Arch. Math. 81 (2003) 609–613
0003–889X/03/060609–05
DOI 10.1007/s00013-003-4768-z

Archiv der Mathematik

Normal growth of large groups

By

Thomas W. Müller and Jan-Christoph Schlage-Puchta

Abstract. For a finitely generated group Γ, denote by $s_n^{\lhd}(\Gamma)$ the number of normal subgroups of index n. A. Lubotzky proved that for the free group F_r of rank r, $s_n^{\lhd}(F_r)$ is of type $n^{\log n}$. We show that the same is true for a much larger class of groups. On the other hand we show that for almost all n, the inequality $s_n^{\lhd}(\Gamma) < n^{r-1+\varepsilon}$ holds true for every r-generated group Γ.

Let Γ be a finitely generated group. Over the last 20 years, there has been a growing interest in the function $s_n(\Gamma)$, counting the number of subgroups of index n in Γ and variants thereof, most notably the functions $m_n(\Gamma)$, counting maximal subgroups, and $s_n^{\lhd}(\Gamma)$ counting normal subgroups. For an overview, see [4] and [6]. For large groups in the sense of Pride [10], i.e., groups having a subgroup of finite index, which maps surjectively onto a non-abelian free group, the first two functions appear to be closely related; in fact, in all known instances almost all finite index subgroups of a large group are maximal; cf. [8, Section 4.4] and [9, Proposition 8]. On the other hand, one might expect $s_n^{\lhd}(\Gamma)$ to carry more group-theoretical information than the functions $s_n(\Gamma)$ and $m_n(\Gamma)$. However, as it turns out, the functions $s_n^{\lhd}(\Gamma)$ behave similar for a substantial class of groups Γ, including all large groups.

Note that as a function of n, $s_n^{\lhd}(\Gamma)$ behaves quite irregular. For example, if Γ is a free product of finite groups, and p is a prime dividing none of the orders of the free factors, then $s_p^{\lhd}(\Gamma) = 0$, while, as we will see below, for other indices there might be as many as $n^{c \log n}$ normal subgroups of index n. Indeed, a comparison of Theorems 1 and 2 below reveals an even greater amount of irregularity. These observations suggest that, instead of $s_n^{\lhd}(\Gamma)$ itself, it is more natural from an asymptotic point of view to consider the summatory function $S_n^{\lhd}(\Gamma) = \sum_{\nu \leqq n} s_\nu^{\lhd}(\Gamma)$. In [5], A. Lubotzky proved that $S_n^{\lhd}(F_r)$ is of type $n^{\log n}$. Here, F_r denotes the free group of rank $r \geqq 2$, and a function $f(n)$ is called of type $n^{\log n}$, if there are positive constants c_1, c_2 such that for n sufficiently large we have

$$n^{c_1 \log n} \leqq f(n) \leqq n^{c_2 \log n}.$$

Mathematics Subject Classification (2000): 20E07, 11N64.

In this note, we will show that the latter behaviour is not characteristic for free groups, but rather pertains to a substantial class of groups, including all large groups. More precisely, we shall prove the following.

Theorem 1. *Let Γ be a finitely generated group, possessing a finite index subgroup Δ which maps surjectively onto a group G such that the pro-p completion $\widehat{G}^p$ of G is a non-abelian free pro-p group for some prime p. Then $S_n^{\lhd}(\Gamma)$ is of type $n^{\log n}$.*

In the proof of Theorem 1 we exhibit a large number of normal subgroups of p-power index, and one might wonder how the function $s_n^{\lhd}(\Gamma)$ behaves for other indices n. Somewhat surprisingly, as our next result shows, $s_n^{\lhd}(\Gamma)$ is 'generically' of polynomial type.

Theorem 2. (i) *Let Γ be an r-generated group. Then, for every $\varepsilon > 0$ and all but $o(x)$ numbers $n \leqq x$, we have $s_n^{\lhd}(\Gamma) \leqq n^{r-1+\varepsilon}$.*
(ii) *We have $s_n^{\lhd}(F_r) \geqq n^{r-1}$ for all $n \geqq 1$.*
(iii) *Suppose that Γ contains a subgroup of finite index projecting onto a free abelian group of rank $r \geqq 2$. Then there exists a set $\mathcal{N} \subseteqq \mathbb{N}$ of positive asymptotic density and a constant $c > 0$, such that*

$$s_n^{\lhd}(\Gamma) \geqq c n^{r-1}, \quad n \in \mathcal{N}.$$

The proof of Theorem 1 requires a slight sharpening of a result of A. Mann [7].

