ON PROBABILITY OF GENERATING A FINITE GROUP

Igor Pak

Department of Mathematics
Yale University
New Haven, CT 06520
paki@math.yale.edu

December 30, 1999

Abstract. Let G be a finite group, and let $\varphi_k(G)$ be the probability that k random group elements generate G. Denote by $\vartheta(G)$ the smallest k such that $\varphi_k(G) > 1/e$. In this paper we analyze quantity $\vartheta(G)$ for different classes of groups. We prove that $\vartheta(G) \leq \varkappa(G) + 1$ when G is *nilpotent* and $\varkappa(G)$ is the minimal number of generators of G. When G is *solvable* we show that $\vartheta(G) \leq 3.25\,\varkappa(G) + 10^7$. We also show that $\vartheta(G) < C \log\log |G|$, where G is a direct product of simple nonabelian groups, and C is a universal constant.

The work is motivated by the applications to the "product replacement algorithm" (see [CLMNO,P4]). This algorithm is an important recent innovation, designed to efficiently generate (nearly) uniform random group elements. Recent work by Babai and the author [BaP] showed that the output of the algorithm must have a strong bias in certain cases. The precise probabilistic estimates we obtain here, combined with a work [P3], give a positive result, proving that no bias exists for several families of groups and certain parameters in the algorithm.

Introduction

Let G be a finite group. A sequence of k group elements $(g_1, \ldots, g_k)$ is called a *generating k-tuple* of G if $\langle g_1, \ldots, g_k \rangle = G$. Let $\mathcal{N}_k(G)$ be a set of all generating k-tuples of G, and let $N_k(G) = |\mathcal{N}_k(G)|$.

The problem of evaluating $N_k(G)$ goes back to Philip Hall, who expressed $N_k(G)$ as a Möbius type summation of $N_k(H)$ over all maximal subgroups $H \subset G$ (see [H1]). In the paper Hall referred to $N_k(G)$ as an *Eulerian function of a group* since in a special case of a cyclic group we have $N_1(\mathbb{Z}_m) = \phi(m)$. The problem was further investigated by Gaschütz (see [Ga]) who studied a problem of when two solvable groups have the same Eulerian function.

The probabilistic approach of Erdős and Turán to what they called *"statistical group theory"* gave a different view on the problem. It led to a proof by Dixon that

Key words and phrases. Simple groups, nilpotent groups, solvable groups, probabilistic method.

two random permutation generate the symmetric or the alternating group with probability approaching 1. The problem of estimating the probability

$$\varphi_k(G) = \frac{N_k(G)}{|G|^k}$$

that k random group elements generate the whole group became of wide interest in both algebra and combinatorics. Our first result deals with the behavior of this probability for general groups. Namely, we show that for all groups of size $|G| \leq 2^m$ we have $\varphi_k(G) \geq \varphi_k(\mathbb{Z}_2^m)$, i.e. groups $\mathbb{Z}_2^m$ are the "worst" group for random generation.

In the recent time, after completion of the classification of finite simple group (CFSG), the problem received another push. For special classes of groups a remarkable progress has been made (see e.g. [Sh]). It was shown first by Kantor and Lubotzky for classical simple groups of Lie type, and then by Liebeck and Shalev for the remaining series that the probability $\varphi_2(G) \to 1$ as $|G| \to \infty$ (see [KL,LS1]). Now a detailed knowledge about the behavior of the probabilities $\varphi_2(G)$ is known for large simple groups (see [B1,BaP,LS2,Sh]).

Denote by $\varkappa(G)$ the minimal number of generators of G. By $\vartheta(G)$ denote the smallest k such that the probability $\varphi_k(G) > 1/e$. We show that $\vartheta(G)$ has a probabilistic interpretation as an expectation of the following random process. Start with an empty set and add uniform random elements of G one by one until they generate the whole group. By τ denote the stopping time of this process. We prove that $c_1 \cdot E(\tau) \leq \vartheta(G) \leq c_2 \cdot E(\tau)$, where c_1, c_2 are certain universal constants.

The rest of the paper deals with the ratio $\vartheta(G)/\varkappa(G)$. We conjecture that for any G we have

$$\vartheta(G) \leq C\, \varkappa(G) \log\log |G|$$

where C is a universal constant. We present a "supporting evidence" in favor of the conjecture, and give some applications to the product replacement algorithm (see below).

First, we show that for any nilpotent group G we have $\vartheta(G) \leq \varkappa(G) + 1$, which improves other known similar bounds (cf. [Ac,DSC2]). The proof is based on explicit calculations.

When G is solvable, we prove that $\vartheta(G) \leq 3.25\, \varkappa + 10^7$. This is related to recent results of A. Mann in [M]. While stated in a different way for prosolvable groups, when translated, his results imply that $\varphi_k(G) > c$, where $k \geq 3.25\, \varkappa + C$. This, in turn, implies that $\vartheta(G) \leq C\, \varkappa(G)$ for a universal constant C. While one can make an effort to translate and improve Mann's results, we chose to give an independent proof, based on the results of Gaschütz, and by using results of Pálfy, Pyber and Wolf, as well as some Mann's ideas (see [Ga,M,Pa,Py,Wo].)

As we mentioned above, when G is a large enough simple group we have $\varkappa(G) = \vartheta(G) = 2$. We prove a general upper bound $\vartheta(G) \leq C \log m$ when $G = F_1 \times \cdots \times F_N$, where where F_i are simple groups and each nonisomorphic copy occurs at most m times. In a different direction, Kantor and Lubotzky in [KL] found a a sequence of groups $\{G_i\}$ such that $\vartheta(G_i)/\varkappa(G_i) \to \infty$ as $i \to \infty$. Namely, they showed that for large n we have $\varkappa(A_n^{n!/8}) = 2$, and $\vartheta(A_n^{n!/8}) \geq c\, n$ for some universal constant $c > 0$ and n large enough. Note here that $\log(n!/8) \sim n \log n$, so our upper bound is virtually tight.

Finally, the interest to the structure of $\mathcal{N}_k(G)$ has intensified in the last few years due to the so called *product replacement algorithm* for generating (nearly) uniform random elements. Incidentally, this was our original motivation for studying $\varphi_k(G)$.

The algorithm was introduced in [CLMNO] Celler et al. and was further investigated in [B3,BaP,CG,DS2,DS3,P3,PB]. It is currently implemented in all major group algebra packages and is often used as a routine for many randomized group algorithms. We refer to the last section and review article [P4] for the references and details.

The idea of the product replacement algorithm is based on running a Markov chain with on a set of states $\mathcal{N}_k(G)$ and a uniform stationary distribution. After running the Markov chain for a large number of steps, the algorithms returns a random component. At the moment the rapid mixing of the Markov chain is still in question. It was shown in [BaP], however, that the probability distribution of components of $\mathcal{N}_k(G)$ can have a strong bias in both probabilistic and computation senses. This becomes a difficult obstacle for the work of the algorithm.

In a recent paper [P3] the author observed that given $\varphi_k(G_i) \to 0$ for a sequence of groups G_i and $k = k_i$, then the bias becomes small for large i. This gives a motivation for our careful bounds on φ_k for various families of groups. In the last section we present several corollaries which directly translate into performance of the algorithm.

Let us conclude by saying that the problem of estimating $\varphi_k(G)$ seem of universal nature. Another application is the algorithm of Acciaro and Atkinson (see [AA,Ac]), whose performance also depends on the above probabilities.

1. Definitions and main results

Let G be a finite group. By $|G|$ denote the order of G. As in the introduction, let $N_k(G) = |\mathcal{N}_k(G)|$ be the number of generating k-tuples $\langle g_1, \ldots, g_k \rangle = G$, and let $\varphi_k(G)$ be the probability $\varphi_k(G)$ that k uniform independent group elements generate G :

$$\varphi_k(G) = \frac{N_k(G)}{|G|^k}$$

Theorem 1.1 *For any finite group G, $1 > \epsilon > 0$, we have*

$$\varphi_k(G) > 1 - \epsilon$$

given $k > \log_2 |G| + 2 + \log_2 1/\epsilon$. Further,

$$\varphi_m(G) > \frac{1}{4} \quad \textit{and} \quad \varphi_{m+1}(G) \geq \frac{1}{2},$$

where $m = \lceil \log_2 |G| \rceil$.

