ISRAEL JOURNAL OF MATHEMATICS 96 (1996), 449–468

SIMPLE GROUPS, MAXIMAL SUBGROUPS, AND PROBABILISTIC ASPECTS OF PROFINITE GROUPS

BY

AVINOAM MANN AND ANER SHALEV*

Institute of Mathematics, The Hebrew University of Jerusalem
Givat Ram, Jerusalem 91904, Israel
e-mail: mann@math.huji.ac.il and shalev@math.huji.ac.il

In memory of our teacher, colleague, and friend, Shimshon Amitsur

ABSTRACT

We show that a finite simple group has at most $n^{1.875+o(1)}$ maximal subgroups of index n. This enables us to characterise profinite groups which are generated with positive probability by boundedly many random elements. It turns out that these groups are exactly those having polynomial maximal subgroup growth. Related results are also established.

1. Introduction

The determination of the maximal subgroups of finite simple groups has been an active programme of research ever since (and even before) the classification of the finite simple groups; see the recent book [KlLi] and the reference list below. Here we employ the results that were obtained so far to derive some asymptotic results about the number of maximal subgroups, first, in finite simple groups, then in arbitrary finite groups and in profinite groups. These results will enable us to solve some probabilistic questions concerning generation of profinite groups.

* This research was supported by The Israel Science Foundation, administered by The Israel Accademy of Sciences and Humanities.
Received January 12, 1995

Given a group G, we denote by $m_n(G)$ the number of maximal subgroups of G of index n. It turns out that, for almost simple groups G, $m_n(G)$ is polynomially bounded. More precisely we have:

THEOREM 1: *For every $\epsilon > 0$ there is a constant $c = c(\epsilon)$ such that $m_n(G) \leq cn^{1.875+\epsilon}$ for all finite almost simple groups G and for all positive integers n.*

In fact the proof shows that $m_n(G) = n^{1+o(1)}$ if G is a classical group or an alternating group, while $m_n(G) \leq n^{1.875+o(1)}$ if G is an exceptional group of Lie type. The recent work [LiSh1] plays an important role in the proof.

Theorem 1 seems to have a wide range of applications. First, it implies that a finite group G has at most $|G|^c$ maximal subgroups (see Pyber [P]). It is also used in [PSh] to estimate the number of primitive permutation groups of given degree, with applications for counting subgroups of infinite groups. Another consequence of Theorem 1 is the following.

COROLLARY 2: *Fix $\epsilon > 0$ and let $c = c(\epsilon)$ be as above. For a positive integer d set $s = s(d) = \max(d, 3, 1.875 + \epsilon + \log c)$. Then a d-generated finite group has at most $2n^s$ maximal subgroups of index n and trivial core. Equivalently, such a group has at most $2n^s$ faithful primitive permutation representations of degree n (up to equivalence).*

In fact the proof of Corollary 2 yields a slightly better bound, and further improvements are possible. For example, L. Pyber informed us that he can bound s independently of d. However, these improvements do not affect the main results of this paper.

Corollary 2 can be implemented in the study of generation probabilities in profinite groups. Recall that if G is a profinite group, then G, as an inverse limit of finite groups, is compact, and hence has a finite Haar measure, which we normalise so that G has measure 1, and is thus a probability space. The group G is termed **positively finitely generated** (PFG) if for some k the measure $P(G, k)$ of the set of k-tuples generating G is positive (in which case we say that G is positively k-generated). This property was first discussed in the context of field arithmetic [FJ].

In [KaLu] it is shown that a free abelian profinite group of finite rank is PFG, but a free non-abelian profinite group is not PFG. Many more examples are given in [Ma2]; in particular finitely generated prosoluble groups are PFG [Ma2, Theorem 10], as are the profinite completions of $\mathrm{SL}_d(\mathbb{Z})$ for $d \geq 3$ [Ma2, Theorem

15]. In fact we can generalise this as follows:

PROPOSITION 3: *Let k be a global field of arbitrary characteristic, S a finite set of valuations of k, and $\mathcal{O}_S$ the ring of S-integers of k. Let G be a simply connected simple algebraic group defined over k, and let $\Gamma = G(\mathcal{O}_S)$. Suppose Γ has the congruence subgroup property. Then the profinite completion of Γ is positively finitely generated.*

We shall not include the proof of Proposition 3, since a much stronger result has just been proved in [BPSh]. It is shown there that every finitely generated profinite group G satisfying the Babai–Cameron–Pálfy type restrictions on its upper composition factors (see [BCP]) is positively finitely generated. Other examples of PFG groups occur in Bhattacharjee's work [Bh].

Most proofs that a group G is PFG proceed by showing that G has another property, that of **polynomial maximal subgroup growth** (PMSG), where by this we mean that there exists a number s, such that $m_n(G) \leq n^s$ for all n.

Let G be a profinite group satisfying $m_n(G) \leq n^s$ for all n. Then a k-tuple of elements of G generates a proper subgroup if and only if these k elements lie in some maxim l subgroup, and the probability of that is at most $\sum_{n\geq 2} m_n(G)n^{-k} \leq \sum_{n\geq 2} n^{s-k}$. Since for $k \geq s+2$ the above sum is less than 1, we see that for these values of k, a k-tuple generates G with positive probability. This simple argument shows that every PMSG profinite group is PFG.

The combination of Corollary 2 with the Borel–Cantelli lemma (see Section 4 below) enables us to prove the converse. We therefore obtain the following characterisation of PFG groups:

THEOREM 4: *A profinite group is positively finitely generated if and only if it is of polynomial maximal subgroup growth.*

Of course, this characterisation, as well as most of our results, rely heavily on the Classification of finite simple groups.

The proof of Theorem 4 shows that, if d elements generate G with positive probability, and $s = s(d)$ is as in Corollary 2, then the sum $\sum_{n\geq 2} m_n(G)n^{-d-s}$ converges; in particular, $m_n(G) = o(n^{d+s(d)})$.

