Hence by [17, Th. 11.1], $|\bar{A}/\overline{T}| \leq 5^s$. Therefore we have

$$|\operatorname{Aut}(T)| \leq |B||\overline{T}|5^s \leq |K||\operatorname{Out}(S)|^s|\overline{T}|5^s \leq (5|\operatorname{Out}(S)|)^s|T|$$

as required. □

LEMMA 2.12. *Let G and T be two groups and K a normal subgroup of T. Then*

(1) $|\operatorname{Epi}(G,T)| \leq |\operatorname{Epi}(G,T/K)||K|^{d(G)}$.

(2) *Let K be a central product of s isomorphic quasisimple subgroups S_i and suppose that T acts transitively on the S_i. Put $S = S_1/Z(S_1)$. Then*

$$|\mathrm{Epi}(G,T)| \leq \log|G|(5|\operatorname{Out}(S)|)^s|T||C_T(K)|^{d(G)}.$$

Proof. (1) This is evident.

(2) Since $C_{T/C_T(K)}(KC_T(K)/C_T(K)) = 1$, using the previous statement, we can suppose that $C_T(K) = 1$. Hence the $S_i \cong S$ are simple groups and K is the unique minimal normal subgroup of T.

Without loss of generality we may assume that the intersection of the kernels of epimorphisms from G onto T is equal to 1. Thus, G is a subdirect product subgroup of T^m, where m is the number of such epimorphism. Let l be the smallest k such that G is a subdirect product subgroup of T^k. Consider G inside T^l and put $L = K^l \cap G$.

By Lemma 2.9, $L = K^l$ and there are at most $l \leq \log|G|$ possibilities for $M = \operatorname{Ker}\phi$, where ϕ is an epimorphism from G onto T. Fix one such M. We want to calculate the number of epimorphisms $\phi\colon G \to T$ such that $M = \operatorname{Ker}\phi$. This number clearly coincides with the number of automorphisms of T. By Corollary 2.11,

$$|\operatorname{Aut}(T)| \leq (5|\operatorname{Out}(S)|)^s|T|. \tag{2.1}$$

Hence we conclude that there are at most

$$\log|G|(5|\operatorname{Out}(S)|)^s|T|$$

epimorphisms from G onto T. □

Remark 2.13. In case T is an almost simple group the proof of the above corollary and lemma yields that $|\mathrm{Epi}(G,T)| \leq |T|\log|G|$.

Remark 2.14. Looking at the proof of Lemma 2.12(2) more carefully we see that the $\log|G|$ term can be replaced by the maximal number $r = \mathrm{rk}_A(G)$ such that a non-abelian normal section of G is the product of r chief factors of G isomorphic to $A = K/Z(K)$.

2.4. *The number of complements.* In this subsection we consider the following situation. Let X be a group containing a normal subgroup D which is the direct product of the X-conjugates of some subgroup L. We want to estimate the number of complements to D in X. The first result is due to M. Aschbacher and L. Scott.

PROPOSITION 2.15 ([2]). *Let $D' = \langle L^X \setminus \{L\}\rangle$ and if T is a complement to D in X define $\mu(T) = D'N_T(L)/D'$. Then μ is a surjective map from the set of all complements to D in X onto the set of all complements to $D/D' \cong L$ in $N_X(L)/D'$, and μ induces a bijection $T^X \to \mu(T)^L$ of conjugacy classes of complements.*

We say that a complement T to D in X is *large* if the image of the natural map from $N_T(L)$ to $\mathrm{Aut}(L)$ contains the inner automorphisms of L. In the next proposition we estimate the number of large complements in the case where L is a simple non-abelian group. A version of Proposition 2.16 which considers this situation appears in [51, §2]. We refer the reader to this paper for more details.

PROPOSITION 2.16. *Let X, D and L as before and suppose, moreover, that L is a simple non-abelian group. Then the number of the X-conjugacy classes of large complements to D in X is at most*

$$|\operatorname{Out}(L)| \log |X/D|.$$

Proof. Since L is a normal subgroup of $N_X(L)$, we have a natural homomorphism $\rho\colon N_X(L) \to \mathrm{Aut}(L)$. Let R be the image of ρ. Now $N_X(L) = DN_T(L)$ and it is easy to see that a complement T to D in X is large if and only if $\rho(N_T(L)) = R$. In the following we identify L and $\mathrm{Inn}(L)$. Thus $L \leq R$.

Let $Q = N_X(L)/D$. Define $\phi\colon N_X(L) \to Q \times R$ by means of $\phi(x) = (xD, \rho(x))$. The kernel of ϕ is $D \cap C_X(L) = D'$. By the above, $\phi(N_T(L))$ is a subdirect pr oduct of $Q \times R$. As a subgroup of $\phi(N_X(L))$ it corresponds to $\mu(T)$ which by Proposition 2.15 is a complement to $\phi(D) \cong L \leq R$. It follows that $\phi(N_T(L))$ is a complement to R in $Q \times R$. Moreover, by Proposition 2.15, if two complements T_1 and T_2 are not X-conjugates, then $\phi(N_{T_1}(L))$ and $\phi(N_{T_2}(L))$ are not L-conjugates.

Let $S = \{s = (q_s, r_s) | q_s \in Q,\ r_s \in R\}$ be a complement to R in $Q \times R$ which is a subdirect product of $Q \times R$. Then the map $\psi_S\colon q_s \to r_s$ is an epimorphism from Q onto R. Note that ψ_S determines S uniquely and two such complements are L-conjugates if and only if ψ_{S_1} and ψ_{S_2} are L-conjugates.

By the remark after Lemma 2.12 the number of epimorphisms from Q onto R is at most $|\operatorname{Aut}(L)| \log |Q|$. Hence the number of X-conjugacy classes of the large complements to D in X is at most $|\operatorname{Out}(L)| \log |X/D|$. □

2.5. *Large G-groups.* Recall that a *G-group* A is a group A with a homomorphism $\theta\colon G \to \mathrm{Aut}(A)$. If there is no danger of confusion we put $a^g = a^{\theta(g)}$, if $a \in A$, $g \in G$. When G is profinite, A is also profinite and the homomorphism θ is assumed to be continuous. Two G-groups A and B are said to be *G-isomorphic*, denoted $A \cong_G B$, if there exists an isomorphism $\phi\colon A \to B$ such that $a^{g\phi} = a^{\phi g}$, $a \in A$, $g \in G$. We say that A is an *irreducible* G-group if A does not have proper normal G-subgroups. We say that A is a *semisimple* G-group if A is a direct product of irreducible G-groups.

Let S be quasisimple group. We say that a group $A = S^k$ is a *large* G-group if A is a G-group associated with $\theta\colon G \to \mathrm{Aut}(A)$ and $\theta(G) \cap \mathrm{Inn}(A)$ is a subdirect product subgroup of $\mathrm{Inn}(A) \cong \mathrm{Inn}(S)^k$. For example, any chief factor of G is large. In the following lemma we give another example.

LEMMA 2.17. *Let F be a profinite group and K_i $(i = 1, \dots, k)$ non-abelian chief factors. Suppose that the K_i are all isomorphic as groups. Then $K_1 \times \cdots \times K_k$ is a large F-group.*

Proof. Without loss of generality we can suppose that F is a subdirect product subgroup of $T_1 \times \cdots \times T_k$, where $T_i = F/C_F(K_i)$. Then using Lemma 2.9, we obtain the result. □

LEMMA 2.18. *Let Q be a group and N a normal subgroup of Q. Suppose that $N = S_1 \times \cdots \times S_s$, where S_1 is a quasisimple group and Q permutes the S_i transitively. Denote by $\widetilde{N}$ the normalizer of all the S_i and put $S = S_1/Z(S_1)$. Then the number of Q-conjugacy classes of d-generated subgroups T of Q such that N is a large T-group (T acts on N by conjugation) and $T\widetilde{N} = Q$ is at most*

$$|C_Q(N)|^d |\operatorname{Out}(S)|^{sd}(1 + |\operatorname{Out}(S)|)^s.$$

Proof. Let T be such a subgroup of Q. Since

$$C_{Q/C_Q(N)}(NC_Q(N)/C_Q(N)) = 1,$$

using Corollary 2.2, we may assume that $C_Q(N) = 1$. Then the $S_i \cong S$ are simple groups, N is the unique minimal normal subgroup of Q and $K = T \cap N$ is a subdirect product subgroup of $N \cong S^s$.

Therefore in order to choose K we should first choose a partition of the set of indices as in Lemma Lemma 2.7(1). Since T acts transitively on $\{S_i\}$ it is enough to choose the first part and the rest of the partition will be determined automatically. There are $\binom{s}{k}$ subsets in $\{1, \dots, s\}$ of size k, whence, by Lemma 2.7(2), there are at most

$$\sum_{k=1}^{s} \binom{s}{k} |\operatorname{Out}(S)|^{k-1} = \frac{(1 + |\operatorname{Out}(S)|)^s - 1}{|\operatorname{Out}(S)|}$$

choices for K.

Fix one such K and consider $L = N_Q(K)$. Then $T \leq L$ and it is easy to see that $L \cap N = K$. Now T projects onto $L/(L \cap \widetilde{N})$ and $(L \cap \widetilde{N})/K$ has order at most $|\operatorname{Out}(S)|^s$. Hence there are at most $|\operatorname{Out}(S)|^{sd}$ choices for T/K inside L/K. But T/K determines T inside L. Thus we conclude that the number of d-generated subgroups T up to conjugacy inside Q, for which N is a large T-group and $Q = T\widetilde{N}$, is at most $|\operatorname{Out}(S)|^{sd}(1 + |\operatorname{Out}(S)|)^s$. □

LEMMA 2.19. *Let $N = S^s = S_1 \times \cdots \times S_s$, where S is a non-abelian simple group. Suppose that N is a large Q-group associated with $\theta\colon Q \to \operatorname{Aut}(N)$ such that Q permutes the S_i transitively. Let $K = N \cap \theta(Q)$. Then either $|K| < l(N)$ or $|C_Q(K)| \leq |C_Q(N)| l(N)$ (here we identify $\operatorname{Inn}(N)$ and N).*

Proof. Without loss of generality we may assume that $C_Q(N) = 1$. Then N is an irreducible Q-group and Q is embedded in $\mathrm{Aut}(N)$. Note that since S is simple, $l(N) = l(S^s) = l(S)^s$.

By Lemma 2.7 there is a partition of the set of indices $\{1, \dots, s\}$ into l parts and for each part, say $\{i_{j1}, \dots, i_{jk}\}$, a diagonal subgroup D_j of $S_{i_{j1}} \times \cdots \times S_{i_{jk}}$ such that K is a direct product of the subgroups D_j. Since Q permutes the S_i transitively, all parts have s/l elements. Suppose that $|K| \geq l(N) = l(S)^s$. Now $|S| \leq l(S)^{l(S)}$, whence $l(S)^{l(S)l} \geq |K| \geq l(S)^s$ and so $s/l \leq l(S)$.

If some element of Q centralizes K, it should fix the partition and centralize all D_j. Hence

$$|C_Q(K)| \leq ((s/l)!)^l \leq (s/l)^s \leq l(S)^s = l(N). \qquad \square$$

3. The number of d-generated transitive groups

In this section we count permutation groups up to permutation isomorphism, i.e., up to conjugacy in $\mathrm{Sym}(n)$. A transitive permutation group T is determined up to permutation isomorphism by the isomorphism type of T and by the orbit of a point stabiliser under $\mathrm{Aut}(T)$ and vice versa.

Let $c_t = (4c_1)^3$, where c_1 is a constant from Proposition 2.4. The aim of this section is to prove the following result.

THEOREM 3.1. *The number of conjugacy classes of transitive d-generated subgroups of* $\mathrm{Sym}(n)$ *is at most* c_t^{nd}.

Proof. We will prove the proposition by induction on n. The base of induction is evident and we assume that $n \geq 5$.

Let $T \leq \mathrm{Sym}(n)$ be a d-generated transitive group of degree n. Suppose that $\{B_1, \dots, B_s\}$ is a system of blocks for T, such that $b = |B_1| > 1$ and $H_1 = \mathrm{St}_T(B_1)$ acts primitively on B_1. Thus, $T \leq \mathrm{St}_{\mathrm{Sym}(n)}(\{B_i\}) \cong \mathrm{Sym}(b) \wr \mathrm{Sym}(s)$. Let P be the image of H_1 in $\mathrm{Sym}(B_1) \cong \mathrm{Sym}(b)$ and let $\widetilde{K}$ be the kernel of the action of T on the blocks. Then $T/\widetilde{K}$ can be naturally embedded into $\mathrm{Sym}(s)$ and T into $P \wr (T/\widetilde{K})$.

We divide the d-generated transitive subgroups of $\mathrm{Sym}(n)$ into three families. We note that some groups can belong to different families.

Family 1. *Suppose that P does not contain* $\mathrm{Alt}(b)$ *or* $b \leq 4$. By induction, there are at most c_t^{ds} choices for $T/\widetilde{K}$ up to conjugacy inside $\mathrm{Sym}(s)$. Fix one such $T/\widetilde{K}$. By Proposition 2.4, there are at most c_1^b choices for P up to conjugacy inside $\mathrm{Sym}(b)$. Also fix one such P. Hence we fixed the embedding of $P \wr (T/\widetilde{K})$ into $\mathrm{Sym}(n)$.

By Proposition 2.3, $|P| \leq 4^b$. Hence $|P|^s \leq 4^n$. By Corollary 2.2, there are at most 4^{nd} possibilities for T inside $P \wr (T/\widetilde{K})$. Thus, we conclude, that

there are at most

$$\sum_{s\leq n/2} c_t^{ds} 4^{nd} c_1^b \leq c_t^{d(\frac{n}{2}+1)} 4^{nd} c_1^n \tag{3.1}$$

transitive d-generated groups in the first family.

Family 2. *Suppose that* $b \geq 5$, P *contains* $\mathrm{Alt}(b)$ *and* $\widetilde{K} \neq 1$. Since $\widetilde{K} \neq 1$ and T permutes the blocks $\{B_i\}$ transitively the image of $\widetilde{K}$ in $P \leq \mathrm{Sym}(B_1) \cong \mathrm{Sym}(b)$ is a nontrivial normal subgroup of P. Hence $K = [\widetilde{K}, \widetilde{K}]$ is a subdirect product subgroup of $\mathrm{Alt}(b)^s$. Since T acts transitively on the blocks $\{B_i\}$, K is a minimal normal subgroup of T.

Applying induction as in the previous case, we obtain that there are at most c_t^{ds} choices for $T/\widetilde{K}$ up to conjugacy inside $\mathrm{Sym}(s)$. We fix one such $T/\widetilde{K}$. This means that we fix $Q = \mathrm{Sym}(b) \wr T/\widetilde{K}$ inside $\mathrm{Sym}(n)$. By Lemma 2.18, there are at most 16^{sd} choices for T up to conjugacy inside Q. Thus we conclude that there are at most

$$\sum_{s\leq n/5} c_t^{ds} 16^{sd} \leq c_t^{d(\frac{n}{5}+1)} 2^{nd} \tag{3.2}$$

conjugacy classes of transitive d-generated groups in the second family.