This is a slight improvement over a more general classical result by Erdős and Rényi in [ER] (see also [P3]). The proof is based on the following lemma, perhaps, of independent interest.

Lemma 1.2 *For any finite group G, $|G| \leq 2^m$ we have*

$$\varphi_k(G) \geq \varphi_k\big(\mathbb{Z}_2^m\big)$$

Define $\varkappa(G)$ to be the minimal possible number of generators of G. In other words,

$$\varkappa(G) = \min\{k \,|\, N_k(G) > 0\}$$

The problem of evaluating $\varkappa(G)$ has been of intense interest for classes of groups as well as for individual groups (see [CM]).

It is known that $\varkappa(G) = 2$ for all simple, nonabelian groups, and that $\varkappa(G) \leq n/2$ for $G \subset S_n$, with equality achieved when $G \simeq \mathbb{Z}_2^{n/2}$, and n is even. Also, it is easy to see that $\varkappa \leq \log_2 |G|$, with equality for $G \simeq \mathbb{Z}_2^m$. Note that Lemma 1.2 is trivial for $\varkappa \leq k < m$.

Define $\vartheta(G)$ to be the smallest k such that at least $1/e$ of the random k-tuples $(g_1, \ldots, g_k)$ generate the whole group. In other words,

$$\vartheta(G) = \min\left\{k \,|\, \varphi_k(G) > \frac{1}{e}\right\}$$

The significance of the constant $1/e$ is minimal, and is chosen for convenience.

Note that Theorem 1.1 immediately implies that

$$\vartheta(G) \leq \log_2 |G| + 1$$

By definition $\vartheta(G)/\varkappa(G) \geq 1$. It is unclear, however, how big this ratio can be (see Conjecture 1.6 below).

Here are few known results. When G is simple, it is known that $\varphi_2(G) \to 1$ as $|G| \to \infty$ (see [Sh]). For $G = A_n$, this is a famous result of Dixon (see [Dx]). For classical simple groups of Lie type the result was conjectured by Kantor and Lubotzky (see [KL]). In full generality it was recently proved by Liebeck and Shalev (see [LS1,LS2]). This immediately implies that $\vartheta(G) < C$ for any simple group G and some universal constant C.

The case when G is a direct product of simple group again goes back to Hall (see [H1]). He showed that

A direct product of m copies of a simple nonabelian groups can be generated by k generators if and only if $m \leq d_k(G)$,

where $d_k(G) = N_k(G)/|Aut(G)|$ is the number of orbits of diagonal action of $Aut(G)$ on $\mathcal{N}_k(G)$. Using Hall's example, A_5^{19} (product of 19 copies of icosahedral group) can be generated by two elements, while A_5^{20} cannot. A different proof was given in [KL], where the authors conclude that the probability that k random elements of A_n^d, $d = d_2(A_n)$ generate the whole group becomes small when $k = o(n)$[1]. In our notation, they show

$$\varphi_n(W_n) \to 0 \quad \text{as} \quad n \to \infty\,,$$

where $W_n = A_n^{d_2(A_n)}$. Note that $n = O(\log\log |W_n|)$. Here we prove an inverse result.

[1] Actually the authors in [KL] use $k = O(\sqrt{n})$. The analysis, however, can be extended to $k = o(n)$ case.

Theorem 1.3 *If G is a direct product of simple groups, then $\vartheta(G) \leq C \log m$, where m is the maximal number of isomorphic copies of each group and C is a universal constant.*

The proof is based on explicit calculations based on the known bounds for $\varphi_2(G)$. The constant C is expected to be relatively small. If only alternating groups are allowed, we show that C can be taken 5. We use sharp bounds of Babai given in [B1]. On the other hand, since our calculations for Chevalley groups use bounds in [KL,LS1,LS2] with unspecified constants, we do not attempt to establish C in these cases.

The case when G is abelian or nilpotent in different versions has been analyzed earlier (see [DS2,NP,PB]. We prove the following result which improves earlier bounds.

Theorem 1.4 *Let G be a finite nilpotent group. Then $\vartheta(G) \leq \varkappa(G) + 1$.*

When G is solvable, the first result in computing $\varphi_k(G)$ were obtained by Gaschütz, who gave in [Ga] a multiplicative formula for $N_k(G)$. Here we prove the following result.

Theorem 1.5 *Let G be a finite solvable group. Then $\vartheta(G) \leq 3.25\, \varkappa(G) + 10^7$.*

This result is an application of the Gaschütz technique, together with Mann's observation (see [M]). Mann went further, and showed that the constant 3.25 cannot be significantly improved. The constant 10^7 is probably unrealistic and can be lowered if care is applied.

We would like to conclude with a the following conjecture which we believe may be of wide interest and importance.

Conjecture 1.6 *For any finite group G we have*

$$\vartheta(G) < C \cdot \varkappa(G) \cdot \log\log |G|$$

where C is a universal constant.

An application of this conjecture is given in the last section on the product replacement algorithm (see above). Given special interest in the subject, we hope to return to the subject in the future.

2. Random group process

Let G be a finite group, and let $A \subseteq G$ be *any* generating subset of G. Define a *random group process* $\{B_t\}$, $t = 0, 1, 2, \ldots$ as follows. Let

$$B_0 = \{id\}\,, \quad B_{t+1} = \langle B_t, a_t \rangle\,,$$

where a_t, $t \geq 0$ are chosen uniformly and independently from A. Denote this random process $\mathcal{B} = \mathcal{B}(G, A)$.

Clearly, if $B_t = G$, then $B_k = G$ for all $k \geq t$. Therefore it is natural to stop the process $\mathcal{B}$ the first time $B_t = G$. Denote by τ the stopping time of the process. Think of τ as of random variable. Since $\langle A \rangle = G$, τ is finite with probability 1. By analogy with the separation distance for random walks (see e.g. [AD,D,P1]), define a *generation distance* $\mathbf{d}(T)$ as follows:

$$\mathbf{d}(t) = \mathbf{P}(\tau > t)$$

where $t = 0, 1, 2, \ldots$.

Proposition 2.1 *Let $A \subset G$ such that $\langle A \rangle = G$, and let $\mathbf{d}(\cdot)$ be the generation distance for a random process $\mathcal{B}(G, A)$. We have*

1) $\mathbf{d}(0) = 1$, $\mathbf{d}(t) \to 0$ *as* $t \to \infty$,

2) $\mathbf{d}(t+1) \leq \mathbf{d}(t)$ *for any* $t \geq 0$,

3) $\mathbf{d}(t+s) \leq \mathbf{d}(t) \cdot \mathbf{d}(s)$ *for any* $t, t \geq 0$.

Proof. Clear. □

Proposition 2.1 is completely analogous to the corresponding results for the separation distance (see [AD,P1]).

Example 2.2 Let $G = \mathbb{Z}_2^n$, and let A consist of n basis elements. Then $\mathbf{d}(t)$ is given by coupon collector's problem (see e.g. [F,D,P1]). Indeed, τ in this case is the first time we obtain *all* the elements in A. Thus we obtain

$$\mathbf{d}(n \log n + c\, n) \to \exp\big(-e^{-c}\big) \quad \text{as} \quad n \to \infty$$

for any fixed $c \in \mathbb{R}$.

Example 2.3 Let $G = \mathbb{Z}_p^n$, $A \subset G$. Assume A is *affine* : with each $a \in A$ it also contains $m \cdot a$, for all $m \in \mathbb{Z}_p$. In this case $\mathbf{d}(t)$ is given by the random matroid process, a generalization of the random graph process. We refer to [P1,PV] for details.

