ISRAEL JOURNAL OF MATHEMATICS 155 (2006), 117–123

ON THE PROBABILITY OF GENERATING FREE PROSOLUBLE GROUPS OF SMALL RANK

BY

MARTA MORIGI

Dipartimento di Matematica, Università di Bologna
Piazza di Porta S. Donato n.5, 40126 Bologna, Italy
e-mail: mmorigi@dm.unibo.it

ABSTRACT

Let F be the free prosoluble group of rank $d \leq 9$. We study the minimum integer k such that the probability of generating F with k elements is positive.

Introduction

The probability of generating a finite group G with k elements is just the proportion of k-tuples of elements of G which generate G. This concept can be generalized to profinite groups, using the normalized Haar measure μ defined on them. Namely, the probability that k random elements generate a profinite group G is defined as

$$P(G,k) = \mu\{(x_1,\dots,x_k) \in G^k | \langle x_1,\dots,x_k\rangle = G\},$$

where μ denotes also the product measure on G^k.

A profinite group G is said to be 'positively finitely generated', PFG for short, if $P(G,k)$ is positive for some natural number k, and the least such natural number is denoted by $\mathrm{d_P}(G)$.

It has been proved that several classes of finitely generated profinite groups are positively finitely generated (see [3], [1] and the beautiful paper [6]) and the value of $P(G,k)$ has been calculated for some of these classes. For instance, W. M. Kantor and A. Lubotzky proved that if F is the free abelian profinite group with d generators then $\mathrm{d_P}(F) = d+1$ (see [3]), and A. Mann proved that

Received April 4, 2005 and in revised form September 7, 2005

the same result holds if F is the free pronilpotent group with d generators (see [6]).

The case of prosoluble groups has been dealt with in [7], [6] and [5]. In particular, in [5] it is proved that if F is the free prosoluble group of rank d, where $d \geq 10$, then $\mathrm{d_P}(F) = \lceil c_3 d - c_3 \rceil + 1$, where $c_3 = 3.243\ldots$ is the constant defined by Palfy and Wolf in [8], [10] (here $\lceil x \rceil$ denotes the smallest integer greater than or equal to x). But in the same paper [5], when $3 \leq d \leq 9$ only the bounds $\lceil c_3 d - c_3 \rceil + 1 \leq \mathrm{d_P}(F) \leq \lceil \max\{c_3 d - c_3 + 1, c_2 d\} \rceil$ are provided, and for $d = 2$ no non-trivial lower bound for $\mathrm{d_P}(F)$ is given. Our results fill this gap, so that the value of $\mathrm{d_P}(F)$ is now known for every finitely generated free prosoluble group. Namely the following holds:

THEOREM A: *Let F be a free prosoluble group of rank d, where $d \geq 2$. Then* $\mathrm{d_P}(F) = \lceil c_3 d - c_3 \rceil + 1$.

(We note that when $d = 1$ then F is abelian, so that $\mathrm{d_P}(F) = 2$ by [3].)

It is well known that a profinite group is PFG if and only if it has polynomial maximal subgroup growth ([4, Theorem 11.1]); for such a group G, following [6], we define the degree of maximal subgroup growth

$$s(G) = \limsup(\log m_n(G)/\log n) = \inf\{s | m_n(G) \leq Cn^s, \text{ for some } C\},$$

where $m_n(G)$ is the number of (closed) maximal subgroups of G of index n.

It turns out that in the case of a prosoluble group G the invariants $s(G)$ and $\mathrm{d_P}(G)$ are strictly related, so that, as in [5], our results can be used to prove the following:

THEOREM B: *Let F be the free prosoluble group of rank d with $d \geq 2$; then* $s(F) = c_3 d - c_3 + 1$.

The line of the proofs is the same as in [5], so rather than repeating here all the details, we prefer to indicate which are the integrations and the modifications that need to be done.

