

THE DENSITY OF SUBGROUP INDICES

ANER SHALEV

(Received 10 April 2008; accepted 8 May 2008)

Communicated by Martin W. Liebeck

Dedicated to Cheryl Praeger for her sixtieth birthday

Abstract

For a group G and a real number $x \geq 1$ we let $s_G(x)$ denote the number of indices $\leq x$ of subgroups of G . We call the function s_G the *subgroup density* of G , and initiate a study of its asymptotics and its relation to the algebraic structure of G . We also count indices $\leq x$ of maximal subgroups of G , and relate it to symmetric and alternating quotients of G .

2000 *Mathematics subject classification*: 20E07, 20F69.

Keywords and phrases: subgroup indices, special linear groups.

1. Introduction

Subgroup growth has been a major research topic over the past decades, with some remarkable achievements, see, for example, the book [13] by Lubotzky and Segal and the references therein.

The purpose of this paper is to introduce a somewhat related, but different, concept, where we count subgroup indices, instead of subgroups of a given index.

To make this precise, let G be a group, n a natural number, and let $a_n(G)$ denote the number of subgroups of index n in G (possibly infinity). Set

$$S_G = \{n \in \mathbb{N} \mid a_n(G) > 0\},$$

the set of finite indices of subgroups of G . Note that S_G is a multiplicative subset of \mathbb{N} , namely if $m, n \in S_G$ and m, n are coprime then $mn \in S_G$. For a real number $x \geq 1$, define

$$s_G(x) = |\{n \in S_G \mid n \leq x\}|.$$

Supported by ISF and BSF grants.

© 2008 Australian Mathematical Society 1446-7887/08 \$A2.00 + 0.00

Thus $s_G(x)$ is the number of indices of subgroups of G which do not exceed x . We refer to the function s_G as the *subgroup density* of G . In this context it is natural to restrict to residually finite groups G , and we shall often assume further that G is finitely generated.

We trivially have $s_G(x) \leq [x]$, with equality when G has subgroups of any finite index. For example, if G maps onto \mathbb{Z} then it has this property. We say that G has *linear subgroup density* if there exists $\epsilon > 0$ such that $s_G(x) \geq \epsilon x$ for all $x \geq 1$. It is easy to see that finitely generated soluble groups have this property (see Proposition 2.3 below). On the other hand, the subgroup density of certain finitely generated residually finite groups can be much smaller. For example, if G is a residually finite infinite finitely generated p -group (as constructed by Golod [3], Grigorchuk [4], and others) then we have $s_G(x) = [\log x / \log p] + 1$ for all $x \geq 1$.

In this paper we propose a systematic study of the asymptotics of $s_G(x)$ for infinite groups G , and its relation to the algebraic structure of G . We shall derive some results and suggest directions for further research.

Our first result shows that the subgroup density of certain linear groups is rather high. Indeed we have the following result.

THEOREM 1.1. *Let G be an infinite finitely generated linear group in characteristic zero. Then there exists a real number $\alpha > 0$ such that*

$$s_G(x) \geq x^\alpha \quad \text{for all sufficiently large } x.$$

In fact, our proof shows that if G is linear in dimension k , then the exponent α above can be bounded below by some positive number depending only on k .

In general, it would be interesting to study the (lower and upper) limit(s) of $\log s_G(x) / \log x$ for linear groups G .

Our next result solves this problem in some cases, and shows that Theorem 1.1 is the best possible in the sense that α may be arbitrarily small.

THEOREM 1.2. *Let $r \geq 1$ and let $G = SL_{r+1}(\mathbb{Z})$. Then*

$$\frac{\log s_G(x)}{\log x} \rightarrow \frac{1}{r} \quad \text{as } x \rightarrow \infty.$$

Our proof of this result involves tools from number theory and finite simple groups, and applies for more general arithmetic groups. Indeed, the subgroup density of linear and arithmetic groups in arbitrary characteristic will be discussed in [15].

It is intriguing that arithmetic groups in positive characteristic behave differently with respect to subgroup density. For example, we show in [15] that if $G = SL_{r+1}(\mathbb{F}_p[t])$ where $r \geq 2$, then $\log s_G(x) / \log x \rightarrow 0$, so the subgroup density is much lower than that determined in Theorem 1.2 above. This also implies that the assumption in Theorem 1.1 on the characteristic of the underlying field is essential.