Let $A = G$. In this case we drop one G and write $\mathcal{B}(G)$ for the random group process $\mathcal{B}(G, G)$. Note that $\mathcal{B}(G)$ has particularly simple interpretation. We start with an empty set B_0 and add random group elements one by one until they generate the whole group. As before, let τ be the stopping time and let $\mathbf{d}(t) = \mathbf{P}(\tau > t)$. We will show that in this case $E(\tau)$ satisfies:

$$c_1\, \vartheta(G) \leq E(\tau) \leq c_2\, \vartheta(G)$$

for some universal constants c_1, c_2.

Theorem 2.4 *Let $\mathbf{d}(t)$ be the generation distance of the random group process $\mathcal{B}(G)$. Then for any $k > 0$ we have*

$$\varphi_k(G) = 1 - \mathbf{d}(k)$$

Proof. Observe that $1 - \mathbf{d}(k) = \mathbf{P}(\tau \le k)$. We have

$$\begin{aligned}\varphi_k(G) &= \mathbf{P}(\langle g_1, \dots, g_k\rangle = G)\\ &= \sum_{i=1}^{k} \mathbf{P}\big(\langle g_1, \dots, g_i\rangle = G,\ \langle g_1, \dots, g_{i-1}\rangle \ne G\big)\\ &= \sum_{i=1}^{k} \mathbf{P}(\tau = k) = \mathbf{P}(\tau \le k)\end{aligned}$$

This completes the proof. □

Theorem 2.5 *Let* $\mathbf{d}(t)$ *be the generation distance of the random group process* $\mathcal{B}(G)$*. We have:*

1) $\sum_{t\ge 0}\big(1 - \mathbf{d}(t)\big) = E(\tau)$
2) $\frac{1}{e}\, E(\tau) \le \vartheta(G) \le \frac{e}{e-1}\, E(\tau)$.

Proof. For the first part we have

$$\sum_{t\ge 0} \big(1 - \mathbf{d}(t)\big) = \sum_{t\ge 0} \mathbf{P}(\tau \le t) = \sum_{t\ge 0} t \cdot \mathbf{P}(\tau = t) = E(\tau)$$

The second inequality in part two follows from the Markov inequality

$$\mathbf{P}\big(\tau > c \cdot E(\tau)\big) < \frac{1}{c}$$

Indeed, take $c = e/(e-1)$ and $k = c \cdot E(\tau)$. We have

$$\varphi_k(G) = \mathbf{P}(\tau \le k) > 1 - \frac{1}{c} = \frac{1}{e}$$

and therefore $k \ge \vartheta(G)$.

The first inequality follows from Proposition 2.1. For any integer $k > 0$ we have

$$E(\tau) \le k + k \cdot \mathbf{d}(k) + k \cdot \big(\mathbf{d}(k)\big)^2 + \dots = \frac{k}{1 - \mathbf{d}(k)} = \frac{k}{\varphi_k(G)}$$

Now take $k = E(\tau)/e$. We get $\varphi_k(G) \le 1/e$ and therefore $k \le \vartheta(G)$. This completes the proof. □

Proof of Lemma 1.2. Let G be a finite group, $|G| \le 2^r$. Let τ be the stopping time for the random matroid process $\mathcal{B}(G)$. Denote by τ' the stopping time for $\mathcal{B}(\mathbb{Z}_2^r)$. We claim that for all t the probability $\mathbf{P}(\tau \le t)$ minimizes when $G \simeq \mathbb{Z}_2^r$. In other words, we claim that

$$\mathbf{P}(\tau \le t) \ge \mathbf{P}(\tau' \le t)$$

for all G and $t \ge 0$. We prove the claim by induction. For $r = 0$ we have $G = \{id\}$ and there is nothing to prove.

Now assume that $|G| \le 2^r$, $r \ge 1$. Denote by $H_i = \langle B_i \rangle$ the subgroup we obtain after i steps of the random group process. Regardless of the group structure, the probability that $H_i \neq H_{i+1}$ for any i is equal to $\big(1 - |H_i|/|G|\big)$. Note that when $H_i \neq H_{i+1}$ we have $|H_{i+1}|/|H_i| \ge 2$, with the equality *always* achieved when $G \simeq \mathbb{Z}_2^r$. Denote by τ_1, τ_2, ... the times when we have $H_{\tau_i} \neq H_{\tau_i - 1}$ in random process for group G. Analogously, for the group $\mathbb{Z}_2^r$ define times τ_1', τ_2', ... when the generated subgroups are $\mathbb{Z}_2$, $\mathbb{Z}_2^2$, ...

Denote $\ell = \ell(\tau)$ the first time i when $H_{\tau_i} = G$. Clearly, $\ell \le \log_2 |G| \le r$. We have then $\tau = \tau_\ell$. We think of τ, τ_i, ℓ as of random variables depending of the random group process. Denote $m = \tau_{\ell-1}$. Working backwards, for every proper subgroup $H \subsetneq G$ we have:

$$(\circ) \quad \mathbf{P}\big(\tau_\ell - \tau_{\ell-1} \le k \,|\, H_m = H\big) \ge \mathbf{P}\big(\tau_r' - \tau_{r-1}' \le k\big).$$

To prove $(\circ)$, fix $\tau_{\ell-1} = m$, and recall that

$$\mathbf{P}\big(\tau_\ell - \tau_{\ell-1} = k \,|\, \tau_{\ell-1} = m, H_m = H\big) = p\,(1-p)^{k-1},$$

where $p = 1 - |H|/|G| \ge 1 - |\mathbb{Z}_2^{r-1}|/|\mathbb{Z}_2^r| = 1/2$. The inequality $(\circ)$ follows after summation over all k, m, and then comparison with the case $p = 1/2$.

Now use inductive assumption for H, $|H| \le 2^{r-1}$:

$$(\circ\circ) \quad \mathbf{P}\big(\tau_{\ell-1} \le k \,|\, H_m = H\big) \ge \mathbf{P}\big(\tau_{r-1}' \le k\big).$$

Combining inequalities $(\circ)$ and $(\circ\circ)$, summing over all proper subgroups H of G, we obtain:

$$\mathbf{P}(\tau \le k) \ge \mathbf{P}(\tau') \le k).$$

This proves the step of induction and implies the claim. Since $\varphi_k(G) = \mathbf{P}(\tau \le k)$ and $\varphi_k(\mathbb{Z}_2^r) \le \mathbf{P}(\tau' \le k)$, this also implies the result. $\square$

Let us note that equality in Lemma 1.2 can occur if and only if $G \simeq \mathbb{Z}^m$. Indeed, from the proof above we must require that $\varkappa(G) = m$, and that $|G| = 2^m$. Now use induction on m. This is a simple exercise in group theory we leave to the reader.

3. p-GROUPS

Let G be a nilpotent group, and let Φ be its Frattini subgroup. We have

$$\varphi_k(G) = \varphi_k(G/\Phi)$$

and the problem of computing the generation probability is reduced to abelian groups.