Proof of Theorem A: Theorem A is proved by showing separately that $\lceil c_3 d - c_3 \rceil + 1$ is both a lower and an upper bound for $\mathrm{d_P}(F)$. Section 1 deals with the lower bound, and only the missing case $d = 2$ needs to be considered. In section 2 we prove that $\lceil c_3 d - c_3 \rceil + 1$ is an upper bound for $\mathrm{d_P}(F)$ for every $d \geq 2$. This, together with Theorem 1 of [5], is enough to prove Theorem A. ∎

The proof of Theorem B is the same as in [5], and will not be reported here.

1. The lower bound

THEOREM 1: *Let F be the free prosoluble group of rank d, with $d \geq 2$; then* $d_P(F) \geq c_3 d - c_3 + 1$.

Proof: We show how to modify the proof of Theorem 1 of [5] in order that it holds also when $d = 2$.

Let G_i be the group described in section 3 of [5]. We need to determine how fast $P(G_i, 2)$ tends to zero when i tends to ∞. By (23) of [5] we have

$$P(G_i,2) = \frac{3}{8}\prod_{r=0}^{i}\left(1-\frac{1}{3^{4^r}}\right)\prod_{r=0}^{i}\prod_{j=0}^{2\cdot 4^r-1}\left(1-\frac{1}{2^{2\cdot 4^r - j}}\right).$$

Use of the fact that $\log(1+x) \geq \frac{7}{5}x$ for every x such that $-\frac{1}{2} \leq x \leq 0$ and the inequalities $\sum_{r=0}^{i} 1/3^{4^r} < \sum_{s=1}^{\infty} 1/3^s = \frac{1}{2}$ and $\sum_{j=0}^{2\cdot 4^r-1} 1/2^{2\cdot 4^r - j} < 1$ give $\prod_{r=0}^{i}(1-1/3^{4^r}) \geq e^{-7/10}$ and $\prod_{j=0}^{2\cdot 4^r-1}(1-1/2^{2\cdot 4^r-j}) \geq e^{-7/5}$, so that

$$P(G_i,2) \geq \frac{3}{8}e^{-\frac{7}{10}}e^{-\frac{7}{5}(i+1)} \geq \bar{C}e^{-\frac{7}{5}i}$$

for some positive constant $\bar{C}$.

As $i = \log_4 \log_9 n = \frac{1}{\log 4}(\log\log n - \log\log 9)$ we obtain

$$P(G_i,2) \geq C(\log n)^{-\frac{7}{5\log 4}} = Cn^{-\frac{7}{5\log 4}\frac{\log\log n}{\log n}},$$

for some positive constant C, so that (14) of [5] becomes

$$\begin{aligned}\nu_i = P(G_i,2)|G_i|^2/|\operatorname{Aut}(G_i)| &\geq ACn^{c_3-1-B\frac{(\log\log n)^2}{\log n}-\frac{7}{5\log 4}\frac{\log\log n}{\log n}} \\ &\geq \bar{A}n^{c_3-1-\bar{B}\frac{(\log\log n)^2}{\log n}},\end{aligned} \tag{1}$$

for some positive constants $\bar{A}, \bar{B}$.

The proof is now the same as in section 2 of [5], using (1) instead of (14). This concludes the proof of Theorem 1. ∎

2. The upper bound

This section is devoted to the proof of the following:

THEOREM 2: *Let F be the free prosoluble group of rank d, with $d \geq 2$; then* $d_P(F) \leq \lceil c_3 d - c_3 \rceil + 1$.

Throughout this section, unless otherwise specified, all our logarithms will be to the base 2.

Proof of Theorem 2: Again, we follow the proof in section 1 of [5]. The following lemma plays the role of Lemma 1.1 in [5].

