ILLINOIS JOURNAL OF MATHEMATICS
Volume 37, Number 1, Spring 1993

RANDOM ELEMENTS OF A FREE PROFINITE GROUP GENERATE A FREE SUBGROUP

ALEXANDER LUBOTZKY[1]

Consider each profinite group as a probability space, the probability being the normalized Haar measure. Jarden proved that almost all $z \in \hat{\mathbf{Z}}$ generate a closed subgroup of infinite index while almost all k-tuples with $k \geq 2$ generate an open subgroup [FJ, Lemma 16.15]. Moreover, the closed subgroup of $\hat{\mathbf{Z}}$ generated by an e-tuple $(z_1, \ldots, z_e)$ which is chosen at random is isomorphic to $\hat{\mathbf{Z}}$. Fried and Jarden ask for $e \geq 2$ about the probability that a e-tuple $(x_1, \ldots, x_e) \in \hat{F}_e$ generates a closed subgroup which is isomorphic to $\hat{F}_e$ and about the probability that a e-tuple of elements of $\hat{F}_e$ generates an open subgroup [FJ, Problem 16.16]. Here $\hat{F}_e$ is the free profinite group of rank e.

W. M. Kantor and the present author show [KL] that the second probability is 0. The aim of this note is to prove that the first probability is 1. Actually the full result is somewhat more general:

THEOREM 1. *Let F be a free profinite group of rank at least* 2, *and let k be a positive integer.*

(a) *The probability that a k-tuple of elements of F generates an open subgroup is* 0.

(b) *The probability that a k-tuple of elements of F generates a closed subgroup which is isomorphic to $\hat{F}_k$ is* 1.

As mentioned, part (a) is proved in [KL]. We supply a proof which replaces the use of Dixon's theorem by more elementary arguments. Some of the ingredients of the proof of (a) are also used in the proof of (b).

Notation. For a finite group and a positive integer e let

$$d_e(G) = \max\{m \in \mathbf{N} \mid G^m \textit{ is generated by e elements}\}$$

$$D_e(G) = \{(x_1, \ldots, x_e) \in G^e \mid \langle x_1, \ldots, x_e \rangle = G\}$$

Received April 15, 1991
1991 Mathematics Subject Classification. Primary 20E18.
[1]Partially supported by a grant from the G.I.F., the German-Israeli Foundation for Scientific Research and Development.

LEMMA 2 (P. Hall). *If G is a simple nonabelian group, then* $d_e(G) = |D_e(G)|/|\mathrm{Aut}|(G)|$.

Proof. Fix a basis $z_1, \ldots, z_e$ of the free discrete group F_e. The map

$$\psi \mapsto (\psi(z_1), \ldots, \psi(z_e))$$

establishes a bijection between the set of all epimorphisms $\psi\colon F_e \to G$ and $D_e(G)$. Two epimorphisms have the same kernel if and only if their images in $D_e(G)$ belong to the same orbit under $\mathrm{Aut}(G)$. It follows that F_e has exactly $d' = |D_e(G)|/|\mathrm{Aut}(G)|$ normal subgroups N such that $F_e/N \cong G$.

List all these subgroups as $N_1, \ldots, N_{d'}$ and let $M = N_1 \cap \cdots \cap N_{d'}$. As G is simple and nonabelian $F_e/M \cong G^{d'}$ (a simple consequence of [H, p. 51, Satz 9.12]). In particular $G^{d'}$ is generated by e elements and therefore $d' \le d = d_e(G)$.

On the other hand the definition implies that G^d is a quotient of F_e. Hence F_e has at least d normal subgroups N with $F_e/N \cong G$. Conclude that $d \le d'$ and therefore $d = d'$, as desired.

Dixon [D] proves that the probability that a pair $(x, y) \in A_n$ generates A_n tends to 1 as $n \to \infty$. In other words

$$\frac{|D_2(A_n)|}{(n!)^2/4} \xrightarrow[n\to\infty]{} 1$$

Thus, if n is large enough, then $|D_2(A_n)| \ge (n!)^2/8$. This inequality is used in [KL] to prove part (a) of the theorem. We would like here to prove a weaker inequality which suffices for proving part (a) of the theorem.

LEMMA 3. *Let $n \ge 7$ be an odd integer. Then* $|D_2(A_n)| \ge (n-3)!(n-7)!$.

