ON THE GRAPH OF GENERATING SETS OF A SIMPLE GROUP

Igor Pak

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

July 6, 1999

Abstract. We prove that the *product replacement graph* on generating k-tuples of a simple group contains a large connected component if $k \geq 3$. This is related to the recent conjecture of Diaconis and Graham. As an application, we also prove that the output of the product replacement algorithm (see [CLMNO]) in this case does not have a strong bias.

Introduction

Let G be a finite group, and let $\varkappa(G)$ be the minimal number of generators of G. For every $k \geq \varkappa(G)$ consider a graph $\Gamma(G,k) = (X,E)$ with vertices to be the generating k-tuples:

$$X = \{ \, (g_1, \dots, g_k) \in G^k, \langle g_1, \dots, g_k \rangle = G \, \}$$

and edges correspond to multiplication of one element in a k-tuple by the other:

$$E = \Big\{ \, \big((g_1, \dots, g_i, \dots, g_k), \, (g_1, \dots, g_i \cdot g_j^{\pm 1}, \dots, g_k)\big), \ 1 \leq i, j, \leq k, i \neq j \, \Big\}$$

This graph naturally arises in a study of the product replacement algorithm (see below). Recently Diaconis and Graham proved that $\Gamma(G,k)$ is connected if G is abelian and $k \geq \varkappa(G) + 1$ (see [DG]). They also state the following conjecture: *Graph* $\Gamma(S_n, k)$ *is connected for all* n, $k \geq 3$. We prove a weaker, but more general result, which suffices for applications.

Theorem 1. *Let G be a finite simple group, $k \geq 3$. Then $\Gamma = \Gamma(G,k)$ contains a connected component Γ' such that*

$$\frac{|\Gamma'|}{|\Gamma|} \to 1 \quad \textit{as} \quad |G| \to \infty$$

Moreover, if $\langle g_1, \dots, g_{k-2} \rangle = G$, *then* $(g_1, \dots, g_{k-2}, id, id) \in \Gamma'$.

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

This basically implies that while we don't know if the graph $\Gamma(G,k)$ is connected, for large G it contains a *unique "large" connected component.* Everywhere below by Γ' we denote the largest connected component of Γ. If the graph $\Gamma(G,k)$ is in fact disconnected, then its "small" connected components cannot contain generating k-tuples in which some $k-2$ elements generate group G.

The proof is based on the following remarkable result:

$$(*) \qquad \mathbf{P}(\langle g_1, g_2\rangle = G, g_1, g_2 \in G) \to 1 \text{ as } |G| \to \infty$$

where G is simple. When $G = A_n$ this is a famous result of Dixon (see [Di]). For classical simple groups of Lie type as well as for certain exceptional groups this is due to Kantor and Lubotzky (see [KL]), and the remaining cases were resolved by Liebeck and Shalev (see [LS1,LS2]).

Note that it is natural to ask whether the second part of the theorem can be strengthened. For example, in the spirit of the Diaconis–Graham conjecture, is it true that given $\langle \sigma_1, \sigma_2\rangle = A_n$ we have $(\sigma_1, \sigma_2, id) \in \Gamma'$? In fact this is true, but the proof is based on more difficult results in probabilistic group theory.

Theorem 2. *With the conditions of Theorem 1, if* $\langle g_1, \ldots, g_{k-1}\rangle = G$, *then* $(g_1, \ldots, g_{k-1}, id) \in \Gamma'$.

The proof of this theorem is heavily based on the recent bounds by Guralnick and Kantor (see [GK]). A special case of the alternating group can be handled separately by using sharp bounds of Babai (see [B1]).

Applications : Product replacement algorithm

The *product replacement algorithm* is an important recent advancement in computational group theory. It arose in conversation between Charles Leedham-Green and Leonard Soicher ([LG]) and was studied by Celler et. al. in [CLMNO].

Let G be a finite permutation or matrix group[1] given by a set of generators. The object is to produce (nearly) uniform elements of G. The product replacement algorithm runs a nearest neighbor random walk on a graph $\Gamma(G,k)$ for a while, and then outputs a random component of the generating k-tuple obtained. The algorithm was found to be very efficient (see [CLMNO,LG]), much more efficient than an ordinary random walk.