Let us now turn to indices of maximal subgroups. Recall that $m_n(G)$ denotes the number of maximal subgroups of index n of a group G . Set

$$MS_G = \{n \in \mathbb{N} \mid m_n(G) > 0\},$$

the set of finite indices of maximal subgroups of G . For a real number $x \geq 1$, define

$$ms_G(x) = |\{n \in MS_G : n \leq x\}|,$$

the number of indices up to x of maximal subgroups of G . We refer to the function ms_G as the *maximal subgroup density* of G . For $G = \mathbb{Z}$, the integers, we have $ms_G(x) = \pi(x)$, the number of primes up to x . Thus the study of the functions ms_G may be viewed as a generalization of counting primes.

We clearly have $ms_G(x) \leq s_G(x) \leq [x]$ for all x . If G maps onto A_n or S_n for all n then both equalities hold. Note, however, that ms_G may be a bounded function (for example when G is a finitely generated p -group) whereas the function s_G is never bounded for infinite residually finite groups.

The study of ms_G is relevant in our proofs of Theorems 1.1 and 1.2. It turns out that for certain arithmetic groups the rate of growth of $ms_G(x)$ can be precisely determined.

THEOREM 1.3. *Let $r \geq 1$ and let $G = SL_{r+1}(\mathbb{Z})$. Then*

$$\frac{\log ms_G(x)}{\log x} \rightarrow \frac{1}{r} \quad \text{as } x \rightarrow \infty.$$

Moreover, for $r \geq 2$,

$$ms_G(x) = (r + o(1)) \frac{x^{1/r}}{\log x}.$$

Here and throughout this paper $o(1)$ denotes a real number tending to zero as $x \rightarrow \infty$.

Theorem 1.3 can be generalized for arithmetic groups with the congruence subgroup property [15].

While the functions s_G and ms_G have not been studied systematically for infinite groups G , there is some related and relevant literature concerning the case where G ranges over certain families of finite groups. In [1], Cameron *et al.* count indices up to x of maximal subgroups of finite simple groups (excluding A_{n-1} in A_n) and apply this to show that for a density 1 subset of natural numbers n the only primitive permutation groups of degree n are A_n and S_n . This is extended in the more recent work [6] by Heath-Brown *et al.*, where we omit the maximality condition, and prove a similar result for quasi-primitive permutation groups. We say that a subgroup $H \leq G$ is *quasi-maximal* if, for every normal subgroup N of G , $NH \neq G$ implies $N \subseteq H$.

The results of [1] and [6] have the following rather striking consequence.

THEOREM 1.4. *Let G be a group which subjects to only finitely many symmetric or alternating groups. Then*

$$ms_G(x) \leq (2 + o(1)) \frac{x}{\log x}.$$

Furthermore, the number of indices $\leq x$ of quasi-maximal subgroups of G is also of the form $O(x/\log x)$.

Theorem 1.4 applies for natural families of groups, such as arithmetic groups with the congruence subgroup property, virtually soluble groups, and groups with the Babai–Cameron–Pálffy restriction on their upper composition factors; it provides upper bounds similar to the one in the prime number theorem.

In fact, the conclusions of Theorem 1.4 hold under the weaker assumption, that G surjects to at most $o(x/\log x)$ groups of the form A_n or S_n for $n \leq x$. See Section 3 for this and related consequences.

While this paper is a first step in understanding subgroup density, much remains to be done. One natural problem is to find the spectrum of possible growth behaviours of s_G and ms_G . It is easy to realize many growth types using infinite products of finite cyclic groups; for example, if $G = \prod C_{p_i}$ where $\{p_i\}$ is a sufficiently sparse set of primes we can make s_G grow arbitrarily slowly. However, these examples are not finitely generated. Constructions by Kassabov and Nikolov [7] of finitely generated groups with various profinite completions (such as certain products of alternating groups) provide a tool for tackling the spectrum problem for finitely generated groups.

Even the case of linear groups G presents some challenges. One is to determine the growth type of s_G and ms_G in terms of relevant data, and to try to characterize groups under some density assumptions. A concrete problem of this type is characterizing finitely generated linear groups G over \mathbb{C} such that $s_G(x) \geq \epsilon x$ for some $\epsilon > 0$ and for all $x \geq 1$; in particular, do all these groups have a finite index subgroup mapping onto \mathbb{Z} ?

