Proceedings of the Edinburgh Mathematical Society (2016) **59**, 899–909
DOI:10.1017/S0013091515000504

PROBABILITY AND BIAS IN GENERATING SUPERSOLUBLE GROUPS

ELEONORA CRESTANI, GIOVANNI DE FRANCESCHI AND ANDREA LUCCHINI

Dipartimento di Matematica, Via Trieste 63, 35121 Padova, Italy
(crestani.eleonora@gmail.com; giovanni.defranceschi@auckland.ac.nz; lucchini@math.unipd.it)

(Received 25 August 2014)

Abstract We discuss some questions related to the generation of supersoluble groups. First we prove that the number of elements needed to generate a finite supersoluble group G with good probability can be quite a lot larger than the smallest cardinality $\mathrm{d}(G)$ of a generating set of G. Indeed, if G is the free prosupersoluble group of rank $d \geqslant 2$ and $\mathrm{d}_{\mathrm{P}}(G)$ is the minimum integer k such that the probability of generating G with k elements is positive, then $\mathrm{d}_{\mathrm{P}}(G) = 2d + 1$. In contrast to this, if $k - \mathrm{d}(G) \geqslant 3$, then the distribution of the first component in a k-tuple chosen uniformly in the set of all the k-tuples generating G is not too far from the uniform distribution.

Keywords: supersoluble groups; product replacement algorithm; generation; profinite groups

2010 *Mathematics subject classification:* Primary 20P05

1. Introduction

It is well known that a profinite group G, being a compact topological group, can be seen as a probability space. If we denote by μ the normalized Haar measure on G, so that $\mu(G) = 1$, the probability that k random elements generate G is defined as

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

where μ also denotes the product measure on G^k. A profinite group G is said to be positively finitely generated (PFG) if $P_G(k)$ is positive for some natural number k, and the least such natural number is denoted by $\mathrm{d}_{\mathrm{P}}(G)$. Not all finitely generated profinite groups are PFG; for example, if $\hat{F}_d$ is the free profinite group of rank $d \geqslant 2$, then $P_{\hat{F}_d}(t) = 0$ for every $t \geqslant d$ (see, for example, [**8**]). However, Mann proved that finitely generated prosoluble groups are PFG [**11**]. In [**10**, **12**] it was proved that if $\hat{F}_{d,\mathrm{sol}}$ is the free prosoluble group of rank $d \geqslant 2$, then $\mathrm{d}_{\mathrm{P}}(\hat{F}_{d,\mathrm{sol}}) = \lceil c(d-1)+1 \rceil$, with $c = \log_9 48 + \frac{1}{3}\log_9 24 + 1 \simeq 3.243$ the Pálfy–Wolf constant. As a consequence, if G is a finitely generated prosoluble group with $\mathrm{d}(G) \neq 1$, then $\mathrm{d}_{\mathrm{P}}(G) \leqslant \lceil c(\mathrm{d}(G)-1)+1 \rceil$. For several prosoluble groups this inequality is far from being sharp. For example, $\mathrm{d}_{\mathrm{P}}(G) \leqslant \mathrm{d}(G)+1$ if G is pronilpotent. The first aim of this paper is to investigate the value of $\mathrm{d}_{\mathrm{P}}(G)$

when G is a finitely generated prosupersoluble group. We will prove that in this case $\mathrm{d}_{\mathrm{P}}(G) \leqslant 2\,\mathrm{d}(G)+1$, and this result is the best possible. Indeed, we have the following theorem.

Theorem 1.1. *If G is the free prosupersoluble group of rank $d \geqslant 2$, then $\mathrm{d}_{\mathrm{P}}(G) = 2d+1$.*

In the second part of the paper we study the bias of group generators in the case of finite supersoluble groups. Let us first recall some definitions. Given a finite group G, a sequence of t group elements $(g_1, \dots, g_t)$ is called a generating t-tuple of G if $\langle g_1, \dots, g_t \rangle = G$. Let $Q_{G,t}$ be the probability distribution on G of the first components of t-tuples chosen uniformly from the set $\Phi_G(t)$ of all generating t-tuples of G. We estimate the bias of the distribution $Q_{G,t}$ considering the variation distance between $Q_{G,t}$ and the uniform distribution U_G:

$$\beta_t(G) = \|Q_{G,t} - U_G\|_{\mathrm{tv}} = \max_{B \subseteq G} |Q_{G,t}(B) - U_G(B)| = \frac{1}{2} \sum_{g \in G} \left| Q_{G,t}(g) - \frac{1}{|G|} \right|.$$