Proof. Let $\gamma = (1\,2\,3)$ and let $\rho = (b_3\, b_4 \cdots b_n)$ be a cyclic permutation of the set $B = \{3, 4, \ldots, n\}$. We claim that

$$A_n = \langle \gamma, \rho \rangle. \tag{1}$$

To prove (1) it suffices to prove that $H = \langle \gamma, \rho\rangle$ contains each 3-cycle. Assume without loss that $b_3 = 3$. Then

$$\sigma = \rho^\gamma = (1\, b_4 \cdots b_n) \in H \quad \text{and} \quad \tau = \rho^{\gamma^2} = (2\, b_4 \cdots b_n) \in H.$$

Hence, for each $k \ge 4$

$$(b_k\, 2\, 3) = \gamma^{\sigma^{k-3}}, \quad (1\, b_k\, 3) = \gamma^{\tau^{k-3}}, \quad \text{and} \quad (1\, 2\, b_k) = \gamma^{\rho^{k-3}}$$

belong to H. Finally, let b, c, d, e be distinct elements of B. Then $(2\ c\ b) = (1\ 2\ b)^{(1\ 2\ c)}$, $(c\ b\ 1) = (1\ b\ 3)^{(1\ c\ 3)}$, $(b\ 3\ c) = (b\ 2\ 3)^{(c\ 2\ 3)}$, and $(d\ b\ c) = (2\ b\ c)^{(2\ d\ 3)}$ belong to H. Conclude that every 3-cycle of $\{1, 2, \ldots, n\}$ belongs to H. Hence, $H = A_n$, as asserted.

An alternative argument was suggested to us by Michael Fried: One observes that H is a primitive subgroup of A_n which contains a 3-cycle. A consequence of a theorem of Jordan therefore implies that $H = A_n$ [H, p. 171, Satz 4.5c)].

Next check the residues modulo 6 to find a positive integer m with $n - 6 \le m \le n - 3$ which is prime to 6. Each cyclic permutation $\alpha = (a_1 a_2 \cdots a_m)$ of m integers in $A = \{4, 5, \ldots, n\}$ belongs to A_n. Moreover, $(\alpha\gamma)^m = \alpha^m \gamma^m = \gamma^m = \gamma^{\pm 1}$. Hence, by (1), $A_n = \langle \alpha\gamma, \rho \rangle$. There are $n(n-1) \cdots (n-m+1)/m$ permutations α and $(n-3)!$ permutations ρ. The former number is $\ge (m-1)!$. Hence, $|D_2(A_n)| \ge (n-7)!(n-3)!$, as asserted. ∎

LEMMA 4. *For each odd integer $n \ge 7$, the group $L_n = A_n^{[(n-3)!(n-7)!/n!]}$ is generated by 2 elements.*

Proof. By [H. p. 175], $\mathrm{Aut}(A_n) \cong S_n$. Hence $|\mathrm{Aut}(A_n)| = n!$. It follows from Lemmas 2 and 3 that $d_2(A_n) = |D_2(A_n)|/n! \ge [(n-3)!(n-7)!/n!]$. Conclude that L_n is generated by 2 elements. ∎

LEMMA 5. *The probability that a k-tuple of elements of L_n generates L_n tends to 0 as n tends to infinity over the odd positive integers.*

Proof. In order for a k-tuple of elements of L_n to generate L_n its projection on each of the factors must generate A_n. The probability of the last event is at most $1 - 1/n^k$, since a k-tuple of elements which belong to the subgroup A_{n-1} of index n, does not generate A_n. Hence the probability that a k-tuple of elements of L_n generates L_n is at most

$$\left(1 - \frac{1}{n^k}\right)^{(n-3)!(n-7)!/n!} = \left\{\left(1 - \frac{1}{n^k}\right)^{n^k}\right\}^{(n-3)!(n-7)!/n!n^k}$$

The expression in the braces tends to $1/e$ (where here e is of course the basis of the natural logarithms) while the exponent tends to infinity as n tends to infinity over the odd positive integers. Conclude that the right hand side tends to 0 as $n \to \infty$. ∎

PROPOSITION 6. *For $e \ge 2$ and $k \ge 1$, the probability for a k-tuple of elements of $\hat{F}_e$ to generate $\hat{F}_e$ is 0.*