Finally, some words on the structure of this paper. In Section 2 we prove preliminary results on subgroup density, which eventually lead to the proof of Theorem 1.1, and to an upper bound crucial in the proof of Theorem 1.2. Section 3 deals with maximal subgroup density, and contains the proofs of Theorems 1.3 and 1.4, and observations on Fuchsian groups. Theorem 1.3 provides the lower bound needed to complete the proof of Theorem 1.2.

2. Subgroup density

We start with some elementary results.

- LEMMA 2.1.** (i) For any normal subgroup H of G we have $s_G(x) \geq s_{G/H}(x)$.
(ii) For any subgroup H of G of finite index f we have $s_G(x) \geq s_H(x/f)$.

PROOF. This is immediate. □

COROLLARY 2.2. Let G be a finitely generated group which has a finite index subgroup H such that $|H/H'| = \infty$. Then G has linear subgroup density.

PROOF. H/H' is an infinite finitely generated abelian group, hence it maps onto \mathbb{Z} . The result now follows easily from the previous lemma. □

PROPOSITION 2.3. Let G be an infinite finitely generated virtually soluble group. Then G has linear subgroup density.

PROOF. Let $K \leq G$ be a soluble subgroup of finite index. Let $K^{(i)}$ ($i \geq 0$) be the derived series of K . If $K^{(i)}/K^{(i+1)}$ is the first infinite derived factor, then Corollary 2.2 (with $H = K^{(i)}$) yields the result. \square

To prove Theorem 1.1 we also need a version of the so-called Lubotzky alternative, based on deep results on strong approximation. See [13, Chapter 9], for extensive background, as well as the recent detailed notes by Nikolov [14]. We say that a set S of primes has positive density if there exists $\epsilon > 0$ such that $|\{p \in S, p \leq x\}| \geq \epsilon x/\log x$ for all sufficiently large x . We shall now state and apply the following known result (see, for instance, [14, Corollary 30]).

THEOREM 2.4. *Let G be a finitely generated linear group over a field of characteristic zero, and suppose G is not virtually soluble. Then there exist a subgroup H of finite index in G , a fixed untwisted simple Lie type X , a set S of primes of positive density, and an epimorphism $\phi : \hat{H} \rightarrow \prod_{p \in S} X(\mathbb{F}_p)$, where \hat{H} is the profinite completion of H .*

PROOF OF THEOREM 1.1. Let G be as in the theorem. If G is virtually soluble then Proposition 2.3 shows that $s_G(x) \geq \epsilon x$ for some $\epsilon > 0$ and for all x , and the conclusion of the theorem follows immediately.

So suppose G is not virtually soluble. Then the conclusion of Theorem 2.4 holds. Set $K = \prod_{p \in S} X(\mathbb{F}_p)$. We claim that it suffices to show that there exists $\beta > 0$ such that

$$s_K(x) \geq x^\beta \quad \text{for all large } x. \tag{2.1}$$

Indeed, this follows from Lemma 2.1 and the inequality $(x/f)^\beta \geq x^{\beta-o(1)}$ where $f = |G : H|$.

Now, the minimal index of a proper subgroup of $X(\mathbb{F}_p)$ is known, and, assuming p is large enough, say $p > c$, is given by the value of some fixed polynomial $g(t)$ (depending on the type X only) at the point $t = p$. See [8, p. 175] and [9]. Moreover, it is easily seen that $g(p)$ is an increasing function of p and that $g(p) \geq p^d$ where $d = \deg(g) \geq 1$. It follows that

$$S_K \supseteq \{g(p) \mid p \in S, c < p \leq x^{1/d}\}.$$

Since S has positive density, we conclude that there exists $\epsilon > 0$ such that, if x is large enough, then S_K contains at least $\epsilon x^{1/d}/\log x^{1/d} - c$ distinct indices up to x . It follows that, for large x ,

$$s_K(x) \geq \epsilon d \frac{x^{1/d}}{\log x} - c \geq x^{1/d-o(1)}.$$

This implies the inequality (2.1) for any $\beta < 1/d$ and concludes the proof. \square

Note that if G above is linear in dimension k , then the dimension of the Lie type X , and hence d too, are bounded above in terms of k . This proves the remark following the statement of Theorem 1.1.

