www.theoryofgroups.ir

International Journal of Group Theory
ISSN (print): 2251-7650, ISSN (on-line): 2251-7669
Vol. 4 No. 2 (2015), pp. 49-67.

www.ui.ac.ir

BIAS OF GROUP GENERATORS IN FINITE AND PROFINITE GROUPS: KNOWN RESULTS AND OPEN PROBLEMS

ELEONORA CRESTANI AND ANDREA LUCCHINI*

Communicated by Patrizia Longobardi

Abstract. We analyze some properties of the distribution $Q_{G,k}$ of the first component in a k-tuple chosen uniformly in the set of all the k-tuples generating a finite group G (the limiting distribution of the product replacement algorithm). In particular, we concentrate our attention on the study of the variation distance $\beta_k(G)$ between $Q_{G,k}$ and the uniform distribution. We review some known results, analyze several examples and propose some intriguing open questions.

1. The product replacement algorithm and the bias of its limiting distribution

The product replacement algorithm (PRA) is a practical algorithm to construct random elements of a finite group. The algorithm was introduced and analyzed in [2], where the authors proved that it produces asymptotically uniformly distributed elements. Since then the algorithm has been widely investigated (see for example [17], [12]). The PRA is defined as follows. Let G be a finite group and let $d(G)$ be the minimal number of generators of G. For any integer $t \geq d(G)$, let $\Phi_G(t) = \{(g_1, \dots, g_t) \in G^t \mid \langle g_1, \dots, g_t \rangle = G\}$ be the set of all generating t-tuples of G. Given a generating t-tuple, a move to another such tuple is defined by first uniformly selecting a pair (i, j) with $1 \leq i \neq j \leq t$ and then applying one of the following operations with equal probability:

$$R_{i,j}^{\pm} : (g_1, \dots, g_i, \dots, g_t) \mapsto (g_1, \dots, g_i \cdot g_j^{\pm 1}, \dots, g_t),$$
$$L_{i,j}^{\pm} : (g_1, \dots, g_i, \dots, g_t) \mapsto (g_1, \dots, g_j^{\pm 1} \cdot g_i, \dots, g_t).$$

MSC(2010): Primary: 20P05; Secondary: 20F69.

Keywords: Product replecement algorithm; profinite groups; group generators.

Received: 11 October 2014, Accepted: 19 June 2015.

*Corresponding author.

To produce a random element in G, start with some generating t-tuple, apply the above moves several times, and finally return a random element of the generating t-tuple that was reached. The moves in the PRA can be conveniently encoded by the PRA graph $\Gamma_t(G)$ whose vertices are the tuples in $\Phi_G(t)$, with edges corresponding to the moves $R_{i,j}^{\pm}, L_{i,j}^{\pm}$. The algorithm consists of running a nearest neighbor random walk on this graph (a product replacement random walk) and returning a random component. Several results ensure that the graph $\Gamma_k(G)$ is connected if k is large enough and that a sufficiently long product replacement random walk reaches an almost uniform distributed generating t-tuple (these results are surveyed in [17]). But even if the graph $\Gamma_k(G)$ is connected and the product replacement random walk mixes rapidly, the resulting distribution of the output can still be biased.

The limiting distribution of the product replacement algorithm is the probability distribution $Q_{G,t}$ on G of the first components of t-tuples chosen uniformly from $\Phi_G(t)$. For the product replacement algorithm to generate "random" group elements, it is necessary that $Q_{G,t}$ be close to U_G, the uniform distribution on 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:

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

We have $0 \leq \beta_t(G) \leq 1$ and the smaller $\beta_t(G)$ is, the closer is $Q_{G,t}$ to the uniform distribution U_G. Let us give an example, considering the case when $G = \mathrm{Sym}(3)$ and $t = 2$. Since

$$\begin{aligned}\Phi_G(2) =\{&((1,2),(1,2,3)),\ ((1,3),(1,2,3)),\ ((2,3),(1,2,3)),((1,2,3),(1,2)),\\ &((1,2,3),(1,3)),\ ((1,2,3),(2,3)),\ ((1,2),(1,3,2)),\ ((1,3),(1,3,2)),\\ &((2,3),(1,3,2)),\ ((1,3,2),(1,2)),\ ((1,3,2),(1,3)),\ ((1,3,2),(2,3)),\\ &((1,2),(1,3)),\ ((1,2),(2,3)),\ ((1,3),(2,3)),\ ((1,3),(1,2)),\\ &((2,3),(1,2)),\ ((2,3),(1,3))\}\end{aligned}$$

we have

$$Q_{G,2}(g) = \begin{cases} 0 & \text{if } g = 1 \\ \frac{4}{18} & \text{if } g = (i,j) \\ \frac{3}{18} & \text{if } g = (i,j,k) \end{cases}$$

and therefore

$$\beta_2(G) = \frac{1}{2} \sum_{g \in G} \Big| Q_{G,2}(g) - \frac{1}{|G|} \Big| = \frac{1}{2} \left(\Big| 0 - \frac{1}{6} \Big| + 3 \Big| \frac{4}{18} - \frac{1}{6} \Big| + 2 \Big| \frac{3}{18} - \frac{1}{6} \Big| \right) = \frac{1}{6}.$$

As we will see in Section 4 we may extend the definition of $\beta_t(G)$ 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 in 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 $\kappa_{G,t}$ 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 the measurable subsets of G.

Partial results concerning the behavior of the bias $\beta_t(G)$ have been obtained in relation with the analysis of the efficiency of the product replacement algorithm. We think that it should be interesting to start a more systematic study, with the aim of understanding how some generation properties of a profinite group G are encoded by the behavior of the function $t \to \beta_t(G)$. In this paper we review some known results, analyze several examples and propose some intriguing open questions.

2. Computing $\beta_t(G)$ when G is a finite group

It this section we consider the case when G is a finite group and we describe how $\beta_t(G)$ can be computed.

For any positive integer t, let $\phi_G(X,t)$ denote the cardinality of the set $\Phi_G(X,t)$ 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 $P_G(\varnothing,t)$.

Now let t be a positive integer with $d(G) \le t$. 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 all the t-tuples which 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

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

For every g let us define

$$\sigma_{G,t}(g) = \frac{P_G(g,t-1)}{P_G(t)}.$$

Moreover let

$$\Delta_G^+(t) = \{g \in G \mid P_G(g,t-1) > P_G(t)\}, \quad \Delta_G^-(t) = \{g \in G \mid P_G(g,t-1) < P_G(t)\}.$$

We have

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

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

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

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

and

$$\beta_t(G) = \frac{1}{|G|}\left(\sum_{g\in\Delta_G^+(t)}(\sigma_{G,t}(g)-1)\right) = \frac{1}{|G|}\left(\sum_{g\in\Delta_G^-(t)}(1-\sigma_{G,t}(g))\right). \tag{2.1}$$

As discovered by P. Hall [7] the function $P_G(X,t)$ can be represented by a suitable Dirichlet polynomial; indeed we have

$$P_G(X,t) = \sum_{X\subseteq H\leq G}\frac{\mu_G(H)}{|G:H|^t}. \tag{2.2}$$

where μ is the Möbius function associated with the subgroup lattice of G. Moreover, let

$$N_l = 1 \leq \cdots \leq N_0 = G$$

be a chief series of G. In [10] it is proved that to each chief factor N_{i-1}/N_i it is associated a Dirichlet polynomial $P_i(X,t)$ with integer coefficients with the property that

$$P_G(X,t) = \prod_{1\leq i\leq l} P_i(X,t).$$

In the particular case when G is soluble,

$$P_G(g,t) = \prod_{1\leq i\leq l}\left(1 - \frac{c_i(g)}{|N_{i-1}/N_i|^t}\right) \tag{2.3}$$

where $c_i(g)$ is the number of complements of N_{i-1}/N_i in G/N_i containing gN_i.

