Publl. Math. Debrecen
69/3 (2006), 379–386

Profinite groups with linear subgroup growth

By ANER SHALEV (Jerusalem)

Dedicated to the memory of Edith Szabó

Abstract. We show that profinite groups with linear subgroup growth have a prosoluble open subgroup, while profinite groups with faster subgroup growth need not have this property. Our proofs involve some number theory and the structure of finite simple groups.

1. Introduction

For a group G and a positive integer n let $a_n(G)$ denote the number of subgroups of index n in G. Understanding the connections between the growth of the series $\{a_n(G)\}$ and the structure of G has been a major research topic in the past two decades (see the book [LS] and the references therein). What can be said about groups with linear subgroup growth (satisfying $a_n(G) \leq cn$ for all n, where c is some constant)?

We may (and will) assume our groups G are residually finite. If in addition G is finitely generated (as an abstract group) then it was shown in Theorem 1.2 of [Sh3] that G has linear subgroup growth if and only if it is virtually cyclic (namely, has a cyclic subgroup of finite index).

Mathematics Subject Classification: 20E07, 20E18.
Key words and phrases: profinite groups, subgroup growth, finite simple groups.
Suppoted by the Israel Science Foundation and by the Bi-National Science Foundation United States–Israel Grant 2004-052.

However, for profinite groups (finitely generated only topologically) this is no longer true. The simplest example is $G = \mathbb{Z}_p \times \mathbb{Z}_p$, where $a_n(G) = (pn-1)/(p-1)$ for all $n = p^k$ (and 0 otherwise). Moreover, pro-p groups with linear subgroup growth need not even be soluble [K1]; their characterization (for odd p) has been obtained by Klopsch [K2].

A natural question which is still open is to characterize profinite groups of linear subgroup growth. Our main result is a step towards such a characterization, showing that such groups are well-behaved in some sense.

Theorem 1.1. *Profinite groups of linear subgroup growth are virtually prosoluble of finite rank.*

Note that while finitely generated abstract groups of polynomial subgroup growth are virtually soluble of finite rank [LMS], this is not true for profinite groups; see [SSh] for the characterization of profinite groups with polynomial subgroup growth.

Can we extend Theorem 1.1 for groups of somewhat faster subgroup growth? Our second result provides a negative answer, thus showing that Theorem 1.1 is best possible in some sense.

Theorem 1.2. *For every function $f : \mathbb{N} \to \mathbb{N}$ such that $f(1) = 1$ and $f(n)/n \to \infty$ there exists a 2-generated profinite group G which is not virtually prosoluble such that $a_n(G) \leq f(n)$ for all n.*

It is noteworthy that our proof of Theorem 1.1 relies on the Classification of Finite Simple Groups.

In Theorem 1.2 we may take for G a cartesian product of the groups $\mathrm{PSL}_2(p)$, where p ranges over a certain infinite set of primes, whose construction requires some number theory.

Notation. By a finite simple group we mean a non-abelian finite simple group. Let p, p_i denote prime numbers, and q a prime power. The field with q elements is denoted by F_q, and $\mathbb{Z}_p$ denotes the p-adic integers. Let C_m be the cyclic group with m elements. A semisimple group is a Cartesian product $\prod_i T_i$ (finite or infinite) of finite simple groups T_i. The rank of a profinite group G is the minimal r (possibly infinity) such that any closed subgroup of G can be generated (topologically) by at most r elements.

2. Proofs

In this section we prove Theorems 1.1 and 1.2.

We start by quoting a structure theorem for profinite groups with polynomial subgroup growth, which will be a main tool in this section.

Theorem 2.1. *Let G be a profinite group with polynomial subgroup growth. Then G has closed normal subgroups $N \leq H \leq G$ such that*

(i) *H is open (hence of finite index) in G;*

(ii) *N is prosoluble;*

(iii) *There are a number $0 \leq k \leq \infty$ and finite simple groups T_i $(1 \leq i < k)$, such that $H/N = \prod_{i<k} T_i$;*

(iv) *Each finite simple group T occurs only finitely many times in the sequence $(T_i : i < k)$;*

(v) *There is a constant c (depending on G) such that each group T_i is a group of Lie type of Lie rank $\leq c$ over the field $F_{p_i^{e_i}}$, where $e_i \leq c$;*

(vi) *G is virtually prosoluble of finite rank if and only if $k < \infty$.*

Proof. This follows from Theorem 1.2 in [Sh1] and the remarks following it. See also the more general result in [SSh]. □

Now let G be a profinite group with linear subgroup growth. Then G has the structure as in Theorem 2.1 above, and to prove Theorem 1.1 it suffices to show that $k < \infty$.

This requires some preparations regarding simple groups of Lie type (see Carter [C] for background).