Theorem 3. *Let $\widehat{F}_r^p$ be the free pro-p group of rank $r \geqq 2$. Then there is some constant $c > 0$, such that for any fixed integer k, $\varepsilon > 0$, and $n > n_0(k, \varepsilon)$, there is a set $\{N_1, \dots, N_t\}$ of normal subgroups of index p^n in $\widehat{F}_r^p$, satisfying $t > p^{(c-\varepsilon)n^2}$ and $(N_i : N_i \cap N_j) > p^k$ for all $i \neq j$.*

Here and in the sequel, subgroups are understood to be closed. We first show how to deduce Theorem 1 from Theorem 3.

Proof of Theorem 1. Let Δ be a subgroup of finite index d in Γ, which maps onto a dense subgroup of a free pro-p group $\widehat{F}_r^p$ for some $r \geqq 2$. Let $N \lhd \Delta$ be a normal subgroup. Then the normalizer of N in Γ has index $\leqq d$, hence, the index of the core of N in Γ has index in N bounded by $d!$, which is independent of N. Call two normal subgroups $N_1, N_2 \lhd \Delta$ of index n equivalent, if their intersection has index $\leqq d!$ in each of them. Then we deduce that the number of inequivalent normal subgroups of Δ of index at most n is a lower bound for the number of normal subgroups in Γ of index $\leqq dd!n$. Indeed, the core of N is normal in Γ of index $\leqq dd!n$, and inequivalent normal subgroups have different core. Using Theorem 3 to estimate the number of inequivalent normal subgroups, we obtain the required lower bound. On the other hand, Lubotzky [5], refining a result of Pyber [11] for finite groups, has shown that $S_n^{\lhd}(\Gamma) \leqq n^{3(d+1)\log n}$ holds for every d-generated group Γ. It follows that $S_n^{\lhd}(\Gamma)$ is indeed of type $n^{\log n}$ as claimed.

We now establish Theorem 3, building on arguments of Mann.

Proof of Theorem 3. In [7] (see also [6, Chapter 3.4]), Mann obtained the following:

(1) $((\widehat{F}_r^p)' \cap \Phi^k(\widehat{F}_r^p))\Phi^{k+1}(\widehat{F}_r^p)/\Phi^{k+1}(\widehat{F}_r^p)$ is an elementary abelian p-group of rank $t \geqq (7/6)^k - r$.

(2) If $n > 14(2r+1)^2 t$, then for every subgroup U of

$$((\widehat{F}_r^p)' \cap \Phi^k(\widehat{F}_r^p))\Phi^{k+1}(\widehat{F}_r^p)/\Phi^{k+1}(\widehat{F}_r^p),$$

there exists a normal subgroup N of index p^n in $\widehat{F}_r^p$ with

$$N\Phi^{k+1}(\widehat{F}_r^p)/\Phi^{k+1}(\widehat{F}_r^p) = U.$$

Here, $\Phi(G)$ denotes the Frattini subgroup of G, and $\Phi^k(G)$ is the k-th iterate of this operator. Obviously, normal subgroups N_1, N_2 in $\widehat{F}_r^p$ such that the intersection of $U_1 = N_1\Phi^{k+1}(\widehat{F}_r^p)/\Phi^{k+1}(\widehat{F}_r^p)$ with $U_2 = N_2\Phi^{k+1}(\widehat{F}_r^p)/\Phi^{k+1}(\widehat{F}_r^p)$ has index at least p^k in both of these groups (we abbreviate this condition by saying that U_1 and U_2 are inequivalent), satisfy $(N_i : N_1 \cap N_2) \geqq p^k$. A subgroup U of C_p^t of rank $\lfloor t/2 \rfloor$ is equivalent to at most p^{2kt} subgroups of C_p^t of the same rank, for U has at most p^{kt} subgroups of index $\leqq k$, and each such subgroup is contained in at most p^{kt} other subgroups of rank $\lfloor t/2 \rfloor$. Hence, there is a set consisting of $p^{t^2/4-2kt}$ subgroups of C_p^t of rank $\lfloor t/2 \rfloor$, such that the intersection of any two of them has index $> p^k$ in each of them. Passing from U to $\widehat{F}_r^p$, we see that the latter group has at least $p^{t^2/4-2kt}$ normal subgroups of index $\leqq p^{14(2r+1)^2 t}$, such that any two of them have an intersection of index $> p^k$ in each of them. Putting $c = (56(2r+1)^2)^{-1}$, the theorem follows.