We have that $0 \leqslant \beta_t(G) \leqslant 1$, and the smaller $\beta_t(G)$ is, the closer is $Q_{G,t}$ to the uniform distribution U_G. The invariant $\beta_t(G)$ plays a crucial role when one analyses the efficiency of the 'product replacement algorithm', a practical algorithm to construct random elements of a finite group, designed by Leedham-Green and Soicher (see [**2**, **14**]). For the product replacement algorithm to generate 'random' group elements, it is necessary that $Q_{G,t}$ be close to U_G. In [**1**] Babai and Pak demonstrated a defect in the product replacement algorithm: for certain groups, $Q_{G,t}$ is far from U_G. We can reformulate their result in the context of profinite groups. Indeed, let G be a t-generated profinite group: G is the inverse limit of its finite epimorphic images G/N, where N runs over the set $\mathcal{N}$ of the open normal subgroups of G and for every choice of $N \in \mathcal{N}$ two probability distributions $Q_{G/N,t}$ and $U_{G/N}$ are defined on the quotient group G/N; this allows us to consider G as a measure space obtained as an inverse system of finite probability spaces in two different ways. One of the two measures obtained in this way is the usual normalized Haar measure μ_G. The other measure $\kappa_{G,t}$ has the property that $\kappa_{G,t}(X) = \inf_{N \in \mathcal{N}} Q_{G/N,t}(XN/N)$ for every closed subset X of G. We estimate the bias of the measure $\kappa_{G,t}$ by considering

$$\beta_t(G) = \|\kappa_{G,t} - \mu_G\|_{\mathrm{tv}} = \sup_{B \in \mathcal{B}(G)} |\kappa_{G,t}(B) - \mu_G(B)| = \sup_{N \in \mathcal{N}} \beta_t(G/N),$$

where $\mathcal{B}(G)$ is the set of measurable subsets of G. The result of Babai and Pak implies that if $\hat{F}_2$ is the free profinite group of rank 2 and $t \geqslant 4$, and then $\beta_t(\hat{F}_2) = 1$. In [**14**] Pak proposed the following problem: can one exhibit the bias for a sequence of finite soluble groups? In other words, can we produce a sequence of t-generated finite soluble groups H_n such that $\beta_t(H_n) \to 1$ as $n \to \infty$? Equivalently, does there exist a t-generated prosoluble group G with $\beta_t(G) = 1$? It is not difficult to give an affirmative answer in the particular case when $t = \mathrm{d}(G)$. For example, in [**3**] it was proved that there exists a 2-generated metabelian profinite group G with the property that

$$\mu_G(\{x \in G \mid \langle x, y \rangle = G \text{ for some } y \in G\}) = 0.$$

A more important and intriguing question is whether we can find a finitely generated prosoluble group G with the property that $\beta_t(G) = 1$ for some integer t significantly larger than $\mathrm{d}(G)$. It follows from [**14**, Proposition 1.5.1] that if G is a t-generated profinite group, then $\beta_t(G) \leqslant 1 - P_G(t)$, and so we can have $\beta_t(G) = 1$ only if $t < \mathrm{d_P}(G)$. In particular, if G is a t-generated prosoluble group with $\beta_t(G) = 1$, then $t < c(\mathrm{d}(G) - 1) + 1$, c being the Pálfy–Wolf constant, and therefore the ratio between t and the smallest cardinality $\mathrm{d}(G)$ of a generating set of G cannot be arbitrarily large. However, in [**3**] examples are given of prosoluble t-generated groups G with $\beta_t(G) = 1$ where the difference $t - \mathrm{d}(G)$ tends to infinity as $\mathrm{d}(G) \to \infty$: if $d \geqslant 3$ and $2k \leqslant d - 3$, then there exists a sequence of d-generated finite soluble groups J_n such that $\lim_{n\to\infty} \beta_{d+k}(J_n) = 1$. The groups described in [**3**] have a quite intricate structure and one would like to produce easier examples. These cannot be obtained just by considering pronilpotent groups, as in this case $\mathrm{d_P}(G) \leqslant \mathrm{d}(G) + 1$. But by Theorem 1.1, if G is the free prosupersoluble group of rank $d \geqslant 2$, then $\mathrm{d_P}(G) - \mathrm{d}(G) = d + 1$, so one could expect to have $\beta_{d+k}(G) = 1$ for k significantly larger than d. However, we will prove that this is not what occurs. In fact we have the following theorem.

Theorem 1.2. *If G is a non-cyclic finite supersoluble group and $k \geqslant 3$, then*

$$\beta_{\mathrm{d}(G)+k}(G) \leqslant \tfrac{6}{10}.$$

This shows that, given a t-generated profinite group G, the condition $P_G(t) > 0$ is sufficient to have $\beta_t(G) < 1$, but is quite far from being necessary. Indeed, the inequality $\beta_t(G) \leqslant 1 - P_G(t)$ is not sharp; in particular, we prove the following theorem.