Lemma 2.2. *Every Coxeter group has a subgroup of index 2.*

Proof. Let G be a Coxeter group. Then there is a length function l defined on G such that $l(g)$ is the minimal length of a word in the canonical generators which represents g. Since the relators of the group all have even length, we have $l(gh) \equiv l(g) + l(h) \bmod 2$. Thus the set of elements of even length in G form a subgroup, which is obviously of index 2. □

Lemma 2.3. *Let $G = G(q)$ be a finite simple group of Lie type over F_q. Suppose q is odd and $q > 11$. Let $B, N \leq G$ form a (B, N)-pair. Then the subgroup N is self-normalizing in G, namely $N_G(N) = N$.*

Proof. We apply a paper of Seitz [S] studying the groups $G(q)$ under our conditions on q. Let $H \leq B$ be a Cartan subgroup. Then $N = N_G(H)$ by result 2.3 in [S], and result 2.8(b) loc. sit. shows that H is a characteristic subgroup of N. Therefore any $g \in N_G(N)$ satisfies $H^g = H$, so $N_G(N) = N$. □

Lemma 2.4. *Let G be a finite simple group of Lie type over F_q, where $q > 11$ is odd. Then G has subgroups $M > K$ satisfying $|M : K| = 2$ and $N_G(M) = M$.*

Proof. Let $B, N \leq G$ form a (B, N)-pair, where B is a Borel subgroup, $H = B \cap N$ is a Cartan subgroup, $H \lhd N$, and the Weyl group $W = N/H$ is a Coxeter group. It follows by Lemma 2.2 that W has a subgroup of index 2. Thus N has a subgroup of index 2, which we denote by K. Lemma 2.3 and our assumptions on q show that N is self-normalizing in G. Setting $M = N$ we obtain the result. □

Remark. The conclusion of Lemma 2.4 also holds for alternating groups $G = A_n$ $(n \geq 5)$. Indeed take $M = (S_{n-2} \times S_2) \cap A_n$ in the natural intransitive embedding. Then M is a maximal subgroup of G, hence it is self-normalizing. Letting K be A_{n-2} acting on the first $n-2$ letters, we obtain the result.

We can also show that the assumptions on q in Lemma 2.4 may be weakened, but the present version is sufficient for our purpose here.

Proposition 2.5. *Let G be an infinite profinite semisimple group. Then the subgroup growth of G is super-linear.*

Proof. Write $G = \prod_{i=1}^{\infty} T_i$ where T_i are finite simple groups. We may assume G has polynomial subgroup growth, otherwise the conclusion holds trivially. Note that, if $H \leq G$ is an open subgroup whose subgroup growth is super-linear, then the subgroup growth of G is super-linear. Applying Theorem 2.1 and replacing G with an open subgroup we may assume that the groups T_i satisfy conclusions (iv) and (v) of the theorem.

Therefore only finitely many groups T_i can be of Lie type in characteristic 2 (otherwise either the Lie ranks, or the extension degrees e_i, will be unbounded). Similarly only finitely many group T_i can be of Lie type over

F_q for $q \leq 11$. By passing again to an open subgroup if needed, we may assume that, for each i, T_i is a simple group of Lie type over F_{q_i}, where q_i are odd prime powers larger than 11.

Applying Lemma 2.4 it now follows that each T_i has a self-normalizing subgroup M_i which has a subgroup K_i of index 2. Set $m_i = |T_i : M_i|$. Given an integer $s \geq 1$, consider the quotient $L = T_1 \times \cdots \times T_s$ of G, and let $M = M_1 \times \cdots \times M_s$ and $K = K_1 \times \cdots \times K_s$. Then $M < L$ is self-normalizing and $M/K \cong C_2^s$. Let N be a subgroup satisfying $K < N \leq M$ such that $N/K \cong C_2$ with the property that N/K projects onto each subgroup M_i/K_i $(i = 1, \ldots, s)$. Then $M/N \cong C_2^{s-1}$, and so there are at least $2^{(s-1)^2/4}$ subgroups $H < L$ such that $N \leq H \leq M$ and $|M : H| = 2^{(s-1)/2}$ (assuming, for simplicity, that s is odd). These subgroups have index $m_1 \cdots m_s 2^{(s-1)/2}$ in L, and their images under the natural projections $L \to T_i$ $(i = 1, \ldots, s)$ are $M_1, \ldots, M_s$ respectively.

The same process can be repeated for all conjugates M^x, K^x of M and K, where x ranges over a set of representatives for the cosets of M in L. Note that there is no overlapping between the subgroups H corresponding to distinct elements x. Set $m = m_1 \cdots m_s$, and $n = m \cdot 2^{(s-1)/2}$. Since there are m possibilities for x, we conclude that

$$a_n(G) \geq a_n(L) \geq m \cdot 2^{(s-1)^2/4} = n \cdot 2^{(s-1)(s-3)/4}.$$

Letting s tend to infinity, we see that the series $\{a_n(G)/n\}$ is unbounded. This completes the proof. □

We can now prove Theorem 1.1. Let G be a profinite group with linear subgroup growth. Then G has polynomial subgroup growth, so its structure is described in Theorem 2.1 above. Now, the open subgroup H of G has linear subgroup growth, and so does $H/N = \prod_{i<k} T_i$. Applying Proposition 2.5 above it follows that k is finite. Hence G is virtually prosoluble of finite rank.

Theorem 1.1 is proved.