The above characterisation of PFG groups yields the following:

COROLLARY 5: *The collection of finitely generated residually finite PMSG groups is extension-closed.*

Indeed, a similar result is proved in [Ma2, Proposition 7] for PFG groups. We are not aware of a direct (or indeed, a Classification-free) proof of this result.

Apart from the notion of PFG groups, some related notions have been examined in [Ma2]. Given a profinite group G and a natural number k, let $Q(G,k)$ denote the probability that k random elements of G generate a finite index subgroup of G. It is known that $Q(G,k) > 0$ if and only if G is a PFG group [Ma2, Proposition 8]. However, while we cannot have $P(G,k) = 1$ (unless $G = 1$), the equality $Q(G,k) = 1$ is certainly possible, and it would be interesting to find the groups for which it holds.

It is easy to see that PSG groups (i.e. groups of polynomial subgroup growth) satisfy $Q(G,k) = 1$ for some k, but the converse was not clear. In Section 5 we construct many examples of non-PSG groups satisfying $Q(G,k) = 1$ (for suitable k). In particular we obtain the following.

PROPOSITION 6: *Let $d \geq 3$ and let G be the profinite completion of $\mathrm{SL}_d(\mathbb{Z})$. Then, for some k, almost all k-tuples of elements of G generate a finite index subgroup.*

Since every group satisfying $Q(G,k) = 1$ is a PFG group, Proposition 6 extends [Ma2, Theorem 15] mentioned above.

A similar result holds for S-arithmetic groups in characteristic 0 which satisfy the congruence subgroup property. The case of arithmetic groups in positive characteristic remains unclear.

In our final result we continue the interplay between probabilistic results and growth behaviour. More specifically, we apply probabilistic arguments in order to shed some light on the number of generators of open subgroups in PSG groups. Recall that, while finitely generated residually finite PSG *abstract* groups have finite rank [LMS], this is not the case for PSG profinite groups. However, we show below that the number of generators of open subgroups in PSG profinite groups grows rather slowly.

THEOREM 7: *Let G be a profinite group of polynomial subgroup growth. Then there exists a constant c such that*

$$d(H) \leq c \cdot \sqrt{\log |G\colon H|},$$

for all open subgroups H of G.

It can be shown that the bound given in Theorem 7 is best possible.

We conclude the introduction by stating a conjecture.

CONJECTURE: *For every $\epsilon > 0$ there is $N = N(\epsilon)$ such that, if G is a finite almost simple group and $n > N(\epsilon)$, then $m_n(G) < n^{1+\epsilon}$.*

This conjecture is proved here for alternating groups, classical groups, as well as small rank exceptional groups. It remains to deal with the groups of type F_4, E_6, ${}^2E_6$, E_7 and E_8. The current information on maximal subgroups of these groups seems insufficient for that purpose.

Some words on the structure of this paper. Section 2 is devoted to the proof of Theorem 1. In Section 3 we use the O'Nan–Scott Theorem in order to deduce Corollary 2 from Theorem 1. Theorem 4 is proved in Section 4. In Section 5 we construct non-PSG groups satisfying $Q(G,k) = 1$. This is where Proposition 6 is proved. The last section is devoted to the proof of Theorem 7.

Notation: The notation is mostly standard. Logarithms are to the base 2. The core H_G of a subgroup $H \subseteq G$ is the maximal normal subgroup of G which is contained in H. By a simple group we mean a nonabelian finite simple group. An almost simple group is a group lying between a simple group and its automorphism group. The socle of a finite group G is denoted by $\mathrm{Soc}(G)$. The (minimal) number of generators of a group G is denoted by $d(G)$. The rank of G is the supremum of $d(H)$ over the finitely generated subgroups H of G. If G is a profinite group then $d(G)$ is interpreted topologically, and subgroups H of G are assumed to be closed. In particular, by a maximal subgroup of a profinite group we mean a closed maximal subgroup, and such subgroups are always open (hence of finite index). Finally, we let $a_n(G)$ denote the number of subgroups of index n in a group G.

2. Counting maximal subgroups: simple groups

Let T be a finite simple group and let $T \subseteq G \subseteq \mathrm{Aut}(T)$. We may ignore finitely many simple groups and assume that T is alternating or of Lie type. We shall sometimes count maximal subgroups of G up to conjugacy, taking into account the fact that a subgroup of index n has at most n conjugates. It is easy to see that G/T has at most $O(n)$ subgroups of index n; this follows from the fact that $\mathrm{Out}(T)$ is metacyclic-by-bounded. It therefore suffices to count maximal subgroups of G which do not contain T.

We note that some of the bounds we shall give may be significantly improved with a bit more careful analysis.

LEMMA 8: *For every $\epsilon > 0$ there is $N = N(\epsilon)$ such that, if* $\mathrm{Soc}(G)$ *is alternating and $n > N(\epsilon)$, then $m_n(G) < n^{1+\epsilon}$.*

Proof: We may assume $G = S_k$, the case $G = A_k$ being similar. We may also disregard finitely many alternating groups and assume that $k \geq 13$. Let $H \subseteq S_k$ be a maximal subgroup of index n not containing A_k. Then $k \leq n$. We distinguish between the following cases:

1. H is not transitive.

Then $H \cong S_{k_1} \times S_{k_2}$ with the natural intransitive action (where $k_1 + k_2 = k$). Obviously the index of H in G determines the pair $\{k_1, k_2\}$, and so H is uniquely determined by n up to conjugacy.

2. H is transitive but not primitive.

Then $H \cong S_{k_1} \wr S_{k_2}$ with the (transitive) imprimitive action, where $k_1 k_2 = k$. Again it is easy to verify that the index n of H determines H up to conjugacy.