Theorem 1.3. *For every positive real number ε there exist a positive integer t and a t-generated prosupersoluble group G such that $P_G(t) = 0$ and $\beta_t(G) \leqslant \varepsilon$.*

2. Proof of Theorem 1.1

Let G be the free prosupersoluble group of rank $d \geqslant 2$. In this section we want to compute the probability $P_G(t)$ that t randomly chosen elements of G generate G. Let $\{p_n\}_{n\in\mathbb{N}}$ be the sequence of the prime numbers in increasing order and for each $m \in \mathbb{N}$ let $\pi_m = \{p_1, \dots, p_m\}$. For every $n \in \mathbb{N}$, G has a unique π_n'-Hall subgroup, say K_n (see, for example, [**13**, Proposition 3.5]). Let $G_n = G/K_n$ and $H_n = G_n/\mathrm{Frat}(G_n)$. By [**11**, Theorem 1], we have

$$P_G(t) = \lim_{n\to\infty} P_{G_n}(t) = \lim_{n\to\infty} P_{H_n}(t). \tag{2.1}$$

The group H_n is finite [**13**, Theorem 3.8] and metabelian [**13**, Proposition 3.5]. We compute $P_{H_n}(t)$ using a formula due to Gaschütz [**5**, Satz 4]. Let X be a finite soluble group and let A be an irreducible X-module. The number $\delta_X(A)$ of complemented factors X-isomorphic to A in a chief series of X is independent of the choice of the chief series and

$$P_X(t) = \prod_A \left(\prod_{0\leqslant i\leqslant \delta_X(A)-1} 1 - \frac{|\mathrm{End}_X(A)|^i |A|^{\theta_X(A)}}{|A|^t} \right), \tag{2.2}$$

where A runs over the set of the X-irreducible modules and $\theta_X(A) = 0$ or 1 according to whether A is the trivial X-module or not. In the supersoluble group H_n any chief factor is cyclic of prime order, so we have

$$P_{H_n}(t) = \prod_{p\in\pi_n}\Bigg(\prod_{|A|=p}\Bigg(\prod_{0\leqslant i\leqslant\delta_{H_n}(A)-1} 1 - \frac{|\mathrm{End}_{H_n}(A)|^i|A|^{\theta_{H_n}(A)}}{|A|^t}\Bigg)\Bigg).$$

We need to know how many pairwise non-H_n-isomorphic H_n-modules of order p are there and, for each of these, to estimate the value of $\delta_{H_n}(A)$. Firstly, A is isomorphic to the cyclic group C_p of order $p \in \pi_n$, so $\mathrm{End}_{H_n}(A)$ is a field with p elements. Any action of H_n over C_p is identified by a homomorphism $\phi\colon H_n \to \mathrm{Aut}(C_p) \cong C_{p-1}$. Any generator of H_n can be sent to any element of C_{p-1}, so there are $(p-1)^d$ choices for ϕ. We are sure that two modules obtained by two different homomorphisms ϕ_1 and ϕ_2 are not H_n-isomorphic. Indeed, in this case we should have an automorphism $\alpha \in \mathrm{Aut}(C_p)$ such that $(x^{h^{\phi_1}})^\alpha = (x^\alpha)^{h^{\phi_2}}$ for every $x \in C_p$ and $h \in H_n$. This implies that $h^{\phi_1}\alpha = \alpha h^{\phi_2}$ for every h, and then $\phi_1 = \phi_2$ because $\mathrm{Aut}(C_p) \cong C_{p-1}$ is abelian. It remains to estimate $\delta_{H_n}(A)$. Let $Y_A = H_n/C_{H_n}(A) \leqslant \mathrm{Aut}(A)$ and for any positive integer t consider the semi-direct product $L_{A,t} = A^t \rtimes Y_A$, where Y_A acts in the same way on each of the t direct factors. Since $A \cong C_p$ with $p \in \pi_n$ and Y_A is cyclic of order dividing $p-1$, $L_{A,t}$ is a finite supersoluble π_n-group. Moreover, it follows from (2.2) that $L_{A,t}$ is d-generated if and only if $t \leqslant d - \theta_{H_n}(A)$. But then $L_{A,t}$ is an epimorphic image of the free prosupersoluble group G of rank d (and consequently of H_n) if and only if $t \leqslant d - \theta_{H_n}(A)$. On the other hand, it follows from the results proved by Gaschütz [**6**] that $L_{A,t}$ is an epimorphic image of H_n if and only if $t \leqslant \delta_{H_n}(A)$. By these two observations we have $\delta_{H_n}(A) = d - \theta_{H_n}(A)$. So