To prove Theorem 1.2 we need the following number theoretic lemma.

LEMMA 2.5. Fix a constant b . Then the number of positive integers $n \leq x$ whose prime divisors are all at most $b \log x$ is of the form $x^{o(1)}$.

PROOF. Let A be the set of primes $p \leq \log x / (\log \log x)^2$, and let B be the set of primes p such that $\log x / (\log \log x)^2 < p \leq b \log x$. Let $C = A \cup B$. We have to count the number N_C of sequences $(k_p)_{p \in C}$ such that $k_p \geq 0$ and $\prod_{p \in C} p^{k_p} \leq x$.

Clearly $k_p \leq \log_2 x$ for all $p \in C$, and $\sum_{p \in C} k_p \log p \leq \log x$. Hence the number N_A of choices for $(k_p)_{p \in A}$ satisfies

$$N_A \leq (\log_2 x)^{|A|} \leq (\log_2 x)^{\log x / (\log \log x)^2} \leq x^{c_1 / \log \log x},$$

for some (small) constant c_1 .

For $p \in B$ we have $\log p \geq \log \log x - 2 \log \log \log x \geq (1 - o(1)) \log \log x$. Therefore

$$\log x \geq \sum_{p \in B} k_p \log p \geq (1 - o(1)) (\log \log x) \sum_{p \in B} k_p.$$

We conclude that $\sum_{p \in B} k_p \leq (1 + o(1)) \log x / \log \log x$. By the prime number theorem we also have $|B| \leq (b + o(1)) \log x / \log \log x$.

Thus the number of possibilities N_B for $(k_p)_{p \in B}$ is at most the number of monomials of total degree at most $d = (1 + o(1)) \log x / \log \log x$ in $f = (b + o(1)) \log x / \log \log x$ variables. It is well known that there are $\binom{d+f}{d} \leq 2^{d+f}$ such monomials. This yields

$$N_B \leq 2^{(b+1+o(1)) \log x / \log \log x} \leq x^{c_2 / \log \log x}$$

for some constant c_2 .

Altogether we obtain

$$N_C \leq N_A N_B \leq x^{c / \log \log x},$$

where $c = c_1 + c_2$. In particular, $N_C \leq x^{o(1)}$, as required. □

We now turn to the core of the proof of Theorem 1.2.

PROPOSITION 2.6. Let $r \geq 1$ and let $G = SL_{r+1}(\mathbb{Z})$. Then $s_G(x) \leq x^{1/r+o(1)}$.

PROOF. For $r = 1$ there is nothing to prove, so suppose $r \geq 2$. Then G has the congruence subgroup property; moreover, by [13, Proposition 6.1.1] there is a constant c such that every index n subgroup of G contains a congruence subgroup $G(m)$ for some $m \leq cn$, and so corresponds to an index n subgroup of the finite group $SL_{r+1}(\mathbb{Z}/m\mathbb{Z})$.

We have $SL_{r+1}(\mathbb{Z}/m\mathbb{Z}) \cong \prod_{p \in S} SL_{r+1}(\mathbb{Z}/p^{k_p}\mathbb{Z})$ if $m = \prod_{p \in S} p^{k_p}$ for a finite set S of primes. Hence if $n \leq x$ and $n \in S_G$, then there exist a finite set S of primes, and a sequence $(k_p : p \in S)$ of positive integers, such that

$$\prod_{p \in S} p^{k_p} \leq cx, \tag{2.2}$$

and

$$n \in S_H \quad \text{where } H = \prod_{p \in S} SL_{r+1}(\mathbb{Z}/p^{k_p}\mathbb{Z}). \tag{2.3}$$

We may assume further that S is minimal, so if $n = |H : K|$ then K does not contain a direct factor $H_p := SL_{r+1}(\mathbb{Z}/p^{k_p}\mathbb{Z})$; therefore the projections of H to each factor H_p map K into a proper subgroup $M_p < H_p$.

Our proof of the proposition will now be carried out in three steps. First we bound the number of choices for S ; then, given S , we bound the number of choices for the sequence $(k_p : p \in S)$; finally, we bound the number of choices for n given S and $(k_p : p \in S)$.