Family 3. *Suppose that* $b \geq 5$, P *contains* $\mathrm{Alt}(b)$ *and* $\widetilde{K} = 1$. In this case T acts faithfully on the set of blocks. By induction we have at most c_t^{sd} choices for T up to conjugacy in $\mathrm{Sym}(s)$. Fix $W = \mathrm{Sym}(b) \wr T$ as a subgroup of $\mathrm{Sym}(n)$. By Corollary 2.2 there are at most 2^{sd} possibilities for $T(\mathrm{Alt}(b))^s$ inside W. Fix one such possibility and put $X = T(\mathrm{Alt}(b))^s$. By Proposition 2.16, there are at most $4 \log |T| \leq 4n^2$ choices for T up to conjugacy in X. Thus, we conclude, that there are at most

$$\sum_{s\leq n/5} 4 c_t^{ds} 2^{sd} n^2 \leq c_t^{d(\frac{n}{5}+1)} 2^{nd} n^2 \tag{3.3}$$

conjugacy classes of transitive d-generated groups in the third family.

Now, putting together (3.1), (3.2) and (3.3) we obtain the theorem. □

4. **The number of transitive representations**

The aim of this section is to prove the following result and several corollaries.

PROPOSITION 4.1. *Let G be a finite d-generated group and T a transitive group of degree n. Then there are at most $|T| \log |G| c_r^{dn}$ epimorphisms from G onto T (where $c_r = 16$).*

Proof. We proceed by induction on n. Suppose that $\{B_1, \ldots, B_s\}$ is a system of blocks for T, such that $b = |B_1| > 1$ and $H_1 = \mathrm{St}_T(B_1)$ acts primitively on B_1. Thus, $T \leq \mathrm{St}_{\mathrm{Sym}(n)}(\{B_i\}) \cong \mathrm{Sym}(b) \wr \mathrm{Sym}(s)$. Let P be the image

of H_1 in $\mathrm{Sym}(B_1) \cong \mathrm{Sym}(b)$ and let $\widetilde{K}$ be the kernel of the action of T on the blocks. Hence $\widetilde{K} = T \cap \mathrm{Sym}(b)^s$. Then T can be naturally embedded in $P \wr (T/\widetilde{K})$.

Case 1. *Suppose that* $|\widetilde{K}| \leq 4^n$. Note that $T/\widetilde{K}$ is a transitive group of degree s. By induction, there are at most $|T/\widetilde{K}| \log |G| c_r^{ds}$ epimorphisms from G onto $T/\widetilde{K}$. Hence, since $|\widetilde{K}| \leq 4^n$, there are at most

$$|T/\widetilde{K}| \log |G| c_r^{ds} 4^{dn} \leq |T| \log |G| c_r^{dn}$$

epimorphisms from G onto T.

Case 2. *Suppose that* $|\widetilde{K}| > 4^n$. Since $\widetilde{K}$ is a subgroup of P^s, $|P| > 4^b$. Hence $b \geq 5$ and P contains $\mathrm{Alt}(B_1)$ (see Proposition 2.3). Therefore as in the proof of Theorem 3.1, $K = [\widetilde{K}, \widetilde{K}] = T \cap (\mathrm{Alt}(b))^s$ is a subdirect product subgroup of $\mathrm{Alt}(b)^s$ and it is a minimal normal subgroup of T. Hence, since $|K| > 2^n$ and $l(\mathrm{Alt}(b)^s) = b^s \leq 2^n$, using Lemma 2.19, we obtain that $|C_T(K)| \leq b^s \leq 2^n$.

Now, applying Lemma 2.12(2), we obtain that

$$|\mathrm{Epi}(G, T)| \leq \log |G| (20)^s |T| |C_T(K)|^d \leq |T| \log |G| c_r^{dn}. \qquad \square$$

Remark 4.2. Using Remark 2.14 we see that the $\log |G|$ term can be replaced by the maximal number r such that a normal section of G is the product of r chief factors of G isomorphic to $A = \mathrm{Alt}(b)^s$ for some b and s with $b^s \leq 2^n$.

Setting $G = T$ we obtain the following amusing estimate.

COROLLARY 4.3. *There exists a constant c such that if T is a d-generated transitive group of degree n then* $|\mathrm{Aut}(T)| \leq |T| c^{dn}$.

Note that if T is a transitive group of degree n then the inequality $|\mathrm{Aut}(T)| \geq |T|/n$ follows from $|Z(T)| \leq n$.

If T and T_1 are conjugate transitive subgroups of $\mathrm{Sym}(n)$ then any permutation representation of a group G with image T_1 is equivalent to one with image T. Moreover, T-conjugate elements of $\mathrm{Epi}(G, T)$ yield equivalent permutation representations. Therefore combining Lemma 2.5, Theorem 3.1 and Proposition 4.1 we immediately obtain the following.

COROLLARY 4.4. *There exists a constant c such that the number of non-equivalent transitive representations of degree n of a finite d-generated group G is at most* $\log |G| c^{nd}$.

A subgroup H of index n in G determines a permutation representation of G. Two such representations are equivalent if and only if the corresponding subgroups are conjugate in G. Clearly H has at most n conjugates. Hence we obtain the following handy result on subgroup growth.

COROLLARY 4.5. *There exists a constant c such that $a_n(G) \leq \log |G| c^{nd}$ for any finite d-generated group G.*

5. **Primitive linear groups**

In this section F denotes a finite field of characteristic p. Let U' and U be two finite dimensional vector spaces over F. Suppose that $X \leq \mathrm{GL}_F(U')$ and $Y \leq \mathrm{GL}_F(U)$. Then $X \times Y$ acts naturally on $W = U' \otimes_F U$. We denote by $X \otimes_F Y$ the image of $X \times Y$ in $\mathrm{GL}_F(W)$. We will identify the image of X in $\mathrm{GL}_F(W)$ with X (and the image of Y with Y).

We say that $H \leq \mathrm{GL}_F(W)$ *fixes* a nontrivial tensor decomposition $U' \otimes_F U$ of W if there are F-spaces U' and U of dimensions greater than 1 over F and an F-linear isomorphism $\phi\colon U' \otimes_F U \to W$ such that $\phi^{-1} \circ g \circ \phi \in \mathrm{GL}_F(U') \otimes_F \mathrm{GL}_F(U)$ for any $g \in H$.

For any F-vector space V we have a natural map

$$\alpha_{F,V}\colon \Gamma\mathrm{L}_F(V) \to \mathrm{Aut}(F) \cong \Gamma\mathrm{L}_F(V)/\mathrm{GL}_F(V).$$

Let $A \leq \Gamma\mathrm{L}_F(U')$ and $B \leq \Gamma\mathrm{L}_F(U)$. Set

$$S = \{(a, b) \in A \times B \mid \alpha_{F,U'}(a) = \alpha_{F,U}(b)\}. \tag{5.1}$$

Then we can make S act on $U' \otimes_F U$: if $(a, b) \in S$, $u' \in U'$ and $u \in U$ then

$$(a, b)(u' \otimes u) = (au') \otimes (bu).$$

By $A \odot_F B$ we define a subgroup of $\Gamma\mathrm{L}_F(U' \otimes_F U)$ consisting of the images of S. We say that $H \leq \Gamma\mathrm{L}_F(W)$ *almost fixes* a nontrivial tensor decomposition $U' \otimes_F U$ of W if there are F-spaces U' and U of dimensions greater than 1 over F and an F-linear isomorphism $\phi\colon U' \otimes_F U \to W$ such that $\phi^{-1} \circ g \circ \phi \in \Gamma\mathrm{L}_F(U') \odot_F \Gamma\mathrm{L}_F(U)$ for any $g \in H$.

LEMMA 5.1. *Let W be a homogenous $\mathbb{F}_p X$-module (that is $W \cong_X U^k$, for some irreducible X-module U and some k). Put $F = \mathrm{End}_X(U)$. Then if $k > 1$ and X is not cyclic, $N_{\mathrm{GL}_{\mathbb{F}_p}(W)}(X)$ almost fixes a nontrivial tensor decomposition $U \otimes_F U'$ of W.*

Proof. Let A be the F-algebra generated by the images of X in $\mathrm{End}_{\mathbb{F}_p}(W)$. Since W is homogenous, $A \cong \mathrm{End}_F(U) \cong \mathbb{M}_s(F)$, where $s = \dim_F U$. Let $B = C_{\mathrm{End}_{\mathbb{F}_p}(W)}(A)$. Then $B \cong \mathbb{M}_k(F)$. Thus, W is an irreducible $A \otimes_F B$-module. Hence there exists a B-module U' such that $W \cong U \otimes_F U'$ as $A \otimes_F B$-modules.

Let $Y = \mathrm{Aut}(A)$ and $Z = \mathrm{Aut}(B)$. Then $Y \cong \Gamma\mathrm{L}_F(U)$, because any automorphism of A is a composition of a field automorphism and a conjugation by an invertible element of A. Since U is the unique A-module, we can consider U also as a Y-module. In the same way U' is a Z-module. We can embed

$\mathrm{Aut}(F)$ in Z in a natural way and so we can consider U' also as an $\mathrm{Aut}(F)$-module. Hence Y almost fixes $U \otimes_F U'$ and from now on we identify Y with $Y \odot_F \mathrm{Aut}(F) \leq Y \odot_F Z \leq \Gamma\mathrm{L}_F(W)$.

Since X is not cyclic and $k > 1$, the decomposition $U \otimes_F U'$ is not trivial. Now, if g normalizes X, g also normalizes A. Hence there are an element $g_1 \in Y$ and an invertible element $g_2 \in B$ such that $g = g_1 g_2$. Hence $g \in Y \odot_F Z$ almost fixes $U \otimes_F U'$. □

Recall that a p-group is said to be of *symplectic type* if it has no non-cyclic characteristic abelian subgroups. The complete description of such groups is given by P. Hall (see, for example, [1, 23.9]). It is a well-known fact that any normal p-subgroup of a linear primitive group is of symplectic type.

For the rest of this section we fix the following notation. Let P be an irreducible primitive subgroup of $\mathrm{GL}_{\mathbb{F}_p}(W)$. Then W is homogenous as an $F^*(P)$-module. Put $F = Z(\mathrm{End}_{F^*(P)}(W))$. Then F is a field and there exists an absolutely irreducible $F[F^*(P)]$-module V such that $W \cong V^k$. We can decompose $F^*(P) = C * K_1 * \cdots * K_s$ as a central product of a cyclic group C and non-abelian groups K_i, such that $K_i Z(F^*(P))/Z(F^*(P))$ is a minimal perfect normal subgroup of $P/Z(F^*(P))$ or K_i is a non cyclic Sylow subgroup of $F(P)$. Note that since the elements from C act on V as multiplications by elements from F, V is also absolutely irreducible as an $F[K_1 * \cdots * K_s]$-module. The space V has a corresponding tensor product decomposition over F: $V = V_1 \otimes \cdots \otimes V_s$, where each V_i is an absolutely irreducible FK_i-module (see [22, Lemma 5.5.5]). In particular, $F = Z(\mathrm{End}_{K_i}(W))$.

LEMMA 5.2. *Suppose that P does not almost fix nontrivial tensor decompositions of W over F. Then $F^*(P)$ is irreducible and one of the following holds*:

(1) *$F^*(P)$ is a product of a q-group (which can be trivial) of symplectic type and a cyclic group of order coprime to p and q and $q \neq p$;*
(2) *$F^*(P)$ is a central product of k copies of quasisimple group S and a cyclic group and P acts transitively on these k copies.*

Proof. First suppose that $F^*(P)$ is cyclic. Then $F^*(P)$ spans F inside $\mathrm{End}_{\mathbb{F}_p}(W)$. Let $K = C_F(P)$. Then K is a subfield of F and $\dim_K F = |P : F^*(P)|$. Hence if A denotes the subalgebra of $\mathrm{End}_{\mathbb{F}_p}(W)$ generated by P, then $Z(A) = K$ and $\dim_{Z(A)} A = \dim_K A = |P : F^*(P)|^2$. Since $A \cong \mathbb{M}_{|P:F^*(P)|}(Z(A))$, $\dim_{Z(A)} W = \sqrt{\dim_{Z(A)} A} = \dim_K F$. Thus W is an irreducible $F^*(P)$-module.

Now suppose that $F^*(P)$ is not cyclic. Since $F = Z(\mathrm{End}_{K_1}(W))$, using Lemma 5.1, we obtain that K_1 is irreducible. In particular, $s = 1$ and $F^*(P)$ is irreducible.

If K_1 is a q-subgroup of P, then since P is irreducible, $p \neq q$ and since P is primitive, K_1 is of symplectic type. The rest of the proposition follows easily. □

Our next aim is to estimate $|P/F^*(P)|$. In order to do this we first investigate the order of the automorphism group of a q-group of symplectic type.

LEMMA 5.3. *Let T be a q-group of symplectic type and W a faithful irreducible $\mathbb{F}_pT$-module. Then $|\operatorname{Aut}(T)| \leq |W|^{14}$ and $|T| \leq |W|^3$.*

Proof. By [1, 23.9], T is a central product of groups E and R, where E is extraspecial or trivial and R is cyclic, dihedral, semidihedral or quaternion.

Suppose first that E is not trivial and let k be such that $|E| = q^{2k+1}$. Then E is generated by $2k$ elements and $|\Omega_2(Z_2(T))| \leq q^{2k+4}$. Let $\phi \in \operatorname{Aut}(T)$. Since $E \leq \Omega_2(Z_2(T))$, we obtain that $\phi(E) \leq \Omega_2(Z_2(T)))$, whence there are at most $q^{2k(2k+4)}$ possibilities for images of $2k$ generators of E. Since R is generated by at most two elements, we obtain that

$$|\operatorname{Aut}(T)| \leq q^{4k(k+2)}|T|^2 = q^{4k^2+12k+2}|R|^2.$$

Now note that $|W| \geq |F|^{q^k} \geq 2^{q^k}$, because the minimal degree of a faithful representation of E is q^k, and $|R| \leq 2|W|$, because R has a cyclic subgroup of index at most 2. Thus, $|\operatorname{Aut}(T)| \leq |W|^{14}$.

If E is trivial we obtain the bound for $|\operatorname{Aut}(T)|$ in a similar way. By the same ideas $|T| \leq |W|^3$. □

LEMMA 5.4. *Let K be a perfect group such that $K/Z(K) \cong S^k$ for some simple group S and some $k \geq 1$. If W is an irreducible $\mathbb{F}_pK$-module, then $|\operatorname{Out}(K)| \leq |W|^2$. Moreover, if $k \geq 2$ then $|K| \leq |W|^3$.*

Proof. The group K is isomorphic to a central product of k quasisimple groups S_i such that $S_i/Z(S_i) \cong S$. Put $F = \operatorname{End}_K(W)$. Then the space W has a corresponding tensor product decomposition over F: $W = W_1 \otimes \cdots \otimes W_k$, where each W_i is an absolutely irreducible FS_i-module (see [22, Lemma 5.5.5]).

By [19] a perfect group has no nontrivial central automorphisms; hence $\operatorname{Aut}(K)$ has a natural embedding into $\operatorname{Aut}(S^k)$. It is also clear that $\operatorname{Aut}(K)$ contains S^k; hence $|\operatorname{Out}(K)| \leq |\operatorname{Out}(S)|^k k!$. By Lemma 2.6

$$|W| \geq \prod_i |W_i| \geq |\operatorname{Out}(S)|^k.$$

Note also that $|W| \geq 2^{2^k} > k!$. Thus, $|\operatorname{Out}(K)| \leq |W|^2$.