Let G be an abelian p-group,

$$G \simeq \mathbb{Z}_p^{\alpha_1} \oplus \mathbb{Z}_{p^2}^{\alpha_2} \oplus \dots$$

Let $\varkappa = \varkappa(G) = \alpha_1 + \alpha_2 + \dots$ be the minimum number of generators. We have $G/\Phi \simeq \mathbb{Z}_p^{\varkappa}$ and

$$\varphi_k(G) = \varphi_k(G/\Phi) = \prod_{i=1}^{\varkappa} \left(1 - \frac{1}{p^{i-\varkappa+k}}\right) \ge \prod_{i=k-\varkappa+1}^{\infty} \left(1 - \frac{1}{p^i}\right)$$

Let $z = 1/p$. By Euler's pentagonal theorem we have:

$$(*) \quad \prod_{i=1}^{\infty}(1-z^i) = 1+\sum_{m=1}^{\infty}(-1)^m\, z^{\frac{m\,(3m\pm1)}{2}} = 1-z-z^2+z^5+z^7-\,\ldots\, \geq 1-z-z^2$$

(see e.g. [An], Corollary 1.7.) Therefore for $k = \varkappa(G)$ we have

$$\varphi_k(F_p) \geq 1-\frac{1}{p}-\frac{1}{p^2} \geq 1-\frac{1}{2}-\frac{1}{4} = \frac{1}{4}$$

Analogously, for $k = \varkappa(G)+1$ we have

$$\varphi_k(F_p) \geq \varphi_{\varkappa+1}(F_p) = \prod_{i=2}^{\infty}\left(1-\frac{1}{p^i}\right) \geq \frac{1-\frac{1}{p}-\frac{1}{p^2}}{1-\frac{1}{p}} = 1-\frac{1}{p\,(p-1)}$$

Recall another Euler's formula:

$$\prod_{i=0}^{\infty}\frac{1}{1-t\,z^i} \;=\; 1+\sum_{n=1}^{\infty}\frac{t^n}{(1-z)(1-z^2)\cdots(1-z^n)}$$

(see e.g. [An], Corollary 2.2.) Take $k = \varkappa+r-1$, $z = 1/p$, $t = 1/p^r$. We get

$$\varphi_k^{-1}(G) \leq \prod_{i=r}^{\infty}\left(1-\frac{1}{p^i}\right) = 1+\sum_{n=1}^{\infty}\frac{\left(\frac{1}{p^r}\right)^n}{\left(1-\frac{1}{p}\right)\left(1-\frac{1}{p^2}\right)\cdots\left(1-\frac{1}{p^n}\right)}$$

Using $(*)$ for the denominator of the last fraction we get

$$\varphi_k^{-1}(G) \leq 1+\sum_{n=1}^{\infty}\frac{\left(\frac{1}{p^r}\right)^n}{\left(1-\frac{1}{p}-\frac{1}{p^2}\right)} = 1+\frac{1}{\left(1-\frac{1}{p}-\frac{1}{p^2}\right)}\cdot\frac{1}{\left(1-\frac{1}{p^r}\right)}\cdot\frac{1}{p^r}$$

Finally, we obtain

$$\varphi_k(G) \geq 1-\frac{1}{p^r\,(1-1/p-1/p^2)\,(1-1/p^r)} \geq 1-8/p^r$$

Let us summarize the results.

Theorem 3.1 *Let G be a finite p-group, and let $\varkappa = \varkappa(G)$. We have*

1) $\varphi_{\varkappa}(G) > 1-1/p-1/p^2$,
2) $\varphi_{\varkappa+1}(G) > 1-1/p(p-1)$,
3) $\varphi_{\varkappa+r-1}(G) > 1-1/(p^r-1)(1-1/p-1/p^2)$, *where* $r \geq 1$.

A similar result was proved in [DS2] by a different approach. For part 1) see also [Ac]. Now we can complete the proof of Theorem 1.1.

Proof of Theorem 1.1. By Lemma 1.2 we have $\varphi_k(G) \geq \varphi_k(\mathbb{Z}_2^k)$ if $k \geq \log_2|G|$. Part three of Theorem 3.1 implies that

$$\varphi_k\big(\mathbb{Z}_2^m\big) > 1-\frac{4}{2^{k-m+1}-1} > 1-2^{2+m-k}$$

Therefore $\varphi_k(G) > (1-\epsilon)$ given $k > \log_2|G| + \log_2 1/\epsilon + 2$. This completes the proof. $\square$

4. Nilpotent groups

Let G be a nilpotent group, $p_1, \ldots, p_m$ are distinct primes, and

$$G = F_{p_1} \oplus \ldots \oplus F_{p_m} \,,$$

where F_p is the Sylow p-subgroup of G. Assume $|F_{p_i}| = p_i^{\lambda_i}$. It is easy to see that

$$\varphi_k(G) = \prod_{i=1}^{m} \varphi_k\big(F_{p_i}\big)$$

(see e.g. [H1,KL]). We will use the results of the previous section to obtain general bounds.

When $k \geq \varkappa(G) + 1$ Theorem 3.1 gives us

$$\varphi_k(G) \geq \prod_{p=2}^{\infty} \left(1 - \frac{1}{p\,(p-1)}\right) > .373 > 1/e$$

where the product is over all primes p. This immediately implies that $\vartheta(G) \leq \varkappa(G) + 1$. The lower bound .373 follows from the following observation:

$$\chi = \prod_{p=2}^{\infty} \left(1 - \frac{1}{p\,(p-1)}\right) \geq \prod_{p \leq 300{,}000} \left(1 - \frac{1}{p\,(p-1)}\right) \cdot \prod_{j \geq 300{,}001} \left(1 - \frac{1}{j\,(j-1)}\right)$$

Direct computation shows that the first product is .3739561835 while the second product satisfies

$$\prod_{j=300{,}001}^{\infty} \left(1 - \frac{1}{j\,(j-1)}\right) > \prod_{j \geq 300{,}000} \frac{(j-1)(j+1)}{j^2} = 1 - \frac{1}{300{,}000} = .999996666(6)$$

This gives $\chi > .373$ and proves the claim.

Now use the first part of Theorem 3.1, when $k \geq \varkappa(G)$. We claim that

$$\varphi_k(G) > \prod_{i=1}^{m} \left(1 - \frac{1}{p_i} - \frac{1}{p_i^2}\right) \geq C\, \frac{1}{\log\log |G|}$$

where $C = .2099612456$ is a universal constant. Indeed, observe that $1 - 1/p - 1/p^2 = (1 - 1/p)(1 - 1/p(p-1)$ and thus the infinite product can be presented as two infinite products, the first equal to χ and the second given by the the Mertens formula

$$\lim_{n \to \infty} \log\log n \cdot \prod_{p \leq n} \left(1 - \frac{1}{p}\right) = e^{-\gamma}$$

where $\gamma = 0.5772156649$ is the Euler-Mascheroni constant (see [HW,WW].

Combining these results into a theorem, we obtain:

Theorem 4.1 *Let G be a nilpotent group, and let $\varkappa = \varkappa(G)$ be the minimum number of generators. Then*

1) $\varphi_{\varkappa}(G) > 1/(5 \log\log |G|)$,

2) $\varphi_{\varkappa+1}(G) > 1/e$,

3) $\varphi_{\varkappa+r-1} > 1 - 8 \cdot 1/(12^{r/4})$, *where* $r \geq 1$.

Proof. Parts 1, 2 were proved earlier. For the last part we have :

$$\varphi_{\varkappa+r-1} \geq \prod_p \left(1 - \frac{8}{p^r}\right) > 1 - \sum_p \frac{8}{p^r} > 1 - 8 \cdot \left(\sum_p \frac{1}{p^4}\right)^{r/4} > 1 - 8 \cdot \left(\sum_{n=2}^{\infty} \frac{1}{n^4}\right)^{r/4}$$

The latter sum can be computed directly as in the previous section. We have $\sum_{n>2} 1/n^4 = .082323234 > 1/12$, and

$$\varphi_{\varkappa+r-1} > 1 - 8 \cdot \frac{1}{12^{r/4}}$$

This completes the proof. □

Note that part 2) of the Theorem implies Theorem 1.4 (cf. [DS2], Remark after Lemma 6.3.) Part 3 shows an exponential decay of the generation distance for $k > \varkappa(G)$.

5. Solvable groups

Let us recall several definitions (see [J]). Let H be a group (not necessarily abelian), and let the group G act on H so that the conditions (1), (2), (3), (4) hold:

(1) $(h_1 h_2)^g = h_1^g h_2^g$

(2) $h^{g_1 g_2} = (h^{g_1})^{g_2}$

(3) $h^1 = h$

for all $h, h_1, h_2 \in H$, $g, g_1, g_2 \in G$. In other words, G is homomorphic to a subgroup of the automorphism group of H.

(4) The image of the above homomorphism includes all the inner automorphisms of H.