It follows from (2.2) that for any $g\in G$ and $t\geq d(G)$ we have

$$\sigma_{G,t}(g) = \frac{\sum_{g\in H\leq G}\frac{\mu_G(H)|G:H|}{|G:H|^t}}{\sum_{H\leq G}\frac{\mu_G(H)}{|G:H|^t}}.$$

In particular $\sigma_{G,t}(g)\to 1$ as $t\to\infty$ and $1-\sigma_{G,t}(g)$ is a monotone function if t is large enough. Together with (2.1) this implies:

Proposition 1. *$\beta_t(G)$ is a monotonically decreasing function when t is large enough and $\beta_t(G)\to 0$ as $t\to\infty$.*

However the behavior of $\sigma_{G,t}(g)$ can be quite unpredictable when t is small: consider for example a cyclic group G of order 15 and let g be an element of order 3: it follows from (2.3) that

$$\sigma_{G,t}(g) = \frac{3^t(5^t-5)}{(3^t-1)(5^t-1)}.$$

The values of $\sigma_{G,t}(g)$ when $t \leq 5$ are described in the following table:

TABLE 1.

t	1	2	3	4	5
$\sigma_{G,t}(g)$	0	15/16	405/403	837/832	94770/94501

The first surprise is that $\sigma_{G,2}(g) < 1$ while $\sigma_{G,3}(g) > 1$, or equivalently $Q_{G,2}(g) < 1/15$ while $Q_{G,3}(g) > 1/15$: the occurrence of g in a generating pair is below average but the occurrence in a generating triple is above average. Moreover $\sigma_{G,3}(g) < \sigma_{G,4}(g)$ but $\sigma_{G,4}(g) > \sigma_{G,5}(g)$. This behavior of $\sigma_{G,t}(g)$ for small values of t makes the following question difficult to be approached:

Question 1. *Is it true that $\beta_{t_1}(G) \leq \beta_{t_2}(G)$ whenever $t_1 \geq t_2$?*

3. Normal subgroups

As one can expect, $\beta_t(G_1) \leq \beta_t(G_2)$ whenever G_1 is an epimorphic image of G_2. For the reader's convenience, we include in this section the proof of this fact, which has been already given in [4].

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

Lemma 2. $Q_{G,t}(gN) = Q_{\overline{G},t}(\overline{g})$.

Proof. We may assume $Q_{\overline{G},t}(\overline{g}) \neq 0$, otherwise we would have $Q_{G,t}(gN) = Q_{\overline{G},t}(\overline{g}) = 0$. In particular there exist $x_1, \ldots, x_{t-1} \in G$ such that $G = \langle g, x_1, \ldots, x_{t-1}, N\rangle$. If $t \in \mathbb{N}$, $X \subseteq G$ and $P_{\overline{G}}(\overline{X}, t) \neq 0$, then $P_{G,N}(X,t) = P_G(X,t)/P_{\overline{G}}(\overline{X},t)$ expresses the conditional probability that t random elements of G generate G together with the elements of X given that they generate G together with those of XN. In our case $P_{G,N}(t)|N|^t$ is the cardinality of the set

$$\Omega = \{(n, n_1, \ldots, n_{t-1}) \in N^t \mid \langle gn, x_1n_1, \ldots, x_{t-1}n_{t-1}\rangle = G\},$$

while, for any n in N, $P_{G,N}(gn, t-1)|N|^{t-1}$ is the cardinality of the set

$$\Omega_n = \{(n_1, \ldots, n_{t-1}) \in N^{t-1} \mid \langle gn, x_1n_1, \ldots, x_{t-1}n_{t-1}\rangle = G\}.$$

Clearly Ω is the disjoint union of the subsets $\{n\} \times \Omega_n$, $n \in N$, and therefore

$$\sum_{n \in N} P_{G,N}(gn, t-1)|N|^{t-1} = P_{G,N}(t)|N|^t.$$

Notice that

$$\frac{Q_{G,t}(gN)}{Q_{\overline{G},t}(\overline{g})} = \frac{\sum_{n\in N} P_G(gn, t-1)}{P_G(t)|G|} \frac{P_{\overline{G}}(t)|G|}{P_{\overline{G}}(\overline{g}, t-1)|N|}$$
$$= \frac{\sum_{n\in N} P_{G,N}(gn, t-1)}{P_{G,N}(t)|N|} = 1$$

and the conclusion follows. □

Proposition 3. *If $N \trianglelefteq G$ and $t \geq d(G)$, then $\beta_t(G) \geq \beta_t(G/N)$. The equality holds if and only if $(\sigma_{G,t}(g_1) - 1)(\sigma_{G,t}(g_2) - 1) \geq 0$ whenever g_1 and g_2 are in the same coset of $N \in G$.*

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

$$\beta_t(G) = \frac{1}{2}\left(\sum_{g\in G}\left|Q_{G,t}(g) - \frac{1}{|G|}\right|\right) = \frac{1}{2}\left(\sum_{1\leq i\leq m}\left(\sum_{n\in N}\left|Q_{G,t}(g_i n) - \frac{1}{|G|}\right|\right)\right)$$
$$\geq \frac{1}{2}\left(\sum_{1\leq i\leq m}\left|\sum_{n\in N}\left(Q_{G,t}(g_i n) - \frac{1}{|G|}\right)\right|\right) = \frac{1}{2}\left(\sum_{1\leq i\leq m}\left|Q_{G,t}(g_i N) - \frac{|N|}{|G|}\right|\right)$$
$$= \frac{1}{2}\left(\sum_{1\leq i\leq m}\left|Q_{\overline{G},t}(\overline{g_i}) - \frac{1}{|\overline{G}|}\right|\right) = \beta_t(\overline{G}).$$

The equality holds if and only if for each $i \in \{1, \ldots, m\}$ we have

$$\sum_{n\in N}\left|Q_{G,t}(g_i n) - \frac{1}{|G|}\right| = \left|\sum_{n\in N}\left(Q_{G,t}(g_i n) - \frac{1}{|G|}\right)\right|$$

or equivalently

$$\sum_{n\in N}|\sigma_{G,t}(g_i n) - 1| = \left|\sum_{n\in N}(\sigma_{G,t}(g_i n) - 1)\right|.$$

This is equivalent to have

$$(\sigma_{G,t}(g_i n_1) - 1)(\sigma_{G,t}(g_i n_2) - 1) \geq 0$$

for every $n_1, n_2 \in N$. □

Clearly, 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 it follows from the previous proposition that:

Corollary 4. *If $N \leq \mathrm{Frat}\, G$ then $\beta_t(G) = \beta_t(G/N)$.*

However the condition $\beta_t(G) = \beta_t(G/N)$ for every $t \geq d(G)$ does not implies that N is contained in the Frattini subgroup of G. For example we will see in Section 9 that $\beta_t(\mathrm{Sym}(3)) = \beta_t(\mathrm{Sym}(3)/\mathrm{Alt}(3))$ for each $t \geq 2$.