Now, suppose that $k \geq 2$. Let $n = \dim_F W$ and $m = \min\{\dim_F W_i\}$. Then $n \geq m^k$ and $|K| \leq |F|^{km^2+1}$. Thus, we have $|K| \leq |W|^3$. □

PROPOSITION 5.5. *We have $|P/F^*(P)| \leq |V|^{c_2}$ (where $c_2 = 15$).*

Proof. Using two previous lemmas, we obtain that

$$|P/F^*(P)| \leq |\operatorname{Out}(C)| \prod |\operatorname{Out}(K_i)| \leq |V|^{15}. \qquad \square$$

PROPOSITION 5.6. *There exists a constant c_3 such that if H is a quasisimple group and U is an absolutely irreducible FH-module (where F is a finite field) such that $|H| > |U|^{c_3}$, then one of the following holds*:

(1) $H = \operatorname{Alt}(m)$ *and W is the natural* $\operatorname{Alt}(m)$*-module.*
(2) $H = \operatorname{Cl}_d(K)$, *a classical group over $K \leq F$ and $U = F \otimes_K U_0$, where U_0 is the natural module for* $\operatorname{Cl}_d(K)$.

Proof. It follows from [26, Prop. 2.2]. $\square$

Let $c_4 = c_2 + 1 + \max\{3, c_3\}$.

PROPOSITION 5.7. *Suppose that $|P| > |W|^{c_4}$. Then there is a tensor decomposition $U' \otimes_F U$ of W with $A \leq \Gamma L_F(U')$ and $B \leq \Gamma L_F(U)$ such that*

(1) $P \leq A \odot_F B$;
(2) $\dim_F(U') \leq \sqrt{\dim_F W}$ *and so* $|A| \leq |W|^2$;
(3) $F(B)$ *is cyclic*;
(4) $E(B) = \operatorname{Alt}(m)$ *and U is the natural* $\operatorname{Alt}(m)$*-module over F or $E(B) = \operatorname{Cl}_d(K)$, a classical group over $K \leq F$ and $U = F \otimes_K U_0$, where U_0 is the natural module for* $\operatorname{Cl}_d(K)$.
(5) $|C_{\mathrm{GL}_{\mathbb{F}_p}(W)}(E(B))| \leq |W|$.
(6) $|A \odot_F B : E(B)| \leq |W|^5$.
(7) $E(B) \leq P$.

Proof. By Proposition 5.5, $|P/F^*(P)| \leq |V|^{c_2}$. Note that for any tensor decomposition $U_1 \otimes_F U_2$ of V fixed by $F^*(P)$ we have that $|A_1| \leq |V|$ or $|A_2| \leq |V|$ (where $A_1 * A_2$ is the corresponding central product decomposition of $F^*(P)$). Therefore since $|F^*(P)| > |W|^{c_4 - c_2} \geq |V|^3$, there exists an i such that $\dim_F V_i \geq \sqrt{\dim_F V}$ and hence $|K_i| > |V|^{c_4 - c_2 - 1}$ (in particular, $F^*(P)$ cannot be cyclic).

If K_i is a p-group, then it is of symplectic type. In this case, by Lemma 5.3, $|K_i| \leq |V_i|^3$, a contradiction.

Hence $K_i = S_1 * \cdots * S_k$ is a central product of k copies of a quasisimple group S_i. If $k > 1$, then by Lemma 5.4, we have $|K_i| \leq |V_i|^3$, a contradiction. Hence $k = 1$.

Thus K_i is a quasisimple group. Put $U = V_i$. Then since $|K_i| > |U|^{c_3}$, we obtain a complete description of K_i and U from Proposition 5.6. If $U = W$, then our statement holds with $A = 1$. Assume $U \neq W$. By Lemma 5.1, P almost fixes $U' \otimes_F U$ for some U'. There are $A \leq \Gamma\mathrm{L}_F(U')$ and $B \leq \Gamma\mathrm{L}_F(U)$ such that $P \leq A \odot_F B$, where $B = N_{\Gamma\mathrm{L}_F(U)}(K_i)$. It is clear that $K_i = E(B)$

and $F(B)$ is cyclic. Moreover since $|K_i| \geq |W|$, $\dim_F(U') \leq \sqrt{\dim_F W}$ and so $|A| \leq |W|^2$ and $|C_{\mathrm{GL}_{\mathbb{F}_p}(W)}(E(B))| \leq |W|$.

It follows that the index of $E(B)$ in B is less than $|W|^3$, whence we obtain that $|A \odot_F B : E(B)| \leq |W|^5$. □

Let F° be the subgroup of nonzero elements in F. We will also view F° as a subgroup of $\Gamma\mathrm{L}_\mathrm{F}(\mathrm{U})$.

LEMMA 5.8. *Let Y_1 and Y_2 be two primitive subgroups of $\mathrm{GL}_{\mathbb{F}_p}(U)$ contained in $\Gamma\mathrm{L}_\mathrm{F}(\mathrm{U})$. Suppose that they are conjugate in $\mathrm{GL}_{\mathbb{F}_p}(U)$ and contain F°. Assume also that either both Y_1 and Y_2 lie in $\mathrm{GL}_F(U)$ or that both Y_1 and Y_2 do not lie in $\mathrm{GL}_F(U)$. Then Y_1 and Y_2 are conjugate in $\Gamma\mathrm{L}_\mathrm{F}(\mathrm{U})$.*

Proof. Let $g \in \mathrm{GL}_{\mathbb{F}_p}(U)$ be such that $Y_1^g = Y_2$. First suppose that Y_1 and Y_2 lie in $\mathrm{GL}_F(U)$. Then $F \leq E_i = \mathrm{End}_{Y_i}(U)$ $(i = 1, 2)$. Since the Y_i are irreducible, E_i is a field. We have that $E_1^g = E_2$ and since $F \leq E_1 \cap E_2$ is the unique subfield of E_i $(i = 1, 2)$ of order $|F|$, we obtain that $F^g = F$ and so $g \in \Gamma\mathrm{L}_\mathrm{F}(\mathrm{U})$.

Now suppose that Y_1 and Y_2 do not lie in $\mathrm{GL}_F(U)$. Take $x \in Y_1$ which does not commute with F. Then $C_F(x)$ is a proper subfield of F. In particular, $|C_F(x)| \leq |F|^{1/2}$. Hence $|C_{F^\circ}(x)| < |F^\circ|^{1/2}$ and so $|[x, F^\circ]| > |F^\circ|^{1/2}$. This implies that $[x, F^\circ]$ spans F over $\mathbb{F}_p$ and so $[Y_1, F^\circ]$ also spans F in $\mathrm{End}_{\mathbb{F}_p}(U)$. In the same way we prove that $[Y_2, F^\circ]$ spans F over $\mathbb{F}_p$.

Thus the subalgebra of $\mathrm{End}_{\mathbb{F}_p}(U)$ generated by Y_i' contains F and lies in $\mathrm{End}_F(U)$. In particular $F \leq E_i = Z(\mathrm{End}_{Y_i'}(U))$. Since Y_i is primitive E_i is a field. We have that $E_1^g = E_2$ and since $F \leq E_1 \cap E_2$ is the unique subfield of E_i $(i = 1, 2)$ of order $|F|$, we obtain that $F^g = F$. Thus $g \in \Gamma\mathrm{L}_\mathrm{F}(\mathrm{U})$. □

Let $c_5 = 6c_4 + 31 + c_2$.

PROPOSITION 5.9. *The number of conjugacy classes of primitive d-generated subgroups P of $\mathrm{GL}_{\mathbb{F}_p}(W)$ is at most $|W|^{c_5 d}$.*

Proof. We prove the proposition by induction on $\dim_{\mathbb{F}_p} W$. Without loss of generality we can assume that $d > 1$.

Put $F = Z(\mathrm{End}_{F^*(P)}(W))$ and let $n = \dim_F W$. There are at most

$$\dim_{\mathbb{F}_p} W \leq |W| \tag{5.2}$$

possibilities for F. Fix one of them. We divide the primitive groups P into several families.

Family 1. *Suppose that $|P| > |W|^{c_4}$.* Then we can apply Proposition 5.7. Recall that $A \odot_F B$ is the image in $\Gamma\mathrm{L}_F(W)$ of the group S defined in (5.1). Let $\widetilde{P}$ be the preimage of P in S. Then without loss of generality we may assume that $\widetilde{P}$ is a subdirect product subgroup of $A \times B$. In particular, A and B can

be generated by $d+1$ elements. Let $s = \dim_F U'$ and $b = \dim_F U$ (whence $n = bs$). Now P from the first family is completely determined if we know:

(1) the choice of b;
(2) a group $A \leq \Gamma\mathrm{L}_F(U')$;
(3) a group $B \leq \Gamma\mathrm{L}_F(U)$, satisfying the conditions of Proposition 5.7;
(4) the image of d generators of P in $(A \odot_F B)/E(B)$.

(1) The number of choices for b is at most $n \leq |W|$.

(2) We have $s \leq \sqrt{n}$, which implies $|\Gamma\mathrm{L}_F(U')| < |W|^2$. The group A is generated by $d+1$ elements, whence the number of possibilities for A is at most $|W|^{2(d+1)}$.

(3) Proposition 5.7 describes all possibilities for $E(B)$ inside $\mathrm{GL}_F(U)$ up to conjugacy. This number is clearly less than $|U|^3$. We fix one such possibility.

Note that $|N_{\Gamma\mathrm{L}_F(U)}(E(B))/E(B)| \leq |U|^2$. Thus, since B is $d{+}1$-generated, there are at most $|U|^3|U|^{2(d+1)} \leq |W|^{2d+5}$ choices for B inside $\Gamma\mathrm{L}_F(U)$ up to conjugacy.

(4) Now $|A \odot_F B/E(B)| \leq |W|^5$. Hence there are at most $|W|^{5d}$ possibilities to choose P inside $A \odot_F B$ with $E(B) \leq P$.

Putting everything together we obtain that there are at most

$$|W|^{9d+9} \tag{5.3}$$

conjugacy classes of primitive d-generated groups in the first family.

Family 2. *Suppose that* $|P| \leq |W|^{c_4}$ *and* P *almost fixes a nontrivial tensor product decomposition* $U' \otimes_F U$ *of* W. Thus, there are F-spaces U' and U of dimensions greater than 1 over F and groups $X \leq \Gamma\mathrm{L}_F(U')$ and $Y \leq \Gamma\mathrm{L}_F(U)$ such that $W = U' \otimes_F U$ and $P \leq X \odot_F Y$. Denote by $\widetilde{P}$ the preimage of P in $X \times Y$. Note that $\widetilde{P}$ is generated by $d+1$ elements. Without loss of generality we can also assume that $F^\circ \leq X$, $F^\circ \leq Y$ and X and Y are homomorphic images of $\widetilde{P}$. In particular, X and Y can be generated by $d+1$ elements. Note also that since P is primitive, X and Y are primitive over $\mathbb{F}_p$ as well.

Let $s = \dim_F U'$ and $b = \dim_F U$. Assuming $s \leq b$ we have $s \leq \sqrt{n}$. Thus, in order to determine $\widetilde{P}$ up to conjugacy in $\Gamma\mathrm{L}_F(U') \times \Gamma\mathrm{L}_F(U)$ it is enough to know:

(1) the decomposition $n = bs$;
(2) the group $F^\circ \leq Y$ up to conjugacy in $\Gamma\mathrm{L}_F(U)$;
(3) the group $F^\circ \leq X$ in $\Gamma\mathrm{L}_F(U')$;
(4) a set of d generators of P in $X \odot_F Y$.

(1) There are at most n decompositions $n = bs$ and $n \leq |W|$.

(2) By induction there are at most $|U|^{c_5(d+1)}$ choices for Y up to conjugacy in $\mathrm{GL}_{\mathbb{F}_p}(U)$. Applying Lemma 5.8, we obtain that there are at most $|U|^{c_5(d+1)}$ choices for Y up to conjugacy in $\Gamma\mathrm{L}_F(U)$.

(3) Note that $X \leq \mathrm{GL}_F(U')$ if and only if $Y \leq \mathrm{GL}_F(U)$. Hence if we fix Y we know whether X should lie or not in $\mathrm{GL}_F(U')$. As above there are at most $|W|^{2(d+1)}$ choices for X in $\Gamma\mathrm{L}_F(U')$.

(4) Since $|P| \leq |W|^{c_4}$ and $|X| \leq |W|^2$, $|X \odot Y| \leq |W|^{c_4+3}$. Hence there are at most $|W|^{d(c_4+3)}$ choices for d generators of P.

Hence we obtain that there are at most

$$n|W|^{2(d+1)}|U|^{c_5(d+1)}|W|^{d(c_4+3)} \leq |W|^{(d+1)(5+c_5/2+c_4)} \tag{5.4}$$

conjugacy classes of primitive d-generated groups in the second family.

Family 3. *Suppose that $|P| \leq |W|^{c_4}$ and P does not almost fix any non-trivial tensor product decompositions $U' \otimes_F U$ of W.* In this case we can use Lemma 5.2. From this lemma we know that there are only two possibilities for $F^*(P)$ and that $F^*(P)$ is irreducible. We divide the third family into two subfamilies.

Subfamily 3.1. *$F^*(P)$ is a product of q-group T of symplectic type and a cyclic group C of order coprime to p and q.* Note first that $|T| \leq |W|^3$ and $|C| \leq |W|$. It follows that there are at most $|W|^4$ possibilities for the isomorphism type of $F^*(P)$, and at most $|W|^4$ nonequivalent irreducible representations over F of degree n for each type. Hence we have at most $|W|^8$ possibilities for $F^*(P)$ inside $\mathrm{GL}_F(W)$ up to conjugacy. Fix one such possibility.

Since $|N_{\mathrm{GL}_{\mathbb{F}_p}(W)}(F^*(P))/F^*(P)| \leq |W|^{c_2}$, by Proposition 5.5, we have at most $|W|^{dc_2}$ possibilities for d generators of $P/F^*(P)$ inside

$$N_{\mathrm{GL}_{\mathbb{F}_p}(W)}(F^*(P))/F^*(P).$$

We conclude that there are at most

$$|W|^4|W|^4|W|^{dc_2} = |W|^{c_2 d+8} \tag{5.5}$$

conjugacy classes of primitive d-generated groups in this subfamily.

Subfamily 3.2. *$F^*(P)$ is a central product of k copies of a quasisimple group S and a cyclic group C; now P acts transitively on these k copies and $Z(F^*(P))$ is cyclic.* Since there are only at most two simple groups of each order, we have only at most$(2|P|) \leq |W|^{c_4+1}$ possibilities for the isomorphism type of $F^*(P)/Z(F^*(P))$ and at most $|F^*(P)| \leq |W|^{c_4}$ nonequivalent irreducible representations in $\mathrm{PGL}_F(W)$ for each type. Hence we have at most $|W|^{2c_4+1}$ possibilities for $F^*(P)/Z(F^*(P))$ inside $\mathrm{PGL}_F(W)$ up to conjugacy. Now $F^*(P)$ is generated by at most $2\log n$ elements. Using Corollary 2.2, we obtain that there are at most $|W|^{2c_4+1}|F|^{2\log_n} \leq |W|^{2c_4+2}$ possibilities for $F^*(P)$ inside $\mathrm{GL}_F(W)$ up to conjugacy. Fix one such possibility. Since

$$|N_{\mathrm{GL}(W)}(F^*(P))/F^*(P)| \leq k!|\operatorname{Out}(S)|^k|W| \leq \log n^{\log n}|W|^2 \leq |W|^3,$$

we have at most $|W|^{4d}$ possibilities for d generators of $P/F^*(P)$ in

$$N_{\Gamma\mathrm{L}(W)}(F^*(P))/F^*(P).$$

We conclude that there are at most

$$|W|^{2c_4+2}|W|^{4d} = |W|^{4d+2c_4+2} \tag{5.6}$$

conjugacy classes of primitive d-generated groups in this subfamily.