Under these conditions H is called a *G-group*. One can think of G-groups as of a generalization of linear representations. One can also define G-homomorphism, G-isomorphism, G-endomorphism, G-subgroup, and G-composition series. The condition (4) ensures the validity of elementary group theoretical statements used below extends also to G-groups. We refer to [J], Chapter 3, for details.

Let G be a finite solvable group, and let

$$G = G_0 \supset G_1 \supset \ldots G_{r-1} \supset G_r \supset 1$$

be a chief series of G going through G_r. The factors $H_i = N_i/N_{i+1}$ are abelian as groups, and simple as G-groups. In other words, they don't have proper G-subgroups. Therefore $H_i \simeq \mathbb{Z}_p^m$ for some integer m and prime p. Also, by Schur's

Lemma, endomorphisms of H_i form a field $\mathbb{F}_q$, where $q = p^r$, $1 \le r \le m$. We say that a subgroup $K \subset G$ is a *complement* of a normal subgroup N of G if $NK = G$ and $N \cap K = 1$.

Following [Ga], denote by $F_1, \ldots, F_h$ the different (up to G-isomorphisms) types of simple G-groups that occur among the composition factors H_i. Let α_i be the number of factors of type F_i that have a complement, and β_i be the number of those of type F_i that do not possess a complement. Let E_i be the field of endomorphisms of F_i. Assume $|F_i| = p_i^{\lambda_i}$, p_i prime, and ω_i is the degree of the endomorphism field E_i. Also, let

$$\zeta_i = \begin{cases} 0, \text{ if } F_i \text{ is fixed element-wise by } G \\ 1, \text{ otherwise} \end{cases}$$

Then Theorem 5 in [Ga] gives

$$N_k(G) = \prod_{i=1}^{h} p_i^{\lambda_i \beta_i k} \cdot \prod_{i=1}^{h} \left(p_i^{\lambda_i k} - p_i^{\lambda_i \zeta_i}\right) \cdot \left(p_i^{\lambda_i k} - p_i^{\lambda_i \zeta_i + \omega_i}\right) \cdot \ldots \cdot \left(p_i^{\lambda_i k} - p_i^{\lambda_i \zeta_i + (\alpha_i - 1)\omega_i}\right)$$

We obtain

$$\varkappa(G) = \max_i \left\lfloor \frac{(\alpha_i - 1)\omega_i}{\lambda_i} + \zeta_i + 1 \right\rfloor$$

We have

$$\varphi_k(G) = \prod_{i=1}^{h} \prod_{j=0}^{\alpha_i - 1} \left(1 - p_i^{\lambda_i(\zeta_i - k) + j\omega_i}\right)$$

Denote by $w(p, \lambda)$ the number of $F_i \simeq \mathbb{Z}_p^{\lambda}$, and let $W(p, \lambda)$ be the maximal possible number of groups $F \simeq \mathbb{Z}_p^{\lambda}$, which are different as G-groups (as we shall see, this number is bounded). When $k = \varkappa(G) + 1$ we have

$$\varphi_{\varkappa + l + 1} \ge \prod_{i=1}^{h} \left(1 - \frac{1}{p_i^{1 + l\,\lambda_i}}\right)^{w(p_i, \lambda_i)} \ge \prod_{p} \prod_{n=1}^{\infty} \left(1 - \frac{1}{p^{1 + l\,n}}\right)^{W(p,n)}$$

where the product is taken over all primes p.

Let us give a bound on $W(p, n)$. Let $\varkappa = \varkappa(G)$, $F = \mathbb{Z}_p^n$. Then $Aut(F) \simeq GL(n, p)$. By definition, the image of G is an irreducible solvable subgroup $H \subset Aut(F)$. By $\widehat{H}$ denote a maximal subgroup which contains H. Observe that the number of homomorphisms of G into H is at most $|\widehat{H}|^{\varkappa}$. Therefore the total number $W(p, n)$ of *different* G-groups is at most $|\widehat{H}|^{\varkappa}$ times the number of conjugacy classes of maximal subgroups. Following [Pa,Wo], we have

$$\left|\widehat{H}\right| \le \frac{|F|^{\beta}}{(24)^{1/3}}\,,$$

where $\beta = (3 \cdot \ln 48 + \ln 24)/(3 \cdot \ln 9) \approx 2.243991050$ is a *Pálfy–Wolf constant*.

By [Py] (see Lemma 3.4.iii), the number of conjugacy classes of maximal solvable subgroups of $GL(n, p)$ is at most $2^{n-1} \cdot n^{20\,(\log_2 n)^3 + 5}$. Combining these together, we obtain:

$$W(p, n) \le \frac{p^{\beta\,\varkappa\,n}}{(24)^{1/3}} \cdot 2^{20\,(\log_2 n)^4 + 5\,\log_2 n + n - 1}\,.$$

Then for $k = \varkappa + l + 1$ we have

$$\varphi_k \geq \prod_p \prod_{n=1}^{\infty} \left(1 - \frac{1}{p^{1+n}}\right) > \frac{1}{e}$$

given $p^{l\,n} > p^{n+1} \cdot W(p,n)$ for all p, n (for the last inequality see above). Solve the latter inequality directly. The worst case being $p = 2$, it follows from :

$$(l - \beta\,\varkappa) \cdot n > \left(20\,(\log_2 n)^4 + 5\,\log_2 n + 2\,n\right)$$

Solving this inequality numerically, we obtain $(l - \beta\,\varkappa) > .48 \cdot 10^7$. Recall that Therefore $\varphi_k(G) > 1/e$ given $k > (1+\beta)\,\varkappa + 10^7$. This completes the proof of Theorem 1.5. $\square$

Theorem 5.1 *There exists a universal constant $C < 10^7$ such that for any solvable group G, $\varkappa = \varkappa(G)$, and $r > 0$ we have*

$$\varphi_{(\beta+1)\varkappa + C + r} < \frac{1}{12^{r/4}}$$

Proof. The proof follows easily from the computations above and part 3 of the Theorem 4.1. We skip the details. $\square$

Remark 5.2. Roughly, Theorem 5.1 says that the the generation distance decreases exponentially after $(\beta+1)\varkappa + C$ steps.

The result of Mann (see [M]) shows that after $(\beta+1)\varkappa + C$ steps the probability of generation of G becomes bounded away from 0. Also, for all d, Mann constructs a family of d-generated solvable groups $\{G_i\}$ such that $\lim \vartheta(G_i) \geq \beta\,d - 1$. This shows that one can never obtain results for solvable groups similar to those in the nilpotent group case.

Let us mention that the result of Pálfy in [Pa] (see also [Se]) contains for each p the best possible bounds on the number of conjugacy classes of maximal solvable subgroups (which agree with ours for $p = 3$). Unfortunately they seem to lead to improvement in our bounds only in very special cases of solvable groups.

Finally, few words about random generation in profinite groups. Beside a pioneer paper [M], a significant progress has been made in the understanding of the so called *positively finite generated* groups. Many of the results are yet to be translated and understood in the finite group setting. We would like to especially note the main result in [BPS], which seems of particular importance. We refer to [Sh] for the review and references.

6. Powers of simple groups

Let G be a nonabelian simple group, and let

$$G^m = G \times G \times \cdots \times G \quad (m \text{ times})$$

be a power of G. Clearly, Denote by $d_k(G)$ the maximal m such that G^N can be generated by k elements. Recall from section 1 the result of Philip Hall :

$$d_k(G) = \frac{\mathcal{N}_k(G)}{|Aut(G)|},$$

where $Aut(G)$ is the group of automorphism of G. It was observed by Kantor and Lubotzky (see [KL], Proposition 9) that in this case one can obtain an explicit multiplicative formula for the number of generating k-tuples:

$$\varphi_k(G^m) = \frac{N_k(G)}{|G|^{k(m-1)}} \prod_{i=1}^{m-1} \left(\varphi_k(G)\,|G|^k - i\,|Aut(G)|\right)$$

Rewriting this differently gives us

$$\varphi_k(G^m) = \varphi_k^m(G) \prod_{i=1}^{m-1} \left(1 - \frac{i}{d_k(G)}\right)$$

We will use this formula to obtain a bound $\vartheta(G) < C\,\log m$ for a universal constant $C > 0$.