3. H is primitive.

Since H does not contain A_k, the order of H is rather small, and so its index n is rather close to $k!$. For our purpose it suffices to use Bochert's 19th century result, showing that the index of H is at least $[(k+1)/2]!$ (see [Wi, p. 41]). This yields $n \geq [(k+1)/2]! \geq 2^k$ (recall that $k \geq 13$). It follows that $k \leq \log n$.

By a result of Babai [B] (which applies the Classification Theorem), S_k has at most $c^{(\log k)^4}$ conjugacy classes of primitive maximal subgroups. Note that

$$c^{(\log k)^4} \leq c^{(\log \log n)^4} = n^{o(1)}.$$

We conclude that S_k has at most $n^{1+o(1)}$ maximal subgroups of index n. ∎

LEMMA 9: *For every $\epsilon > 0$ there is $N = N(\epsilon)$ such that, if* $\mathrm{Soc}(G)$ *is a classical group and $n > N(\epsilon)$, then $m_n(G) < n^{1+\epsilon}$.*

Proof: Write $T = \mathrm{Soc}(G) = X_k(q)$, where k is the dimension of the natural module, and $q = p^e$ is the order of the underlying field. Note that

$$|G| > q^{\delta k^2}$$

for a suitable constant $\delta > 0$.

By a recent result of Guralnick, Kantor and Saxl [GKS, Theorem 2.7], G has at most $c_1(k)(\log q)^{\log k}$ conjugacy classes of maximal subgroups, where $c_1(k)$ is a constant depending on k. Suppose first that k is bounded, say $k \leq c_2$. Then $c_1(k)(\log q)^{\log k} = |G|^{o(1)}$. Note that, if n is the index of a maximal subgroup M of G (not containing T), then $|G| \leq n^{c_3}$ where c_3 depends on c_2 (see [KlLi, 5.2.2]). Thus the number of conjugacy classes of such maximal subgroups M is at most $n^{c_3 o(1)} = n^{o(1)}$.

It remains to deal with classical groups in unbounded dimension k. By a theorem of Liebeck [Li], the maximal subgroups M of G are either of known types, or they are almost simple, with $|M| < q^{3k}$. In the first case the conjugacy classes of the subgroups M are known, and it is easily verified that there are $n^{o(1)}$ classes of such subgroups of index n. See, for instance, [GKS, Lemma 2.1]. So it suffices to consider the almost simple subgroups M satisfying $|M| < q^{3k}$.

Let M be such a subgroup and let S be the socle of M. Then $M = N_G(S)$, so it suffices to count the possibilities for S. We follow the method of [KaLu]. It is known that the covering group $\widetilde{S}$ of S acts absolutely irreducibly on the natural module V of T. Hence the number of choices for S up to conjugacy can be estimated by bounding the number of absolutely irreducible representations of $\widetilde{S}$ in characteristic p.

Let $s = |S|$ and $t = q^{3k}$. Then $|\operatorname{Out}(S)| \leq \log s \leq \log t$, and this implies that, given n, there are at most $\log t$ choices for s. Now, fixing s, there are at most 2 possibilities for the simple group S up to isomorphism, and the covering group of S has at most $s \log s \leq t \log t$ absolutely irreducible representations in characteristic p. Any such representation corresponds to a Δ-conjugacy class of subgroups of G which are isomorphic to S, where Δ is the normalizer of G in the respective projective group $\mathrm{PGL}(V)$. It is known that a Δ-conjugacy class of a subgroup of G breaks into at most k conjugacy classes in G.

Altogether it follows that there are at most

$$B := 2 \cdot \log t \cdot t \log t \cdot k = 18k^3 \log^2 q \cdot q^{3k}$$

conjugacy classes for M (given its index n). Recall that $n > |G|q^{-3k} > q^{\delta k^2 - 3k}$. Fixing $\epsilon > 0$ and choosing $c_2 = c_2(\epsilon)$ large enough, we obtain $B < n^{\epsilon}$. This completes the proof. ∎

We now deal with exceptional groups of Lie type.

LEMMA 10: *For every $\epsilon > 0$ there is $N = N(\epsilon)$ such that, if $T = \mathrm{Soc}(G)$ is an exceptional group of Lie type and $n > N(\epsilon)$, then the following hold:*

(i) $m_n(G) < n^{1+\epsilon}$ *if T is of type ${}^2B_2$, G_2, ${}^2G_2$, ${}^3D_4$, or ${}^2F_4$.*

(ii) $m_n(G) < n^{1+7/8+\epsilon}$ *if T is of type F_4.*

(iii) $m_n(G) < n^{1+4/5+\epsilon}$ *if T is of type E_6 or ${}^2E_6$.*

(iv) $m_n(G) < n^{1+70/103+\epsilon}$ *if T is of type E_7.*

(v) $m_n(G) < n^{1+2/3+\epsilon}$ *if T is of type E_8.*

Proof: Let G, T be as above. As before, it suffices to count maximal subgroups of G not containing T. Given the fact that G has such a subgroup of index n, we obtain $|G| \leq n^c$ for some absolute constant c (this is a particular case of [BCP]). This implies that $|\mathrm{Out}(T)| \leq O(\log n)$, an inequality which will be useful in what follows.

By Theorem 2 of Liebeck and Seitz [LiSe], if H is a maximal subgroup of G (not containing T), then one of the following holds:

1. H is a parabolic subgroup.
2. H is a subgroup of maximal rank (see [LSS] for the terminology).
3. $H = N_G(E)$, the normalizer of an elementary abelian subgroup E.
4. $H = C_G(\sigma)$, the centralizer of an automorphism $\sigma \in \mathrm{Aut}(T)$ whose order is prime; moreover, σ is a field automorphism, or a graph automorphism, or a graph-field automorphism.
5. The generalized Fitting subgroup $F^*(H)$ of H is a direct product of 2 or 3 simple groups of known types (cf. [LiSe, pp. 355–356]).
6. H is almost simple.