LEMMA 3: *Let $M \leq \mathrm{GL}(p,n)$ be a maximal irreducible solvable linear group. Then $n = rs$ and $M = H \wr S$, where $H \leq \mathrm{GL}(r,p)$, $S \leq \mathrm{Sym}(s)$ and either $|M| \leq p^{\frac{6}{5}n}$ or $r < k$ for some absolute constant k.*

Proof: We have that $M = H \,\mathrm{wr}\, S$, where $H \leq \mathrm{GL}(r,p)$ is a maximal primitive solvable subgroup of $\mathrm{GL}(r,p)$, S is a maximal solvable transitive permutation subgroup of $\mathrm{Sym}(s)$ and $n = rs$. The structure of maximal primitive solvable groups is described by Suprunenko [9, §19–21]. Let F be the maximal abelian normal subgroup of H, $V = C_H(F)$, and let A/F be the maximal abelian normal subgroup of H/F contained in V/F. Then the following hold: $r = ab$, $|H/V| \leq a$, $|F| = p^a - 1$, $|A/F| = b^2$ and if

$$b = \prod_{i=1}^{m} q_i^{e_i}$$

is the factorization of b in the product of distinct primes q_i, we have that V/A is isomorphic to a solvable subgroup of the direct product of the symplectic groups $\mathrm{Sp}(2e_i, q_i)$. It follows that

$$|V/A| \leq \prod_{i=1}^{m} |\mathrm{Sp}(2e_i, q_i)| < \prod_{i=1}^{m} q_i^{(2e_i)^2}.$$

We note that $e_i = \log_{q_i} q_i^{e_i} \leq \log q_i^{e_i} \leq \log b$, so that

$$\prod_{i=1}^{m} q_i^{4e_i^2} \leq \prod_{i=1}^{m} (q_i^{e_i})^{4\log b} \leq b^{4\log b}.$$

It follows that

$$|H| = |H/V||V/A||A/F||F| \leq ab^2 b^{4\log b}(p^a - 1).$$

By Theorem 3 of [2] we have that $|S| \leq \frac{1}{\sqrt[3]{24}} 24^{s/3}$, so it follows that

$$|M| = |H|^s|S| < a^s b^{(4\log b+2)s}(p^a - 1)^s 24^{s/3} < a^s b^{(4\log b+2)s} p^{as} 24^{s/3}.$$

We note that

$$\log a < \frac{1}{10} a \quad \text{for all } a > 64. \tag{2}$$

Let now B_1 and A_1 be positive integers such that:

$$4\log^2 b + 2\log b + \frac{1}{3}\log 24 + \log 64 < \frac{1}{10}b \quad \text{for all } b \geq B_1 \tag{3}$$

and

$$\log a + 4\log^2 B_1 + 2\log B_1 + \frac{1}{3}\log 24 < \frac{1}{5}a \quad \text{for all } a \geq A_1. \tag{4}$$

We now prove the following:

$$\text{if } a \geq A_1 \text{ or } b \geq B_1 \text{ then } |M| < p^{\frac{6}{5}abs}. \tag{5}$$

To prove (5) it is enough to show that $ab^{4\log b+2}24^{\frac{1}{3}} < p^{\frac{1}{5}ab}$, i.e. that

$$\log_p a + (4\log b + 2)\log_p b + \frac{1}{3}\log_p 24 < \frac{1}{5}ab. \tag{6}$$

Moreover, as $\log_p x \leq \log_2 x$, it is enough to prove (6) for $p = 2$.

If $b \geq B_1$ we have

$$\begin{aligned}\log a + (4\log b + 2)\log b + \frac{1}{3}\log 24 &\leq \max\left\{\frac{1}{10}a, \log 64\right\} \\ &\quad + 4\log^2 b + 2\log b + \frac{1}{3}\log 24 \\ &< \frac{1}{10}a + \frac{1}{10}b \leq \frac{1}{5}ab,\end{aligned}$$

as we wanted.

If $1 \leq b < B_1$ and $a \geq A_1$ by (3) we have

$$\log a + (4\log b + 2)\log b + \frac{1}{3}\log 24 < \frac{1}{5}a \leq \frac{1}{5}ab,$$

and this concludes the proof of (5).