Proof. Let $n \geq 7$ be an odd integer. By Lemma 4, there is an epimorphism $\psi\colon \hat{F}_e \to L_n$. If $(x_1, \dots, x_k) \in (\hat{F}_e)^k$ generates $\hat{F}_e$, then its image under ψ generates L_n. Hence, the probability for a k-tuple of elements of $\hat{F}_e$ to generate $\hat{F}_e$ is at most the probability for a k-tuple of elements of L_n to generate L_n. By Lemma 5, the latter probability tends to 0 as $n \to \infty$. Hence the former probability is 0. ■

Proof of Theorem 1(a). If rank(F) is infinite, then so is the rank of each open subgroup. Hence, we may assume that $F = \hat{F}_e$ with $e \geq 2$.

Each open subgroup of $\hat{F}_e$ is isomorphic to $\hat{F}_f$ for some f [FJ, Prop. 15.27]. For each f, the group $\hat{F}_e$ has only finitely many open subgroups of index at most f [FJ, Lemma 15.1]. So, apply Proposition 6, to these subgroups to conclude that the probability of a k-tuple to generate an open subgroup of F is 0. ■

Proof of Theorem 1(b). First note that F can be mapped onto $\hat{F}_e$ with $e \geq 2$. If the theorem holds for the quotient, it holds for F. So, we may assume that $F = \hat{F}_e$ with $e \geq 2$. There are two cases to consider.

Case A. $e \geq k + 3$. To prove that $G = \langle x_1, \dots, x_k \rangle$ is isomorphic to $\hat{F}_k$ it suffices to show that each finite group B which is generated by k elements is a quotient of G [FJ, Lemma 15.29]. Since there are only countably many finite groups, it suffices to fix a finite group B and to prove that for almost all $(x_1, \dots, x_k) \in F^k$ the group B is a quotient of $\langle x_1, \dots, x_k \rangle$.

Indeed, fix such a B. Let $l = |B|$. Then B can be embedded in the symmetric group S_l. Consider the cycle $\kappa = (l + 1\ l + 2)$ of S_{l+2}. Define an embedding f of S_l into A_{l+2} by the following rule: $f(\pi) = \pi$ if $\pi \in A_l$ and $f(\pi) = \pi\kappa$ if $\pi \notin A_l$. Let $n(B) = \max\{7, l + 2\}$. Then we can view B as a subgroup of A_n for each $n \geq n(B)$.

Let $n \geq 7$ be an odd integer. Since A_n is generated by two elements (Lemma 3)[2],

$$|D_e(A_n)| \geq |A_n|^{e-2}.$$

Also, $|\mathrm{Aut}(A_n)| = |S_n| = 2|A_n|$ [H, p. 175]. Hence, by Lemma 2,

$$d_e(A_n) \geq \tfrac{1}{2}|A_n|^{e-3} \geq \tfrac{1}{2}|A_n|^{k}. \tag{2}$$

---

[2]Of course, this is true also for n even. For example, for $r = (1\ 2)$ and $\sigma = (2 \cdots n)$ we have $A_n = \langle \sigma, \tau\sigma\tau \rangle$. However, one of the goals of this proof is to be as self contained and as short as possible. Hence we argue only with odd n.

By definition, $A_n^{d_e(A_n)}$ is generated by e elements. Hence $A_n^{d_e(A_n)}$ is a quotient of F, with kernel N. Since A_n is simple nonabelian, it follows from the proof of Lemma 2 that F has exactly $d_e(A_n)$ open normal subgroups N_i which contain N such that $F/N_i \cong A_n$.

For each i let $\varphi_i\colon F \to A_n$ be an epimorphism with kernel N_i, and

$$B_{n,i} = \{(x_1,\dots,x_k) \in F^k \mid \langle \varphi_i(x_1),\dots,\varphi_i(x_k)\rangle = B\}.$$

Denote the probability that k elements of B generate B by $p_k(B)$. Then

$$(3) \quad \mu(B_{n,i}) = \operatorname{Prob}(\varphi_i(x_1),\dots,\varphi_i(x_k) \in B)p_k(B) = \left(\frac{|B|}{|A_n|}\right)^k p_k(B).$$

The sets $B_{n,i}$, $n \geq n(B)$, $i = 1,\dots,d_e(A_n)$ are μ-independent (again, since A_n are simple nonabelian). By (2) and (3),

$$\sum_{n\geq n(B)} \sum_{i=1}^{d_e(A_n)} \mu(B_{n,i}) = \sum_{n\geq n(B)} d_e(A_n)p_k(B)\left(\frac{|B|}{|A_n|}\right)^k$$
$$\geq \sum_{n\geq n(B)} \frac{1}{2}p_k(B)|B|^k = \infty,$$

because all terms are constant and $p_k(B) \neq 0$, since B is generated by k elements.