We claim that there are $n^{o(1)}$ conjugacy classes of subgroups H of types 1–5.

Clearly, there are $O(1)$ conjugacy classes of parabolic subgroups in G. Now, the maximal subgroups of type 2 are determined by Liebeck, Saxl and Seitz [LSS]. It is clear from the main theorem and table 5.1 of [LSS] that there are $O(1)$ choices for H up to conjugacy. The maximal subgroups of type 3 are determined by Cohen, Liebeck, Saxl and Seitz [CLSS]. By Theorem 1 and table 1 there, E is uniquely determined given T up to conjugacy in $\mathrm{Aut}(T)$. Note that $|\mathrm{Aut}(T)\colon G| \leq |\mathrm{Out}(T)| \leq O(\log n)$. It follows that, up to conjugacy in G, E can be chosen in $O(\log n)$ ways. In case 4, note that σ can be chosen in at most $|\mathrm{Out}(T)| \leq O(\log n)$ ways (up to conjugacy), and this bounds the number of choices for H up to conjugacy. Conjugacy classes of subgroups of type 5 are determined in [LiSe], and there are $O(1)$ of them. This proves the claim.

It remains to enumerate maximal subgroups of type 6. If T is of type ${}^2B_2$, G_2, ${}^2G_2$, ${}^3D_4$, or ${}^2F_4$ then the conjugacy classes of such subgroups are also known (cf. [Su], [Co], [A2], [Kl1], [Kl2], [M]) and it easily follows that there are $O(1)$ conjugacy classes. Thus part (i) of the lemma follows.

So assume that T is of type F_4, E_6, ${}^2E_6$, E_7, or E_8. Let H be an almost simple maximal subgroup of G and let S be the simple socle of H. By [LiSh1, Section 1] we may assume that S is of Lie type and that its (untwisted) Lie rank is at most half of the Lie rank of G, otherwise there are at most $c \log q < c' \log n$ choices for H up to conjugacy. Applying Theorem 1.2 of [LiSh1] we conclude that

$$|H| < 12q^a \log_p q, \tag{1}$$

where $a = 20, 28, 28, 30, 56$ if $T = F_4$, E_6, ${}^2E_6$, E_7, E_8 respectively. This yields

$$n = |G|/|H| > |G|/(12q^a \log_p q) > \frac{1}{24 \log_p q} \cdot q^{b-a},$$

where $b = 52, 78, 78, 133, 248$ respectively. It easily follows that

$$q < n^{(b-a)^{-1}+o(1)}. \tag{2}$$

Clearly, $S = \mathrm{Soc}(H)$ is a subgroup of T and $H = N_G(S)$. To count the number of choices for the subgroup S of T we use Lemma 3.1 of [LiSh1], according to which

$$\sum |S| \le |T| i(T),$$

where S ranges over all simple subgroups of T and $i(T)$ is the number of involutions in T. In our case $|S| \le n$ (as follows from (1) and (2)) and $|H/S| \le |\mathrm{Out}(S)| \le \log n$. Thus $|S| \ge |H|/\log n = |G|/(n \log n)$. By restricting the above sum to subgroups of order $\ge |G|/(n \log n)$, we see that there are at most

$$n \log n |T| i(T)/|G| \le n \log n \cdot i(T)$$

choices for $S \subseteq T$.

It remains to evaluate the number of involutions $i(T)$ in the respective groups T. By the proof of [LiSh1, Proposition 2.1] we have $i(T) < cq^d$ where c is an absolute constant and $d = 28, 40, 40, 70, 128$ if $T = F_4$, E_6, ${}^2E_6$, E_7, E_8 respectively. We see that the number of possibilities for H is at most $n \log n \cdot q^d = n^{1+o(1)} \cdot q^d$. In view of (2) we conclude that H can be chosen in at most

$$n^{1+\frac{d}{b-a}+o(1)}$$

ways. Substituting the values for a, b, d we obtain the result. ∎

Theorem 1 is proved.

3. Counting maximal subgroups: finite groups

Recall that the maximal subgroups with trivial core of a finite group are described by the result known as the O'Nan–Scott Theorem. There are several versions of this result (see, e.g., [LPS], as well as [AS] for a more refined version). We shall need only the weak version below. Before stating it we recall that a **diagonal** subgroup of a direct product $T_1 \times \cdots \times T_k$ of isomorphic groups $\{T_i\}$ is a subgroup D for which the projection on each component T_i is an isomorphism between D and T_i.

O'NAN–SCOTT THEOREM: *Let G be a finite group and let M be a minimal normal subgroup of G, so that $M = T_1 \times \cdots \times T_k$ for some set of isomorphic simple subgroups T_i. Let H be a maximal subgroup of G with a trivial core. Then H belongs to one of the following types.*

1. *H is a complement of M.*
2. *$N := H \cap M \neq 1$, $H = N_G(N)$, the subgroups $\{T_i\}$ are non-abelian and constitute a full conjugacy class of subgroups, and either*

2a. *$N = N_1 \times \cdots \times N_k$, where N_i is a proper subgroup of T_i and the N_i's are conjugate in H, or*

2b. *There exists a partition $\{1, \ldots, k\} = \bigcup_{i=1}^{r} A(i)$, such that $N = D_1 \times \cdots \times D_r$, where D_i is a diagonal subgroup of $\prod_{j \in A(i)} T_j$ and the subgroups $\{D_i\}$ are conjugate in H.*

(For a given index n, there cannot exist maximal subgroups both of type 1 and of type 2.)

We now count the number of maximal subgroups of G with a trivial core and index n. Using the notation of the above result, we begin with the complements of M. If H is one of them, and K another one, then each element $x \in K$ can be written as $x = hm(h)$, where $h \in H$ and $m(h) \in M$. The function $h \mapsto m(h)$ is a so-called crossed homomorphism, i.e. it satisfies $m(h_1 h_2) = m(h_1)^{h_2} m(h_2)$. From this equation it is clear that the crossed homomorphism in question, and with it K, is determined by its values on a set of generators for H. Since $H \cong G/M$, the group H is also generated by d elements, and therefore the number of crossed homomorphisms from H to M is at most $|M|^d = n^d$.