Now, putting together (5.2), (5.3), (5.4), (5.5) and (5.6) we obtain the desired result. □

6. **Irreducible linear groups**

Let $c_i = 7 + c_4 + c_5 + \log c_t$.

PROPOSITION 6.1. *The number of conjugacy classes of d-generated irreducible subgroups of $\mathrm{GL}_{\mathbb{F}_p}(V)$ is at most $|V|^{c_i d}$.*

Proof. Let T be an irreducible d-generated subgroup of $\mathrm{GL}_{\mathbb{F}_p}(V)$ and H a subgroup of T such that the representation of T is induced from a primitive representation of H. Denote by W a primitive H-module such that $V = T \otimes_H W$. Let P be the image of H in $\mathrm{GL}_{\mathbb{F}_p}(W)$ and $b = \dim_{\mathbb{F}_p} W$. Put $\widetilde{K} = \operatorname{core} H$. Then $T/\widetilde{K}$ is a transitive group of degree $s = n/b$, where $n = \dim_{\mathbb{F}_p} V$, and T is a subgroup of $P \wr T/\widetilde{K}$.

We divide the d-generated irreducible subgroups of $\mathrm{GL}_{\mathbb{F}_p}(V)$ into three families. We note that some of the groups can belong to different families.

Family 1. *Suppose that* $|P| \leq |W|^{c_4}$. In this case in order to determine T we have to know firstly the decomposition $n = bs$. There are at most n possibilities for this. Fix one such decomposition. Then, by Proposition 5.9, there are at most $|W|^{c_5 d(H)}$ choices for a primitive $d(H)$-generated subgroup P up to conjugacy in $\mathrm{GL}_{\mathbb{F}_p}(W)$. Since $d(H) \leq |T : H|(d(T)-1)+1 \leq sd$, we obtain that there are at most $|V|^{c_5 d}$ such possibilities. Fix one such P. By Theorem 3.1, there are at most c_t^{sd} choices for $T/\widetilde{K}$ up to conjugacy inside $\mathrm{Sym}(s)$. Fix one such possibility. Thus we fixed an embedding of $P \wr T/\widetilde{K}$ into $\mathrm{GL}_{\mathbb{F}_p}(V)$. Now, by Lemma 2.2, we obtain that there are at most $|P|^{sd}$ choices for T inside $P \wr T/\widetilde{K}$. Putting everything together, we obtain that there are at most

$$n|V|^{c_5 d} c_t^{sd} |V|^{c_4 d} \leq |V|^{(1+c_4+c_5+\log c_t)d} \tag{6.1}$$

conjugacy classes of d-generated irreducible subgroups in the first family.

Family 2. *Suppose that* $|P| > |W|^{c_4}$. Thus, we can use Proposition 5.7. We use the notation of this proposition. Let $E(B)$ be a homogenous subgroup of $\mathrm{GL}_{\mathbb{F}_p}(W)$ as in Proposition 5.7 and denote $E(B)/Z(E(B))$ by S. Put $N = E(B)^s \leq P^s \leq \mathrm{GL}_{\mathbb{F}_p}(V)$.

In order to determine T up to conjugacy inside $\mathrm{GL}_{\mathbb{F}_p}(V)$, we should know the decomposition $n = sb$. There at most n possibilities for this. Fix one such decomposition. Then we have to fix $E(B)$ as a homogenous subgroup of $\mathrm{GL}_{\mathbb{F}_p}(W)$ up to conjugacy. In view of Proposition 5.7, there are at most $7b^2$ such possibilities. Fix one of them. Thus we obtain an embedding of N into $\mathrm{GL}_{\mathbb{F}_p}(V)$.

Let $R = N_{\mathrm{GL}_{\mathbb{F}_p}(V)}(N)$. Then R permutes the direct factors of N and hence the subspaces of V on which they act nontrivially. Therefore

$$R \cong N_{\mathrm{GL}_{\mathbb{F}_p}(W)}(E(B)) \wr \mathrm{Sym}(s).$$

Denote by $\widetilde{N}$ the base of this wreath product and put $Q = T\widetilde{N}$. The group T is a subgroup of R and $\widetilde{K} = \widetilde{N} \cap T$. It follows that $N \cap T$ and hence $K = (N \cap T)'$ is a normal subgroup of T. Applying Theorem 3.1 as in the previous case, we obtain that there are at most c_t^{ds} choices for $T/\widetilde{K}$ up to conjugacy inside $\mathrm{Sym}(s)$. Hence we have that there are at most $7c_t^{ds}n^3$ choices for Q up to conjugacy inside $\mathrm{GL}_{\mathbb{F}_p}(V)$. Fix one such Q.

Subfamily 2.1 *Suppose that* $|P| > |W|^{c_4}$ *and* $K \neq 1$. In this case the image of $T \cap N$ in a direct factor $E(B)$ of N is a non-abelian normal subgroup of P contained in $E(B)$, whence it is equal to $E(B)$. Therefore K is a subdirect product subgroup of $E(B)^s$. By Lemma 2.18, there are at most

$$|C_Q(N)|^d |\operatorname{Out}(S)|^{sd}(1 + |\operatorname{Out}(S)|)^s$$

choices for T up to conjugacy inside Q. Now, $|C_Q(N)| \leq |V|$ by Proposition 5.7 and $|\operatorname{Out}(S)|^s \leq |V|$. Thus we obtain that there are at most

$$7n^3 c_t^{ds} |V|^{3d} \leq |V|^{3d+4} c_t^{dn} \tag{6.2}$$

conjugacy classes of d-generated irreducible subgroups in the second family.

Family 2.2. *Suppose that* $|P| > |W|^{c_4}$ *and* $K = 1$. Since

$$|N_{\mathrm{GL}_{\mathbb{F}_p}(W)}(E(B))/E(B)| \leq |W|^2,$$

there are at most $|W|^{2sd} = |V|^{2d}$ possibilities for TN/N inside Q/N. Fix $TN \leq \mathrm{GL}_{\mathbb{F}_p}(V)$. In this case $T \cap N$ is contained in $Z = Z(E(B))^s$. Hence $T/(T \cap Z)$ is a complement to N/Z in T/Z. Moreover, it is a large complement to $N/Z \cong S^s$. Using Proposition 2.16, we obtain that the number of such complements up to conjugacy in Q is at most $|\operatorname{Out}(S)| \log |T| \leq |V|^2$. Given $T/T \cap Z$ we have at most $|Z|^d$ choices for T itself. Thus, we conclude, that there are at most

$$7n^3 |V|^{3d} |V|^2 c_t^{dn} \leq |V|^{3d+5} c_t^{dn} \tag{6.3}$$

conjugacy classes of d-generated irreducible subgroups in the third family.

Now, putting together (6.1), (6.2) and (6.3) we obtain the proposition. □

7. The number of irreducible linear representations

To express our results in the sharpest form we have to introduce an auxiliary function. Denote by $\mathrm{rk}_n(G)$ the maximum of the numbers $\mathrm{rk}_A(G)$ with $l(A) \leq n$. It is clear that $\mathrm{rk}_n(G) \leq \log |G|$.

The aim of this section is to prove the following result.

PROPOSITION 7.1. *Let G be a finite d-generated group and T an irreducible linear subgroup of $\mathrm{GL}_{\mathbb{F}_p}(V)$. Then there are at most $\mathrm{rk}_{|V|}(G)|T||V|^{dc_l}$ epimorphisms from G onto T (where $c_l = 4 + \max\{c_4, 4\}$).*

Proof. Let H be a subgroup of T such that the representation of T is induced from a primitive representation of H. Denote by W a primitive H-module such that $V = T \otimes_H W$. Let P be the image of H in $\mathrm{End}_{\mathbb{F}_p}(W)$ and $b = \dim_{\mathbb{F}_p} W$. Put $\widetilde{K} = \mathrm{core}\, H$. Then $T/\widetilde{K}$ is a transitive group of degree $s = n/b$ and T is a subgroup of $P \wr T/\widetilde{K}$.

Case 1. *Suppose that* $|\widetilde{K}| \leq |V|^{c_4}$. Since $T/\widetilde{K}$ is a transitive group of degree s, where $2^s \leq |V|$, by Proposition 4.1 and Remark 4.2, there are at most $\mathrm{rk}_{|V|}(G)|T/\widetilde{K}|c_r^{ds}$ epimorphisms from G onto $T/\widetilde{K}$. On the other hand $|\widetilde{K}| \leq |V|^{c_4}$, whence there are at most

$$|T/\widetilde{K}|\,\mathrm{rk}_{|V|}(G)c_r^{ds}|V|^{c_4 d} \leq |T|\,\mathrm{rk}_{|V|}(G)|V|^{dc_l}$$

epimorphisms from G onto T.

Case 2. *Suppose that* $|\widetilde{K}| > |V|^{c_4}$. Thus, $|P| > |W|^{c_4}$, and so we can use Proposition 5.7 and the notation of that proposition. Denote $E(B)/Z(E(B)$ by S. Let $K = (T \cap E(B)^s)'$. As in the proof of Proposition 6.1 we obtain that K is a normal subgroup of T and it is a subdirect product subgroup of $E(B)^s$. Also, T acts transitively on factors of $N = E(B)^s$. Since $l(S) \leq p^b$, for $A = K/Z(K)$ we have $l(A) \leq l(S)^s \leq |V|$.

By [19], a perfect group has no nontrivial central automorphisms, whence $C_T(N/Z(N)) = C_T(N)$. Note that $|KZ(N)/Z(N)| > |W|^s \geq l(N/Z(N))$. Hence, by Lemma 2.19,

$$\begin{aligned} |C_T(K)| \leq |C_T(K/Z(K))| &\leq |C_T(N/Z(N))|l(N/Z(N)) \\ &= |C_T(N)|l(N/Z(N)) \leq |V|^3. \end{aligned}$$

Now, using Lemma 2.12(2)and Remark 2.14, we obtain that

$$\begin{aligned} |\mathrm{Epi}(G,T)| &\leq \mathrm{rk}_{|V|}(G)(5|\,\mathrm{Out}(S)|)^s|T||C_T(K)|^d \\ &\leq \mathrm{rk}_{|V|}(G)|T||V|^{4d}. \end{aligned}$$

□

We need the following obvious analogue of Lemma 2.5.

LEMMA 7.2. *Let T be an irreducible subgroup of $\mathrm{GL}_{\mathbb{F}_p}(V)$. Then the number of T-conjugacy classes of epimorphisms from a group G onto T is at most $|V||\mathrm{Epi}(G,T)|/|T|$.*

Combining Propositions 6.1 and 7.1 and Lemma 7.2, we obtain the following corollary.

COROLLARY 7.3. *Let G be a finite d-generated group. There exists a constant c_6 such that the number of irreducible G-modules of size n is at most $\log |G| n^{dc_6}$.*

8. **The number of primitive permutation groups**

In this section we prove the following theorem which is our main technical result. It was conjectured in [49].

THEOREM 8.1. *There exists a constant c_p such that there are at most $n^{c_p d}$ conjugacy classes of d-generated primitive groups of degree n.*

Proof. In view of [38, Cor. 2] we only need to show that the number of isomorphism classes of d-generated primitive groups of degree n is at most n^{cd} for some c. Let P be a d-generated primitive group of degree n and M the socle of P. Then we have two possibilities:

Case 1. *M is abelian (P is of affine type).* In this case $n = p^m$ and we have to calculate the number of conjugacy classes of irreducible subgroups of $\mathrm{GL}_m(\mathbb{F}_p)$. By Proposition 6.1 this number is at most $p^{c_i m d} = n^{c_i d}$.

Case 2. *M is non-abelian.* Then $M \cong S^s = S_1 \times \cdots \times S_s$ for some non-abelian simple group S and some s. By [8, Lemma 2.3] there are at most $O(n)$ possibilities for S. Hence there are at most $O(n^2)$ possibilities for M. We fix one of them. Then P is a subgroup of $\mathrm{Aut}(M) \cong \mathrm{Aut}(S) \wr \mathrm{Sym}(s)$.

The image $\bar{P}$ of P in $\mathrm{Sym}(s)$ is transitive or has two orbits of size $s/2$. In the latter case the actions of $\bar{P}$ on the two orbits are faithful and equivalent. By Theorem 3.1 there are at most c_t^{sd} choices for $\bar{P}$ up to conjugacy in $\mathrm{Sym}(s)$. Since $|\mathrm{Aut}(S)/S|^s \leq n^2$, using Corollary 2.2, we obtain that there are at most $c_t^{sd} n^{2d}$ choices for P up to conjugacy inside $\mathrm{Aut}(M)$. Note that $n \geq 2^s$, whence the number of isomorphism types of d-generated primitive groups of degree n with non-abelian socle is at most $O(n^{d(\log c_t + 3)})$. □

COROLLARY 8.2. *There exists a constant c such that the number of conjugacy classes of primitive groups of degree n is at most $n^{\frac{c \log n}{\sqrt{\log \log n}}}$.*

Proof. By [34], if G is a primitive permutation group of degree $n > 2$, then there is a constant a such that $d(G) \leq a \log n / \sqrt{\log \log n}$. Now, applying Theorem 8.1, we obtain the desired result. □

Corollary 8.2 improves an $n^{c \log n}$ bound which is the main result of [49]. Note that for infinitely many positive integers n even, the number of isomorphism types of primitive soluble groups is at least $n^{\frac{\epsilon \log n}{\log \log n}}$ [49].

9. **The expected number of random elements generating a finite group**

As another consequence of Theorem 8.1 we obtain the following.

COROLLARY 9.1. *There exists a constant c such that for any finite d-generated group G, $m_n(G) \leq n^{cd} \operatorname{rk}_n(G) \leq n^{cd} \log |G|$.*

Proof. In view of Theorem 8.1, in order to prove this corollary we have to show that the following claim holds:

Claim. There exists a constant c such that for any primitive permutation group P of degree n, $|\mathrm{Epi}(G, P)| \leq \operatorname{rk}_n(G)|P|n^{cd}$.

Let M be the socle of P. If P is of affine type (i.e. M is abelian) then $T = P/M$ is a linear irreducible group acting on a vector space of size $n = |M|$. Hence the claim follows from Proposition 7.1 and Lemma 2.12(1).

Now, suppose that M is not abelian and it is a minimal normal subgroup of P. Then M is a transitive characteristically simple group with $l(M) \leq n$. In this case the claim follows directly from Lemma 2.12(2), Remark 2.14 and Lemma 2.6.

Now, suppose that M is not a minimal normal subgroup of P. Then M is a product of two minimal normal subgroups M_1 and M_2 and $n = |M_1| = |M_2|$. Then we bound first $|\mathrm{Epi}(G, P/M_2)$ using Lemma 2.12(2)and Lemma 2.6 and then we obtain the desired bound for $|\mathrm{Epi}(G, P)|$ from Lemma 2.12(1). □

In [29] Lubotzky has obtained a slightly different estimate namely that $m_n(G) \leq n^{d+2}(\log |G|)^2$.