STEP 1. Suppose $p > 2$. Then the minimal index of a proper subgroup of $SL_{r+1}(\mathbb{F}_p)$ is $(p^{r+1} - 1)/(p - 1)$ (see [8, p. 175]). Since the Frattini subgroup of $SL_{r+1}(\mathbb{Z}_p)$ is the first congruence subgroup, it follows that the minimal index of a proper subgroup of H_p is also $(p^{r+1} - 1)/(p - 1)$. In particular,

$$|H_p : M_p| \geq p^r + p^{r-1} + \dots + p + 1 > p^r.$$

Note that $n = |H : K|$ where $K \leq \prod_{p \in S} M_p$, and so

$$x \geq n \geq \prod_{p \in S} |H_p : M_p| \geq \prod_{p \in S, p > 2} p^r.$$

We conclude that $\prod_{p \in S, p > 2} p \leq x^{1/r}$. By the unique factorization in \mathbb{Z} we see that the set of primes $S \setminus \{2\}$ can be chosen in at most $x^{1/r}$ ways. Thus S can be chosen in at most $2x^{1/r}$ ways.

STEP 2. Suppose S is given. We now estimate the number of sequences $(k_p : p \in S)$ of positive integers such that the inequality (2.2) above holds. Let $m = |S|$ and let p_1, p_2, \dots, p_m be the first m primes. Then

$$cx \geq \prod_{p \in S} p^{k_p} \geq \prod_{p \in S} p \geq \prod_{i=1}^m p_i.$$

It follows from the prime number theorem that $p_m \sim m \log m$ and $\prod_{i=1}^m p_i \geq e^{(1-o(1))m \log m} \geq e^{(1-o(1))p_m}$. Hence $(1 - o(1))p_m \leq \log(cx)$, which implies

$$p_m \leq b \log x$$

for some constant b .

Now, to each sequence $(k_p : p \in S)$ we attach the number $\prod_{i=1}^m p_i^{n_i}$ so that n_i is k_p for the i th prime p in S . Since $\prod_{i=1}^m p_i^{n_i} \leq \prod_{p \in S} p^{k_p} \leq cx$ we obtain an injective map from the set of sequences $(k_p : p \in S)$ to the set of positive integers $n \leq cx$ whose prime divisors are all $\leq p_m \leq b \log x$. By Lemma 2.5 the size of the latter set is of

the form $x^{o(1)}$. Therefore, given S , there are at most $x^{o(1)}$ choices for the sequence $(k_p : p \in S)$.

STEP 3. Suppose both S and $(k_p : p \in S)$ are given. We now count indices n which arise from this data. Such indices are divisors of the order of the group $H = \prod_{p \in S} SL_{r+1}(\mathbb{Z}/p^{k_p}\mathbb{Z})$. Note that

$$|H| \leq \prod_{p \in S} (p^{k_p})^{(r+1)^2} \leq (cx)^{(r+1)^2},$$

by (2.2). It is well known that a given number h has at most $h^{c_3/\log \log h}$ divisors, for some constant c_3 (see [5, Chapter 18]). Therefore, the number of divisors of $|H|$ is at most

$$((cx)^{(r+1)^2})^{c_3/\log \log((cx)^{(r+1)^2})} \leq x^{c_4/\log \log x}$$

for a suitable constant c_4 . In particular, there are at most $x^{o(1)}$ choices for the index n given S and $(k_p : p \in S)$.

Combining all three steps we see that the number of indices $n \leq x$ of subgroups of G is at most $x^{1/r+o(1)}$, as required. In fact our arguments establish a slightly stronger result, namely

$$s_G(x) \leq x^{1/r+c_5/\log \log x}$$

for some constant c_5 and for all x . □

It now follows immediately that, if $G = SL_{r+1}(\mathbb{Z})$, then

$$\limsup \frac{\log s_G(x)}{\log x} \leq \frac{1}{r}, \tag{2.4}$$

establishing one inequality in the conclusion of Theorem 1.2. The remaining inequality will be proved in the next section.

3. Maximal subgroup density

The following result is immediate, but useful.