Next let H be of type 2a. Denote $L = N_H(N_1) = N_H(T_1)$. Then L is just the stabiliser of 1 in the transitive permutation representation of H on the set of indices $\{1, \ldots, k\}$. Let R_1 be an L-invariant subgroup of T_1 containing N_1, and let $R_2, \ldots, R_k$ be the H-conjugates of R_1. We choose the notation so that $R_i \subseteq T_i$, and then $R = R_1 \times \cdots \times R_k$ is H-invariant and HR is a subgroup of G; hence either $HR = H$ or $HR = G$; this means that $R_1 = N_1$ or T_1. Thus N_1 is a maximal L-invariant subgroup of T_1, and similarly for $N_2, \ldots, N_k$.

We write $C = C_{LT_1}(T_1)$ and $S = LT_1/C$. Then S is an almost simple group with socle T_1, and $K = LN_1$ is a maximal subgroup of S satisfying $K \cap T_1 = N_1$. Here $|S\colon K| = |T_1\colon N_1| = m$, say, so $n = |G\colon H| = m^k$ and $k \leq \log n$. Now Theorem 1 shows that the number of possibilities for choosing K, and with it N_1, is at most $cm^{1.875+\epsilon}$, and similarly for $N_2, \ldots, N_k$. Thus the number of possibilities for choosing N, and with it H, is at most $(cn^{1.875+\epsilon})^k = c^k n^{1.875+\epsilon} \leq n^{\log c + 1.875 + \epsilon}$.

Finally, let H be of type 2b. To determine the number of possibilities in this case we have first to determine the number of allowed partitions of $\{1, \ldots, k\}$. Each such partition is a system of imprimitivity for the permutation group that G induces on $\{1, \ldots, k\}$. Denoting $L = N_G(T_1)$, such systems of imprimitivity correspond to subgroups of G containing L. Since $|G\colon L| = k$, each such subgroup is generated by L and at most further $\log k$ elements; replacing a generator by another element of the same coset of L does not change the subgroup, so the number of subgroups is at most $k^{\log k}$. Now $n = |G\colon H| = |M\colon N| = |T_1|^{k-r}$, and if $t = |A(1)|$, then $t \geq 2$ (otherwise $N = M$), so $r = k/t \leq k/2$, thus $k \leq \log n$ and $k^{\log k} \leq n$.

Once the partition $\{A(i)\}$ is given, the subgroup D_1 is determined by a set of isomorphisms between T_1 and the other T_j's for $j \in A(1)$, and the number of choices for these isomorphisms is $|\operatorname{Aut}(T_1)|^{t-1}$, and similarly for the other D_i's; hence the number of possibilities for D is $|\operatorname{Aut}(T_1)|^{(t-1)r} \leq |T_1|^{2(t-1)r} = n^2$. Here we have used the very crude estimate $|\operatorname{Aut}(T_1)| \leq |T_1|^2$, which follows, e.g., from the fact that T_1 can be generated by 2 elements, and the equalities $n = |M\colon N|$, $|M| = |T_1|^k = |T_1|^{rt}$, $|N| = |D_1|^r = |T_1|^r$. Altogether we find that there are at most n^3 possibilities for choosing H in case 2b.

Note that, given the index n, some of the maximal subgroups of index n may be of type 2a, and some of type 2b. It follows that the number of maximal

subgroups of index n with trivial core is at most

$$\max(n^d, n^{1.875+\epsilon+\log c} + n^3) \leq 2n^{s(d)}.$$

This completes the deduction of Corollary 2 from Theorem 1.

Remark: If the minimal normal subgroup M is abelian then, as is well known, all maximal subgroups of trivial core are complements of M, and their number is $n|H^1(G, M)|$. Moreover, $|H^1(G, M)| \leq n^{2/3}$ in this case [Gu, Theorem B], yielding a better value for s.

4. Characterising PFG groups

In this section we apply the results obtained so far in order to prove Theorem 4. We start by quoting the following well known probabilistic result.

BOREL–CANTELLI LEMMA ([Re, pp. 389–392]): *Let X_i be a series of events in a probability space X with probabilities p_i.*

(i) *If X_i are pairwise independent and $\sum p_i$ diverges, then the probability that infinitely many of the X_i happen is* 1.

(ii) *If $\sum p_i$ converges, then the probability that infinitely many of the X_i happen is* 0.

Now, let G be a PFG profinite group, and suppose d elements generate G with positive probability. Let X be the product G^d of d copies of G (with a normalised Haar measure), considered as a probability space.

If H and K are two finite index subgroups of G, then the events H^d and K^d are independent exactly when

$$|G: H \cap K| = |G: H||G: K|,$$

which is equivalent to $G = HK$. Suppose that H and K are maximal subgroups, and that they have distinct cores. Then we may assume, without loss of generality, that $H_G \not\subseteq K_G$. It follows that H_G is not contained in K, so that $H_G K = G$ (by the maximality of K). This in turn yields $HK = G$. We conclude that, if $H, K \subset G$ are maximal subgroups with distinct cores, then H^d and K^d are independent events in the probability space X.