Corollary 9.1 is essentially best possible. To see this we need the following. Recall that we denote by $l^*(L)$ the smallest degree of a faithful primitive permutation representation of L (if such a representation exists).

LEMMA 9.2. *There exists a constant c_7 such that if L is a group with a unique minimal normal subgroup M, with M non-abelian, then $l^*(L) \leq l(M)^{c_7}$.*

Proof. By our assumptions $M \cong S^k = S_1 \times \cdots \times S_k$ for some non-abelian simple groups $S_i \cong S$. The group $N_L(S_1)$ acts on S_1. Define by R the image of $N_L(S_1)$ in $\mathrm{Aut}(S_1)$. Then L is embedded in $W = R \wr L/\widetilde{M}$, where $\widetilde{M}$ is the core of $N_L(S_1)$. We have $\Phi(R) = 1$ and this implies that R has a faithful primitive representation. Let Ω be a set of size $l^*(R)$ on which R acts faithfully and primitively. Then the group W has a faithful primitive permutation representation of degree $l^*(R)^k$ constructed via the product action

on the set Ω^k. By [2, Th. 1(C)(3)], the restriction of this representation on G is also primitive and faithful. On the other hand we have $l(M) = l(S)^k$ (see [22, Prop. 5.2.7] and the comment afterwards).

Thus, in order to finish the proof of the lemma it will be enough to show that $l^*(R) \leq l(S)^c$ for some constant c. It is clear for sporadic groups and alternating groups S. Also since, $l(G(q)) \geq q$ for any simple group $S = G(q)$ of Lie type, we can assume that S is a classical simple group. In this case, from [22] we obtain that $l^*(R) \leq l(S)^2$ (moreover $l^*(R) = l(S)$ except when $S \cong \mathrm{PSL}_n(\mathbb{F}_q)$ and $R \not\leq \mathrm{P\Gamma L}_n(\mathbb{F}_q)$). □

Corollary 9.3. *Let G be a finite group. Then $m_x(G) \geq \mathrm{rk}_n(G)$ for some $x \leq n^{c_7}$.*

Proof. By the definition of $\mathrm{rk}_n(G)$ there is a normal section H/N of G which is the direct product of $r = \mathrm{rk}_n(G)$ chief factors isomorphic to some non-abelian characteristically simple group A with $l(A) \leq n$, say $H/N = A_1 \times A_2 \times \cdots \times A_r$. The centralisers $C_i = C_G(A_i)$ are different normal subgroups of G. The quotients G/C_i are groups with a unique minimal normal subgroup isomorphic to A. By Lemma 9.2 for each C_i there is a maximal subgroup M_i of G such that $\mathrm{core}_G(M_i) = C_i$ and $|G : M_i| \leq n^{c_7}$. Our statement follows. □

Recall that $\nu(G)$ is the minimal number k such that G is generated by k random elements with probability $\geq 1/e$. Using his estimate on $m_n(G)$ Lubotzky [29] proved that $\nu(G) \leq d + 2\log\log|G| + 4.02$ (essentially the same result was obtained in [11]).

Combining his argument with the above bounds for $m_n(G)$ we now prove Theorem 1. As a finite version of the Mann-Shalev theorem quoted in the introduction Lubotzky first proves the following [29].

Proposition 9.4. *Let $\mathcal{M}(G) = \max_{n\geq 2} \frac{\log m_n(G)}{\log n}$. Then*

$$\mathcal{M}(G) - 4 \leq \nu(G) \leq \mathcal{M}(G) + 3.$$

The following is a slightly stronger form of Theorem 1.

Theorem 9.5. *Let G be finite d-generated group. Then*

$$\max\left\{d, \max_n \frac{\log \mathrm{rk}_n(G)}{c_7 \log n} - 4\right\} \leq \nu(G) \leq cd + \max_n \frac{\log \mathrm{rk}_n(G)}{\log n} + 3,$$

where c is as in Corollary 9.1.

Proof. By Corollary 9.1 and Proposition 9.4, we have

$$\nu(G) \leq \max_n \frac{\log m_n(G)}{\log n} + 3 \leq cd + \max_n \frac{\log \mathrm{rk}_n(G)}{\log n} + 3.$$

On the other hand, let N be such that

$$\max_n \frac{\log \mathrm{rk}_n(G)}{\log n} = \frac{\log \mathrm{rk}_N(G)}{\log N}.$$

By Corollary 9.3 we have $m_x(G) \geq \mathrm{rk}_N(G)$ for some $x \leq N^{c_7}$. This implies

$$\nu(G) + 4 \geq \frac{m_x(G)}{\log x} \geq \frac{\log \mathrm{rk}_N(G)}{\log x} \geq \frac{\log \mathrm{rk}_N(G)}{c_7 \log N} = \max_n \frac{\log \mathrm{rk}_n(G)}{c_7 \log n}.$$

The obvious inequality $\nu(G) \geq d$ completes the proof. □

Denote by $\mathrm{rk}(G)$ the maximal number of isomorphic chief factors that appear in a normal section of G which is a direct power of some non-abelian simple group.

COROLLARY 9.6. *If G is a finite d-generated group then $\nu(G) \leq cd + \log \mathrm{rk}(G)$ for some absolute constant c.*

Note that $\mathrm{rk}(G)$ is at most the maximal number k such that G has a normal section which is the k-th power of a non-abelian simple group; in particular, $\mathrm{rk}(G) \leq \log |G|$. Since for finite linear groups $\mathrm{rk}(G)$ is less than the dimension [14], we obtain the following.

COROLLARY 9.7. *If G is a finite d-generated linear group of dimension n over some field F then $\nu(G) \leq cd + \log n$ for some absolute constant c.*

It is somewhat surprising that the number of random generators does not depend on the field F.

The above results are partly motivated by applications to the analysis of the product replacement algorithm first presented in [9]. We describe this briefly. The algorithm starts from a list $\{g_1, \ldots, g_m\}$ of generators of a finite group G, selects positions i and j at random and replaces g_i either by $g_i g_j$ or $g_j g_i$. This step is repeated a number of times and finally after K iterations a randomly chosen g_i is declared to be a "random element of G". This heuristic for finding nearly uniform random elements is an essential building block for efficient matrix group algorithms. There are two critical parameters: m and K.

Let G be a finite group. A generating set S of G is called **minimal** if any proper subset of S generates a proper subgroup of G. Denote by $\tilde{d}(G)$ the maximum of the size of a minimal generating set of G. It was already shown in [9] that if $m \geq 2\tilde{d}(G)$ then the algorithm actually outputs a random m-tuple if K is large enough. The time it takes to obtain a random m-tuple is investigated in [12] and [31].

As observed in [9] although in the limit each generating m-tuple is equally likely (if m is large enough) this does not imply that the algorithm will yield each element with equal probability. As noted there, this problem leads to the question of determining what proportion of m-tuples generates G.

It was later shown by Pak [45] that indeed if most m-tuples generate G then bias in the distribution of the random component of the last m-tuple does not occur, at least for some variant of the original algorithm. Hence for the important case of matrix groups, $m = cd + \log n$ is a reasonable choice in the algorithm. For general groups we have the following unexpected result.

COROLLARY 9.8. *If G is a finite d-generated group then $\nu(G) \leq cd + \log \tilde{d}(G)$.*

This follows from Corollary 9.6 and the following observation. (Recall that a chief-factor N/K of a group G is called non Frattini if there exists a maximal subgroup H of G which contains K but does not contain N.)

PROPOSITION 9.9. *Let G be a finite group. Then $\tilde{d}(G)$ is at least the number of non Frattini chief-factors of G.*

Proof. The proof is by induction on $|G|$. Suppose N is a minimal non-Frattini normal subgroup of G. Then we need to show that $\tilde{d}(G) \geq \tilde{d}(G/N)+1$. Let H be a maximal subgroup of G that does not contain N. Put $\bar{G} = G/N$. Let $z_1, \ldots, z_k$ be a minimal generating of $\bar{G}$ with $k = \tilde{d}(\bar{G})$. Since $G = HN$, we can choose $x_i \in H$ such that $z_i = x_i N$. Take some elements $y_1, \ldots, y_l$ from N such that $S = x_1, \ldots, x_k, y_1, \ldots, y_l$ generates G. Then a minimal generating subset of S contains $x_1, \ldots, x_k$ and so it has at least $k + 1$ elements. □

Diaconis and Saloff-Coste [12] found the first general bounds for the mixing time of the product replacement algorithm. Their estimates are too involved to be reproduced here. The effectiveness of a version of their main result [12, Th. 5.5] depends crucially (among others) on the proportion of generating m_*-tuples for some $m_* < m$. By Corollary 9.8 and $m_* = cd + \log \tilde{d}(G)$, this quantity becomes a constant.

Remark 9.10. The other parameter which affects the usefulness of the bounds in [12] is $D(G)$,the maximum diameter of Cayley graphs of G over all generating sets. Until recently this seemed quite intractable. By a very recent result of Helfgott [18] for $G = \mathrm{SL}(2, p)$ we have $D(G) \leq (\log p)^c$ where c does not depend on p. It is expected that the results in [18] can be extended to nonsolvable linear algebraic groups over finite fields. This would nicely complement our results.

10. Characterization of groups of at most exponential subgroup growth

In [32, Chap. 3] Lubotzky and Segal consider finitely generated groups of exponential subgroup growth. They ask the "difficult question" as to whether such groups can be characterized algebraically. The aim of this section is to

provide such a characterization (which will be used in proving our characterization theorem for PFG groups).

Actually we will give several related characterizations. Let us introduce some necessary notation. Let L be a finite group with a unique minimal normal subgroup M. We say that L is **associated** with a non-abelian group A if A is isomorphic to M. In this case A is a direct power of some non-abelian simple group S. Recall that for each such L we have defined the crown-based power of L of size k as the subgroup $L(k)$ of L^k defined by

$$L(k) = \{(l_1, \dots, l_k) \in L^k \mid l_1 \equiv \cdots \equiv l_k \mod M\}.$$

Remark 10.1. Clearly the quotient group of $L(k)$ over any minimal normal subgroup is isomorphic to $L(k-1)$ and any subdirect product subgroup of L^k which is also a subgroup of $L(k)$ is isomorphic to a crown-based power of L.

THEOREM 10.2. *Let F be a finitely generated profinite group. Then the following conditions are equivalent*:

(1) *There exists a constant c such that $a_n(F) \leq c^n$.*
(2) *There exists a constant c such that for any group L associated with $\mathrm{Alt}(b)^s$ for some s and b,*
$$|\mathrm{Epi}(F, L)| \leq |L| c^{bs}.$$
(3) *There exists a constant c such that for any group L associated with $\mathrm{Alt}(b)^s$ for some s and b, the size of a crown-based power of L, which occurs as a quotient of F, is at most c^{bs}.*
(4) *There exists a constant c_a for some $a \geq 5$ such that for any group L associated with $\mathrm{Alt}(b)^s$ for some s and $b \geq a$, the size of a crown-based power of L, which occurs as a quotient of F is at most c_a^{bs}.*
(5) *There exists a constant c such that each open subgroup H of F has at most $c^{b|F:H|}$ quotients isomorphic to $\mathrm{Alt}(b)$ for any $b \geq 5$.*

Proof. The implications (1) $\Rightarrow$ (2), (2) $\Rightarrow$ (3) and (3) $\Rightarrow$ (4) are immediate (see the arguments in §4).

We prove now that (4) $\Rightarrow$ (1). In view of Theorem 3.1, we only need to prove that for any transitive group T of degree n, $|\mathrm{Epi}(F, T)| \leq |T| c^n$ for some c. We do it by induction on n with $c = (\max\{(a!)^{d(F)},\ 4c_a 2^{d(F)}\})^2$.

Suppose that $\{B_1, \dots, B_s\}$ is a system of blocks for T, such that $b = |B_1| > 1$ and $H_1 = \mathrm{St}_T(B_1)$ acts primitively on B_1. Thus, $T \leq \mathrm{St}_{\mathrm{Sym}(n)}(\{B_i\}) \cong \mathrm{Sym}(b) \wr \mathrm{Sym}(s)$. Let P be the image of H_1 in $\mathrm{Sym}(B_1) \cong \mathrm{Sym}(b)$ and put $\widetilde{K} = \mathrm{core}(H_1)$. Hence $\widetilde{K} = T \cap \mathrm{Sym}(b)^s$. Then T can be naturally embedded in $P \wr (T/\widetilde{K})$.

Case 1. *Suppose that* $|\widetilde{K}| \leq (a!)^n$. Note that $T/\widetilde{K}$ is a transitive group of degree s. By induction, there are at most $|T/\widetilde{K}| c^s$ epimorphisms from F onto

$T/\widetilde{K}$. Hence, since $|\widetilde{K}| \leq (a!)^n$, there are at most

$$|T/\widetilde{K}|c^s(a!)^{d(F)n} \leq |T|c^n$$

epimorphisms from F onto T.

Case 2. *Suppose that* $|\widetilde{K}| > (a!)^n$. Since $\widetilde{K}$ is a subgroup of P^s, $|P| > (a!)^b$. Hence $b > a$ and P contains $\mathrm{Alt}(B_1)$ (see Proposition 2.3). Therefore as in the proof of Theorem 3.1, $K = [\widetilde{K}, \widetilde{K}] = T \cap (\mathrm{Alt}(b))^s$ is a subdirect product subgroup of $\mathrm{Alt}(b)^s$ which is a minimal normal subgroup of T.

Let l be such that $K \cong \mathrm{Alt}(b)^l$. Put $L = T/C_T(K)$. Then L has a unique minimal normal subgroup $M \cong \mathrm{Alt}(b)^l$. We want to estimate $|\mathrm{Epi}(F, L)|$ first.

Take $\phi \in \mathrm{Epi}(F, L)$. Then ϕ induces an epimorphism $\bar{\phi}\colon F \to L/M$. Note that L/M is a transitive group of degree l or $2l$. Hence, by induction, there are at most $|L/M|c^{2l} \leq |L/M|c^{n/2}$ possibilities for $\bar{\phi}$. Fix one such $\bar{\phi} \in \mathrm{Epi}(F, L/M)$ and call it ψ. Denote by $\mathrm{Epi}_\psi(F, L)$ the set

$$\{\phi \in \mathrm{Epi}(F, L) \mid \bar{\phi} = \psi\} = \{\phi_1, \ldots, \phi_k\},$$

where $k = |\mathrm{Epi}_\psi(F, L)|$.