Recall the classification of finite simple group (CFSG). It is known that beside the alternating groups A_n, $n \geq 5$, and simple groups of Lie type there exist only a finite number of *sporadic* simple groups (see [Go]).

We start with the case when $G \simeq A_n$. Then $|Aut(A_n)| = |S_n| = n!$ Denote by M the order of A_n: $M = n!/2$. Recall that in this case we have

$$\varphi_2(n) = 1 - \frac{1}{n} + O\left(\frac{1}{n^2}\right)$$

(see [B1]). Thus for n large enough, say for all $n \geq n_0$, we have $\vartheta(A_n) = 2$. Then for all $n \geq n_0$, $k \geq 2$ we have

$$d_k(A_n) = \frac{\varphi_k(A_n)\,|A_n|^k}{|Aut(A_n)|} \geq \frac{1/2\,(n!/2)^k}{n!} = \frac{M^{k-1}}{4}$$

By submulticativity of $\mathbf{d}(k) = 1 - \varphi_k(G)$ we have

$$\varphi_k(A_n) \geq 1 - (1 - \varphi_2(A_n))^{k/2} = 1 - \frac{1}{n^{k/2}} + O\left(\frac{1}{n^{k/2+1}}\right)$$

where k is even and $n \to \infty$. Now take $k = c \log_n m$. For n large enough we have

$$\begin{aligned}\varphi_k(A_n^m) = \varphi_k^m(A_n) \prod_{i=1}^{m-1} \left(1 - \frac{i}{d_k(A_n)}\right) &> \left(1 - \frac{1}{2\,n^{k/2}}\right)^m \prod_{i=1}^{m-1} \left(1 - \frac{i}{M^k/4}\right) \\ &> \left(1 - \frac{1}{n^{c/2\,\log_n m}}\right)^m \left(1 - \frac{4\,m}{n^{c\log_n m}}\right)^{m-1} > \left(1 - \frac{1}{m^{c/2}}\right)^m \left(1 - \frac{4}{m^{c-1}}\right)^m\end{aligned}$$

It is easy to see that when $c = 5$ the right hand side is $> 1/e$ given $m \geq 2$, $k \geq 2$ and n large enough. We obtain the following result.

Theorem 6.1 *For any $m \geq 1$, and any n large enough we have*

$$\vartheta(A_n^k) \leq \max\{2,\, 5\log_n m\}\,.$$

Now let G be a simple group of Lie type over the field $\mathbb{F}_q$, where $q = p^r$. By n denote the rank of G. It was shown in [KL,LS2] that

$$\varphi_2(G) = 1 - O\left(\frac{n^3(\log q)^2}{q^n}\right)$$

Therefore

$$\varphi_{2k}(G) \geq 1 - (1-\varphi_2)^k \geq 1 - \left(\frac{c\, n^3(\log q)^2}{q^n}\right)^k$$

for some universal constant c. Observe that

$$\varphi_{2k}(G) \to 1 \quad \text{as} \quad |G| \to \infty$$

(see e.g. [Go], Table 6 in [CCNPW]).

For the order of the automorphism group $Aut(G)$ we have the following crude bound

$$|Aut(G)| < C\,|G|\log^2|G|$$

for some universal constant C. To obtain this bound one has to consider groups $A_n(q)$ and ${}^2A_n(q)$ separately from the rest. For the remaining groups we have

$$|Aut(G)|/|G| \leq 6\cdot r \leq c\cdot\log q \leq c\cdot\log|G|$$

For $G = A_n(q)$ or $G = {}^2A_n(q)$, $n \geq 2$ we have

$$|Aut(G)|/|G| \leq 6\cdot r\cdot(n+1, q\pm 1) \leq c\cdot\log q\cdot\log|G| \leq c\cdot\log^2|G|$$

We refer to [CCNPW] for the explicit formulas. We conclude

$$d_k(G) = \frac{\varphi_k(G)\cdot|G|^k}{|Aut(G)|} \geq \frac{c\,|G|^{k-1}}{\log^2|G|}$$

We can now obtain a generalization of Theorem 6.1 for every nonabelian simple group Lie of Lie type. We have

$$\varphi_{2k}(G^m) = \big(\varphi_{2k}(G)\big)^m \cdot \prod_{i=1}^{m-1}\left(1 - \frac{i}{d_{2k}(G)}\right)$$

For the product on the right we have

$$\prod_{i=1}^{m-1}\left(1 - \frac{i}{d_{2k}(G)}\right) > \left(1 - \frac{m}{c\,|G|^{k-1}/\log^2|G|}\right)^m > \left(1 - \frac{m^2}{|G|^{k-2}}\right)$$

when $|G|$ is large enough. Thus for $m \le |G|^{k/2-2}$ and $|G|$ large enough we have $\prod > 1 - 1/|G|$. Analogously, we get

$$\big(\varphi_{2k}(G)\big)^m > 1 - \frac{c\,m\,\big(n^3(\log q)^2\big)^k}{q^{kn}} > 1 - \frac{1}{q^n}$$

where $k > C \log m$, and C is a universal constant. One can also improve this to

$$\varphi_{2k}(G^m) > 1 - \frac{1}{q^n}$$

since the product above is small. This implies the following result.

Theorem 6.2 *Let $\{G_n\}$ be any sequence of Chevalley groups $|G_n| \to \infty$ as $n \to \infty$. Then for all $m \ge 1$ we have*

$$\varphi_k(G^m) \to 1 \quad \text{as} \quad n \to \infty$$

where $k > C \log m$, and C is a universal constant.

7. Direct products of simple groups

Let $G = H_1^{m_1} \times \cdots \times H_l^{m_l}$, where H_i are distinct simple nonabelian groups. It is easy to see that

$$\varphi_k(G) = \varphi_k\big(H_1^{m_1}\big) \cdot \ \ldots \ \cdot \varphi_k\big(H_l^{m_l}\big)$$

(see e.g. Lemma 5 in [KL].) Thus we can use the estimates from the previous section to estimate $\varphi_k(G)$. Namely, we will prove the following result.

Theorem 7.1 *Let G be as above. Then for all $k > C \max\{\log m_i\}$ we have*

$$\varphi_k(G) \ge \frac{1}{e}$$

where C is a universal constant.

Observe that Theorem 7.1 is equivalent to Theorem 1.3. This also shows that Conjecture 1.6 holds in this case. Indeed, note that

$$\log\log|H^m| = \log(m \cdot \log|H_i|) > \log m_i$$

for all i. Therefore $\log\log|G| > \max\{\log m_i\}$, which implies the claim.

Before we prove the theorem we need the following technical Lemma.