Let N_i be an enumeration of all cores of maximal subgroups of G (each core occurring only once). For each core N_i choose a maximal subgroup M_i such that

$(M_i)_G = N_i$, and let $c_n(G)$ be the number of the maximal subgroups of index n obtained in this way. Let X_i be the event defined by M_i^d in X. By construction X_i are independent events whose probabilities are $p_i = |G: M_i|^{-d}$ respectively. Note that

$$\sum p_i = \sum_{n \geq 2} c_n(G) n^{-d}.$$

If the right hand side diverges then the Borel–Cantelli Lemma shows that, with probability 1, a d-tuple belongs to infinitely many of the M_i's, so the set of d-tuples generating G has measure 0. This contradicts our choice of d. We conclude that

$$\sum_{n \geq 2} c_n(G) n^{-d} < \infty.$$

Consequently we have $c_n(G) = o(n^d)$ (in fact, using a quantitative version of the Borel–Cantelli Lemma it can be shown that $\sum_{n \geq 2} c_n(G) n^{-d} \leq 1/P(G,d)$; in particular, $c_n(G) \leq n^d / P(G,d)$ for all n).

We now apply Corollary 2 for each group G/N_i, where N_i is the core of a maximal subgroup of index n. Since G can be generated by d elements we conclude that

$$m_n(G) \leq c_n(G) \cdot 2n^{s(d)}.$$

It follows that

$$m_n(G) = o(n^{d+s(d)}).$$

Therefore G is a PMSG group.

Theorem 4 is proved.

Remarks: 1. If d is large and G is positively d-generated, then we obtain $m_n(G) = o(n^{2d})$.

2. The proof given above actually holds under the weaker assumption that $Q(G,d) > 0$ (recall that $Q(G,d)$ denotes the probability that d random elements of G generate a finite index subgroup).

5. The probability of generating a finite index subgroup

In this section we give some conditions which imply the equality $Q(G,k) = 1$. In particular, we shall construct various non-PSG groups in which k random elements generate a finite index subgroup with probability 1.

Let G be a profinite group, and let F be a collection of open subgroups of G. We shall say that F is a **cover** if every closed subgroup H of infinite index in G is contained in infinitely many subgroups from F. We denote by $a_n(G,F)$ the number of subgroups $H \in F$ satisfying $|G\colon H| = n$. The collection F will be called **polynomial** if, for some c, $a_n(G,F) \leq n^c$ for all n.

LEMMA 11: *Let G be a profinite group which admits a polynomial cover. Then $Q(G,k) = 1$ for some k.*

Proof: For each subgroup $M \in F$, let X_M be the event M^k inside the probability space $X = G^k$. Then X_M occurs with probability $|G\colon M|^{-k}$, and $\sum_{M\in F} |G\colon M|^{-k} = \sum_{n\geq 1} a_n(G,F)n^{-k}$. Suppose $a_n(G,F) \leq n^c$ for all n. Choosing $k > c+1$, we see that

$$\sum_{M\in F} P(X_M) \leq \sum_n n^{c-k} < \infty,$$

where P is the probability measure on X. By part (ii) of the Borel–Cantelli Lemma we conclude that, with probability 1, only finitely many of the events X_M happen. This means that, if $x_1, \ldots, x_k$ are k random elements of G, and H is the closed subgroup they generate, then, with probability 1, H is contained in only finitely many subgroups $M \in F$. Since F is a cover it follows that, with probability 1, $|G\colon H| < \infty$. ∎

COROLLARY 12: *Let G be a profinite PMSG group with the property that every closed subgroup $H \subset G$ of infinite index is contained in infinitely many maximal subgroups $M \subset G$. Then $Q(G,k) = 1$ for some k.*

Proof: In this case the collection of maximal subgroups of G is a polynomial cover. ∎

It would be interesting to find out which profinite groups satisfy the conditions of Corollary 12. One type of example is given below. Let G be the Cartesian product of infinitely many pairwise non-isomorphic finite simple groups T_i. It is easy to see that every maximal subgroup of G is of the form $M_i \times \prod_{j\neq i} T_j$, where M_i is a maximal subgroup of T_i (see, e.g., [Ma2, Lemma 16]). Now, let H be a closed subgroup of G, and suppose H is contained in only finitely many maximal subgroups. Then there exists a finite set S such that, if $i \notin S$, then H is mapped onto T_i by the natural projection $G \to T_i$. By the structure of the

maximal subgroups of $\prod_{i\notin S} T_i$ we see that H is mapped onto $\prod_{i\notin S} T_i$. Hence $H \cdot \prod_{i\in S} T_i = G$, and since $\prod_{i\in S} T_i$ is finite we have $|G\colon H| < \infty$.

It follows from the above discussion that

$$m_n(G) = \sum_i m_n(T_i).$$

Using Theorem 1 we have $m_n(T_i) \leq cn^{1.875+\epsilon}$. This yields

$$m_n(G) \leq f(n) \cdot cn^{1.875+\epsilon},$$

where $f(n)$ equals the number of indices i such that T_i has a maximal subgroup of index n.

Using the information on the minimal degrees of permutation representations for the finite simple groups (see [KlLi, 5.2.2] and [LaSe]), it is straightforward to verify that $f(n) \leq Cn$ for some absolute constant C (and by letting T_i range over certain families of simple groups, $f(n)$ can be made much smaller). We conclude that

$$m_n(G) = O(n^{2.875+\epsilon}).$$

Thus G is a PMSG group.

We have proved that $G = \prod T_i$ satisfies the conditions of Corollary 12. It follows that $Q(G,k) = 1$ for some k (in fact, using results from [LiSh1], [LiSh2], it can be shown that $k = 3$ will always do, and quite often we can take $k = 2$). On the other hand, there are many ways to choose T_i such that the resulting group G is not a PSG group.

Proof of Proposition 6: It is well known that $G \cong \prod_p \mathrm{SL}_d(\mathbb{Z}_p)$, where p ranges over the rational primes. Let F be the collection of all open subgroups of G which have the form $H_p \times \prod_{q\neq p} \mathrm{SL}_d(\mathbb{Z}_q)$, where p is a prime and H_p is an open subgroup of $\mathrm{SL}_d(\mathbb{Z}_p)$. We claim that F is a polynomial cover.