Let $R = \bigcap_{i=1}^k \ker \phi_i$. Then F/R is isomorphic to the following subgroup of L^k: $\{(\phi_1(l), \ldots, \phi_k(l)) \mid l \in L\}$. By Remark 10.1, F/R is a crown-based power of L. Hence, if we denote by $\mathrm{Aut}_1(L)$ the set of automorphisms of L which induce identity on L/M, we obtain that $k \leq c_a^{bl} |\mathrm{Aut}_1(L)|$. By a slight modification of the proof of Corollary 2.11, we obtain that $|\mathrm{Aut}_1(L)| \leq l|\mathrm{Aut}(\mathrm{Alt}(b)|^l$. Thus,

$$|\mathrm{Epi}(F, L)| \leq |L/M|c^{n/2}c_a^{bl}l|\mathrm{Aut}(\mathrm{Alt}(b)|^l \leq |L|4^l l c^{n/2}c_a^n \leq |L|(4c_a)^n c^{n/2}$$

As in Theorem 4.1, we can prove that $|C_T(K)| \leq 2^n$. Therefore, by Lemma 2.12(1),

$$|\mathrm{Epi}(F, T)| \leq c^{n/2}(4c_a)^n |L| 2^{d(F)n} \leq |T|c^n.$$

The implication (1) $\Rightarrow$ (5) is immediate. Let us prove (5) $\Rightarrow$ (3). Assume that condition (5) holds but condition (3) does not hold. Then for any c_0 there exists $b \geq 5$ and L associated with $A = \mathrm{Alt}(b)^s$ such that $L(k)$ is a quotient of G and $k > c_0^{bs}$. Let $\widetilde{K}$ be the normalizer of an $\mathrm{Alt}(b)$ component in L. We have a natural homomorphism from $\widetilde{K}$ to $\mathrm{Aut}(\mathrm{Alt}(b))$. Let K be the preimage of $\mathrm{Inn}(\mathrm{Alt}(b))$. Then the index of K in L is at most $4s$.

Let M be the minimal normal subgroup of L. There is a natural epimorphism from F onto $L/M \cong L(k)/M^k$. Let H be the preimage of K/M. Then $|F : H| \leq 4s$ and it is clear that H has at least k quotients isomorphic to $\mathrm{Alt}(b)$. Hence taking $c_0 > c^4$, we obtain a contradiction. □

Note that Theorem 10.2 implies that a finitely generated group without arbitrarily large alternating upper composition factors has at most exponential

subgroup growth. This result was stated in [48]. However there is a gap in the proof of Corollary 2.2(ii) of that paper (which does not affect the validity of a slightly weaker form of the above result stated in the abstract of [48]).

One can prove analogous results for groups with a super-exponential subgroup growth function (which satisfies some mild conditions). For example the proof of Theorem 10.2 can easily be modified to yield the following.

THEOREM 10.3. *Let Γ be a finitely generated group. Let $f(n)$ be a monotone increasing function satisfying $f(2m) \geq 2^m f(m)$ for all natural numbers m. Assume that for any group L associated with $\mathrm{Alt}(b)^s$ for some s and b the size of a crown-based power of L which occurs as a quotient of Γ is at most $f(bs)$. Then $a_n(\Gamma) \leq f(n)^{cd(\Gamma)}$ for some absolute constant c.*

11. **Characterization of positively finitely generated profinite groups**

In this section we prove one of our main results, an algebraic characterization of PFG groups. It is motivated by a (much weaker) conjecture of Lucchini [33] according to which non-PFG groups have quotients which are crown-based powers of unbounded size.

Note that crown-based powers together with some affine variants were introduced in [10], where it is shown that any finite group which needs more generators than its proper quotients is isomorphic to one of these (more general) crown-based powers. Hence these groups can be used to characterise the class of d-generator finite (or profinite) groups.

THEOREM 11.1. *Let F be a finitely generated profinite group. Then the following conditions are equivalent*:

(1) *There exists a constant c such that $m_m(F) \leq m^c$ for all m.*
(2) *There exists a constant c such that for any group L associated with a characteristically simple group A,*

$$|\mathrm{Epi}(F, L)| \leq |L| l(A)^c.$$

(3) *There exists a constant c such that for any group L associated with a characteristically simple group A, the size of a crown-based power of L, which occurs as a quotient of F is at most $l(A)^c$.*
(4) *There exists a constant c_a for some a such that for any group L associated with a characteristically simple group A such that $|A| > l(A)^a$, the size of a crown-based power of L, which occurs as a quotient of F is at most $l(A)^{c_a}$.*
(5) *There exists a constant c such that for any characteristically simple group A the number of F-isomorphism types of non-abelian irreducible large F-groups isomorphic to A as groups is at most $l(A)^c$.*

(6) *There exists a constant c such that for any almost simple group R, any open subgroup H of F has at most $l(R)^{c|F:H|}$ quotients isomorphic to R.*
(7) *There exists a constant c such that for any non-abelian characteristically simple group A if a normal section H/N of G is the product of r chief factors isomorphic to A as groups then $r \leq l(A)^c$.*

Proof. We begin the proof with the implication (1) $\Rightarrow$ (2). By Lemma 9.2, there exist a primitive faithful representation $L \to \mathrm{Sym}(\Omega)$ such that $|\Omega| \leq l(A)^{c_7}$.

The composition of an epimorphism $\phi \in \mathrm{Epi}(F, L)$ with the constructed representation $L \to \mathrm{Sym}(\Omega)$ induces a primitive action of F on Ω. Let $w \in \Omega$ and denote by S_ϕ the stabilizer of w in F with respect to the action induced by ϕ. It is clear that S_ϕ is a subgroup of index $|\Omega|$. Note that the number of epimorphisms from $\mathrm{Epi}(F, L)$ with the same S_ϕ is at most $|\mathrm{Aut}(L)| \leq l(A)^2|L|$, by Corollary 2.11 and Lemma 2.6. Using our assumptions, we obtain that

$$|\mathrm{Epi}(F, L)| \leq l(A)^{c_7(c+1)} l(A)^2 |L| \leq l(A)^{c_7(c+1)+2} |L|$$

as required.

The implications (2) $\Rightarrow$ (3) and (3) $\Rightarrow$ (4) are immediate.

We prove now that (4) $\Rightarrow$ (1). In view of Theorem 8.1, we only need to prove that for any primitive permutation group P of degree m, $|\mathrm{Epi}(F, P)| \leq |P| m^c$ for some c.

Note that from Theorem 10.2 it follows that there exists a constant e_1 such that $|\mathrm{Epi}(F, L)| \leq |L| e_1^l$ for any transitive group L of degree at most l. Let P be a primitive group of degree m and M the socle of P. Then we have two possibilities:

Case 1. *M is not abelian and it is a minimal normal subgroup of P.* We divide this case into two subcases.

Case 1a. $|M| \leq l(M)^a$. Now $M = S_1 \times \cdots \times S_l$ is a direct product of groups isomorphic to a non-abelian simple group S. Denote by $\widetilde{M}$ the intersection of the normalizers of the S_i in P. Setting $\mathrm{O} = N_P(S_1)/S_1 C_P(S_1)$ we see clearly that P/M is equivalent to a transitive subgroup of $O \wr P/\widetilde{M}$ (where O is considered as a regular permutation group). Since O is isomorphic to a subgroup of $\mathrm{Out}(S)$, by Lemma 1.6, P/M is a transitive group of degree at most $3l \log l(S) \leq 3 \log l(M)$. Hence there are at most $|P/M| e_1^{3 \log l(M)} = |P/M| l(M)^{3 \log e_1}$ epimorphisms from F onto P/M. Therefore, by Proposition 2.12(1) there are at most

$$|P/M| l(M)^{3 \log e_1} |M|^{d(F)} \leq |P/M| l(M)^{3 \log e_1} |l(M)|^{d(F) c_a}$$

epimorphisms from F onto P. Thus $|\mathrm{Epi}(F, P)| \leq |P| m^{d(F) c_a + 3 \log e_1}$.

Case 1b. $|M| > l(M)^a$. Note that P is associated with a characteristically simple group $A \cong M$ and we can apply our assumptions. There is a non-abelian simple group S such that $A \cong S^l$.

Take $\phi \in \mathrm{Epi}(F, P)$. Then ϕ induces an epimorphism $\bar{\phi}\colon F \to P/M$. Note that P/M is a transitive group of degree at most $3 \log l(M)$. Hence there are at most $|P/M| l(M)^{3 \log e_1}$ possibilities for $\bar{\phi}$. Fix one such $\bar{\phi} \in \mathrm{Epi}(F, P/M)$ and call it ψ. Denote by $\mathrm{Epi}_\psi(F, P)$ the set

$$\{\phi \in \mathrm{Epi}(F, P) \mid \bar{\phi} = \psi\} = \{\phi_1, \dots, \phi_k\},$$

where $k = |\mathrm{Epi}_\psi(F, P)|$.

Let $R = \bigcap_{i=1}^k \ker \phi_i$. Then F/R is isomorphic to the following subgroup of P^k: $\{(\phi_1(l), \dots, \phi_k(l)) \mid l \in P\}$. By Remark 10.1, F/R is a crown-based power of P. Hence, if we denote by $\mathrm{Aut}_1(P)$ the set of automorphisms of P which induce identity on P/M, we obtain that $k \leq l(M)^{c_a} |\mathrm{Aut}_1(P)|$. Repeating the proof of Corollary 2.11, we obtain that $|\mathrm{Aut}_1(P)| \leq l |\mathrm{Aut}(S)|^l$. Thus,

$$|\mathrm{Epi}(F, P)| \leq |P/M| l(M)^{3 \log e_1} l(M)^{c_a} l |\mathrm{Aut}(S)|^l.$$

Note that $l(M) \leq m$ and by Lemma 2.6, $|\mathrm{Out}(S)| \leq l(S)$. Thus we obtain that $|\mathrm{Epi}(F, P)| \leq m^{2+c_a+3 \log e_1} |P|$.

Case 2. *M is not a minimal normal subgroup.* Then M is a product of two minimal normal subgroups M_1 and M_2 and $m = |M_1| = |M_2|$. Then we first bound $|\mathrm{Epi}(F, P/M_2)|$, repeating the argument of the proof of Case 1 and then we obtain the desired bound for $|\mathrm{Epi}(G, P)|$ from Lemma 2.12(1).

Case 3. *M is abelian (P is of affine type).* In this case $m = p^n$ and $P = TM$ where T is an irreducible subgroup of $\mathrm{GL}_{\mathbb{F}_p}(V)$, where $V = M$ is considered as an n-dimensional $\mathbb{F}_p$-vector space.

Let H be a subgroup of T such that the representation of T is induced from a primitive representation of H. Denote by W a primitive H-module such that $V = T \otimes_H W$. Let P_0 be the image of H in $\mathrm{End}_{\mathbb{F}_p}(W)$ and $b = \dim_{\mathbb{F}_p} W$. Put $\widetilde{K} = \mathrm{core}\, H$. Then $T/\widetilde{K}$ is a transitive group of degree $s = n/b$ and T is a subgroup of $P_0 \wr T/\widetilde{K}$.

Subcase 3a. *Suppose that* $|\widetilde{K}| \leq |V|^{\max\{a+6, c_4\}}$. Since $T/\widetilde{K}$ is a transitive group of degree s, there are at most $|T/\widetilde{K}| e_1^s$ epimorphisms from F onto $T/\widetilde{K}$. On the other hand $|\widetilde{K}| \leq |V|^{\max\{a+6, c_4\}}$, whence there are at most

$$|T/\widetilde{K}| e_1^s |V|^{d(F) \max\{a+6, c_4\}} \leq |T| m^{d(F) \max\{a+6, c_4\} + \log e_1}$$

epimorphisms from F onto T. Thus $|\mathrm{Epi}(F, P)| \leq |P| m^{d(F)(\max\{a+6, c_4\}+1) + \log e_1}$.

Subcase 3b. *Suppose that* $|\widetilde{K}| > |V|^{\max\{a+6, c_4\}}$. Thus, $|P_0| > |W|^{c_4}$, and so we can use Proposition 5.7 and the notation of that proposition. Put $N = E(B)^s \leq P_0^s$. Note that T acts transitively on the factors of N. Denote $E(B)/Z(E(B))$ by S. Since $|P_0| \geq |W|^{a+6}$, by Proposition 5.7(6), $|S| > |U|^a \geq$

$l(S)^a$. As in the proof of Proposition 6.1 we obtain that $K = (N \cap T)'$ is a normal subgroup of T and it is a subdirect product subgroup of N.

Put $L = T/C_T(K)$. Then L is associated with $S^l \cong M = KC_T(K)/C_T(K)$, and so it is isomorphic to a primitive group of degree at most $l(S)^{lc_7}$. Using the same argument as in the proof of Case 1 we can estimate $|\mathrm{Epi}(F, L)|$ and obtain that

$$|\mathrm{Epi}(F, L)| \leq l(S)^{lc_8}|L|$$

for some constant c_8 depending on F. Note that $l(S)^l \leq m$ since $l \leq s$. Thus we obtain that $|\mathrm{Epi}(F, L)| \leq m^{c_8}|L|$.

As in the proof of Proposition 7.1, we have $|C_T(K)| \leq |V|^3$, and so $|C_T(K)V| \leq m^4$. Now, using Lemma 2.12(1), we obtain that

$$|\mathrm{Epi}(G, P)| \leq m^{c_8+4d(F)}|P|$$

and the implication (4) $\Rightarrow$ (1) is proved.

The implication (5) $\Rightarrow$ (3) is trivial. We prove now (2) $\Rightarrow$ (5). Let $A \cong S^s$ be a large F-irreducible group associated with $\theta\colon F \to \mathrm{Aut}(A)$. First we prove the following claim:

Claim. There is a constant e such that the number of d-generated subgroups T up to conjugacy inside $\mathrm{Aut}(A)$ for which A is irreducible and large is at most $l(A)^{ed}$.

Let T be such a subgroup of $\mathrm{Aut}(A)$. Then $K = T \cap A$ is a subdirect product subgroup of A. Let $\tilde{A}$ be the normalizer of all simple factors of A in $\mathrm{Aut}(A)$ and $\widetilde{K} = \tilde{A} \cap T$. Then T is a subgroup of $W = \mathrm{Aut}(S) \wr T/\widetilde{K}$. Applying Theorem 3.1, we obtain that there are at most c_t^{ds} choices for $T\tilde{A}/\tilde{A} \cong T/\widetilde{K}$ up to conjugacy inside $\mathrm{Aut}(A)/\tilde{A} \cong \mathrm{Sym}(s)$. Fix one such choice. Now, $Q = T\tilde{A}$. By Lemma 2.18 the number of d-generated subgroups T up to conjugacy inside Q for which A is irreducible and large is at most $|\mathrm{Out}(S)|^{sd}(1 + |\mathrm{Out}(S)|)^s \leq l(A)^{2d}$ (see Lemma 2.6). Thus we conclude that there exists a constant e such that the number of d-generated subgroups T up to conjugacy inside $\mathrm{Aut}(A)$ for which A is irreducible and large is at most

$$c_t^{ds} l(A)^{2d} \leq l(A)^{ed}.$$

Thus, in order to prove (2) $\Rightarrow$ (5) we can fix a group T inside $\mathrm{Aut}(A)$ and we only need to show that $|\mathrm{Epi}(F, T)| \leq |T|l(A)^f$ for some constant f. As before, $K = T \cap A$ and $\widetilde{K} = \tilde{A} \cap T$.

Case 1. $|K| \leq l(A)$. By Theorem 10.2 there exists a constant e_1 such that $|\mathrm{Epi}(F, T/\widetilde{K}))| \leq |T/\widetilde{K}|e_1^s$. Since $|K| \leq l(A)$, $|\widetilde{K}| \leq l(A)^2$. Hence, by Corollary 2.12(1),

$$|\mathrm{Epi}(F, T)| \leq |T/\widetilde{K}|e_1^s l(A)^{2d(F)}.$$

Case 2. $|K| \geq l(A)$. By Lemma 2.19, $|C_T(K)| \leq l(A)$ and our assumptions, $|\mathrm{Epi}(F, T/C_T(K))| \leq l(K)^c|T|$. Hence, by Lemma 2.12(1)

$$|\mathrm{Epi}(F,T)| \leq |\mathrm{Epi}(F,T/C_T(K))||C_T(K)|^{d(F)} \leq |T|l(A)^{c+d(F)}.$$

Now, we prove (5) $\Rightarrow$ (6). Let H be an open subgroup of F and R an almost simple group. Denote by S the unique normal subgroup of R. Let k be the number of quotients of H isomorphic to R. Each such quotient induces a homomorphism of H to $\mathrm{Aut}(S)$. We denote by $S_1, \ldots, S_k$ the (pairwise nonisomorphic) H-groups associated with these homomorphisms.