Finally, we turn to the proof of Theorem 2.

Proof of Theorem 2. (i) The proof relies on the fact that, for almost all n (in the above probabilistic sense), all groups of order n are subject to a severe structural restriction. Erdős and Pálfy [1] showed that, for every $\varepsilon > 0$, almost all odd n have a divisor d with $d \leqq (\log n)^{1+\varepsilon}$, n/d squarefree and prime to d, such that every group of order n contains a cyclic direct factor of index d. The same proof strategy gives the existence of a cyclic normal subgroup of index d for almost all even n. In fact, by Sylow's Theorem, the product of all prime divisors p of n such that $p^2 \nmid n$, and such that there is no divisor t of n with $t > 1$ and $t \equiv 1\,(p)$ may serve as n/d; the problem to determine the normal size of d is then treated using methods from analytic number theory. Let $\mathcal{N}$ be the set consisting of those integers n such that every group of order n has the structure described above. For $n \in \mathcal{N}$ we want to bound the number $f(n)$ of groups G of order n. Let N be the cyclic normal subgroup of G of index d. Since $(n/d, d) = 1$, the extension

$$0 \longrightarrow N \longrightarrow G \longrightarrow H \longrightarrow 0$$

splits by the Schur-Zassenhaus Theorem. Hence, G is determined up to isomorphism by the isomorphism type of H and the action of H on N, and we obtain for $n \in \mathcal{N}$

$$\begin{aligned} f(n) &= \sum_{\substack{H \\ |H|=d}} |\mathrm{Hom}(H, \mathrm{Aut}(N))| \leqq f(d) \cdot \max_{|H|=d} |\mathrm{Hom}(H, \mathrm{Aut}(N))| \\ &\leqq n^{\varepsilon} \cdot \max_{|H|=d} |\mathrm{Hom}(H/[H,H], \mathrm{Aut}(N))|, \end{aligned}$$

where we have used the bound $f(d) \leqq d^{c\log d}$ due to Pyber [11] and the fact that $\mathrm{Aut}(N)$ is abelian. $\mathrm{Aut}(N)$ is isomorphic to the group of units

$$\left(\mathbb{Z}/_{\frac{n}{d}}\mathbb{Z}\right)^* \cong \prod_{\substack{p>2\\ p|\frac{n}{d}}} C_{p-1},$$

since n/d is squarefree; cf. for instance [3, Section 2.5]. Decomposing $H/[H,H]$ as a direct product of cyclic groups of prime power order, we find that

$$|\mathrm{Hom}(H/[H,H], \mathrm{Aut}(N))| \leqq \prod_{p|\frac{n}{d}} (d, p-1).$$

Taking into account all possible choices for d, we deduce that

$$\sum_{\substack{n\in\mathcal{N}\\ n\leqq x}} \log(\max_{|H|=d} |\mathrm{Hom}(H, \mathrm{Aut}(N))|) \leqq \sum_{d\leqq \log^{1+\varepsilon} x} \sum_{p} \sum_{\substack{n\in\mathcal{N}\\ n\leqq x\\ pd|n}} \log(d, p-1)$$

$$\leqq 2\log\log x \sum_{d\leqq \log^{1+\varepsilon} x} \sum_{p\leqq x} \frac{x}{pd} \leqq x\log^{\varepsilon} x.$$

We conclude that, with the exception of at most $\frac{x}{\sqrt{\log x}}$ integers $n \leqq x$ of $\mathcal{N}$, we have $f(n) \leqq n^{\varepsilon}$. Moreover, for $n \in \mathcal{N}$ we have $|\mathrm{Aut}(G)| \geqq n^{1-\varepsilon}$, since we can lift each of the $\varphi(n/d)$ automorphisms of N to G due to the fact that $\mathrm{Aut}(N)$ is abelian. Putting the last two estimates together, we conclude that, for almost all n,

$$s_n^{\triangleleft}(\Gamma) = \sum_{|G|=n} |\mathrm{Epi}(\Gamma, G)| \cdot |\mathrm{Aut}(G)|^{-1} \leqq n^{r-1+2\varepsilon}$$

as claimed.