$$\begin{aligned} P_{H_n}(t) &= \prod_{p\in\pi_n}\Bigg(\prod_{|A|=p}\Bigg(\prod_{0\leqslant i\leqslant\delta_{H_n}(A)-1} 1 - \frac{|\mathrm{End}_{H_n}(A)|^i|A|^{\theta_{H_n}(A)}}{|A|^t}\Bigg)\Bigg) \\ &= \prod_{p\in\pi_n}\Bigg(\Bigg(\prod_{i=0}^{d-2} 1 - \frac{p^{i+1}}{p^t}\Bigg)^{\alpha_p}\Bigg(\prod_{i=0}^{d-1} 1 - \frac{p^i}{p^t}\Bigg)\Bigg) \\ &= \prod_{p\in\pi_n}\Bigg(\Bigg(\prod_{i=1}^{d-1} 1 - \frac{p^{i}}{p^t}\Bigg)^{\alpha_p}\Bigg(\prod_{i=0}^{d-1} 1 - \frac{p^i}{p^t}\Bigg)\Bigg), \end{aligned}$$

where $\alpha_p = (p-1)^d - 1$; the first factor involves all non-trivial H_n-submodules A of order p, and the second factor regards the trivial H_n-submodule. But then, by (2.1), we obtain

$$P_G(t) = \prod_{p}\Bigg(\Bigg(\prod_{i=1}^{d-1} 1 - \frac{p^{i}}{p^t}\Bigg)^{\alpha_p}\Bigg(\prod_{i=0}^{d-1} 1 - \frac{p^i}{p^t}\Bigg)\Bigg).$$

We are looking for the minimum integer t such that $P_G(t) > 0$. Since the factors in this product lie between 0 and 1, writing the product as $\prod_n(1 + x_n)$, its convergence is equivalent to the convergence of the sum $\sum_n x_n$. Hence, $P_G(t)$ is positive if and only if

https://doi.org/10.1017/S0013091515000504 Published online by Cambridge University Press

the sum

$$\sum_p \left(\sum_{i=1}^{d-1} \Big((p-1)^d - 1 \Big) \frac{p^i}{p^t} + \sum_{i=0}^{d-1} \frac{p^i}{p^t} \right) \sim \sum_p \frac{p^{2d-1}}{p^t}$$

is convergent, i.e. if and only if $t \geqslant 2d+1$.

3. Some properties of $\beta_t(G)$

Given a finite group G and a subset X of G, for any positive integer t let $\phi_G(X,t)$ denote the number of ordered t-tuples $(g_1,\dots,g_t)$ of group elements such that $G = \langle X, g_1, \dots, g_t \rangle$. The number

$$P_G(X,t) = \frac{\phi_G(X,t)}{|G|^t}$$

is the probability that t randomly chosen elements generate G together with the elements of the subset X. We will write $P_G(g,t)$ instead of $P_G(\{g\},t)$ and $P_G(t)$ instead of $P_G(\emptyset,t)$.

Now let t be a positive integer with $\mathrm{d}(G) \leqslant t$. Let $Q_{G,t}$ be the probability distribution of the first component of $(g_1,\dots,g_t)$, where $(g_1,\dots,g_t)$ is selected uniformly at random from among all the t-tuples that generate G. So if $X \subseteq G$, then $Q_{G,t}(X)$ is the probability that $g_1 \in X$ given that $\langle g_1,\dots,g_t\rangle = G$. In particular,

$$Q_{G,t}(X) = \frac{\sum_{x\in X} |\varPhi_G(x,t-1)|}{|\varPhi_G(t)|} = \frac{\sum_{x\in X} P_G(x,t-1)}{P_G(t)|G|}.$$

We estimate the bias of the distribution $Q_{G,t}$ considering the variation distance between $Q_{G,t}$ and U_G:

$$\|Q_{G,t} - U_G\|_{\mathrm{tv}} = \max_{B\subseteq G} |Q_{G,t}(B) - U_G(B)| = \frac{1}{2} \sum_{g\in G} \left| Q_{G,t}(g) - \frac{1}{|G|} \right|.$$

We will use the notation

$$\beta_t(G) := \|Q_{G,t} - U_G\|_{\mathrm{tv}} \quad \text{and} \quad \sigma_{G,t}(g) := \frac{P_G(g,t-1)}{P_G(t)}.$$

Moreover, let

$$\varDelta_G^+(t) = \{g \in G \mid P_G(g,t-1) \geqslant P_G(t)\}, \qquad \varDelta_G^-(t) = \{g \in G \mid P_G(g,t-1) < P_G(t)\}.$$

We have

$$\beta_t(G) = \frac{1}{2|G|} \sum_{g\in G} |\sigma_{G,t}(g) - 1| = \frac{1}{2|G|} \left(\sum_{g\in \varDelta_G^+(t)} (\sigma_{G,t}(g) - 1) + \sum_{g\in \varDelta_G^-(t)} (1 - \sigma_{G,t}(g)) \right).$$