It follows that $\mu(\bigcup_{n,i}B_{n,i}) = 1$ [FJ, Lemma 16.6]. Each k-tuple in the union generates a closed subgroup of F which has B as a quotient.

Case B. The general case. By Part (a) of Theorem 1, almost all $(x_1,\dots,x_k)$ generate a closed subgroup G of F of infinite index. The group G is contained in an open subgroup H of F of index at least $k+2$ [R, p. 11]. Since $e \geq 2$, the group H is free of rank at least $k+3$ [FJ, Prop. 15.27]. So, by Case A, the probability for G to be contained in H and not to be free is zero. Since F has only countably many open subgroups, the probability for G not to be free is zero. This concludes the proof of Theorem 1(b). ■

Theorem 1 gets a new form if we consider free pro-p-groups instead of free profinite groups.

PROPOSITION 7. *Let $F = \hat{F}_e(p)$ be the free pro-p-group of rank e and let k be a positive integer. Let*

$$A_k = \{(x_1,\dots,x_k) \in F^k \mid \langle x_1,\dots,x_k\rangle \text{ is open in } F\}$$
$$B_k = \{(x_1,\dots,x_k) \in F^k \mid \langle x_1,\dots,x_k\rangle \cong \hat{F}_k(p)\}.$$

Then:

(a) *If* $k < e$, *then* $\mu(A_k) = 0$ *and* $\mu(B_k) = 1$;

(b) $0 < \mu(A_e) < 1$ *and* $\mu(B_e) = 1$;

(c) *If* $k > e$, *then* $0 < \mu(A_k) < 1$ *and* $0 < \mu(B_k) < 1$.

Proof of (b). By the Nielsen-Schreier Formula [FJ, Prop. 15.27], the rank of each proper open subgroup of F is greater than e. Hence,

$$A_e = \{(x_1, \ldots, x_e) \in F^e | \langle x_1, \ldots, x_e \rangle = F\}. \tag{4}$$

Let $V = F_p^e \cong F/\Phi(F)$, where $\Phi(F)$ is the Frattini subgroup of F [FJ, Lemma 20.36]. The basic property of the Frattini subgroup implies that $x_1, \ldots, x_e$ generate F if and only if their reductions $v_1, \ldots, v_e$ modulo $\Phi(F)$ generate V. The latter happens exactly if $v_1, \ldots, v_e$ are linearly independent. Hence, $\mu(A_e)$ is the probability in V^e that $v_1, \ldots, v_e$ are linearly independent. Thus

$$\mu(A_e) = \left(1 - \frac{1}{p^e}\right)\left(1 - \frac{1}{p^{e-1}}\right) \cdots \left(1 - \frac{1}{p}\right).$$

So, $0 < \mu(A_e) < 1$.

To compute $\mu(B_e)$ let $Z = \mathbf{Z}_p^e$ and choose an epimorphism $\pi \colon F \to Z$. Consider each element of Z as a column of e elements of $\mathbf{Z}_p$. In this notation $(z_1 \cdots z_e)$ denotes an $e \times e$ matrix with entries in $\mathbf{Z}_p$. Then

$$\begin{aligned} \bar{B}_e &= \{(z_1, \ldots, z_e) \in Z^e | \langle z_1, \ldots, z_e \rangle \cong Z\} \\ &= \{(z_1, \ldots, z_e) \in Z^e | \operatorname{rank}\langle z_1, \ldots, z_e \rangle = e\} \\ &= \left\{(z_1, \ldots, z_e) \in \mathbf{Z}_p^{e^2} | \operatorname{rank}(z_1 \cdots z_e) = e\right\} \\ &= \left\{(z_1, \ldots, z_e) \in \mathbf{Z}_p^{e^2} | \det(z_1 \cdots z_e) \neq 0\right\}. \end{aligned}$$

It is well known, that for each n and each nonzero polynomial $f \in \mathbf{Z}_p[X_1, \ldots, X_n]$, the hypersurface $\{(x_1, \ldots, x_n) | f(x_1, \ldots, x_n) = 0\}$ has measure 0 in $\mathbf{Z}_p^n$. Hence, $\mu(\bar{B}_e) = 1$.