Lemma 7.2 *For any $n \ge 2$ we have*

$$\prod_{q=2}^{\infty} \left(1 - \frac{1}{q^n}\right) > \exp\left(-\frac{3}{2^n}\right)$$

Proof. Observe that $\log(1-x) > -x - x^2$ for $0 < x < 1/2$. We have

$$\prod_{q=2}^{\infty}\left(1-\frac{1}{q^n}\right) = \exp\left(\sum_{q=2}^{\infty}\log\left(1-\frac{1}{q^n}\right)\right) > \exp\left(\sum_{q=2}^{\infty}-\frac{1}{q^n}-\frac{1}{q^{2n}}\right)$$

On the other hand

$$\sum_{q=2}^{\infty}\frac{1}{q^n} = \frac{1}{2^n}\left(1+\sum_{q=3}^{\infty}\frac{2^n}{q^n}\right) \le \frac{1}{2^n}\left(1+4\sum_{q=3}^{\infty}\frac{1}{q^2}\right) = \frac{1}{2^n}\left(\frac{2\pi^2}{3}-4\right) < \frac{2.58}{2^n}$$

Analogously

$$\sum_{q=2}^{\infty}\frac{1}{q^{2n}} = \frac{1}{2^{2n}}\left(1+\sum_{q=3}^{\infty}\frac{2^{2n}}{q^{2n}}\right) \le \frac{1}{2^{2n}}\left(1+16\sum_{q=3}^{\infty}\frac{1}{q^4}\right) \le \frac{1}{2^n}\cdot\frac{1}{4}\left(-16+\frac{8\pi^4}{45}\right) < \frac{0.33}{2^n}$$

Combining the results we obtain

$$\prod_{q=2}^{\infty}\left(1-\frac{1}{q^n}\right) > \exp\left(-\frac{2.58}{2^n}-\frac{0.33}{2^n}\right) > \exp\left(-\frac{3}{2^n}\right)$$

This completes proof of the lemma. □

Proof of Theorem 7.1. We proved in the previous section that there exist a universal constant C such that

$$\varphi_k\left(H_i^{m_i}\right) > 1-\frac{1}{q^n}$$

given $k > C\log m_i$ and $|H_i| > N$, where N is some universal constant.

Now recall classification of finite simple nonabelian groups. There are only six series where n grows: $A_n(q)$, ${}^2A_n(q)$ $B_n(q)$, $C_n(q)$, $D_n(q)$, and ${}^2D_n(q)$ (see e.g. [Go,CCNPW]). Here $q = p^r$ is the size of finite field.

By the lemma, when k as in the theorem, we have

$$\prod_q \varphi_k\left((R_n(q))^m\right) > \prod_q 1\left(-\frac{1}{q^n}\right) > \exp\left(-\frac{3}{2^n}\right)$$

where R_n is the name of the series $A_n \ldots {}^2F_4$. This shows that $\prod_q \varphi_k(\cdot) > c > 0$ for all series with bounded n. For the six series as above we have

$$\prod_n\prod_q \varphi_k\left((R_n(q))^m\right) > \prod_n \exp\left(-\frac{3}{2^n}\right) > \exp(-3) > 0$$

This gives us

$$\prod_i \varphi_k(H_i^{m_i}) > c_1,$$

where $c_1 > 0$ is a universal constant and $|H_i| > N$.

Now consider all simple groups H_i, $|H_i| \le N$. There is a finite number of them. However, the powers m_i can be large, so we have to treat these groups accordingly.

Recall that $\varphi_k(H_i) > 1/2$ suffices to hold for the argument in the previous section. On the other hand, by Theorem 1.1, this is satisfied given $k > \log N + 3 \ge \log H_i + 3$. Now, the condition $k \ge \max\{\log m_i, \log N + 3\}$ implies that $\varphi_k(H_i^{m_i}) > c > 0$ for all i. Since the number of simple groups $H_i \le N$ is finite, we obtain

$$\prod_i \varphi_k(H_i^{m_i}) > c_2,$$

where $c_2 > 0$ is a universal constant and $|H_i| \le N$. We conclude

$$\varphi_k(G) = \prod_i \varphi_k(H_i^{m_i}) > c_1 \cdot c_2$$

This completes the proof. □

8. Applications : Product replacement algorithm

The *product replacement algorithm* is an important recent advancement in symbolic algebra (see [CLMNO], also [B3,BaP,P4,P5,PB]). It was designed by Leedham–Green and Soicher to generate efficiently (nearly) uniform group elements ([LG]). It is by far the most popular "practical" generator of random group elements, implemented in both *GAP* (see [Sc] and *Magma* (see [BCP]) group algebra packages. In this section we describe problems related to the algorithm in connection with the results in the previous section.

In a pioneer paper [CLMNO] Celler et al. defined a Markov chain $\mathcal{M} = \{X_t\}$ on $\mathcal{N}_k(G)$ as follows. Let $X_t = (g_1, \ldots, g_k) \in \mathcal{N}_k(G)$. Define

$$X_{t+1} = (g_1, \ldots, h_j, \ldots, g_k),$$

where $h_j = g_j g_i^{\pm 1}$ or $h_j = g_i^{\pm 1} g_j$, where the pair (i,j), $1 \le i, j \le k$, $i \ne j$ is chosen uniformly; the multiplication order and the ± 1 degree are determined by independent flips of a fair coin. The algorithm runs the Markov chain for a time T, starting at a given set of generators. Then it outputs a random component $g = g_i$ of the group elements in a generating k-tuple X_T. It is known that g is distributed (nearly) uniformly given $k = \Omega(\log |G|)$ and T is large enough.

Observe that there can be two types of error when we generate a (nearly) uniform group element as above. The first type comes from the distribution of $X_T \in \mathcal{N}_k(G)$ being far from the uniform distribution U on $\mathcal{N}_k(G)$. The second one comes from having group elements in generating k-tuples distributed not uniformly. Let us concentrate here on the second type of error leaving aside the issue of determining the mixing time of the Markov chain $\mathcal{M}$.

Consider a graph $\Gamma = \Gamma(G,k)$ with a set of vertices $\mathcal{N}_k(G)$ and edges corresponding to Markov chain moves. Assume that the graph Γ is connected, so that the stationary distribution is indeed uniform on $\mathcal{N}_k(G)$. Denote by Q_k the probability distribution of the random component of uniform elements in $\mathcal{N}_k(G)$. Thus Q_k is a limiting distribution of the algorithm output (as time $T \to \infty$). We measure how far Q_k from the uniform distribution U on G by the *total variation distance*:

$$\xi_k(G) = \|Q_k - U\|_{\text{tv}} = \max_{B \subset G} |Q_k(B) - U(B)| = \frac{1}{2} \sum_{g \in G} \left| Q_k(g) - \frac{1}{|G|} \right|$$

In [BaP] Babai and the author showed that for groups $G = A_n^{n!/8}$ and $k = o(n)$ we have $\xi_k(G) \to 1$ as $n \to \infty$.[2] We also show in [BaP] that the error is large enough to be detected by a short straight line program. Practical experiments seem to support the theoretical conclusion ([LG]).

In [P5] the author observed that there can be no bias in the distribution Q_k given k is at least $\vartheta(G)$. Formally, we prove the following result:

Theorem 8.1 (see [P5]) *Let $\{G_i\}$ be a sequence of groups, $\varkappa_i = \varkappa(G_i)$, and let k_i be a sequence such that*

$$\varphi_{k_i}(G_i) \to 0 \quad as \quad i \to \infty$$

Then

$$\xi_{k_i+\varkappa_i}(G_i) \to 0 \quad as \quad i \to \infty$$

Therefore one can apply sharp bound for φ_k to to obtain the following corollaries. By $\omega(n)$ denote any increasing function with $w(n) \to \infty$ as $n \to \infty$ (e.g. $\omega(n) = \log\log n$ will work).

Corollary 8.2 *Let G_i be a sequence of nilpotent groups, $\varkappa_i = \varkappa(G_i)$ and $\omega(i)$ be as above. Then*

$$\xi(G_k) \to 0 \quad as \quad i \to \infty\,,$$

given $k = k_i > 2\,\varkappa_i + \omega(i)$.

Corollary 8.3 *Let G_i be a sequence of solvable groups, $\varkappa_i = \varkappa(G_i)$ and $\omega(i)$ be as above. By β denote Pálfy–Wolf constant, $2.24 < \beta < 2.25$. Then*

$$\xi(G_k) \to 0 \quad as \quad i \to \infty\,,$$

given $k = k_i > (2+\beta)\varkappa_i + \omega(i)$.

Corollary 8.4 *Let G_i be a sequence of direct products of simple groups, m_i be the maximum number of times a copy is contained in G_i, and let $\omega(i)$ be as above. Then*

$$\xi(G_k) \to 0 \quad as \quad i \to \infty\,,$$

given $k = k_i > \log(m_i) \cdot \omega(i)$.