On the other hand, $\varPhi_G(t)$ is the disjoint union of the subsets $\varPhi_G(g,t-1)$, $g \in G$, and hence $\sum_{g\in G} \sigma_{G,t}(g) = |G|$, and therefore

$$\left(\sum_{g\in \varDelta_G^+(t)} (\sigma_{G,t}(g) - 1) \right) + \left(\sum_{g\in \varDelta_G^-(t)} (\sigma_{G,t}(g) - 1) \right) = 0$$

https://doi.org/10.1017/S0013091515000504 Published online by Cambridge University Press

and

$$\beta_t(G) = \frac{1}{|G|}\Bigg(\sum_{g\in\Delta_G^+(t)}(\sigma_{G,t}(g)-1)\Bigg) = \frac{1}{|G|}\Bigg(\sum_{g\in\Delta_G^-(t)}(1-\sigma_{G,t}(g))\Bigg). \tag{3.1}$$

Assume that N is a normal subgroup of the finite group G. We want to compare $\beta_t(G)$ and $\beta_t(G/N)$. First we need to study the relation between the two probability distributions $Q_{G,t}$ and $Q_{G/N,t}$. Let $\bar{G} = G/N$ and, for any $g \in G$, denote by $\bar{g}$ the element gN of $\bar{G}$.

Lemma 3.1 (Crestani and Lucchini [3, Lemma 4]). $Q_{G,t}(gN) = Q_{\bar{G},t}(\bar{g})$.

Proposition 3.2. *If $N \trianglelefteq G$ and $t \geqslant \mathrm{d}(G)$, then $\beta_t(G) \geqslant \beta_t(G/N)$. Equality holds if and only if $(\sigma_{G,t}(g_1)-1)(\sigma_{G,t}(g_2)-1) \geqslant 0$ whenever g_1 and g_2 are in the same coset of N in G.*

Proof. Let $g_1,\dots,g_m$ be a transversal of N in G. We have

$$\begin{aligned}\beta_t(G) = \frac{1}{2}\Bigg(\sum_{g\in G}\bigg|Q_{G,t}(g)-\frac{1}{|G|}\bigg|\Bigg) &= \frac{1}{2}\Bigg(\sum_{1\leqslant i\leqslant m}\Bigg(\sum_{n\in N}\bigg|Q_{G,t}(g_in)-\frac{1}{|G|}\bigg|\Bigg)\Bigg)\\ &\geqslant \frac{1}{2}\Bigg(\sum_{1\leqslant i\leqslant m}\bigg|\sum_{n\in N}\bigg(Q_{G,t}(g_in)-\frac{1}{|G|}\bigg)\bigg|\Bigg)\\ &= \frac{1}{2}\Bigg(\sum_{1\leqslant i\leqslant m}\bigg|Q_{G,t}(g_iN)-\frac{|N|}{|G|}\bigg|\Bigg)\\ &= \frac{1}{2}\Bigg(\sum_{1\leqslant i\leqslant m}\bigg|Q_{\bar{G},t}(\overline{g_i})-\frac{1}{|\bar{G}|}\bigg|\Bigg)\\ &= \beta_t(\bar{G}).\end{aligned}$$

To conclude, notice that the equality holds if and only if for each $i \in \{1,\dots,m\}$ we have

$$\sum_{n\in N}\bigg|Q_{G,t}(g_in)-\frac{1}{|G|}\bigg| = \bigg|\sum_{n\in N}\bigg(Q_{G,t}(g_in)-\frac{1}{|G|}\bigg)\bigg|$$

or, equivalently,

$$\sum_{n\in N}|\sigma_{G,t}(g_in)-1| = \bigg|\sum_{n\in N}(\sigma_{G,t}(g_in)-1)\bigg|.$$

This is equivalent to saying that $(\sigma_{G,t}(g_in_1)-1)(\sigma_{G,t}(g_in_2)-1) \geqslant 0$ for every $n_1, n_2 \in N$. □

If $f \in \mathrm{Frat}(G)$, the Frattini subgroup of G, then $P_G(g,t) = P_G(gf,t)$ for each $g \in G$. This implies that $\sigma_{G,t}(g_1) = \sigma_{G,t}(g_2)$ whenever $g_1\,\mathrm{Frat}(G) = g_2\,\mathrm{Frat}(G)$, and therefore, by the previous proposition, $\beta_t(G) = \beta_t(G/N)$ whenever $N \leqslant \mathrm{Frat}\,G$.

4. Proofs of Theorems 1.2 and 1.3

Before we start with the proof of Theorem 1.2, we need to recall some results that make it possible to compute $P_G(x, t-1)$ and consequently $\sigma_{G,t}(g)$.