Taking $k = A_1B_1$ we obtain what we wanted. ∎

Lemma 4: *Let $M = H \wr S \leq \mathrm{GL}(n,p)$ be an irreducible linear group, where $n = rs$, $H \leq \mathrm{GL}(r,p)$ and $S \leq \mathrm{Sym}(s)$ is transitive. If T is an irreducible subgroup of M, then $|C_M(T)| \leq p^{2r}n$.*

Proof: The proof is the same as Lemma 1.2 in [5]. We just note that an element $g \in GL(r,p)$ has order at most p^{2r}, because the p-part of the order is at most p^{r-1} and the p'-part of the order is at most $p^r - 1$. ∎

We now resume the proof of Theorem 2. The argument in section 1 of [5] shows that we need to study

$$\sum_{p\in P}\sum_{n=1}^{\infty}\frac{W(p,n)}{(p-1)p^{(k-d)n}},$$

where $W(p,n)$ is the number of isomorphism classes of irreducible G-modules of order p^n.

By the definition of c_p (see [8, Theorem 1]) we have that $\lim_{p\to\infty} c_p = 2$, so there exists a prime q such that

$$c_p < \frac{11}{5} \quad \text{for all primes } p > q. \tag{7}$$

For these primes formula (7) of [5] gives

$$W(p,n) \le \frac{1}{\sqrt[3]{24}}p^{[\frac{6}{5}d+f_p(n)]n}.$$

Now we deal separately with the primes $p \le q$, arguing for all of them as is done in [5] for $p = 3$ and using Lemmas 3 and 4 in place of Lemma 1.1 and Lemma 1.2 of [5], respectively.

Arguing in the same way as for (9) of [5] we obtain

$$W(p,n) \le p^{[\frac{6}{5}d+f_p(n)]n} + \frac{q^{2k}}{\sqrt[3]{24}}p^{[(c_p-1)d-c_p+1+\frac{\log_p n}{n}+f_p(n)]n}, \tag{8}$$

and as $(c_3-1)d-c_3+1 \ge \max_{p\neq 3}\{(c_p-1)d-c_p+1, \frac{6}{5}d\}$ for all $d \ge 2$ we have

$$W(p,n) \le p^{[(c_3-1)d-c_3+1+o(1)]n}, \tag{9}$$

for all primes $p \le q$.

We are now reduced to studying the following series:

$$\sum_{2\le p\le q}\sum_{n=1}^{\infty}\frac{p^{[(c_3-1)d-c_3+1+o(1)]n}}{p^{(k-d)n}} + \sum_{p>q}\sum_{n=1}^{\infty}\frac{p^{\frac{6}{5}dn+f_p(n)n}}{p^{1+(k-d)n}}. \tag{10}$$

By the same arguments as in [5] we obtain that the series (10) converges for $k > \max\{c_3d - c_3 + 1, \frac{11}{5}d\} = c_3d - c_3 + 1$, and this concludes the proof of Theorem 2. ∎

References

[1] A. V. Borovik, L. Pyber and A. Shalev, *Maximal subgroups in finite and profinite groups*, Transactions of the American Mathematical Society **348** (1996), 3745–3761.

[2] J. D. Dixon, *The Fitting subgroup of a linear solvable group*, Journal of the Australian Mathematical Society **7** (1967), 417–424.

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

[4] A. Lubotzky and D. Segal, *Subgroup Growth*, Progress in Mathematics, 212, Birkhäuser Verlag, Basel, 2003.

[5] A. Lucchini, F. Menegazzo and M. Morigi, *On the probability of generating prosoluble groups*, Israel Journal of Mathematics, this volume.

[6] A. Mann, *Positively finitely generated groups*, Forum Mathematicum **8** (1996), 429–459.

[7] I. Pak, *On probability of generating a finite group*, preprint.

[8] P. P. Palfy, *A polynomial bound for the orders of primitive solvable groups*, Journal of Algebra **77** (1982), 127–137.

[9] D. A. Suprunenko, *Matrix Groups*, American Mathematical Society, Providence, R.I., 1976.

[10] T. R. Wolf, *Solvable and nilpotent subgroups of* $\mathrm{GL}(n, q^m)$, Canadian Journal of Mathematics **34** (1982), 1097–1111.