Now, if $x_1, \ldots, x_e \in F$ and $(\pi(x_1), \ldots, \pi(x_e)) \in \bar{B}_e$, then $\operatorname{rank}\langle x_1, \ldots, x_e \rangle = e$. Since each closed subgroup of F is a free pro-p-group [FJ, Cor. 20.38], this implies that $\langle x_1, \ldots, x_e \rangle \cong F$ and therefore $(x_1, \ldots, x_e) \in B_e$. Thus $\pi^{-1}(\bar{B}_e) \subseteq B_e$. It follows from the preceding paragraph that $\mu(B_e) = 1$.

Proof of (a). By the above mentioned formula of Nielsen and Schreier, the rank of each open subgroup of F is at least e. Hence, in case (a), $A_k = \varnothing$ and therefore $\mu(A_k) = 0$.

To compute $\mu(B_k)$ consider the projection $\tau: F^e \to F^k$ on the first k coordinates. If $(x_1, \ldots, x_e) \in B_e$, then $\text{rank}\langle x_1, \ldots, x_k \rangle = k$ hence, $\langle x_1, \ldots, x_k \rangle \cong \hat{F}_k(p)$, and therefore $(x_1, \ldots, x_k) \in B_k$. Thus $B_e \subseteq \tau^{-1}(B_k)$. By (b), $\mu(B_k) = 1$.

Proof of (c). Let $\rho: F^k \to F^e$ be the projection on the first e coordinates. Suppose that $(x_1, \ldots, x_e) \in A_e$. By (4), $\langle x_1, \ldots, x_e \rangle = F$ and therefore $\langle x_1, \ldots, x_k \rangle = F$. Thus $\rho^{-1}(A_e) \subseteq A_k$. Hence, by (b), $0 < \mu(A_e) \leq \mu(A_k)$. Also, since $F \not\cong \hat{F}_k(p)$, we have, $\rho(B_k) < 1$.

Next use the Nielsen-Schreier formula to choose an open subgroup U of F such that $l = \text{rank}(U) > k$. The rank of each open subgroup of U is also greater than k. Hence $U^k \cap A_k = \varnothing$. Since $\mu(U^k) > 0$, this implies that $\mu(A_k) < 1$.

Finally, let $\lambda: F^l \to F^k$ be the projection on the first k coordinates. Then $B_l \subseteq \lambda^{-1}(B_k)$. Hence, $\mu(B_l) \leq \mu(B_k)$. Apply (b) to U and l instead of to F and e and conclude that $\mu(B_l) > 0$. Hence $\mu(B_k) > 0$. This concludes the proof of (c) and the proposition. ■

It will be interesting to compute the measure of A_k and B_k in the case where F is the free prosolvable group on e generators. The methods of this note do not apply to this case.

Acknowledgement. The author is indebted to Moshe Jarden for his help in writing this paper, and in particular for encouraging him to find a self contained proof of Theorem 1.

Added in proof. Recently, A. Mann showed that for the free prosolvable group on φ generators $\mu(A_k) > 0$ when k is sufficiently large ($k \geq 13/4\varphi$ + constant).

REFERENCES

[D] J. D. Dixon, *The probability of generating the symmetric group*, Math. Zeit-schrift, vol. 110 (1969), pp. 199–205.

[FJ] M. D. Fried and M. Jarden, *Field Arithmetic*, Erg. Mat. III, vol. 11, Springer, Heidelberg, 1986.

[H] B. Huppert, *Endliche Gruppen I*, Grundlehren Math. Wiss., no. 134, Springer, Berlin, 1967.

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

[R] L. Ribes, *Introduction to profinite groups and Galois cohomology*, Queen's papers in Pure and Appl. Math., vol. 24, Queen's University, Kingston, 1970.

The Hebrew University of Jerusalem
Jerusalem, Israel