First note that there is a constant c (depending only on d) such that $a_n(\mathrm{SL}_d(\mathbb{Z}_p)) \leq n^c$ for all n and p. This follows, for instance, from [Sh2, Prop. 1.1], using the fact that the rank of $\mathrm{SL}_d(\mathbb{Z}_p)$ is bounded in terms of d alone. By the definition of F we see that

$$a_n(G,F) = \sum_p a_n(\mathrm{SL}_d(\mathbb{Z}_p)) \leq f(n)n^c,$$

where $f(n)$ equals the number of primes p with the property that $\mathrm{SL}_d(\mathbb{Z}_p)$ has a subgroup of index n. Since the minimal index of a proper subgroup of $\mathrm{SL}_d(\mathbb{Z}_p)$

is bounded below by p, it follows that $f(n) \leq n$ (in fact $f(n) = o(n^{1/(d-1)})$). We see that $a_n(G, F) \leq n^{c+1}$, so F is a polynomial collection.

It remains to show that F is a cover. Let $H \subset G$ be a closed subgroup which is contained in only finitely many members of F. Then we immediately see that H is mapped onto $\mathrm{SL}_d(\mathbb{Z}_p)$ for almost all p, and so there is a finite set S of primes such that $H \supseteq \prod_{p \notin S} \mathrm{SL}_d(\mathbb{Z}_p)$.

Fix a prime $p \in S$. Then the image of H under the projection $G \to \mathrm{SL}_d(\mathbb{Z}_p)$ is contained in only finitely many open subgroups of $\mathrm{SL}_d(\mathbb{Z}_p)$. Therefore this image has finite index in $\mathrm{SL}_d(\mathbb{Z}_p)$, and this is valid for each $p \in S$. It follows easily that $|G: H| < \infty$.

We have shown that F is a polynomial cover. Proposition 6 now follows by applying Lemma 11.

Recall that $\mathrm{SL}_d(\mathbb{Z})$ is not a PSG group (see [Lu] for its precise growth type).

Finally, note that Lemma 11, the fact that $Q(G, k) = 1$ implies that G is PFG, and Theorem 4 give rise to the following result on the subgroup structure of profinite groups.

COROLLARY 13: *Let G be a profinite group which admits a polynomial cover. Then G has polynomial maximal subgroup growth.*

It would be interesting to try to find a Classification-free proof of this result.

6. The rank function

In this section we use probabilistic ideas in order to shed some light on the relation between rank and subgroup growth.

While finitely generated residually finite abstract groups of polynomial subgroup growth have finite rank [LMS], this is not the case for profinite groups. Examples of finitely generated PSG profinite groups of infinite rank were constructed in [MS]. Such examples also give rise to countably generated residually finite (abstract) PSG groups of infinite rank. The structure of such groups is not well-understood.

In view of this situation it makes sense to pose the following question: *assuming G is a PSG profinite group, how fast can the number of generators of open subgroups of G tend to infinity?* We remark that, by [Ma1, Theorem 2], PSG profinite groups are always finitely generated (as profinite groups), and so are their open subgroups.

The information we need is encoded in the following function, which will be referred to as the **rank function** of G:

$$r_n(G) = \max\{d(H)\colon\ H \text{ is an open subgroup of } G \text{ with } |G\colon H| \leq n\}.$$

Note that $r_n(G)$ (as a function of n) is monotonically increasing, and that it is bounded if and only if G has finite rank. Note also that, by [Sh1, Lemma 2.4], if G is a pro-p group and $r_n(G)$ is unbounded, then $r_n(G) \geq c \log n$ for all n (where $c > 0$ is a suitable constant). Of course, if G is a free profinite group on $d > 1$ generators, then $r_n(G)$ grows linearly with n. However, for PSG groups one expects a much slower rate of growth. Indeed, in [Ma1, Theorem 5] it is shown that $r_n(G) = o(\log n)$ for a PSG profinite group G. In this section we modify that proof to find the fastest possible growth of the rank function in such groups, showing that

$$r_n(G) = O(\sqrt{\log n}) \quad \text{for all PSG groups } G. \tag{3}$$

To prove (3), let G be a PSG profinite group, and suppose $a_n(G) \leq n^c$ for all n. Let $H \subseteq G$ be an open subgroup of index n. Let $P(H, k, m)$ be the probability that k elements chosen at random from H generate a subgroup of index $> m$ in H. Then

$$P(H,k,m) \leq \sum_{i>m} a_i(H) i^{-k} \leq \sum_{i>m} a_{ni}(G) i^{-k} \leq \sum_{i>m} (ni)^c i^{-k}.$$

This yields

$$P(H,k,m) \leq n^c \sum_{i>m} i^{c-k}.$$

Setting $k = c + r + 1$ for $r \geq 1$ we obtain $\sum_{i>m} i^{c-k} = \sum_{i>m} i^{-r-1} < m^{-r}$. Suppose m and r are chosen so that

$$m^r \geq n^c. \tag{4}$$

Then $P(H,k,m) < n^c m^{-r} \leq 1$. This implies that a certain k-tuple from H generates a subgroup M of index at most m in H, and so

$$d(H) \leq d(M) + \log |H\colon M| \leq k + \log m = c + r + 1 + \log m. \tag{5}$$

Let r, m be the minimal integers such that $r \geq \sqrt{c \log n}$ and $\log m \geq \sqrt{c \log n}$. Then $r \log m \geq c \log n$, so condition (4), and with it (5), are satisfied. Using the

obvious inequalities $r, \log m \leq \sqrt{c \log n} + 1$ we obtain

$$d(H) \leq 2\sqrt{c}\sqrt{\log n} + c + 3.$$

Thus (3) follows, and with it Theorem 7. ∎

It will be shown in [Sh2] that the bound in (3) is best possible: there exists a PSG profinite group G and a constant $c > 0$ such that $r_n(G) \geq c\sqrt{\log n}$ for all n. The group constructed is a Cartesian product of certain (carefully chosen) finite simple groups, and the construction relies heavily on number-theoretic methods.