4. **Profinite groups**

Let G be a t-generated profinite group and let $\mathcal{N}$ be the set of the open normal subgroups of G. The group G is the inverse limit of the factor groups G/N where N runs in $\mathcal{N}$; for each $N \in \mathcal{N}$, the group G/N is a finite probability space with respect to the distribution $Q_{G/N,t}$. If N_1, N_2 are open normal subgroups of G with $N_1 \leq N_2$ then there is a natural epimorphism

$$\pi_{N_1,N_2} : G/N_1 \to G/N_2$$

and Lemma 2 ensures that if X is a subset of G containing N_2, then

$$Q_{G/N_2,t}(X/N_2) = Q_{G/N_1,t}(\pi^{-1}_{N_1,N_2}(X/N_2)) = Q_{G/N_1,t}(X/N_1).$$

In particular

$$(\{G/N, Q_{G/N,t}\}_{N\in\mathcal{N}}, \{\pi_{N,M}\}_{N,M\in\mathcal{N},N\leq M})$$

is an inverse system of probability spaces (see [18, Definition 2.1]). In [18] the author gives a condition on a inverse system of measure spaces that guarantees the existence and uniqueness of a limit measure space. This condition is trivially satisfied by the inverse limits of discrete probability spaces: hence there is a uniquely defined measure $\kappa_{G,t}$ on G with the property that, for any $N \in \mathcal{N}$ and any union X of cosets of N we have $\kappa_{G,t}(X) = Q_{G/N,t}(X/N)$. We estimate the bias of the measure $\kappa_{G,t}$ considering

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

where $\mathcal{B}(G)$ is the set of the measurable subsets of G.

Proposition 5. *If G is a t-generated profinite group, then*

$$\beta_t(G) = \sup_{N\in\mathcal{N}} \beta_t(G/N).$$

Proof. Let $N \in \mathcal{N}$ and let $\mathcal{B}_N(G)$ be the set of the subsets of G that are union of cosets of N in G. We have $\mathcal{B}_N(G) \subseteq \mathcal{B}(G)$ and if $B \in \mathcal{B}_N(G)$, then $\kappa_{G,t}(B) = Q_{G/N,t}(B/N)$ and $\mu_G(B) = U_{G/N}(B/N) = |B/N|/|G/N|$. But then

$$\begin{aligned}\beta_t(G/N) &= \max_{B\in\mathcal{B}_N(G)} |Q_{G/N,t}(B/N) - U_{G/N}(B/N)| \\ &= \max_{B\in\mathcal{B}_N(G)} |\kappa_{G,t}(B) - \mu_G(B)| \\ &\leq \sup_{B\in\mathcal{B}(G)} |\kappa_{G,t}(B) - \mu_G(B)| = \beta_t(G).\end{aligned}$$

This implies

$$\beta_t(G) \geq \sup_{N\in\mathcal{N}} \beta_t(G/N).$$

To conclude our proof, it suffices to show that for every positive real number ϵ, there exists $N \in \mathcal{N}$ such that $\beta_t(G) \leq \beta_t(G/N) + \epsilon$. By definition there exists $B \in \mathcal{B}$ such that

$$|\kappa_{G,t}(B) - \mu_G(B)| \geq \beta_t(G) - \frac{\epsilon}{2}. \tag{4.1}$$

Notice that being G finitely generated, there exists a descending chain $\{N_i\}_{i\in\mathbb{N}}$ of open normal subgroups of G such that $\cap_{i\in\mathbb{N}} N_i = 1$. For every $n \in \mathbb{N}$, let

$$\gamma_n(B) = \frac{|BN_n/N_n|}{|G/N_n|} \quad \text{and} \quad \delta_n(B) = Q_{G/N_n,t}(BN_n/N_n).$$

We have that $\{\gamma_n\}_{n\in\mathbb{N}}$ and $\{\delta_n\}_{n\in\mathbb{N}}$ are decreasing functions and

$$\mu_G(B) = \inf_{n\in\mathbb{N}} \gamma_n(B) \quad \text{and} \quad \kappa_{G,t}(B) = \inf_{n\in\mathbb{N}} \delta_n(B).$$

In particular there exists $n \in \mathbb{N}$ such that

$$\gamma_n(B) - \frac{\epsilon}{2} \leq \mu_G(B) \leq \gamma_n(B), \quad \delta_n(B) - \frac{\epsilon}{2} \leq \kappa_{G,t} \leq \delta_n(B)$$

and consequently

$$|\kappa_{G,t}(B) - \mu_G(B)| \leq |\gamma_n(B) - \delta_n(B)| + \frac{\epsilon}{2} \leq \beta_t(G/N_n) + \frac{\epsilon}{2}. \tag{4.2}$$

From (4.1) and (4.2) we immediately conclude that $\beta_t(G) \leq \beta_t(G/N_n) + \epsilon$. □

5. **Nilpotent and pronilpotent groups**

We can now apply the results described in Sections 2 and 3 in order to compute $\beta_t(G)$ when G is a t-generated pronilpotent group.

First assume that G is a finite nilpotent group. Let $I = \{p_1, \dots, p_t\}$ be a set of prime numbers, and let $G = \prod_{i\in I} P_i$ where $P_i \cong C_{p_i}^{d_i}$ is an elementary abelian p_i group of rank $d_i > 0$. By (2.3) we have

$$P_G(t) = \prod_{i\in I} \left(\prod_{0\leq u\leq d_i-1} \left(1 - \frac{p_i^u}{p_i^t}\right)\right).$$

For any subset J of I, let $\Omega_J = \{g \in G \mid |g| = \prod_{j\in J} p_j\}$. If $g \in \Omega_J$ then by (2.3)

$$P_G(g, t-1) = \left(\prod_{i\in J} \left(\prod_{0\leq u\leq d_i-2} \left(1 - \frac{p_i^u}{p_i^{t-1}}\right)\right)\right) \left(\prod_{i\notin J} \left(\prod_{0\leq u\leq d_i-1} \left(1 - \frac{p_i^u}{p_i^{t-1}}\right)\right)\right).$$

It follows:

$$\begin{aligned} \sigma_{G,t}(g) = \frac{P_G(g,t-1)}{P_G(t)} &= \left(\prod_{i\in J} \frac{1}{1-\frac{1}{p_i^t}}\right) \left(\prod_{i\notin J} \frac{1-\frac{p_i^{d_i}}{p_i^t}}{1-\frac{1}{p_i^t}}\right) \\ &= \frac{\left(\prod_{i\in J} p_i^t\right) \left(\prod_{i\notin J} (p_i^t - p_i^{d_i})\right)}{\prod_{i\in I}(p_i^t - 1)}. \end{aligned} \tag{5.1}$$