(ii) This follows from the facts that F_r projects onto the free abelian group C_∞^r of rank r, and that

$$s_n(C_\infty^r) = 1 * n * n^2 * \cdots * n^{r-1} \geqq n^{r-1};$$

cf. [2, Proposition 1.1].

(iii) As in the proof of Theorem 1, it suffices to produce a large set of finite index subgroups of $\bar{\Delta} = C_\infty^r$ having pairwise intersections of large index. Let d and n be integers, U a subgroup of index n in $\bar{\Delta}$. We bound the number of subgroups V of index n satisfying $(U : U \cap V) = d$ as follows. Since $U \cong \bar{\Delta}$, there are $s_d(\bar{\Delta})$ possibilities for $U \cap V$. Fixing a subgroup H of index nd in $\bar{\Delta}$, the number of index n subgroups containing H equals

$$s_n(\bar{\Delta}/H) = s_d(\bar{\Delta}/H) \leqq s_d(\bar{\Delta})$$

by duality. Hence, there exists a set $\{U_1, U_2, \ldots, U_t\}$ of index n subgroups in $\bar{\Delta}$ such that $t > cn^{r-1}$ for some positive constant c, and such that $(U_i : U_i \cap U_j) > d$ for all $i \neq j$.

Let Δ be a finite index subgroup of Γ projecting onto $\bar{\Delta}$. The core of the preimage of U_i in Γ has index bounded above in terms of $(\Gamma : \Delta)$ alone. It follows that, for each n, there exists $\nu \leqq C$, such that $s_{n\nu}^{\triangleleft}(\Gamma) \geqq cn^{r-1}$, whence our claim.

Remark. In Theorem 2 (ii), the occurrance of both the free group F_r and of the free abelian group C_∞^r is somewhat arbitrary. As it stands, the proof of (ii) works for every group projecting onto C_∞^r. Also, other groups with known normal growth may be used for comparison.

References

[1] P. ERDŐS and P. P. PÁLFY, On the order of directly indecomposable groups. Mat. Lapok **33**, 289–298 (1986).

[2] F. GRUNEWALD, D. SEGAL and G. SMITH, Subgroups of finite index in nilpotent groups. Invent. Math. **93**, 185–223 (1988).

[3] E. KRÄTZEL, Zahlentheorie, Berlin 1981.

[4] A. LUBOTZKY, Counting finite-index subgroups. In: Groups Galway/St Andrews 1993. London Math. Soc. Lect. Ser. **212**, 368–404 (1995).

[5] A. LUBOTZKY, Enumerating boundedly generated finite groups. J. Algebra **238**, 194–199 (2001).

[6] A. LUBOTZKY and D. SEGAL, Subgroup Growth. Basel 2003.

[7] A. MANN, Enumerating finite groups and their defining relations. J. Group Theory **1**, 59–64 (1998).

[8] T. MÜLLER and J. -C. PUCHTA, Character theory of symmetric groups and subgroup growth of surface groups. J. London Math. Soc. (2) **66**, 623–640 (2002).

[9] T. MÜLLER and J. -C. PUCHTA, Classification and statistics of finite index subgroups in free products. Adv. in Math. To appear.

[10] S. J. PRIDE, The concept of largeness in group theory. In: Word problems II. Amsterdam 299–335 (1980).

[11] L. PYBER, Enumerating finite groups of given order. Ann. of Math. **137**, 203–220 (1993).

Received: 30 October 2002

T. W. Müller
School of Mathematical Sciences
Queen Mary, University of London
Mile End Road
London E1 4NS
United Kingdom
T.W.Muller@qmul.ac.uk

J.-C. Schlage-Puchta
Mathematisches Institut
Albert-Ludwigs-Universität
Eckerstr. 1
D-79104 Freiburg
Germany
jcp@arcade.mathematik:uni-freiburg.de