Corollary 8.5 *Let G_i be any sequence of groups, and let $\omega(i)$ be as above. Then*

$$\xi(G_k) \to 0 \quad as \quad i \to \infty\,,$$

given $k = k_i > 2\log_2|G| + \omega(i)$.

The result of Corollaries should be compared with the connectivity results for $\Gamma(G,k)$. Namely it was shown by Dunwoody [Du] (see also [P4,P5]) that for all

[2] This was announced earlier by the author in [PB].

finite solvable groups G the graph $\Gamma(G, \varkappa(G))$ is connected. It is conjectured that $\Gamma(G,k)$ is connected when $k \geq 3$ and G is simple (see [P4,P5]). It is known that this conjecture implies that $\Gamma(G^m,k)$ is also connected given $m < d_{k-1}(G)$ (see [P4] for references and details.

Proof The corollaries follow immediately from Theorem 8.1 and Theorems 4.1.3, 5.1, 7.1 and 1.1 respectively. $\square$

Remark 8.6 Observe that Corollary 8.5 implies that for *general* group take k to be $\log_2 |G| + C$ rather than $2\log_2 |G| + C$, as presumed in [B3,DS2]. Note also that if conjecture 1.6 holds, this would imply that k should be roughly $C \varkappa \log\log |G|$. If true, this would have immediate implications on use and design of the algorithm.

Acknowledgments

We would like to thank L. Babai, S. Bratus, G. Cooperman, P. Diaconis, W. Feit, L. Finkelstein, W. Kantor, L. Lovasz, A. Lubotzky, G. Margulis, R. Muchnik, A. Retakh, A. Shalev and E. Zelmanov for helpful conversations. Special thanks to L. Pyber for showing me [Ac,Pa] and explaining some of the results in the paper [M], and to K. Brown for pointing out an error in the previous version of the paper.

The author was supported by the NSF Postdoctoral Research Fellowship in Mathematical Sciences.

References

[Ac] V. Acciaro, *The probability of generating some common families of finite groups*, Utilitas Math. **49** (1996), 243–254.

[AA] V. Acciaro, M.D. Atkinson, *A new algorithm for testing the regularity of a permutation group*, Congressus Numerantium **90** (1992), 151–160.

[AD] D. Aldous, P. Diaconis, *Strong uniform times and finite random walks*, Advances in Applied Math. **8** (1987), 69–97.

[ASE] N. Alon, J.H. Spencer, P. Erdős, *The Probabilistic Method*, Wiley, New York, 1992.

[An] G. Andrews, *The Theory of Partitions*, Addison-Wesley, New York, 1976.

[B1] L. Babai, *The probability of generating the symmetric group*, J. Comb. Th. Ser. A **52** (1989), 148–153.

[B2] L. Babai, *Automorphism groups, isomorphism, reconstruction*, in Handbook of Combinatorics (R. L. Graham, M. Groetschel, and L. Lovasz, eds.) (1996), Elsevier.

[B3] L. Babai, *Randomization in group algorithms: Conceptual questions*, in Groups and Computation II (L. Finkelstein, W.M. Kantor, eds.) DIMACS Workshops on Groups and Computation (1997), AMS, Providence.

[BaP] L. Babai, I. Pak, *in preparation* (1999).

[BCP] W. Bosma, J. Cannon, C. Playoust, *The Magma algebra system* in "Computational algebra and number theory (London, 1993)", J. Symbolic Comput. **24** (1997), 235–265.

[BPS] A.V. Borovik, L. Pyber, A. Shalev, *Maximal subgroups in finite and profinite groups*, Trans. Amer. Math. Soc. **348** (1996), 3745–3761.

[Ca] R. Carter, *Simple Groups of Lie Type*, Wiley, New York, 1972.

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

[CG] F.R.K. Chung, R.L. Graham, *Random walks on generating sets for finite groups*, The Electronic J. of Comb. **4 No 2.** (1997), #R7.

[CCNPW] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker, R.A. Wilson, *Atlas of Finite Simple Groups*, Claredon Press, Oxford, 1985.

[CM] H.S.M. Coxeter, W.O.J. Moser, *Generators and relations for discrete groups* (third edition), Springer, Berlin, 1972.

[D] P. Diaconis, *Group Representations in Probability and Statistics*, IMS, Hayward, California, 1988.

[DS1] P. Diaconis, L. Saloff-Coste, *Walks on generating sets of abelian groups*, Prob. Th. Rel. Fields **105** (1996), 393–421.

[DS2] P. Diaconis, L. Saloff-Coste, *Walks on generating sets of groups*, Invent. Math. **134** (1998), 251–299.

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

[Du] M.J. Dunwoody, *Nielsen Transformations*, in Computational Problems in Abstract Algebra (Proc. Conf., Oxford, 1967) (1970), Pergamon, Oxford, 45–46.

[ER] P. Erdős, A. Rényi, *Probabilistic methods in group theory*, Jour. Analyse Mathématique **14** (1965), 127–138.

[F] W. Feller, *An introduction to Probability theory and its applications, Vol. 1* (third edition), John Wiley, New York, 1968.

[Ga] W. Gaschütz, *Die Eulersche Funktion auflösbarer Gruppen*, Ill. J. Math. **3** (1959), 469–476.

[Go] D. Gorenstein, *Finite Simple Groups*, Plenum,, New York, 1982.

[H1] P. Hall, *The Eulerian functions of a group*, Quart. J. Math. **7** (1936), 134–151.

[H2] M. Hall, *The Theory of Groups*, Chelsea, New York, 1976.

[HW] G.H. Hardy, J.E. Wright, *Basic analytic number theory,* (Fourth Edition), Clarendon Press, Oxford, UK, 1960.

[J] N. Jacobson, *Basic Algebra I.*, Freeman, San Francisco, 1974.

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

[LG] C. Leedham–Green, personal communication.

[LS1] M.W. Liebeck, A. Shalev, *The probability of generating a finite simple group*, Geom. Dedicata **56** (1995), 103–113.

[LS2] M.W. Liebeck, A. Shalev, *Simple groups, probabilistic methods, and a conjecture of Kantor and Lubotzky*, J. Algebra **184** (1996), 31–57.

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

[NP] P. Neumann, C. Praeger, *Cyclic matrices over finite fields*, J. London Math. Soc. (2) **52** (1995), 263–284.

[P1] I. Pak, *Random walks on groups: strong uniform time approach*, Ph.D. Thesis, Harvard U., 1997.

[P2] I. Pak, *When and how n choose k,* in AMS DIMACS Series, vol. 43, 1998, 191–238.

[P3] I. Pak, *Random walks on finite groups with few random generators*, Electr. J. Prob. **4** (1999), 1–11.

[P4] I. Pak, *What do we know about the product replacement random walk?*, in preparation (1999).

[P5] I. Pak, *On the graph of generating sets of a simple group*, preprint (1999).

[PB] I. Pak, S. Bratus, *On sampling generating sets of finite groups and product replacement algorithm* (1999), to appear in Proceedings of ISSAC'99.

[PV] I. Pak, V. H. Vu, *On finite geometric random walks*, preprint (1998).

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

[Py] L. Pyber, *Enumerating finite groups of given order*, Ann. of Math. **137** (1993), 203–220.

[Sc] M. Schönert et al., *GAP – Groups, Algorithms, and Programming*, Lehrstuhl D für Mathematik, RWTH Aachen, Germany, 1995.

[Se] Y. Segev, *On completely reducible solvable subgroups of* $GL(n, \Delta)$, Israel J. Math. **51** (1985), 163–176.

[Sh] A. Shalev, *Probabilistic group theory*, St. Andrews Lectures, Bath, 1997.

[WW] E. T. Whittaker, G. N. Watson, *A Course of Modern Analysis* (Fourth Edition), Cambridge University Press, Cambridge, UK, 1927.

[Wo] T. Wolf, *Solvable and nilpotent subgroups of* $GL(n, q^m)$, Canad. J. Math. **34** (1982), 1097–1111.