LEMMA 3.1. *Let G be a group and H a normal subgroup. Then $MS_G \supseteq MS_{G/H}$ and $ms_G(x) \geq ms_{G/H}(x)$ for all x .*

Next we quote a theorem, which settled positively a famous conjecture of Higman. Recall that a *Fuchsian group* is a finitely generated nonelementary discrete group of isometries of the hyperbolic plane. Examples include free groups, surface groups (oriented or not), the modular group $SL_2(\mathbb{Z})$, and hyperbolic triangle groups.

THEOREM 3.2. *Let G be a Fuchsian group (oriented or nonoriented). Then G subjects to all but finitely many alternating groups A_n .*

This is proved by Everitt [2] for oriented groups, and later in [11] for oriented and nonoriented groups (using probabilistic methods).

We now deduce the following result, showing that Fuchsian groups have very large maximal subgroup density.

PROPOSITION 3.3. *Let G be a Fuchsian group. Then there exists a constant c such that*

$$ms_G(x) = [x] - c \quad \text{for all large } x.$$

PROOF. Since A_n has a maximal subgroup of index n this follows immediately from the two results above. \square

We shall now show that there is a more general connection between the function ms_G and alternating and symmetric quotients of G . For a group G define

$$Q_G = \{n \in \mathbb{N} \mid G \text{ subjects to } A_n \text{ or } S_n\}.$$

We clearly have $MS_G \supseteq Q_G$. The next result, based on [1], shows that the difference $MS_G \setminus Q_G$ is small in some sense.

PROPOSITION 3.4. *The number of positive integers $n \in MS_G \setminus Q_G$ satisfying $n \leq x$ is at most $(2 + o(1))x/\log x$.*

PROOF. Let $n \in MS_G \setminus Q_G$, and let H be a maximal subgroup of index n in G . Let $N = H_G$ be the core of H . Then G/N is a primitive permutation group of degree n , and G/N is not isomorphic to A_n or S_n (since $n \notin Q_G$).

Let D be the set of natural numbers n with the property that there exists a primitive permutation group of degree n not isomorphic to A_n or S_n . We have shown that

$$MS_G \setminus Q_G \subseteq D.$$

The main result of [1] shows that the number of positive integers $n \leq x$ such that $n \in D$ is $(2 + o(1))x/\log x$. The result follows. \square

Let $[1, x]$ denote the interval $\{y \in \mathbb{R} \mid 1 \leq y \leq x\}$.

COROLLARY 3.5. *For every group G ,*

$$|Q_G \cap [1, x]| \leq ms_G(x) \leq |Q_G \cap [1, x]| + (2 + o(1))x/\log x.$$

PROOF OF THEOREM 1.4. The first assertion follows immediately from the above corollary. The second one is proved similarly using [6] instead of [1]. \square

Note that the somewhat stronger version of Theorem 1.4 mentioned in the introduction also follows from Corollary 3.5.

We say that a subset $L \subseteq \mathbb{N}$ has density α if $\lim_{x \rightarrow \infty} |L \cap [1, x]|/x = \alpha$.

Another consequence of Corollary 3.5 is the following result.

COROLLARY 3.6. *If Q_G has density α then so does MS_G .*

We now discuss the maximal subgroup density of $SL_{r+1}(\mathbb{Z})$.

PROOF OF THEOREM 1.3. If $r = 1$ then $G = SL_2(\mathbb{Z})$ is Fuchsian, and so the result follows from Proposition 3.3 above. So suppose $r \geq 2$. Then $G = SL_{r+1}(\mathbb{Z})$ has the congruence subgroup property and its profinite completion satisfies

$$\hat{G} \cong \prod_p SL_d(\mathbb{Z}_p).$$

Hence every maximal subgroup of finite index in G comes from a maximal open subgroup of $SL_d(\mathbb{Z}_p)$ for some prime p . We may ignore $p = 2$ (as this only reduces the maximal subgroup density by a constant). For $p > 2$ the maximal open subgroups of $SL_{r+1}(\mathbb{Z}_p)$ correspond to those of $G_p := SL_{r+1}(\mathbb{F}_p)$. As noted in the proof of Proposition 2.6 above, the minimal index $m(G_p)$ of such a subgroup is $(p^{r+1} - 1)/(p - 1)$. Using the prime number theorem it is easy to see that the number of indices $(p^{r+1} - 1)/(p - 1) \leq x$ is $(r + o(1))x^{1/r}/\log x$. This yields