Suppose now that the graph $\Gamma(G,k)$ is connected. One can ask about the mixing time of the random walk. There are few interesting rigorous results on the subject. We refer to [DS1,DS2,PB] for (usually weak) bounds on convergence of the random walk on $\Gamma(G,k)$. Babai in [B2] found an $O(\log^2|G|)$ bound on the diameter of $\Gamma(G,k)$. All these bounds assume that $k \geq \varkappa(G) + \widetilde{\varkappa}(G)$ where $\widetilde{\varkappa}(G)$ is the maximum size of the minimal generating sets (i.e. a generating set such that no generator can be omitted). For instance, a set of adjacent transpositions in S_n shows that $\widetilde{\varkappa}(G) \geq n-1$, which makes the Diaconis–Graham conjecture of particular interest.

However, even if the graph is connected, the algorithm can still fail. The author recently discovered (see [P2,PB]) that for direct products of large numbers of simple

[1] In general, it can be any *black box* group (see [B2]).

groups the probability distribution of a component in a random generating k-tuple has a strong bias. The result was made even stronger by Babai and the author in [BP] who showed that the bias can be detected by a short straight line program. Thus one should require an extra condition on k.

Now, assume, as occurs often in practice, that our finite group is simple. Let $g_1, \dots, g_r$ be given generators. Let $k = r + 1$ and consider a graph $\Gamma = \Gamma(G, k)$. While Γ is not known to be necessarily connected, by Theorem 1 it contains a "large" connected component Γ'. Further, by Theorem 2 we know that $\Gamma \setminus \Gamma'$ can contain only minimal generating k-tuples. By $(*)$ we immediately obtain

$$|\Gamma'| = |G|^k \cdot (1 - o(1)).$$

Therefore the projection on any component of the generating k-tuple has a probability distribution which is (nearly) uniform (in total variation distance).

To summarize, we obtained the following claim. Let G be a group presented by r generators $g_1, \dots, g_r$, and let $r \le k$. Consider a nearest neighbor random walk on $\Gamma(G, k)$ starting at $(g_1, \dots, g_r, id, \dots, id)$. Denote by Q_t^k the probability probability distribution of the random component of the state of the walk after t steps. Let $Q^k = lim_{t\to\infty} Q_t^k$. The *total variation distance* is defined as

$$\|Q^k - U\| = \frac{1}{2} \sum_{g \in G} \left| Q^k(g) - \frac{1}{|G|} \right|$$

where U is a uniform distribution on G.

Theorem 3. *Let G be a finite simple group, $k \ge r + 1$. Then*

$$\|Q^k - U\| \to 0 \quad \textit{as} \quad |G| \to \infty$$

We refer to review article [P2] for further results on the product replacement algorithm.

Proof of Theorems

Proof of Theorem 1. Let $(g) = (g_1, \dots, g_k)$, $(h) = (h_1, \dots, h_k)$ be two random k-tuples chosen uniformly from G^k (of course, not necessarily generating G). By $\varphi = \varphi(G)$ denote the probability $\mathbf{P}(\langle g_1, g_2 \rangle \ne G)$. Thus with probability $1 - \varphi$ we have $\langle g_1, g_2 \rangle = G$ and we can multiply the remaining elements by g_1, g_2 to obtain any $h_3, \dots, h_k$. This implies that (g) and $(g_1, g_2, h_3, \dots, h_k)$ are in the same connected component. Since g_1 and h_3 are chosen independently, with probability $1-\varphi$ we have $\langle g_1, h_3 \rangle = G$ and $(g_1, g_2, h_3, \dots, h_k)$ is connected to $(g_1, h_2, h_3, \dots, h_k)$. Finally, since h_2 and h_3 are chosen independently, with probability $1 - \varphi$ we have $\langle h_2, h_3 \rangle = G$ and $(g_1, h_2, h_3, \dots, h_k)$ is connected to $(h_1, h_2, h_3, \dots, h_k)$.

Recall that by $(*)$ we have $\varphi = \varphi(G) \to 0$ as $|G| \to \infty$. All three (not independent) events occur with probability $> 1 - 3\varphi(G) \to 1$. Therefore two random vertices in G^k are in $\Gamma(G, k)$ and connected with probability $\to 1$. We conclude that $\Gamma(G, k)$ contains a connected component of size $|G|^k(1 - o(1))$. This completes the proof of the first part.