Let $\mathcal{R}$ be the ring of Dirichlet polynomials $P(s) = \sum_n a_n/n^s$ with integer coefficients. As was noticed by Hall [**7**], applying the Möbius inversion formula we obtain

$$\phi_G(X, t) = \sum_{X \subseteq H \leqslant G} \mu(H, G)|H|^t, \tag{4.1}$$

where μ is the Möbius function associated with the subgroup lattice of G. In view of (4.1) we may write

$$P_G(X, t) = \sum_{X \subseteq H \leqslant G} \frac{\mu(H, G)}{|G : H|^t}. \tag{4.2}$$

By rearranging the summands in (4.2) we obtain a Dirichlet polynomial as follows:

$$P_G(X, s) := \sum_{n \in \mathbb{N}} \frac{a_n}{n^s} \quad \text{where } a_n := \sum_{\substack{|G:H|=n,\\ X \subseteq H \leqslant G}} \mu(H, G).$$

Let $1 = N_l \leqslant \cdots \leqslant N_0 = G$ be a chief series of G. In [**9**] it is proved that to each chief factor N_{i-1}/N_i one can associate a Dirichlet polynomial $P_{G/N_i, N_{i-1}/N_i}(X, s)$ with integer coefficients with the property that

$$P_G(X, s) = \prod_{1 \leqslant i \leqslant l} P_{G/N_i, N_{i-1}/N_i}(X, s). \tag{4.3}$$

In particular, if N is a normal subgroup of G, then there exists $P_{G,N}(X, s) \in \mathcal{R}$ with $P_G(X, s) = P_{G/N}(XN/N, s)P_{G,N}(X, s)$. More precisely, we have (see [**9**, Proposition 16])

$$P_{G,N}(X, t) = \sum_{X \subseteq H,\, NH = G} \frac{\mu(H, G)}{|G : H|^t}. \tag{4.4}$$

When G is soluble the factorization of $P_G(X, s)$ given by (4.3) is particularly simple. It was studied when $X = \emptyset$ by Gaschütz [**5**], and in [**9**] it is noted that Gaschütz's arguments can be generalized for arbitrary choices of X. The Dirichlet polynomial $P_{G/N_i, N_{i-1}/N_i}(X, s)$ corresponding to the chief factor N_{i-1}/N_i can be easily described via

$$P_{G/N_i, N_{i-1}/N_i}(X, s) = 1 - \frac{c_i}{|N_{i-1}/N_i|^s},$$

where c_i is the number of complements of N_{i-1}/N_i in G/N_i containing XN_i/N_i. In particular, $P_{G/N_i, N_{i-1}/N_i}(s) = 1$ if there is no complement of N_{i-1}/N_i in G/N_i containing XN_i/N_i (in this case we will say that N_{i-1}/N_i is an X-Frattini factor of G).

We are going to apply the previous consideration to the proof of Theorem 1.2. Let J be a finite supersoluble group with $d = \mathrm{d}(G) \geqslant 2$. Clearly, J is an epimorphic image of the free prosupersoluble group G of rank d, which was studied in § 2. Using the same notation, there exists $n \in \mathbb{N}$ with the property that all the prime divisors of $|J|$ belong to π_n, so J is indeed an epimorphic image of G_n, and therefore $J/\operatorname{Frat} J$ is an epimorphic image of $H_n = G_n/\operatorname{Frat}(G_n)$. It follows from Proposition 3.2 that

$$\beta_{d+k}(J) = \beta_{d+k}(J/\operatorname{Frat} J) \leqslant \beta_{d+k}(H_n),$$

and therefore in order to prove Theorem 1.2 it suffices to show that $\beta_{d+k}(H_n) \leqslant 0.6$ if $k \geqslant 3$.

Notice that H_n has the following structure. Let $t_n := \operatorname{lcm}\{p(p-1) \mid p \in \pi_n\}$. There are $\alpha_p = (p-1)^d - 1$ non-trivial homomorphisms $\rho_{p,1}, \dots, \rho_{p,\alpha_p}$ from $Y = (C_{t_n})^d$ to $\operatorname{Aut}(C_p) \cong C_{p-1}$ and we have

$$H_n \cong \left(\prod_{p \in \pi_n} \left(\prod_{1 \leqslant j \leqslant (p-1)^d - 1} W_{p,j}^{d-1} \right) \right) \rtimes Y,$$

where $W_{p,j} \cong C_p$ and, for each $y \in Y$ and $w \in W_{p,j}$, $w^y = w^{y^{\rho_{p,j}}}$. For any pair $(p,j) \in \pi_n \times \{1, \dots, \alpha_p\}$ let $U_{p,j} = W_{p-1}^{d-1}$ and let $W = \prod_{p,j} U_{p,j}$. We will denote by $\pi_{p,j}$ the projection $\pi_{p,j} \colon W \to U_{p,j}$.