To prove Theorem 1.2 we make use of a construction devised in [Sh1]. We choose an infinite series $\{p_i\}$ of primes satisfying $p_i \equiv 67 \bmod 72$ such that $|\operatorname{PSL}_2(p_i)| = p_i(p_i^2-1)/2$ is not divisible by any prime $p>3$ dividing $|\operatorname{PSL}_2(p_j)| = p_j(p_j^2-1)/2$ for some $j<i$. This can be done using Dirichlet's Theorem.

It then follows that

$$\gcd(|\operatorname{PSL}_2(p_i)|, |\operatorname{PSL}_2(p_j)|) = 12 \quad \text{for all} \quad i \neq j.$$

Set $G = \prod_{i=1}^{\infty} \operatorname{PSL}_2(p_i)$. It is well known that G is 2-generated as a profinite group. Clearly G is not virtually prosoluble, and has infinite rank.

The subgroup growth of groups G constructed as above is analyzed in Section 5 of [Sh1]. Lemma 5.1 there shows that there exists a constant $A>1$ such that for any integer $n \geq 1$ there is an integer $s \geq 0$ satisfying

$$p_1 \cdots p_s \leq n \quad \text{and} \quad a_n(G) \leq nA^{s^2}. \tag{1}$$

Next, given a function f with $f(1)=1$ and $f(n)/n \to \infty$ we construct a sequence of primes $\{p_i\}$ as above, which grows fast enough, so as to satisfy the additional requirement

$$p_1 p_2 \cdots p_s \leq n \Rightarrow A^{s^2} \leq f(n)/n. \tag{2}$$

This can be done inductively, requiring that $p_s > n_s/(p_1 \cdots p_{s-1})$, where $n_s = \max\{n : f(n)/n < A^{s^2}\}$.

It now follows from (1) and (2) that $a_n(G) \leq f(n)$ for all n.

Theorem 1.2 is proved.

3. Concluding remarks

Profinite groups with sublinear subgroup growth are exactly those which have an open pro-cyclic central subgroup (see [Sh2]). Can we expect a concise description of profinite groups with linear subgroup growth? The purpose of this section is to indicate a negative answer. Indeed, we give some examples, which show that any characterization of profinite groups with linear subgroup growth must have an essential arithmetic component.

Let G be a pro-nilpotent profinite group. Then $G = \prod_p G_p$, where, for each prime p, G_p is the pro-p Sylow subgroup of G. We also have, for $n = \prod_p p^{k_p}$,

$$a_n(G) = \prod_p a_{p^{k_p}}(G_p).$$

Suppose G has linear subgroup growth. Then it follows that each pro-p group G_p has linear subgroup growth, and so its structure is given in [K2]. Furthermore, setting $c_p = \sup_k a_{p^k}(G_p)/p^k$, we must have $\prod_p c_p < \infty$. Conversely, a Cartesian product of pro-p groups G_p satisfying $a_n(G_p) \leq c_p n$ and $\prod c_p < \infty$ is itself of linear subgroup growth. These remarks essentially reduce the pro-nilpotent case to the pro-p case and the determination of the constants c_p. For example, for $G_p = \mathbb{Z}_p \times \mathbb{Z}_p$ we have $c_p = p/(p-1) = 1+(p-1)^{-1}$, and the above discussion yields the following

Corollary 3.1. *Consider the abelian profinite group $G = \prod_p \mathbb{Z}_p^{b_p}$ where p ranges over the prime numbers and b_p are natural numbers. Then G has linear subgroup growth if and only if $b_p \leq 2$ for all p, and*

$$\sum_{\{p:b_p=2\}} p^{-1} < \infty.$$

References

[C] R. W. Carter, Simple Groups of Lie Type, *John Wiley*, *London*, 1972.

[K1] B. Klopsch, Zeta functions related to the pro-p group $SL_1(\Delta_p)$, *Math. Proc. Cambr. Phil. Soc.* **135** (2003), 45–57.

[K2] B. Klopsch, Pro-p groups with linear subgroup growth, *Math. Z.* **245** (2003), 335–370.

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

[LS] A. Lubotzky and D. Segal, Subgroup Growth, Progress in Math. **212**, *Birkhäuser*, 2003.

[SSh] D. Segal and A. Shalev, Profinite groups with polynomial subgroup growth, *J. London Math. Soc.* **55** (1997), 320–334, (Hartley memorial issue).

[S] G. M. Seitz, Subgroups of finite groups of Lie type, *J. Algebra* **61** (1979), 16–27.

[Sh1] A. Shalev, Subgroup growth and sieve methods, *Proc. London Math. Soc.* **74** (1997), 335–359.

[Sh2] A. Shalev, Groups whose subgroup growth is less than linear, *International Journal of Algebra and Computation* **7** (1997), 77–91.

[Sh3] A. Shalev, On the degree of groups of polynomial subgroup growth, *Trans. Amer. Math. Soc.* **351** (1999), 3793–3822.

ANER SHALEV
INSTITUTE OF MATHEMATICS
THE HEBREW UNIVERSITY
JERUSALEM 91904
ISRAEL

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

(Received October 27, 2005; revised March 4, 2006)