For each i define B_i to be the set of functions from F to S_i satisfying $f(xq) = f(x)^q$, where $x \in F$ and $q \in H$. The multiplication in S_i defines a multiplication in B_i and F acts on the B_i by means of $f^y(x) = f(xy)$ where $f \in B_i$ and $x, y \in F$. Then the B_i are irreducible F-groups and $B_i \cong S^{|F:H|}$ as a group. Also note that among the B_i there are at least $\frac{k}{|F:H|}$ nonisomorphic H-groups. Thus we have constructed at least $\frac{k}{|F:H|}$ irreducible F-groups.

Let B be an F-group such that $B \cong S^{|F:H|}$ as a group and let $\theta\colon F \to \mathrm{Aut}(S^{|F:H|})$ be the homomorphism corresponding to the F-group B. We want to find an upper bound on the number of F-groups B such that $\theta(F)$ is a large complement to $S^{|F:H|}$ in $X = \theta(F)S^{|F:H|}$ (as usual, we identify S and $\mathrm{Inn}(S)$).

By the usual argument using Theorem 3.1 we obtain that there are at most

$$(c_t|\,\mathrm{Out}(S)|)^{d(F)|F:H|} \tag{11.1}$$

possibilities for X up to conjugacy in $\mathrm{Aut}(S^{|F:H|})$ and, by Proposition 2.16, there are at most

$$(|\,\mathrm{Out}(S)||F:H|)^2 \tag{11.2}$$

X-conjugacy classes of large complements to $S^{|F:H|}$ in X.

Now fix X and a complement D to $S^{|F:H|}$ in X. Note that from Theorem 10.2 it follows that there exists a constant e_1 such that $|\mathrm{Epi}(F,L)| \leq |L|e_1^l$ for any transitive group L of degree at most l. Applying this to $L = D\,\mathrm{Aut}(S)^{|G:H|}/\,\mathrm{Aut}(S)^{|G:H|}$, we obtain that there are at most

$$|F:H|e_1^{|F:H|}|\,\mathrm{Out}(S)|^{|F:H|d(F)} \tag{11.3}$$

D-conjugacy classes of epimorphisms from F onto D.

Putting together (11.1), (11.2) and (11.3), we obtain that there exists a constant e_2 (which depends only on c_t, e_1 and $d(F)$) such that the number of nonisomorphic F-groups B such that $B \cong S^{|F:H|}$ and $\theta(F)$ is a large complement to $S^{|F:H|}$ in $X = \theta(F)S^{|F:H|}$ is at most $l(S)^{e_2|F:H|}$.

Now note that B_i is either large or of the type considered in the previous paragraphs. Hence there at most $l(S)^{|F:H|c} + l(S)^{|F:H|e_2}$ nonisomorphic F-groups among the B_i. Hence $k \leq l(S)^{|F:H|(c+e_2+1)} \leq l(R)^{|F:H|(c+e_2+1)}$ and we are done.

We now prove (6) $\Rightarrow$ (3). Let L be a group associated with a characteristically simple group $A \cong S^l$ and let k be the maximal size of a crown-based power of L, which occurs as a quotient of F. Denote by $M \cong S^l$ the minimal normal subgroup of L. Let $\widetilde{K}$ be the normalizer of an S-component in L. The index of $\widetilde{K}$ in L is l. We have a natural homomorphism from $\widetilde{K}$ to $\mathrm{Aut}(S)$. Denote by R the image of this homomorphism. Then R is an almost simple group.

There is a natural epimorphism from F onto $L/M \cong L(k)/M^k$. Let H be the preimage of $\widetilde{K}/M$. Then $|F : H| = l$ and H has k quotients isomorphic to R. Hence

$$k \leq l(R)^{lc} \leq l(S)^{c_7 lc} = l(A)^{c_7 c}$$

and we are done.

The implications (5) $\Rightarrow$ (7) $\Rightarrow$ (3) are immediate. □

We have obtained several related characterizations of PFG groups. Perhaps the most revealing is (3). The equivalence PFG $\Leftrightarrow$ (4) extends the main result of [8] which states that finitely generated non-PFG groups have arbitrarily large alternating sections. The equivalence PFG $\Leftrightarrow$ (7) also follows from Theorem 1. A simple consequence of (5) is that if F is a PFG group then the number of non-abelian chief factors of order n is at most n^c. Instead of a direct analogue of Theorem 10.2(5) we have the following.

COROLLARY 11.2. *Let G be a finitely generated profinite group which is not positively finitely generated and let a be an arbitrary positive constant. Then for infinitely many natural numbers i, G has an open normal subgroup H_i of index i such that H_i has at least a^i quotients isomorphic to some non-abelian simple group S_i.*

Proof. Let c be a constant such that $2^c > a^3$. By Theorem 11.1 there exist infinitely many non-abelian simple groups S such that the following holds. There are a characteristically simple group $A \cong S^l$ and a group L associated with A such that the crown-based power $L(k)$ is a quotient of G where $k \leq l(S)^{lc}$. Put $j = [3\log(l(S))l]$.

Let M be the minimal normal subgroup of L and $\widetilde{K}$ the normalizer of an S-component of M in L. The index of $\widetilde{K}$ in L is l. The normalizer $\widetilde{K}$ contains a subgroup $\widetilde{H}$ of index at most $|\mathrm{Out}(S)| \leq 3\log(l(S))$ which has S as a quotient. Let H be the preimage of $\widetilde{H}/M$ in G. Then $|G : H| \leq j$ and H has at least k quotients isomorphic to S. Now $k \geq l(S)^{lc} \geq (2^{c/3})^j \geq a^j$.

Let us call the subgroup H just constructed by $H(S)$ (note that $H(S)$ is not defined for all non-abelian simple groups S but is defined for infinitely many of them). If the indices of all the $H(S)$ are unbounded, we are done (we put $H_{|G:H(S)|} = H(S)$).

Suppose now that the indices of all the $H(S)$ are bounded. Then without loss of generality we can assume that all the $H(S)$ are equal to the same group H. Let H/K be the maximal quotient of H isomorphic to the product of simple groups and let N be an open normal subgroup of H which contains K. Note that for infinitely many non-abelian simple groups S, N has at least k_S quotients isomorphic to S, where $\lim_{|S|\to\infty} k_S = \infty$. Thus, $\{H_i\}$ can be any decreasing chain of open normal subgroups of H which contain K. This completes the proof. □

12. **Applications**

In this section we collect various consequences of our main result, Theorem 11.1.

COROLLARY 12.1. *Let F be a* PFG *profinite group and H an open subgroup of F. Then H is also* PFG.

Proof. This follows directly from Theorem 11.1(6). □

This corollary answers a question of Mann [35] which has been mentioned in several places including [32]. A partial result was obtained in [42]. It seems intriguing that no more direct proof has been found.

Our results can be used to shed light on the relationship between PFG groups and various other classes of groups. In [32, Chap. 12] groups of polynomial index growth are considered, that is, groups G for which $|\bar{G} : \bar{G}^n| < n^s$ holds for some s, independent of n and $\bar{G}$, for all finite quotients $\bar{G}$ of G. It is asked in [32, p. 431] whether a finitely generated group G with this property has polynomial maximal subgroup growth. The positive answer follows from Theorem 11.1 and an observation in [6], namely that if S^r is an upper factor of G with S a non-abelian simple group then r is bounded.

Comparing Theorems 10.2 and 11.1 we see that PFG groups have at most exponential subgroup growth answering a question of Mann and Segal [37, p. 192].

Let G be a group. We denote by $r_n(G)$ (respectively $\hat{r}_n(G)$) the number of isomorphism classes of irreducible n-dimensional complex representations (respectively with finite image) of G. Following [30] we call $r_n(G)$ the *representation growth* function of G. When G is profinite we only consider continuous representations. In this case $r_n(G) = \hat{r}_n(G)$.

COROLLARY 12.2. *Let G be a profinite group. Then the following holds.*

(1) *If $r_n(G)$ grows at most exponentially, then $a_n(G)$ grows at most exponentially*;
(2) *If $r_n(G)$ grows at most polynomially, then $m_n(G)$ grows at most polynomially*; *i.e.*, *G is a* PFG *group.*

Proof. We prove the first statement. The second statement follows by a similar argument.

Suppose that G has super-exponential subgroup growth. Then by Theorem 10.2, for any c there exists a group L with a unique minimal normal subgroup M isomorphic to $\mathrm{Alt}(b)^s$ for some s and b, such that $L(k)$ is a quotient of G and $k > c^{bs}$. The projections of $L(k)$ onto each factor of L^k induce k homomorphisms of G onto L with different kernels. Since L is a transitive group of degree $n = bs$ and L has a unique minimal normal subgroup, L has a faithful irreducible representation of degree at most $n-1$ (this representation is a subrepresentation of the permutation representation). Thus, we have constructed $k > c^n$ different irreducible representations of G of degree at most $n-1$. Hence $r_n(G)$ grows faster than any exponential function, a contradiction. □

Note that in the second statement of the previous proposition we can not change $m_n(G)$ to $a_n(G)$ because there are examples of pro-p groups with polynomial representation growth but with nonpolynomial subgroup growth (see [20]). Moreover it is shown in [30] that S-arithmetic groups with the congruence subgroup property have polynomial representation growth and it is known that such groups have subgroup growth of type $n^{c \log n / \log \log n}$ [27].

13. The number of finite groups with a bounded number of defining relations

Let $h(n, r)$ be the number of (isomorphism types of) groups of order n that can be defined by r relations. In [36] A. Mann posed the following conjecture.

CONJECTURE 1. *$h(n, r) \leq n^{cr}$, for some constant c.*

In [36] this bound was established for the number of nilpotent groups of order n that can be defined by r relations. In this section we prove the conjecture as a corollary to our results on irreducible representations of finite groups.

Let F be a finitely generated profinite group. Denote by $t_{n,r}(F)$ the number of open normal subgroups N of F of index n such that N can be generated by r elements as a normal subgroup. The aim of this section is to prove the following theorem.

THEOREM 13.1. *There exists a constant c such that if F is a d-generated profinite group then $t_{n,r}(F) \leq n^{cd+r}$ for all $n \geq 1$.*

First we prove another corollary of Theorem 3.1. Let F be a profinite group, N a normal subgroup of F and S a non-abelian finite F-group with respect to a homomorphism $\phi\colon F \to \mathrm{Aut}(S)$. We say that S is an irreducible (F,N)-group if S is an irreducible F-group and $\phi(N) = \mathrm{Inn}(S)$.

COROLLARY 13.2. *There exists a constant c_9 such that the number of non-abelian nonisomorphic irreducible (F,N)-groups of order m is at most $\log|F/N| m^{c_9 d}$ for any profinite d-generated group F.*

Proof. Let A be a non-abelian irreducible (F,N)-group. Then $A = S_1 \times \cdots \times S_s$, where the S_i are isomorphic simple groups. Since there are at most two non-abelian finite simple groups of any given order it follows that there are at most m possibilities for the isomorphism type of A. We fix one such isomorphism type.

We want to calculate the number of homomorphisms ϕ from F to $\mathrm{Aut}(A) \cong \mathrm{Aut}(S_1) \wr \mathrm{Sym}(s)$ up to conjugacy in $\mathrm{Aut}(A)$ such that $\phi(N) = \mathrm{Inn}(A)$ and the image acts transitively on the S_i. The homomorphism ϕ induces a homomorphism $\bar{\phi}\colon F \to \mathrm{Sym}(s)$ such that the kernel of $\bar{\phi}$ contains N. Using Corollary 4.4, we obtain that there are at most

$$c^{sd} \log|F/N|$$

such homomorphisms up to conjugacy. Now ϕ is a homomorphism from F to $\mathrm{Aut}(S_1) \wr \mathrm{Im}(\bar{\phi})$. Given $\bar{\phi}$, such a homomorphism is determined by the images of a system of generators of F in the cosets of the base group $\mathrm{Aut}(S_1)^s$ which correspond to the images of this generating system under $\bar{\phi}$. Hence, there are at most

$$|\mathrm{Aut}(S_1)|^{sd} c^{sd} \log|F/N| \leq m^{2d} m^{d \log c} \log|F/N| \leq m^{(2+\log c)d} \log|F/N|$$

conjugacy classes of appropriate homomorphisms ϕ from F to $\mathrm{Aut}(A)$. This implies that there are at most $m^{(2+\log c)d+1} \log|F/N|$ non-abelian nonisomorphic irreducible (F,N)-groups of order m. □

Proof of Theorem 13.1. Let $\mathcal{N}$ be the set of open normal subgroups N with $|F/N| = n$, such that N can be generated by r elements as a normal subgroup. Thus $t_{n,r}(F) = |\mathcal{N}|$.

We now estimate the probability that an open normal subgroup generated by s random elements from F belongs to $\mathcal{N}$. If N is any such subgroup, then our s elements lie in N with probability $1/n^s$. For any profinite F-group R, let $P(R,s)$ be the probability that a set of s random elements from R generates R as a normal F-subgroup. Since generating distinct subgroups are disjoint

events, the probability that we seek is

$$\frac{\sum_{N\in\mathcal{N}} P(N,s)}{n^s}. \tag{13.1}$$

Let $c = \max\{c_9, c_6\}$ be the maximum of the constants from Corollaries 13.2 and 7.3. Put $s = cd + r + 2$. Fix $N \in \mathcal{N}$ and put $G = F/N$. We now estimate $P(N,s)$. Let $M(N)$ be the set of open normal subgroups M of F contained in N and maximal with respect to this property. Then N/M is an irreducible F-group. Let $\mathbf{S}$ be the set of all irreducible F-groups which occur in this way. These are either irreducible $\mathbb{Z}G$-modules or non-abelian irreducible (F,N)-groups. If $S \in \mathbf{S}$ put $M_S(N) = \{M \in M(N) \mid N/M \cong_F S\}$. Set

$$\bar{N} = N/\bigcap_{M\in M(N)} M \text{ and for every } S \in \mathbf{S},\ N_S = N/\bigcap_{M\in M_S(N)} M.$$

Then, $\bar{N} \cong \prod_{S\in\mathbf{S}} N_S$ as an F-group (this follows e.g. from an analogue of Lemma 2.7 for subdirect products of irreducible F-groups). Hence

$$P(N,s) = P(\bar{N},s) = \prod_{S\in\mathbf{S}} P(N_S,s). \tag{13.2}$$

Let $P(N,M,s)$ be the probability that a set of s random elements from N lie in M. Then $P(N,M,s) = 1/|N/M|^s$. Hence we have

$$1 - P(N_S,s) \le \sum_{M\in M_S(N)} P(N,M,s) = \frac{|M_S(N)|}{|S|^s}. \tag{13.3}$$

If S is non-abelian, then $|M_S(N)| = 1$. If S is abelian, then the number of subgroups in $M_S(N)$ is less than or equal to the number of F-homomorphisms from N onto S. Since N is generated by r elements as a normal subgroup of F, the number of such homomorphisms is at most $|S|^r$. Hence from (13.2) and (13.3) we obtain that

$$P(N,s) \ge \prod_{S\in\mathbf{S}} \left(1 - \frac{1}{|S|^{s-r}}\right). \tag{13.4}$$

Now, from Corollary 7.3 the number of irreducible G-modules of the same order m is less than $m^{cd}\log n$.