Lemma 4.1. *Let $h = wy \in H_n$ with $w \in W$ and $y \in Y$. Define*

$$\begin{aligned} \Gamma_{p,h} &= \{j \in \{1, \dots, \alpha_p\} \mid y \in \ker \rho_{p,j}\}, & \gamma_{p,h} &= |\Gamma_{p,h}|, \\ \Lambda_{p,h} &= \{j \in \Gamma_{p,h} \mid w \in \ker \pi_{p,j}\}, & \lambda_{p,h} &= |\Lambda_{p,h}|, \\ \epsilon_{p,y} &= \begin{cases} 0 & \text{if } y \notin Y^p, \\ 1 & \text{otherwise.} \end{cases} \end{aligned}$$

We have

$$\sigma_{H_n,d+k}(h) = \prod_{p \in \pi_n} \frac{(1 - \epsilon_{p,y}/p^k)}{(1 - 1/p^{d+k})} \frac{(1 - 1/p^k)^{\lambda_{p,h}}}{(1 - 1/p^{d+k-1})^{\gamma_{p,h}}}.$$

Proof. We have

$$\sigma_{H_n,d+k}(h) = \frac{P_{H_n}(h, d+k-1)}{P_{H_n}(d+k)} = \frac{P_Y(y, d+k-1)}{P_Y(d+k)} \frac{P_{H_n,W}(h, d+k-1)}{P_{H_n,W}(d+k)}.$$

We also have

$$\frac{P_Y(y, d+k-1)}{P_Y(d+k)} = \frac{P_V(v, d+k-1)}{P_V(d+k)},$$

where $V = Y/\operatorname{Frat} Y \cong \prod_{p \in \pi_n} C_p^d$ and $v = y \operatorname{Frat} Y$. Let ω be the set of the prime divisors of $|v|$. Then

$$P_V(v, d+k-1) = \prod_{p \in \omega} \left(\prod_{0 \leqslant u \leqslant d-2} (1 - p^u/p^{d+k-1}) \right) \prod_{p \in \pi_n \setminus \omega} \left(\prod_{0 \leqslant u \leqslant d-1} (1 - p^u/p^{d+k-1}) \right).$$

It follows that

$$\frac{P_V(v,d+k-1)}{P_V(d+k)} = \frac{\prod_{p\in\omega}(\prod_{0=u}^{d-2}(1-p^u/p^{d+k-1}))\prod_{p\in\pi_n\setminus\omega}(\prod_{0=u}^{d-1}(1-p^u/p^{d+k-1}))}{\prod_{p\in\pi_n}(\prod_{0=u}^{d-1}(1-p^u/p^{d+k}))}$$
$$= \left(\prod_{\pi\in\omega}\frac{1}{1-p^{-(d+k)}}\right)\left(\prod_{p\in\pi_n\setminus\omega}\frac{1-p^{-k}}{1-p^{-(d+k)}}\right).$$

Since $p\in\omega$ if and only if $y\notin Y^p$, we conclude that

$$\frac{P_Y(y,d+k-1)}{P_Y(d+k)} = \frac{P_V(a,d+k-1)}{P_V(d+k)} = \prod_{p\in\pi_n}\frac{(1-\epsilon_{p,y}/p^k)}{(1-p^{-(d+k)})}.$$

The Y-modules $W_{p,j}$ are pairwise non-Y-isomorphic and not Y-isomorphic to any non-Frattini chief factor of Y. It follows from [**9**, Theorems 19 and 20] that this implies that

$$\frac{P_{H_n,W}(h,d+k-1)}{P_{H_n,W}(d+k)} = \prod_{p,j}\frac{P_{H_n,U_{p,j}}(h,d+k-1)}{P_{H_n,U_{p,j}}(d+k)}.$$

The value of $P_{H_n,U_{p,j}}(h,d+k-1)/P_{H_n,U_{p,j}}(d+k)$ can be determined using [**3**, Lemmas 5 and 6]. We have

$$\frac{P_{H_n,U_{p,j}}(h,d+k-1)}{P_{H_n,U_{p,j}}(d+k)} = \begin{cases} 1 & \text{if } j\notin\Gamma_{p,h}, \\ \dfrac{1-1/p^k}{1-1/p^{d+k}} & \text{if } j\in\Lambda_{p,h}, \\ \dfrac{1}{1-1/p^{d+k}} & \text{if } j\in\Gamma_{p,h}\setminus\Lambda_{p,h}, \end{cases}$$

and from this our formula can be immediately deduced. □

Now it follows from Lemma 4.1 that for every $h\in H_n$ we have

$$\begin{aligned}\sigma_{H_n,d+k}(h) &\leqslant \prod_{p\in\pi_n}\left(1-\frac{1}{p^{d+k}}\right)^{-1}\left(1-\frac{1}{p^{d+k-1}}\right)^{-\alpha_p} \\ &\leqslant \prod_{p\in\pi_n}\left(1-\frac{1}{p^{d+k-1}}\right)^{-(p-1)^d} \\ &\leqslant \prod_{p\in\pi_n}\left(1-\frac{1}{p^{d+k-1}}\right)^{-p^d} \\ &= \prod_{p\in\pi_n}\left(\left(1-\frac{1}{p^{d+k-1}}\right)^{-p^{d+k-1}}\right)^{p^{1-k}}.\end{aligned}$$