Hence

$$2\beta_t(G)|G| = \sum_{J\subseteq I} \left(\left| \frac{\left(\prod_{i\in J} p_i^t\right) \left(\prod_{i\notin J} (p_i^t - p_i^{d_i})\right)}{\prod_{i\in I}(p_i^t - 1)} - 1 \right| |\Omega_J| \right)$$

and

$$\beta_t(G) = \frac{1}{2}\sum_{J\subseteq I}\left(\left|\frac{\left(\prod_{i\in J} p_i^t\right)\left(\prod_{i\notin J}(p_i^t - p_i^{d_i})\right)}{\prod_{i\in I}(p_i^t-1)} - 1\right| \frac{\prod_{i\in J}(p_i^{d_i}-1)}{\prod_{i\in I} p_i^{d_i}}\right).$$

In particular if $|G| = C_p^d$ and $t \geq d$, then

$$\frac{P_G(g,t-1)}{P_G(t)} = \begin{cases} \frac{p^t-p^d}{p^t-1} < 1 & \text{if } g = 1 \\ \frac{p^t}{p^t-1} > 1 & \text{if } g \neq 1 \end{cases}$$

and by (2.1)

$$\beta_t(G) = \left(1 - \left(\frac{p^t-p^d}{p^t-1}\right)\right)\frac{1}{p^d} = \left(\frac{p^d-1}{p^t-1}\right)\frac{1}{p^d}.$$

Since $\beta_t(G) = \beta_t(G/\operatorname{Frat} G)$ for every t-generated profinite group G, we deduce:

Proposition 6. *If G is a finitely generated pro-p group and $t \geq d(G)$, then*

$$\beta_t(G) = \left(\frac{p^{d(G)}-1}{p^t-1}\right)\frac{1}{p^{d(G)}}.$$

Proposition 7. *Let G be a t-generated pronilpotent group. If $t \geq 2$, then*

$$\beta_t(G) \leq \frac{\pi^2}{6} - 1 \sim 0.645.$$

Proof. By Proposition 5, it suffices to prove the statement for finite nilpotent groups. Moreover, since $\beta_t(G) = \beta_t(G/\operatorname{Frat}(G))$, we may assume that G is a finite abelian group with a square-free exponent. By (5.1), for every $g \in G$ we have

$$\sigma_{G,t}(g) \leq \prod_{p||G|}\left(1-\frac{1}{p^t}\right)^{-1} \leq \prod_{p}^{\infty}\left(1-\frac{1}{p^2}\right)^{-1} = \zeta(2) = \frac{\pi^2}{6}.$$

But then, by (2.1), we have

$$\beta_t(G) = \frac{1}{|G|}\left(\sum_{g\in\Delta_G^+(t)}(\sigma_{G,t}(g)-1)\right) \leq \frac{|\Delta_G^+(t)|}{|G|}\left(\frac{\pi^2}{6}-1\right) \leq \frac{\pi^2}{6}-1,$$

hence our claim is proved. □

It is interesting to analyze in more details the case $G = \langle x\rangle$ cyclic of order $p\cdot q$ where p and q primes with $p < q$. We have

$$\sigma_{G,t}(g,t) = \frac{(p^t-p)(q^t-q)}{(p^t-1)(q^t-1)} < 1 \quad \text{if } |g| = 1,$$

$$\sigma_{G,t}(g,t) = \frac{p^t(q^t-q)}{(p^t-1)(q^t-1)} \quad \text{if } |g| = p,$$

$$\sigma_{G,t}(g,t) = \frac{(p^t-p)q^t}{(p^t-1)(q^t-1)} < 1 \quad \text{if } |g| = q,$$

$$\sigma_{G,t}(g,t) = \frac{p^tq^t}{(p^t-1)(q^t-1)} > 1 \quad \text{if } |g| = pq.$$

Notice that if $|g| = p$, then $\sigma_{G,t}(g,t) \geq 1$ if and only if $(q^t-1)/(q-1) \geq p^t$, which is true if t is large enough. If $(q^t-1)/(q-1) \geq p^t$, then $\sigma_{G,t}(g,t) \leq 1$ if and only if g is contained in the subgroup $N = \langle x^p \rangle$ of G of order q, so, by Proposition 3, $\beta_t(G) = \beta_t(G/N) = \beta_t(C_p)$; hence

$$\beta_t(C_{pq}) = \beta_t(C_p) = \frac{p-1}{p(p^t-1)} \quad \text{if} \quad \frac{q^t-1}{q-1} \geq p^t.$$

For example, if $p = 2$, then $(q^t-1)/(q-1) \geq 2^t$ whenever q is an odd prime and $t \geq 2$ so $\beta_t(C_{2q}) = \beta_t(C_2) = (2(2^t-1))^{-1}$ if $t \geq 2$.

If $(q^t-1)/(q-1) < p^t$, then $\sigma_{G,t}(g,t) > 1$ if and only if $|g| = pq$, so

$$\beta_t(C_{pq}) = \frac{\phi(pq)}{pq}\left(\frac{p^tq^t}{(p^t-1)(q^t-1)} - 1\right) = \frac{(p^t+q^t-1)(p-1)(q-1)}{(p^t-1)(q^t-1)pq} \text{ if } \frac{q^t-1}{q-1} < p^t.$$

In particular, for $t = 1$ we have

$$\beta_1(C_{pq}) = \frac{p+q-1}{pq} = 1 - \frac{\phi(pq)}{pq}.$$

This is a particular case of a more general situation: indeed if $G = C_n$ then $\sigma_{G,1}(g) = 0$ if $\langle g \rangle \neq G$, $\sigma_{G,1}(g) = 1/P_G(1) = n/\phi(n)$ otherwise, so

$$\beta_1(G) = \frac{\phi(n)}{n}\left(\frac{n}{\phi(n)} - 1\right) = 1 - \frac{\phi(n)}{n}.$$

6. **Comparing $\beta_t(G)$ and $P_G(t)$**

We concluded the previous section, showing that $\beta_1(G) = 1 - P_G(1)$ if G is a cyclic group. This is a particular instance of a more general result (see also [17, Proposition 1.5.1]):

Proposition 8. *If G is a finite group and $t \geq d(G)$, then $\beta_t(G) \leq 1 - P_G(t)$. Moreover if $G \neq 1$ then the equality holds if and only if G is cyclic and $t = 1$.*

Proof. Set $\delta(g_1,\dots,g_t)=1$ if $\langle g_1,\dots,g_t\rangle = G$, $\delta(g_1,\dots,g_t)=0$ otherwise. We have