To prove the second part, observe that if we are given a generating k-tuple $(g) = (g_1, \dots, g_{k-2}, id, id)$ we can always connect it with $(g_1, \dots, g_{k-2}, h_{k-1}, h_k)$. The last two elements generate G with probability $(1 - \varphi(G))$ so we can connect (g) with any of the k-tuples $(h_1, \dots, h_{k-1}, h_k)$ such that $\langle h_{k-1}, h_k \rangle = G$. But the set B of such k-tuples satisfies $|B| = |G|^k(1 - o(1))$ and therefore $B \cap \Gamma' \neq \emptyset$. Thus $B \subset \Gamma'$ and this completes the second part of the proof. □

Remark 1. For $G = A_n$ the result of Babai (see [B1]) gives

$$\varphi(A_n) = \frac{1}{n} + O\left(\frac{1}{n^2}\right).$$

One can deduce from this bound and the proof that for $k \geq 3$ we have

$$|\Gamma'| = |A_n|^k \cdot \left(1 - O\left(\frac{1}{n^{k-2}}\right)\right)$$

Note also that the result of Babai is based on the classification of finite simple groups, while for the proof of Theorem 1 for $G = A_n$ a weak classification free bound of Dixon suffices.

Proof of Theorem 2. We will need the following notation. Let $C \subset G$ be a conjugacy class, $C \neq 1$, and let

$$\psi(C, G) = \min_{g \in G, g \neq id} \mathbf{P}(\langle g, h \rangle = G, h \in C)$$

Observe that $\langle g, h \rangle = G$ is equivalent to $\langle g^a, h^a \rangle = G$ for any $a \in G$. By $C(g)$ denote the conjugacy class of G which contains g. Therefore for all $h \in C$

$$\psi(C, G) = \min_{g \in G, g \neq id} \mathbf{P}\big(\langle g', h \rangle = G, g' \in C(g)\big)$$

Finally, denote by $\psi(G) = \max_{g \in G} \psi(C(g), G)$. By C_0 denote the conjugacy class C on which $\psi(C, G)$ maximizes. It was shown in [GK] that $\psi(G) = \psi(C_0, G) > 1/10$ for *all* simple groups G. Further, the authors prove that

$$\liminf \psi(G) = \frac{1}{2} \quad \text{as} \quad |G| \to \infty$$

Now, let $k = r + 1$, $(g) = (g_1, \dots, g_r, id)$ be a generating k-tuple of the simple group G. Choose a uniform $z \in C_0$. We have that (g) is connected to $(g_1, \dots, g_r, z)$. Without loss of generality assume that $g_1 \neq id$. Now, $\langle g_1, z \rangle = G$ with probability $> \psi(G)$ (by definition) and then $(g_1, \dots, g_r, z)$ is connected to $(g_1, h_2, \dots, h_{k-1}, z)$, for any $h_i \in G$. Consider two cases : $k = 3$ and $k > 3$.

If $k > 3$, with probability $1 - \varphi(G)$ we have $\langle h_2, h_3 \rangle = G$. But then the k-tuple $(g_1, h_2, h_3, \dots, h_{k-1}, z)$ is connected to $(h) = (h_1, h_2, \dots, h_{k-1}, h_k)$. We conclude : with probability $> \psi(G) - \varphi(G)$ we have that (g) is connected to (h) chosen uniformly from G^k. Since $\liminf\big(\psi(G) - \varphi(G)\big) = 1/2$, we have that (g) is connected to the "large" component Γ'.

Assume that $k = 3$. We have that $(g) = (g_1, g_2, id)$ is connected to (g_1, h_2, z), h_2 is uniform in G, z is uniform in C_0, with probability $\psi(G)$. Now fix z. Recall that for any $h_2 \neq id$ we have $\mathbf{P}(\langle h_2, z\rangle = G) = \psi(C(h_2), G) \geq \psi(G)$. Thus with probability $\geq \psi(G)$ the vertex (g_1, h_2, z) is connected to (h_1, h_2, z), h_1 - uniform in G. Finally, with probability $1 - \varphi(G)$ the latter is connected to (h_1, h_2, h_3).

Observe now that the events $\langle g_1, z\rangle = G$ and $\langle h_2, z\rangle = G$ are *independent*. This implies that the probability that $(g) = (g_1, g_2, id)$ is connected to a uniform $(h_1, h_2, h_3) \in G^3$ is at least $\psi^2(G) - \varphi(G)$. Since $\liminf \psi(G) - \varphi(G) = 1/4$, we see that (g) is connected to the "large" component. This completes the proof. □

Proof of Theorem 3. Observe that by Theorem 2 we have that $(g) = (g_1, \dots, g_r, id, \dots, id) \in \Gamma'$. Observe that Γ' is symmetric under action of S_k. Indeed, if $(h) \in \Gamma$ is connected to (g), then $\sigma \cdot (h)$ is connected to $\sigma \cdot (g)$ for any $\sigma \in S_k$. But both (g) and $\sigma \cdot (g)$ lie in Γ' and thus connected. Therefore (h) is connected to $\sigma \cdot (h)$ for any $(h) \in \Gamma'$, $\sigma \in S_k$, and the symmetry follows. From here Q^k is the probability distribution of the first component of uniform elements of Γ'.