References

[A1] M. Aschbacher, *On the maximal subgroups of the finite classical groups*, Inventiones mathematicae **76** (1984), 469–514.

[A2] M. Aschbacher, *Chevalley groups of type $G_2(q)$ as the group of a trilinear form*, Journal of Algebra **109** (1987), 193–259.

[AS] M. Aschbacher and L. Scott, *Maximal subgroups of finite groups*, Journal of Algebra **92** (1985), 44–80.

[B] L. Babai, *The probability of generating the symmetric group*, Journal of Combinatorial Theory, Series A **52** (1989), 148–153.

[BCP] L. Babai, P. J. Cameron and P. P. Pálfy, *On the orders of primitive permutation groups with restricted nonabelian composition factors*, Journal of Algebra **79** (1982), 161–168.

[Bh] M. Bhattacharjee, *The probability of generating certain profinite groups by two elements*, Israel Journal of Mathematics **86** (1994), 311–329.

[BPSh] A. Borovik, L. Pyber and A. Shalev, *Maximal subgroups of finite and profinite groups*, Transactions of the American Mathematical Society, to appear.

[C] P. J. Cameron, *Finite permutation groups and finite simple groups*, The Bulletin of the London Mathematical Society **13** (1981), 1–22.

[Co] B. N. Cooperstein, *Maximal subgroups of $G_2(2^n)$*, Journal of Algebra **70** (1981), 23–36.

[CLSS] A. M. Cohen, M. W. Liebeck, J. Saxl and G. M. Seitz, *The local maximal subgroups of exceptional groups of Lie type, finite and algebraic*, Proceedings of the London Mathematical Society (3) **64** (1992), 21–48.

[FJ] M. D. Fried and M. Jarden, *Field Arithmetic*, Springer, Berlin, 1986.

[Gu] R. M. Guralnick, *Generation of simple groups*, Journal of Algebra **103** (1986), 381–401.

[GKS] R. M. Guralnick, W. M. Kantor and J. Saxl, *The probability of generating a classical group*, Communications in Algebra **22** (1994), 1395–1402.

[KaLu] W. M. Kantor and A. Lubotzky, *The probability of generating a classical group*, Geometriae Dedicata **36** (1990), 67–87.

[Kl1] P. B. Kleidman, *The maximal subgroups of the finite Steinberg triality groups ${}^3D_4(q)$ and of their automorphism groups,*, Journal of Algebra **115** (1988), 182–199.

[Kl2] P. B. Kleidman, *The maximal subgroups of the Chevalley groups $G_2(q)$ with q odd, the Ree groups ${}^2G_2(q)$, and their automorphism groups*, Journal of Algebra **117** (1988), 30–71.

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

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

[Li] M. W. Liebeck, *On the orders of the maximal subgroups of the finite classical groups*, Proceedings of the London Mathematical Society (3) **50** (1985), 426–446.

[LPS] M. W. Liebeck, C. E. Praeger and J. Saxl, *On the O'Nan–Scott theorem for finite primitive permutation groups*, Journal of the Australian Mathematical Society, Series A **44** (1988), 389–396.

[LiSa] M. W. Liebeck and J. Saxl, *On the orders of maximal subgroups of the finite exceptional groups of Lie type*, Proceedings of the London Mathematical Society (3) **55** (1987), 299–330.

[LSS] M. W. Liebeck, J. Saxl and G. M. Seitz, *Subgroups of maximal rank in finite exceptional groups of Lie type*, Proceedings of the London Mathematical Society (3) **65** (1992), 297–325.

[LiSe] M. W. Liebeck and G. M. Seitz, *Maximal subgroups of exceptional groups of Lie type, finite and algebraic*, Geometriae Dedicata **35** (1990), 353–387.

[LiSh1] M. W. Liebeck and A. Shalev, *The probability of generating a finite simple group*, Geometriae Dedicata **56** (1995), 103–113.

[LiSh2] M. W. Liebeck and A. Shalev, *Classical groups, probabilistic methods, and the $(2,3)$-generation problem*, Annals of Mathematics, to appear.

[Lu] A. Lubotzky, *Subgroup growth and congruence subgroups*, Inventiones mathematicae **119** (1995), 267–295.

[LMS] A. Lubotzky, A. Mann and D. Segal, *Finitely generated groups of polynomial subgroup growth groups*, Israel Journal of Mathematics **82** (1993), 363–371.

[M] G. Malle, *The maximal subgroups of* ${}^2F_4(q^2)$, Journal of Algebra **139** (1991), 52–69.

[Ma1] A. Mann, *Some properties of polynomial subgroup growth groups*, Israel Journal of Mathematics **82** (1993), 373–380.

[Ma2] A. Mann, *Positively finitely generated groups*, Forum Mathematicum, to appear.

[MS] A. Mann and D. Segal, *Uniform finiteness conditions in residually finite groups*, Proceedings of the London Mathematical Society **61** (1990), 529–545.

[P] L. Pyber, *Maximal subgroups, growth functions, and Dixon type results*, in preparation.

[PSh] L. Pyber and A. Shalev, *Asymptotic results for primitive permutation groups*, in preparation.

[Re] A. Renyi, *Probability Theory*, North-Holland, Amsterdam, 1970.

[Sh1] A. Shalev, *Growth functions, p-adic analytic groups, and groups of finite coclass*, Journal of the London Mathematical Society **46** (1992), 111–122.

[Sh2] A. Shalev, *Subgroup growth and sieve methods*, Proceedings of the London Mathematical Society, to appear.

[Su] M. Suzuki, *On a class of doubly transitive groups*, Annals of Mathematics **75** (1962), 105–145.

[Wi] H. Wielandt, *Finite Permutation Groups*, Academic Press, New York, 1964.