$$ms_G(x) \geq (r + o(1))x^{1/r}/\log x.$$

It is known that the number of conjugacy classes of maximal subgroups of $SL_{r+1}(\mathbb{F}_p)$ is bounded (independently of p); see, for instance, [12, Lemma 2.1], for a more general result. Hence each group $G_p = SL_{r+1}(\mathbb{F}_p)$ contributes at most c indices of maximal subgroups, where c is some constant (depending on r only). Excluding the minimal index $m(G_p)$, each such index is at least $bm(G_p)^{1+\epsilon} \geq bp^{(1+\epsilon)r}$ for some absolute constants $b, \epsilon > 0$ (see [10, Lemma 6.6] for this and a more general result). Thus, such an index $n \leq x$ arises from a factor G_p for some $p \leq (x/b)^{1/(1+\epsilon)r}$. We conclude that the contribution to $ms_G(x)$ of those indices is at most $O(x^{1/(1+\epsilon)r}) \leq o(x^{1/r}/\log x)$.

Altogether it follows that, if $r \geq 2$, then

$$ms_G(x) = (r + o(1))x^{1/r}/\log x.$$

This completes the proof of the second assertion in Theorem 1.3. The first assertion follows immediately. □

PROOF OF THEOREM 1.2. Let $G = SL_{r+1}(\mathbb{Z})$. Since $s_G(x) \geq ms_G(x)$,

$$\liminf \frac{\log s_G(x)}{\log x} \geq \lim \frac{\log ms_G(x)}{\log x} = \frac{1}{r}.$$

Combining this with inequality (2.4) the result follows. □

References

- [1] Peter J. Cameron, Peter M. Neumann and David N. Teague, ‘On the degrees of primitive permutation groups’, *Math. Z.* **180** (1982), 141–149.
- [2] Brent Everitt, ‘Alternating quotients of Fuchsian groups’, *J. Algebra* **223** (2000), 457–476.
- [3] E. S. Golod, ‘On nil-algebras and finitely approximable p -groups’, *Izv. Akad. Nauk. SSSR Ser. Mat.* **28** (1964), 273–276.

- [4] R. I. Grigorchuk, 'On Burnside's problem on periodic groups', *Funktsional Anal. i Prilozhen* **14** (1980), 53–54.
- [5] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th edn (Oxford University Press, New York, 1979).
- [6] D. R. Heath-Brown, Cheryl E. Praeger and Aner Shalev, 'Permutation groups, simple groups, and sieve methods', *Israel J. Math.* **148** (2005), 347–375. (Furstenberg Volume).
- [7] Martin Kassabov and Nikolay Nikolov, 'Cartesian products as profinite completions', *Int. Math. Res. Not.*, **ID 72947** (2006), 17 pp.
- [8] Peter Kleidman and Martin Liebeck, *The Subgroup Structure of the Finite Classical Groups*, London Mathematical Society Lecture Note Series, 129 (Cambridge University Press, Cambridge, 1990).
- [9] Martin W. Liebeck and Jan Saxl, 'On the orders of maximal subgroups of the finite simple exceptional groups of Lie type', *Proc. London Math. Soc.* **55** (1987), 299–330.
- [10] Martin W. Liebeck and Aner Shalev, 'Simple groups, probabilistic methods, and a conjecture of Kantor and Lubotzky', *J. Algebra* **184** (1996), 31–57.
- [11] ———, 'Fuchsian groups, coverings of Riemann surfaces, subgroup growth, random quotients and random walks', *J. Algebra* **276** (2004), 552–601.
- [12] Martin W. Liebeck, Laszlo Pyber and Aner Shalev, 'On a conjecture of G.E. Wall', *J. Algebra* **317** (2007), 184–197.
- [13] Alexander Lubotzky and Dan Segal, *Subgroup Growth*, Progress in Mathematics, 212 (Birkhäuser, Basel, 2003).
- [14] Nikolay Nikolov, Strong approximation methods in group theory — LMS/EPSRC short course, (2007). arxiv:math.GR 0803.4165v2.
- [15] Aner Shalev, The density of subgroup indices, II, in preparation.

ANER SHALEV, Institute of Mathematics, Hebrew University, Jerusalem 91904, Israel

e-mail: shalev@math.huji.ac.il