$$\begin{aligned}
2\beta_t(G) &= \sum_{g_1\in G}\left|Q_G(g_1)-\frac{1}{|G|}\right| = \sum_{g_1\in G}\left|\frac{|\Phi_G(g_1,t-1)|}{|\Phi_G(t)|}-\frac{1}{|G|}\right| \\
&= \sum_{g_1\in G}\left|\left(\sum_{(g_2,\dots,g_t)\in G^{t-1}}\frac{\delta(g_1,g_2,\dots,g_t)}{|\Phi_G(t)|}\right)-\frac{1}{|G|}\right| \\
&= \sum_{g_1\in G}\left|\sum_{(g_2,\dots,g_t)\in G^{t-1}}\left(\frac{\delta(g_1,g_2,\dots,g_t)}{|\Phi_G(t)|}-\frac{1}{|G|^t}\right)\right| \\
&\leq \sum_{(g_1,g_2,\dots,g_t)\in G^t}\left|\frac{\delta(g_1,g_2,\dots,g_t)}{|\Phi_G(t)|}-\frac{1}{|G|^t}\right| \\
&= \sum_{(g_1,\dots,g_t)\in\phi_G(t)}\left|\frac{\delta(g_1,\dots,g_t)}{|\Phi_G(t)|}-\frac{1}{|G|^t}\right| + \sum_{(g_1,\dots,g_t)\notin\phi_G(t)}\left|\frac{\delta(g_1,\dots,g_t)}{|\Phi_G(t)|}-\frac{1}{|G|^t}\right| \\
&= \sum_{(g_1,\dots,g_t)\in\phi_G(t)}\left|\frac{1}{|\Phi_G(t)|}-\frac{1}{|G|^t}\right| + \sum_{(g_1,\dots,g_t)\notin\phi_G(t)}\frac{1}{|G|^t} \\
&= |\Phi_G(t)|\left(\frac{1}{|\Phi_G(t)|}-\frac{1}{|G|^t}\right)+\frac{|G|^t-|\Phi_G(t)|}{|G|^t} = 2\left(1-\frac{|\Phi_G(t)|}{|G|^t}\right).
\end{aligned}$$

The equality is satisfied if and only if for each $g_1\in G$ we have that

$$\left|\sum_{(g_2,\dots,g_t)\in G^{t-1}}\left(\frac{\delta(g_1,g_2,\dots,g_t)}{|\Phi_G(t)|}-\frac{1}{|G|^t}\right)\right| = \sum_{(g_2,\dots,g_t)\in G^t}\left|\frac{\delta(g_1,g_2,\dots,g_t)}{|\Phi_G(t)|}-\frac{1}{|G|^t}\right|$$

or equivalently if and only if

$$\left(\frac{\delta(g_1,x_2,\dots,x_t)}{|\Phi_G(t)|}-\frac{1}{|G|^t}\right)\left(\frac{\delta(g_1,y_2,\dots,y_t)}{|\Phi_G(t)|}-\frac{1}{|G|^t}\right)\geq 0 \qquad (*)$$

for each $g_1,x_2,\dots,x_t,y_2,\dots,y_t\in G$. This is true if $G=1$ or if G is cyclic and $t=1$. Conversely assume that $(*)$ is satisfied: in particular we can choose $g_1,x_2,\dots,x_t$ such that $\langle g_1,x_2,\dots,x_t\rangle = G$ and take $y_2=\cdots=y_t=1$: we have

$$\left(\frac{1}{|\Phi_G(t)|}-\frac{1}{|G|^t}\right)\left(\frac{\delta(g_1,1,\dots,1)}{|\Phi_G(t)|}-\frac{1}{|G|^t}\right)\geq 0,$$

hence $\delta(g_1,1,\dots,1)=1$, i.e. $G=\langle g_1\rangle$. Moreover $t=1$, otherwise

$$\left(\frac{\delta(1,1,\dots,1)}{|\Phi_G(t)|}-\frac{1}{|G|^t}\right)\left(\frac{\delta(1,g_1,1,\dots,1)}{|\Phi_G(t)|}-\frac{1}{|G|^t}\right)=\frac{-1}{|G|^t}\left(\frac{1}{|\Phi_G(t)|}-\frac{1}{|G|^t}\right)<0.$$

This concludes the proof of our statement. □

It is well-known that a profinite group G, being a compact topological group, can be seen as a probability space. If we denote with 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 denotes also the product measure on G^k. By [14, Theorem 1] we have

$$P_G(t) = \inf_{N \in \mathcal{N}} P_{G/N}(t). \tag{6.1}$$

But then

$$\begin{aligned}\beta_t(G) &= \sup_{N \in \mathcal{N}} \beta_t(G/N) \leq \sup_{N \in \mathcal{N}} (1 - P_{G/N}(t)) \\ &= 1 - \inf_{N \in \mathcal{N}} P_{G/N}(t) = 1 - P_G(t).\end{aligned}$$

So we have:

Corollary 9. *If G is a t-generated profinite group, then $\beta_t(G) \leq 1 - P_G(t)$.*

As a consequence of Proposition 8, we are ensured that the distribution $Q_{G,t}$ is "almost" uniform if t randomly chosen elements from G almost certainly generate G: in this case $P_G(t)$ is closed to 1 and so $\beta_t(G)$ is closed to 0. However this condition is quite far from being necessary. Indeed the inequality $\beta_t(G) \leq 1 - P_G(t)$ is not sharp. For example we have:

Theorem 10 ([4, Theorem 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 $\beta_t(G) \leq \varepsilon$.*

7. A defect in the product replacement algorithm

In [1] Babai and Pak demonstrated a defect in the product replacement algorithm. For certain groups G the distribution $Q_{G,t}$ is far from U_G. More precisely:

Theorem 11 ([1, Theorem 2.1])**.** *Let $G = \mathrm{Alt}(n)^{n!/8}$. If $n \geq 5$, then G is 2-generated but, for $t \geq 4$, $\beta_t(G)$ tends to 1 as $n \to \infty$.*

The result of Babai and Pak implies that if $\hat{F}_2$ is the free profinite group of rank 2 and $t \geq 4$, then $\beta_t(\hat{F}_2) = 1$. In [17] 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 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 $t = d(G)$. For example in [3] the following result has been proved:

Theorem 12 ([3, Theorem 1])**.** *There exists a 2-generated metabelian profinite G group with the property that $\mu_G(\Omega) = 0$, where*

$$\Omega = \{x \in G \mid \langle x, y \rangle = G \text{ for some } y \in G\}.$$

By definition $\kappa_{G,2}(\Omega) = 1$ and consequently $\beta_2(G) \geq |\kappa_{G,2}(\Omega) - \mu_G(\Omega)| = 1$.

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 given integer t significantly larger than $d(G)$. It follows from Corollary 9 that we can have $\beta_t(G) = 1$ only if $P_G(t) = 0$. If we consider arbitrary profinite groups, this does not represent a serious obstacle: for example if $G = \hat{F}_d$ is the free profinite group of

rank $d \geq 2$ then $P_{\hat{F}_d}(t) = 0$ for every $t \geq d$ (see for example [8]). The situation is different in the case of finitely generated prosoluble groups. If G is a finitely generated prosoluble group then $P_G(t) > 0$ if $t \geq \lceil c(d(G) - 1) + 1 \rceil$, with $c \backsimeq 3.243$, the Pàlfy-Wolf constant (see [11] and [13]): so if G is a t-generated prosoluble group with $\beta_G(t) = 1$, then the ratio between t and the smallest cardinality $d(G)$ of a generating set of G cannot be arbitrarily large. However in [3] examples have been constructed of prosoluble d-generated groups G_d for which there exists an integer t_d with $\beta_{t_d}(G_d) = 1$ and where the difference $t_d - d$ tends to infinity as $d \to \infty$. More precisely:

Theorem 13 ([3, Theorem 1])**.** *Let $d \in \mathbb{N}$ with $d \geq 3$ and let k be a non negative integer with $2k \leq d - 3$. There exists a sequence of d-generated finite soluble groups J_m with $\beta_{d+k}(J_m) \geq 1 - \epsilon_m$ for a certain sequence ϵ_m such that ϵ_m tends to 0 as m tends to infinity.*