Assume that $k\geqslant 3$. Since $(1-1/n)^{-n}$ is a decreasing function, we obtain

$$\left(1-\frac{1}{p^{d+k-1}}\right)^{-p^{d+k-1}} \leqslant \left(1-\frac{1}{2^4}\right)^{-2^4} = a \leqslant 2.8084.$$

Given $n \in \mathbb{N}$, let $N_n = \sum_p 1/p^n$. We have

$$\sigma_{H_n,d+k}(h) \leqslant \prod_p a^{p^{1-k}} \leqslant a^{\sum_p 1/p^{k-1}} \leqslant a^{N_{k-1}} \leqslant a^{N_2}. \tag{4.5}$$

Since (see, for example, [**4**, p. 95])

$$N_2 = \sum_p \frac{1}{p^2} = \sum_{k=1}^{\infty} \frac{\mu(k)}{k} \ln(\zeta(2k)) = 0.4522474200\cdots,$$

we have

$$\sigma_{H_n,d+k}(h) \leqslant a^{N_2} \leqslant \tfrac{16}{10}.$$

But then, by (3.1), we conclude that

$$\beta_{d+k}(H_n) = \frac{1}{|H_n|}\Bigg(\sum_{h\in\Delta^+_{H_n}(d+k)} (\sigma_{H_n,d+k}(h) - 1)\Bigg) \leqslant \frac{|\Delta^+_{H_n}(d+k)|}{|H_n|}\frac{6}{10} \leqslant \frac{6}{10}$$

and this finishes the proof of Theorem 1.2.

With the same argument we obtain that

$$\beta_{d+k}(H_n) = \frac{1}{|H_n|}\Bigg(\sum_{h\in\Delta^+_{H_n}(d+k)} (\sigma_{H_n,d+k}(h) - 1)\Bigg) \leqslant a^{N_{k-1}} - 1.$$

Now let ε be a positive real number. Since $\lim_{m\to\infty} N_m = 0$, there exists $m_\epsilon \in \mathbb{N}$ such that $a^{N_{m_\epsilon}} - 1 \leqslant \varepsilon$. Let $d = m_\epsilon$, $t = 2m_\epsilon$ and consider the free prosupersoluble group of rank d: $\mathrm{d}_{\mathrm{P}}(G) = 0$, by Theorem 1.1, while

$$\beta_t(G) = \inf_{n\in\mathbb{N}} \beta_t(H_n) \leqslant a^{N_{m_\epsilon}} - 1 \leqslant \varepsilon,$$

and this proves Theorem 1.3.

References

1. L. Babai and I. Pak, Strong bias of group generators: an obstacle to the 'product replacement algorithm', in *Proc. 11th Annual ACM-SIAM Symposium on Discrete Algorithms, San Francisco, CA, 2000*, pp. 627–635 (ACM Press, New York, 2000).
2. F. Celler, C. R. Leedham-Green, S. Murray, A. Niemeyer and E. A. O'Brien, Generating random elements of a finite group, *Commun. Alg.* **23** (1995), 4931–4948.
3. E. Crestani and A. Lucchini, Bias of group generators in the solvable case, *Israel J. Math.* **207**(2) (2015), 739–761.
4. S. Finch, *Mathematical constants*, Encyclopedia of Mathematics and Its Applications, Volume 94 (Cambridge University Press, 2003).
5. W. Gaschütz, Die Eulersche Funktion endlicher auflösbarer Gruppen, *Illinois J. Math.* **3** (1959), 469–476.
6. W. Gaschütz, Praefrattinigruppen, *Arch. Math.* **13** (1962), 418–426.
7. P. Hall, The Eulerian functions of a group, *Q. J. Math.* **7** (1936), 134–151.

8. W. M. Kantor and A. Lubotzky, The probability of generating a finite classical group, *Geom. Dedicata* **36** (1990), 67–87.
9. A. Lucchini, The X-Dirichlet polynomial of a finite group, *J. Group Theory* **8**(2) (2005), 171–188.
10. A. Lucchini, F. Menegazzo and M. Morigi, On the probability of generating prosoluble groups, *Israel J. Math.* **155** (2006), 93–115.
11. A. Mann, Positively finitely generated groups, *Forum Math.* **8**(4) (1996), 429–459.
12. M. Morigi, On the probability of generating free prosoluble groups of small rank, *Israel J. Math.* **155** (2006), 117–123.
13. B. C. Oltikar and L. Ribes, On prosupersolvable groups, *Pac. J. Math.* **77**(1) (1978), 183–188.
14. I. Pak, What do we know about the product replacement algorithm?, in *Groups and computation III*, Ohio State University Mathematics Research Institute Publications, Volume 8, pp. 301–347 (Walter de Gruyter, Berlin, 2001).