Using Corollary 13.2, we obtain that there are at most $m^{cd}\log n$ non-abelian elements in $\mathbf{S}$ of order m. Hence, using (13.4) and taking into account that $(1-\frac{1}{t})^t \ge \frac{1}{4}$ for any $t \ge 2$, we obtain that

$$P(N,s) \ge \prod_{m\ge 2} (1 - \frac{1}{m^{s-r}})^{(m^{cd}\log n)} \ge n^{-2\sum_{m=2}^{\infty} m^{r-s+cd}} \ge n^{2(1-\zeta(2))}. \tag{13.5}$$

Now, (13.1) and (13.5) imply that

$$1 \ge \frac{\sum_{N\in\mathcal{N}} P(N,s)}{n^s} \ge \frac{t_{n,r}(F) n^{2(1-\zeta(2))}}{n^s}.$$

This gives us the theorem. □

Applying Theorem 13.1 to the free profinite group on r generators we obtain Mann's conjecture

COROLLARY 13.3. *There exists a constant c such that $h(n,r) \leq n^{cr}$ for all natural numbers n.*

Next we give an upper bound for the number of d-generated finite groups of order n without abelian composition factors. The problem of enumeration of these groups was considered recently by B. Klopsch [23]. It was established in [23] that there exists a constant c such that the number of finite groups of order n without abelian composition factors is at most $n^{c \log\log n}$. On the other hand if G does not have abelian composition factors, then $d(G) \leq 3 \log\log |G| + 2$ ([23, Prop. 1.1]). Thus, the following corollary is a generalization of the result of Klopsch.

COROLLARY 13.4. *There exists a constant c such that the number of d-generated finite groups of order n without abelian composition factors is at most n^{cd}.*

Proof. Let F be a free profinite group on d generators and R the intersection of all open normal subgroups N of F such that F/N has only non-abelian composition factors. Put $\bar{F} = F/R$. Then each d-generated finite group without abelian composition factors is a quotient of $\bar{F}$. The composition factors of $\bar{F}$ are non-abelian, whence the same is true for any open normal subgroup H of $\bar{F}$. It follows that H can be generated by a single element as an open normal subgroup of $\bar{F}$. Thus, using Theorem 13.1, we obtain the corollary. □

In [28] A. Lubotzky proved that the number of d-generated groups of order n is at most $n^{cd \log n}$. In the course of the proof he established that such groups can always be defined by at most $cd \log n$ profinite relations. Since Corollary 13.3 clearly holds for groups with r profinite defining relations it may be viewed as a refinement of Lubotzky's result.

Note that since every group of order n can be generated by $\log n$ elements, we see (already by Lubotzky's result) that the total number of groups of order n is at most $n^{c(\log n)^2}$, a classic result of P. M. Neumann [41] (see [47] for the best possible constant in such an estimate).

References

[1] M. ASCHBACHER, *Finite Group Theory*, *Cambridge Studies Adv. Math.* **10**, Cambridge Univ. Press, Cambridge, 1986. MR 0895134. Zbl 0583.20001.

[2] M. ASCHBACHER and L. SCOTT, Maximal subgroups of finite groups, *J. Algebra* **92** (1985), 44–80. MR 0772471. Zbl 0549.20011. doi: 10.1016/0021-8693(85)90145-0.

[3] L. Babai, The probability of generating the symmetric group, *J. Combin. Theory Ser. A* **52** (1989), 148–153. MR 1008166. Zbl 0685.60012. doi: 10.1016/0097-3165(89)90068-X.

[4] L. Babai, B. Beals, and Á. Seress, Polynomial time theory of matrix groups, in *Proc. 41st* ACM *Symposium on Theory of Computing* (STOC '09), ACM Press, 2009, pp. 55–64. doi: 10.1145/1536414.1536425.

[5] L. Babai, P. J. Cameron, and P. P. Pálfy, On the orders of primitive groups with restricted nonabelian composition factors, *J. Algebra* **79** (1982), 161–168. MR 0679977. Zbl 0493.20001. doi: 10.1016/0021-8693(82)90323-4.

[6] A. Balog, L. Pyber, and A. Mann, Polynomial index growth groups, *Internat. J. Algebra Comput.* **10** (2000), 773–782. MR 1809384. Zbl 0986.20032. doi: 10.1142/S0218196700000364.

[7] M. Bhattacharjee, The probability of generating certain profinite groups by two elements, *Israel J. Math.* **86** (1994), 311–329. MR 1276141. Zbl 0810.20020. doi: 10.1007/BF02773684.

[8] A. V. Borovik, L. Pyber, and A. Shalev, Maximal subgroups in finite and profinite groups, *Trans. Amer. Math. Soc.* **348** (1996), 3745–3761. MR 1360222. Zbl 0866.20018. doi: 10.1090/S0002-9947-96-01665-0.

[9] F. Celler, C. R. Leedham-Green, S. H. Murray, A. C. Niemeyer, and E. A. O'Brien, Generating random elements of a finite group, *Comm. Algebra* **23** (1995), 4931–4948. MR 1356111. Zbl 0836.20094. doi: 10.1080/00927879508825509.

[10] F. Dalla Volta and A. Lucchini, Finite groups that need more generators than any proper quotient, *J. Austral. Math. Soc. Ser. A* **64** (1998), 82–91. MR 1490148. Zbl 0902.20013. doi: 10.1017/S1446788700001312.

[11] E. Detomi and A. Lucchini, Crowns and factorization of the probabilistic zeta function of a finite group, *J. Algebra* **265** (2003), 651–668. MR 1987022. Zbl 1072.20031. doi: 10.1016/S0021-8693(03)00275-8.

[12] P. Diaconis and L. Saloff-Coste, Walks on generating sets of groups, *Invent. Math.* **134** (1998), 251–299. MR 1650316. Zbl 0921.60003. doi: 10.1007/s002220050265.

[13] J. D. Dixon, The probability of generating the symmetric group, *Math. Z.* **110** (1969), 199–205. MR 0251758. Zbl 0176.29901. doi: 10.1007/BF01110210.

[14] R. K. Fisher, The number of non-solvable sections in linear groups, *J. London Math. Soc.* **9** (1974/75), 80–86. MR 0360853. Zbl 0298.20038. doi: 10.1112/jlms/s2-9.1.80.

[15] M. D. Fried and M. Jarden, *Field Arithmetic*, *Ergeb. Math. Grenzgeb.* **11**, Springer-Verlag, New York, 1986. MR 0868860. Zbl 0625.12001.

[16] ———, *Field Arithmetic*, Second ed., *Ergeb. Math. Grenzgeb.* **11**, Springer-Verlag, New York, 2005. MR 2102046. Zbl 1055.12003.

[17] R. Guralnick and L. Pyber, Normalizers of primitive permutation groups, in preparation.

[18] H. A. Helfgott, Growth and generation in $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, *Ann. of Math.* **167** (2008), 601–623. MR 2415382. doi: 10.4007/annals.2008.167.601.

[19] N. S. Hughes, The structure and order of the group of central automorphisms of a finite group, *Proc. London Math. Soc.* **52** (1951), 377–385. MR 0041129. Zbl 0042.02301. doi: 10.1112/plms/s2-52.5.377.

[20] A. Jaikin-Zapirain, Representation growth of pro-p groups, unpublished.

[21] W. M. Kantor and A. Lubotzky, The probability of generating a finite classical group, *Geom. Dedicata* **36** (1990), 67–87. MR 1065213. Zbl 0718.20011. doi: 10.1007/BF00181465.

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

[23] B. Klopsch, Enumerating finite groups without abelian composition factors, *Israel J. Math.* **137** (2003), 265–284. MR 2013359. Zbl 1128.20306. doi: 10.1007/BF02785965.

[24] M. W. Liebeck and A. Shalev, The probability of generating a finite simple group, *Geom. Dedicata* **56** (1995), 103–113. MR 1338320. Zbl 0836.20068. doi: 10.1007/BF01263616.

[25] ———, Simple groups, permutation groups, and probability, *J. Amer. Math. Soc.* **12** (1999), 497–520. MR 1639620. Zbl 0916.20003. doi: 10.1090/S0894-0347-99-00288-X.

[26] ———, Bases of primitive linear groups, *J. Algebra* **252** (2002), 95–113. MR 1922387. Zbl 1034.20001. doi: 10.1016/S0021-8693(02)00001-7.

[27] A. Lubotzky, Subgroup growth and congruence subgroups, *Invent. Math.* **119** (1995), 267–295. MR 1312501. Zbl 0848.20036. doi: 10.1007/BF01245183.

[28] ———, Enumerating boundedly generated finite groups, *J. Algebra* **238** (2001), 194–199. MR 1822189. Zbl 1052.20017. doi: 10.1006/jabr.2000.8650.

[29] ———, The expected number of random elements to generate a finite group, *J. Algebra* **257** (2002), 452–459. MR 1947971. Zbl 1042.20047. doi: 10.1016/S0021-8693(02)00528-8.

[30] A. Lubotzky and B. Martin, Polynomial representation growth and the congruence subgroup problem, *Israel J. Math.* **144** (2004), 293–316. MR 2121543. Zbl 1134.20056. doi: 10.1007/BF02916715.

[31] A. Lubotzky and I. Pak, The product replacement algorithm and Kazhdan's property (T), *J. Amer. Math. Soc.* **14** (2001), 347–363. MR 1815215. Zbl 0980.20078. doi: 10.1090/S0894-0347-00-00356-8.

[32] A. Lubotzky and D. Segal, *Subgroup Growth*, *Progr. Math.* **212**, Birkhäuser, Basel, 2003. MR 01978431. Zbl 1071.20033.

[33] A. Lucchini, A 2-generated just-infinite profinite group which is not positively generated, *Israel J. Math.* **141** (2004), 119–123. MR 2063028. Zbl 1074.20024. doi: 10.1007/BF02772214.

[34] A. Lucchini, F. Menegazzo, and M. Morigi, Asymptotic results for primitive permutation groups and irreducible linear groups, *J. Algebra* **223** (2000), 154–170. MR 1738257. Zbl 1063.20501. doi: 10.1006/jabr.1999.8081.

[35] A. Mann, Positively finitely generated groups, *Forum Math.* **8** (1996), 429–459. MR 1393323. Zbl 0852.20019. doi: 10.1515/form.1996.8.429.

[36] A. Mann, Enumerating finite groups and their defining relations. II, *J. Algebra* **302** (2006), 586–592. MR 2293772. Zbl 1116.20017. doi: 10.1016/j.jalgebra.2004.02.003.

[37] A. Mann and D. Segal, Subgroup growth: some current developments, in *Infinite Groups*, Walter de Gruyter, Berlin, 1996, pp. 179–197. MR 1477175. Zbl 0867.20023.

[38] A. Mann and A. Shalev, Simple groups, maximal subgroups, and probabilistic aspects of profinite groups, *Israel J. Math.* **96** (1996), 449–468. MR 1433701. Zbl 0877.20017. doi: 10.1007/BF02785528.

[39] A. McIver and P. M. Neumann, Enumerating finite groups, *Quart. J. Math. Oxford Ser.* **38** (1987), 473–488. MR 0916229. Zbl 0627.20014.

[40] E. Netto, *Substitutionentheorie und ihre Anwendungen auf die Algebra*, Teubner, Leipzig, 1882, English transl. 1892, second edition, Chelsea, New York, 1964. MR 0175908. JFM 14.0090.01.

[41] P. M. Neumann, An enumeration theorem for finite groups, *Quart. J. Math. Oxford Ser.* **20** (1969), 395–401. MR 0254134. Zbl 0204.34701.

[42] N. Nikolov, On subgroups of finite index in positively finitely generated groups, *Bull. London Math. Soc.* **37** (2005), 873–877. MR 2186720. Zbl 1097.20028. doi: 10.1112/S0024609305004947.

[43] N. Nikolov and D. Segal, On finitely generated profinite groups. I. Strong completeness and uniform bounds, *Ann. of Math.* **165** (2007), 171–238. MR 2276769. Zbl 1126.20018. doi: 10.4007/annals.2007.165.171.

[44] I. Pak, On probability of generating a finite group, preprint, 2009.

[45] I. Pak, What do we know about the product replacement algorithm?, in *Groups and Computation*, III, *Ohio State Univ. Math. Res. Inst. Publ.* **8**, Walter de Gruyter, Berlin, 2001, pp. 301–347. MR 1829489. Zbl 0986.68172.

[46] C. E. Praeger and J. Saxl, On the orders of primitive permutation groups, *Bull. London Math. Soc.* **12** (1980), 303–307. MR 0576980. Zbl 0443.20001. doi: 10.1112/blms/12.4.303.

[47] L. Pyber, Enumerating finite groups of given order, *Ann. of Math.* **137** (1993), 203–220. MR 1200081. Zbl 0778.20012. doi: 10.2307/2946623.

[48] L. Pyber and A. Shalev, Groups with super-exponential subgroup growth, *Combinatorica* **16** (1996), 527–533. MR 1433640. Zbl 0880.20019. doi: 10.1007/BF01271271.

[49] L. Pyber and A. Shalev, Asymptotic results for primitive permutation groups, *J. Algebra* **188** (1997), 103–124. MR 1432350. Zbl 0877.20004. doi: 10.1006/jabr.1996.6818.

[50] ———, Residual properties of groups and probabilistic methods, *C. R. Acad. Sci. Paris Sér. I Math.* **333** (2001), 275–278. MR 1854764. Zbl 0991.20026. doi: 10.1016/S0764-4442(01)02044-4.

[51] M. Quick, Probabilistic generation of wreath products of non-abelian finite simple groups. ii, *Internat. J. Algebra Comput.* **16** (2006), 493–503. MR 2241619. Zbl 1103.20066. doi: 10.1142/S0218196706003074.

[52] J. S. Rose, Automorphism groups of groups with trivial centre, *Proc. London Math. Soc.* **31** (1975), 167–193. MR 0419601. Zbl 0315.20021. doi: 10.1112/plms/s3-31.2.167.

[53] A. Shalev, Simple groups, permutation groups, and probability, in *Proc. Int. Congr. Math.*, *Vol.* II (Berlin, 1998), **Extra Vol. II**, 1998, pp. 129–137. MR 1648063. Zbl 0898.20005.

[54] ———, Asymptotic group theory, *Notices Amer. Math. Soc.* **48** (2001), 383–389. MR 1816298. Zbl 1048.20027.

(Received: August 7, 2007)
(Revised: October 15, 2009)

Departamento de Matemáticas, Universidad Autónoma de Madrid, Spain and Instituto de Ciencias Matemáticas, CSIC-UAM-UC3M-UCM
E-mail: andrei.jaikin@uam.es
http://www.uam.es/personal_pdi/ciencias/ajaikin/welc.html

Alfréd Rényi Institute of Mathematics, Hungarian Academy of Sciences, Budapest, Hungary
E-mail: pyber@renyi.hu
http://www.renyi.hu/~pyber/