Corollary 14. *Let $d \in \mathbb{N}$ with $d \geq 3$ and let F be the free prosoluble group of rank d. Then $\beta_{d+k}(F) = 1$ for every k such that $2k \leq d - 3$.*

The groups described in [3] have a quite intricate structure and one would like to produce easier examples. By Proposition 7 these cannot be obtained just considering pronilpotent groups. However in [4] it is proved that if G is the free prosupersoluble group of rank $d \geq 2$, then $P_G(t) > 0$ if and only if $t \geq 2d + 1$ so one could expect to have $\beta_{d+k}(G) = 1$ for k significantly larger than d. However this is not what occurs. In fact we have:

Theorem 15 ([4, Theorem 2])**.** *If G is a noncylic finite supersoluble group and $k \geq 3$, then $\beta_{d(G)+k}(G) \leq$ 0.6*

8. **Positively unbiased groups**

A profinite group G is called positively finitely generated (PFG) if $P_G(k) > 0$ for some $k \in \mathbb{N}$. This concept actually first arose in the context of field arithmetic. Various theorems that are valid for "almost all" k-tuples in the absolute Galois group $G(F)$ of a field F appear in [6]. Answering a question of Fried and Jarden [6], Kantor and Lubotzky [8] have shown that the free profinite group of rank d is not PFG if $d \geq 2$. On the other hand, Mann [14] has proved that finitely generated prosoluble groups have this property. Denote by $m_n(G)$ the number of index n maximal subgroups of G. A group G is said to have polynomial maximal subgroup growth (PMSG) if $m_n(G) \leq n^c$ for all n (for some constant c). A one-line argument shows that PMSG groups are positively finitely generated. By a very surprising result of Mann and Shalev [15] the converse also holds: a profinite group is PFG if and only if it has polynomial maximal subgroup growth.

We introduce a similar notion in relation with the study of $\beta_k(G)$. We say that a finitely generated profinite group is positively unbiased generated (PUG) is $\beta_k(G) < 1$ for some $k \in \mathbb{N}$. It follows from Corollary 9 that if $P_G(t) > 0$ then $\beta_t(G) < 1$, so PFG groups are PUG. However, as we noticed at the end of the Section 6, it can be that $\beta_t(G) < 1$ even if $P_G(t) = 0$. On the other hand we don't know examples of PUG groups that are not PFG. So we propose the following question:

Question 2. *Is it true that a profinite groups G is PFG if and only if it is PUG?*

9. **Some Frobenius groups**

In the remaining part of this survey, we compute $\beta_t(G)$ in other significant families of finite groups. We start considering some Forbenius groups. Assume that p and q are prime numbers and let a be the multiplicative order of p module q. The affine group $\mathrm{Aff}(1,p^a)$ contains a subgroup $G \cong C_p^a \rtimes C_q$. The socle N of G is isomorphic to C_p^a and is the unique minimal normal series of G. We can compute $P_G(g,t)$ applying formula (2.3) to the chief series $1 < N < G$.

(1) If $g = 1$, then, since N has p^a complements in G, we have

$$P_G(g,t) = P_G(t) = \left(1 - \frac{p^a}{p^{at}}\right)\left(1 - \frac{1}{q^t}\right).$$

(2) If $|g| = p$, then there is no complement of N in G containing g hence

$$P_G(g,t) = \left(1 - \frac{1}{q^t}\right).$$

(3) If $|g| = q$, then $\langle g\rangle N = G$ and there is no complement of G/N in G/N containing gN, while $\langle g\rangle$ is the unique complement of N in G containing g. Therefore

$$P_G(g,t) = \left(1 - \frac{1}{p^{at}}\right).$$

It follows that for $t \geq 2$ we have

$$\begin{aligned}
\sigma_{G,t}(g,t) &= \frac{(p^{at}-p^{2a})}{(p^{at}-p^a)}\frac{(q^t-q)}{(q^t-1)} && \text{if } |g| = 1,\\
\sigma_{G,t}(g,t) &= \frac{p^{at}}{(p^{at}-p^a)}\frac{(q^t-q)}{(q^t-1)} && \text{if } |g| = p,\\
\sigma_{G,t}(g,t) &= \frac{q^t}{q^t-1} && \text{if } |g| = q.
\end{aligned}$$

Notice that $p^{at}(q^t-q) \leq (p^{at}-p^a)(q^t-1)$ if and only $(q^t-1)/(q-1) \leq p^{a(t-1)}$. Since $q \leq p^a - 1$ we have $(q^t-1)/(q-1) \leq (q+1)^{t-1} \leq p^{a(t-1)}$. But then $\sigma_{G,t}(g,t) \leq 1$ if and only if $g \in N$ and this implies

$$\beta_t(G) = \beta_t(G/N) = \beta_t(C_q) = \frac{(q-1)}{(q^t-1)q}.$$

In the particular case when $p = 3$ and $q = 2$, we get

$$\beta_t(\mathrm{Sym}(3)) = \beta_t(C_2) = \frac{1}{(2^t-1)2}.$$

10. $G = \mathrm{Sym}(4)$

If $G = \mathrm{Sym}(4)$, we have

$$P_G(t) = \left(1 - \frac{1}{2^t}\right)\left(1 - \frac{3}{3^t}\right)\left(1 - \frac{4}{4^t}\right).$$

We compute $\sigma_{G,t}(g) = P_G(g, t-1)/P_G(t)$ where g belongs to a set of representatives for the conjugacy classes of G :

$$\begin{aligned}
\sigma_{G,t}(1) &= \frac{\left(1 - \frac{1}{2^{t-1}}\right)\left(1 - \frac{3}{3^{t-1}}\right)\left(1 - \frac{4}{4^{t-1}}\right)}{P_G(t)} = \frac{(2^t-2)(3^t-9)(4^t-16)}{(2^t-1)(3^t-3)(4^t-4)} \\
\sigma_{G,t}((1,2)(3,4)) &= \frac{\left(1 - \frac{1}{2^{t-1}}\right)\left(1 - \frac{3}{3^{t-1}}\right)}{P_G(t)} = \frac{(2^t-2)(3^t-9)4^t}{(2^t-1)(3^t-3)(4^t-4)} \\
\sigma_{G,t}((1,2,3)) &= \frac{\left(1 - \frac{1}{2^{t-1}}\right)\left(1 - \frac{1}{4^{t-1}}\right)}{P_G(t)} = \frac{(2^t-2)3^t(4^t-4)}{(2^t-1)(3^t-3)(4^t-4)} \\
\sigma_{G,t}((1,2)) &= \frac{\left(1 - \frac{1}{3^{t-1}}\right)\left(1 - \frac{2}{4^{t-1}}\right)}{P_G(t)} = \frac{2^t(3^t-3)(4^t-8)}{(2^t-1)(3^t-3)(4^t-4)} \\
\sigma_{G,t}((1,2,3,4)) &= \frac{\left(1 - \frac{1}{3^{t-1}}\right)}{P_G(t)} = \frac{2^t(3^t-3)4^t}{(2^t-1)(3^t-3)(4^t-4)}.
\end{aligned}$$

Notice that

- $\sigma_{G,t}(1) < 1$ for every $t \geq 2$;
- $\sigma_{G,t}((1,2)(3,4)) < 1$ for every $t \geq 2$;
- $\sigma_{G,t}((1,2,3)) < 1$ for every $t \geq 2$;
- $\sigma_{G,t}((1,2)) > 1$ for every $t \geq 3$ while $\sigma_{G,2}((1,2,3)) < 1$;
- $\sigma_{G,t}((1,2,3,4)) > 1$ for every $t \geq 2$.