Clearly, the probability distribution of the first component of uniform elements in G^k is uniform. We conclude

$$\|Q^k - U\| = \max_{B \subset G} |Q^k(B) - U(B)| \leq \max_{B \subset G} \left| \frac{|\Gamma(G,k) \cap B \times G^{k-1}|}{|G|^k} - \frac{|B \times G^{k-1}|}{G|^k} \right|$$
$$\leq \frac{|\Gamma(G,k)|}{|G|^k} \to 0 \quad \text{as} \quad |G| \to \infty$$

This completes the proof. □

Odds and ends

Let us first note that in this paper we deal only with simple groups. In particular, we prove that the graph $\Gamma(A_n, 3)$ has a "large" connected component, rather than the graph $\Gamma(S_n, 3)$ which appears in the Diaconis–Graham conjecture. A simple modification of the argument in the proof of Theorem 1 allows us to prove the existence of the "large" component in the latter graph as well. We leave the (simple) details to the reader.

Also, the whole proof of Theorem 1 (in contrast with the proof of Theorem 2) is based only only on the property $(*)$. We can generalize this into the following result.

Theorem 4. *Let G_i, $r(i)$ be a sequence of groups such that $\mathbf{P}(\langle g_1, \dots, g_{r(i)}\rangle \neq G_i) \to 0$ as $i \to \infty$. Then a sequence of graphs $\Gamma_i = \Gamma(G, k(i))$, $k(i) \geq r(i) + 1$ contains a "large" connected component $\Gamma'_i \subset \Gamma_i$ such that*

$$\frac{|\Gamma'_i|}{|\Gamma_i|} \to 1 \quad \textit{as} \quad i \to \infty$$

Moreover, if $(g) = (g_1, \dots, g_{k-r(i)}, id, \dots, id) \in \Gamma(G,k)$, then $(g) \in \Gamma'$. □

Let $f(i)$ be any increasing function, $f(i) \to \infty$ as $i \to \infty$. Consider a sequence of nilpotent groups G_i with $r(i) = \varkappa(G_i) + f(i)$. Then one can show that $(G_i, f(i))$

satisfies the conditions of Theorem 3 (see [DS2,P1,PB]). Analogous result holds for a sequence of solvable groups G_i, where $r(i) = f(i) \cdot \varkappa(G_i)$, and for products of simple groups G_i with $r(i) = f(i) \cdot \varkappa(G_i) \cdot \log\log|G_i|$ (see [P1] for details.) An analog of Theorem 3 is straightforward.

While we cannot prove that the graph $\Gamma(G,k)$ is connected for S_n and, perhaps, all simple groups, the case of general groups is of interest as well. Interestingly, we do not know of any finite group G generated by r elements such that $\Gamma(G, r+1)$ is disconnected. We believe that there such groups do exist (cf. [BP]).

It is possible that Theorem 2 might not have a generalization to other families of finite groups. On the other hand, it appears useful from the computational point of view. An unexpected bonus is the efficient computer check[2] of the Diaconis–Graham conjecture for $n \leq 10$. Indeed, instead of checking the connectivity of the triples of permutations in the brute force approach, we can check connectivity of generating triples with the "large" connected component. The revised computation runs the product replacement algorithm and checks if the triple is minimal at every stage. If at some point it's not, by Theorem 2 it is thus connected to the "large" connected component. This idea was recently implemented by Gene Cooperman and the author and will be reported elsewhere[3].

Acknowledgments

We would like to thank L. Babai, A. Borovik, G. Cooperman, P. Diaconis, L. Pyber and A. Shalev for helpful conversations. Special thanks to B. Kantor and C. Leedham–Green, who read and commented on the manuscript.

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

[2] It was reported in [DG] that Lafferty and Rockmore checked the conjecture for $n \leq 5$.

[3] We also use ideas from search in the presence of symmetry to further reduce the time for checking.

References

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

[B2] 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.

[BP] L. Babai, I. Pak, *Small sets of generators can have strong bias : an obstacle to the efficiency of the product replacement algorithm,* preprint (1999).

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

[DG] P. Diaconis, R. Graham, *The graph of generating sets of an abelian group*, Colloq. Math. **80** (1999), 1–38.

[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.

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

[GK] R.M. Guralnick, W.M. Kantor, *Probabilistic generation of finite simple groups*, J. Algebra, to appear.

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

[KM] 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.

[P1] I. Pak, *On the probability of generating a finite group*, in preparation (1999).

[P2] I. Pak, *What do we know about the product replacement random walk?*, in preparation (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.

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