It $t \geq 3$, then $\sigma_{G,t}(g) \leq 1$ if and only if $g \in \mathrm{Alt}(n)$ and therefore

$$\beta_t(\mathrm{Sym}(4)) = \beta_t(\mathrm{Sym}(4)/\mathrm{Alt}(4)) = \beta_t(C_2) = \frac{1}{(2^t-1)2}.$$

However if $t = 2$ then $\sigma_{G,t}(g) > 1$ only if g is a 4-cycle and

$$\beta_2(\mathrm{Sym}(4)) = \frac{6}{24}\left(\frac{2^2}{2^2-1}\frac{4^2}{4^2-4} - 1\right) = \frac{7}{36} > \beta_2(C_2) = \frac{1}{6}.$$

11. $G = \mathrm{Sym}(n)$

We have seen in the previous two examples that if $G \in \{\mathrm{Sym}(3), \mathrm{Sym}(4)\}$ and $t \geq 3$, then $\beta_t(G) = \beta_t(C_2)$. The situation is similar for all the symmetric groups. By (2.2), for $g \in G = \mathrm{Sym}(n)$, we have

$$P_G(g,t) = \sum_{n \in \mathbb{N}} \frac{a(n,g)}{n^t} \quad \text{with} \quad a(n,g) = \sum_{g \in H, |G:H| = n} \mu_G(H).$$

Since $\mathrm{Alt}(n)$ is the unique subgroup of $\mathrm{Sym}(n)$ of index 2 we have

$$P_G(g,t) = \begin{cases} 1 - \frac{1}{2^t} + \sum_{n\geq 3} \frac{a(n,g)}{n^t} & \text{if } g \in \mathrm{Alt}(n) \\ 1 + \sum_{n\geq 3} \frac{a(n,g)}{n^t} & \text{otherwise.} \end{cases}$$

This implies that if t is large enough then

$$\sigma_{G,t}(g) \sim \begin{cases} \frac{2^t-2}{2^t-1} < 1 & \text{if } g \in \mathrm{Alt}(n) \\ \frac{2^t}{2^t-1} > 1 & \text{otherwise.} \end{cases}$$

Therefore, by Proposition 3, if t is large enough, we have

$$\beta_t(\mathrm{Sym}(n)) = \beta_t\left(\frac{\mathrm{Sym}(n)}{\mathrm{Alt}(n)}\right) = \beta_t(C_2) = \frac{1}{(2^t-1)2}.$$

12. **Asymptotically unbiased normal subgroups**

We say that a normal subgroup N of a finite group G is asymptotically unbiased if there exists $\bar{t} \in \mathbb{N}$ such that $\beta_t(G) = \beta_t(G/N)$ for all $t \geq \bar{t}$.

Let $l(G) = \min_{H<G} |G : H|$ and for each g in G denote by $\rho(G,g)$ the number of (maximal) subgroups of G of index $l(G)$ containing g. It follows from (2.2) that

$$\sigma_{G,t}(g) = \frac{P_G(g,t-1)}{P_G(g)} = \frac{1 - \frac{l(G)\rho(G,g)}{l(G)^t} + o\left(\frac{1}{l(G)^t}\right)}{1 - \frac{\rho(G,1)}{l(G)^t} + o\left(\frac{1}{l(G)^t}\right)}.$$

This implies

- if $\rho(G,1) < l(G)\rho(G,g)$ then $g \in \Delta_G^-(t)$ for t large enough;
- if $\rho(G,1) > l(G)\rho(G,g)$ then $g \in \Delta_G^+(t)$ for t large enough.

Corollary 16. *If N is asymptotically unbiased, then $\rho(G,1) \leq l(G)\rho(G,n)$ for each $n \in N$.*

Proof. Notice that $\sigma_{G,t}(1) < 1$ for each $t \in \mathbb{N}$. Since $1 \in N$, we deduce from Proposition 3 that if $\beta_t(G) = \beta_t(G/N)$ then $n \notin \Delta_G^+(t)$ for each $n \in N$. □

Proposition 17. *Assume that $|G : N| = 2$. Then N is asymptotically unbiased if and only if N is the unique subgroup of G of index 2.*

Proof. Assume that N is the unique subgroup of G of index 2. We have $l(G) = 2$, $\rho(G,g) = 1$ if $g \in N$, $\rho(G,g) = 0$ otherwise. This implies that if t is large enough, then $g \in \Delta_G^-(t)$ if $g \in N$, $g \in \Delta_G^+(t)$ if $g \notin N$ and the conclusion follows from Proposition 3. On the other hand, if N is not the unique subgroup of G of index 2, then there exists $M \trianglelefteq G$ such that $G/M \cong C_2 \times C_2$. By Proposition 6 we deduce

$$\beta_t(G) \geq \beta_t(G/M) = \beta_t(C_2 \times C_2) = \frac{p^2-1}{(p^t-1)p^2} > \frac{p-1}{(p^t-1)p} = \beta_t(C_2) = \beta_t(G/N)$$

hence $\beta_t(G) \neq \beta_t(G/N)$ for each $t \in \mathbb{N}$ and N is not asymptotically unbiased. □

13. $G = \mathrm{Alt}(5)$

We compute $P_G(g,t)$ using the formula (2.2). The subgroups H of G with $\mu_G(H) \neq 0$ are listed in Table 2.

TABLE 2.

H	Alt(5)	Alt(4)	D_{10}	Sym(3)	C_3	C_2	1
$\mu_G(H)$	1	-1	-1	-1	2	4	-60

We have in particular

$$\begin{aligned} P_G(1,t) &= 1 - \frac{5}{5^t} - \frac{6}{6^t} - \frac{10}{10^t} + \frac{20}{20^t} + \frac{60}{30^t} - \frac{60}{60^t} \\ P_G((1,2,3,4,5),t) &= 1 - \frac{1}{6^t} \\ P_G((1,2,3),t) &= 1 - \frac{2}{5^t} - \frac{1}{10^t} + \frac{2}{20^t} \\ P_G((1,2)(3,4),t) &= 1 - \frac{1}{5^t} - \frac{2}{6^t} - \frac{2}{10^t} + \frac{4}{30^t}. \end{aligned}$$

It can be easily checked that for $t \geq 2$ we have that $P_G(g,t-1) \geq P_G(t)$ if and only if $|g| = 5$ and therefore by Proposition 3

$$\beta_t(G) = \frac{24}{60}\left(\frac{1-\frac{1}{6^{t-1}}}{P_G(t)} - 1\right) = \frac{24\left(\frac{5}{5^t} + \frac{10}{10^t} - \frac{20}{20^t} - \frac{60}{30^t} + \frac{60}{60^t}\right)}{60\left(1 - \frac{5}{5^t} - \frac{6}{6^t} - \frac{10}{10^t} + \frac{20}{20^t} + \frac{60}{30^t} - \frac{60}{60^t}\right)}.$$

In particular $\beta_2(\mathrm{Alt}(5)) = 12/95$.

14. **Other simple groups**

If S is a nonabelian finite simple group, then $d(G) = 2$ and results of Dixon [5], Kantor-Lubotzky [8] and Liebeck-Shalev [9] establish that $P_S(2) \to 1$ as $|S| \to \infty$. In a recent paper [16] it was proved that $P_S(2) \geq 53/90$ for each nonabelian simple group S. Since $\beta_S(2) \leq 1 - P_S(2)$, we deduce that

$$\beta_2(S) \leq 47/90$$

and $\beta_2(S) \to 0$ as $|S| \to \infty$. In [16] it is also proved that the equality $P_S(2) = 53/90$ is satisfied if and only if $S = \mathrm{Alt}(6)$. It is a natural question to ask which is the largest value for $\beta_2(S)$ and for which simple group this value is assumed. We have seen in the previous section that $\beta_2(\mathrm{Alt}(5)) = 12/95$. We check whether there exists a finite nonabelian simple group $T \neq \mathrm{Alt}(5)$ with $\beta_2(T) \geq 12/95$. We should have $12/95 \leq \beta_2(T) \leq 1 - P_T(2)$ hence $P_T(2) \leq 83/95$: by [16, Theorem 1.1], T is one of the following groups: $\mathrm{Alt}(5), \mathrm{Alt}(6), \mathrm{Alt}(7), \mathrm{Alt}(8), \mathrm{Alt}(9), \mathrm{Alt}(10)$, $L_2(7), L_2(8), L_2(11), L_3(3), L_3(4), M_{11}, M_{12}$. The behavior of these groups is described in Table 3. From this table we conclude that does not exist such a nonabelian finite simple group being non-isomorphic to Alt(5). So we have proved:

Proposition 18. *If S is a finite nonabelian simple group, then $\beta_2(S) \leq 12/95$ with equality if and only if $S = \mathrm{Alt}(5)$.*

This gives another evidence that the estimations for $\beta_t(G)$ deduced from the inequality $\beta_t(G) \leq 1 - P_G(t)$ are not sharp. Since $P_S(2)$ assumes its minimal value when $S = \mathrm{Alt}(6)$, one could expect that the maximus value for $\beta_t(G)$ is assumed again when $G = \mathrm{Alt}(6)$. On the contrary, we get $\beta_2(\mathrm{Alt}(5)) > \beta_2(\mathrm{Alt}(6))$.

TABLE 3.

T	$\beta_2(T)$	$P_T(2)$
$\mathrm{Alt}(5)$	$12/95 \sim 0.126$	$19/30 \sim 0.633$
$\mathrm{Alt}(6)$	$131/1060 \sim 0.124$	$53/90 \sim 0.588$
$\mathrm{Alt}(7)$	$1469/19236 \sim 0.076$	$229/315 \sim 0.726$
$\mathrm{Alt}(8)$	$4027/55860 \sim 0.072$	$133/180 \sim 0.738$
$\mathrm{Alt}(9)$	$5314873/99811440 \sim 0.053$	$15403/18144 \sim 0.849$
$\mathrm{Alt}(10)$	$6509536/138919725 \sim 0.047$	$29401/33600 \sim 0.875$
$\mathrm{L}_2(7)$	$181/1596 \sim 0.113$	$19/28 \sim 0.678$
$\mathrm{L}_2(11)$	$338/4191 \sim 0.081$	$127/165 \sim 0.769$
$\mathrm{L}_2(8)$	$40/639 \sim 0.063$	$71/84 \sim 0.845$
$\mathrm{L}_3(3)$	$243/5252 \sim 0.047$	$101/117 \sim 0.863$
$\mathrm{L}_3(4)$	$1021/25410 \sim 0.040$	$121/140 \sim 0.864$
M_{11}	$24223/427548 \sim 0.057$	$3239/3960 \sim 0.818$
M_{12}	$30851/708840 \sim 0.044$	$179/220 \sim 0.814$

REFERENCES

[1] L. Babai and I. Pak, *Strong bias of group generators: an obstacle to the "product replacement algorithm"*, Proceedings of the Eleventh Annual ACM-SIAM Symposium on Discrete Algorithms (San Francisco, CA, 2000), ACM, New York, 2000 627–635.

[2] F. Celler, C. R. Leedham-Green, S. Murray, A. Niemeyer and E.A. OBrien, Generating random elements of a finite group, *Comm. Algebra*, **23** (1995) 4931–4948.

[3] E. Crestani and A. Lucchini, Bias of group generators in the solvable case, *Israel J. Math.*, to appear, DOI: 10.1007/s11856-015-1159-7.

[4] E. Crestani, G. De Franceschi and A. Lucchini, Probability and bias in generating supersoluble groups, *Proc. Edinb. Math. Soc*, to appear.

[5] J. D. Dixon, The probability of generating the symmetric group, *Math. Z.*, **110** (1969) 199–205.

[6] M. D. Fried and M. Jarden, Field Arithmetic, Ergebnisse der Mathematik und ihrer Grenzgebiete, **11**, Springer-Verlag, New York, 1986.

[7] P. Hall, The Eulerian functions of a group, *Quart. J. Math.*, **7** (1936) 134–151.

[8] W. M. Kantor and A. Lubotzky, The probability of generating a finite classical group, *Geom. Dedicata*, **36** no. 1 (1990) 67–87.

[9] M. W. Liebeck and A. Shalev, The probability of generating a finite simple group, *Geom. Dedicata*, **56** no. 1 (1995) 103–113.

[10] A. Lucchini, The X-Dirichlet polynomial of a finite group, *J. Group Theory*, **8** no. 2 (2005) 171–188.

[11] A. Lucchini, F. Menegazzo and M. Morigi, On the probability of generating prosoluble groups, *Israel J. Math.*, **155** (2006) 93–115.

[12] A. Lubotzky and I. Pak, The product replacement algorithm and Kazhdan's property (T), *J. Amer. Math. Soc.*, **14** no. 2 (2001) 347--363.

[13] M. Morigi, On the probability of generating free prosoluble groups of small rank, *Israel J. Math.*, **155** (2006) 117–123.

[14] A. Mann, Positively finitely generated groups, *Forum. Math.*, **8** no. 4 (1996), 429–459.

[15] A. Mann and A. Shalev, Simple groups, maximal subgroups, and probabilistic aspects of profinite groups, *Israel J. Math.*, **96** part B (1996) 449–468.

[16] N. E. Menezes, M. Quick and C. M. Roney-Dougal, The probability of generating a finite simple group, *Israel J. Math.*, **198** no. 1 (2013) 371–392.

[17] I. Pak, *What do we know about the product replacement algorithm*, in Groups and computation, III, de Gruyter, Berlin, 2001, 301–347.

[18] M. Pintér, The existence of an inverse limit of an inverse system of measure spaces - a purely measurable case, *Acta Math. Hungar.*, **126** no. 1-2 (2010) 65–77.

Eleonora Crestani

Dipartimento di Matematica , Via Trieste 63 , 35121 Padova , Italy

crestani@math.unipd.it

Andrea Lucchini

Dipartimento di Matematica , Via Trieste 63 , 35121 Padova , Italy

lucchini@math.unipd.it