EXPANSION OF PRODUCT REPLACEMENT GRAPHS

Alexander Gamburd

Department of Mathematics
Stanford University, Stanford, CA 94305
E-mail: agamburd@math.stanford.edu

Igor Pak

Department of Mathematics
MIT, Cambridge, MA 02139
E-mail: pak@math.mit.edu

Introduction

Expanders are highly connected sparse graphs of great interest in computer science, in areas ranging from parallel computation to complexity theory, from cryptography to coding theory, and, most recently, computational group theory (see e.g. [AKS,G+,LP,SS,V,WZ].) The explicit constructions of expander graphs [M1, M2, LPS] (see also [GG, Lu]) use deep mathematical tools to construct families of Cayley graphs of finite groups. The Independence Problem [LW], is whether being an expander family is a property of the groups alone, independent of the choice of generators. A counterexample to the general the problem was recently obtained in [ALW], by using a new combinatorial construction of expanders [RVW]. The problem remains for all classical series of finite simple groups (A_n, $\mathrm{PSL}(2,p)$, etc.)

Let G be a finite group generated by at most d elements. The *product replacement graph* $\Gamma_k(G)$ is defined to be a graph, with vertices corresponding to generating k-tuples in G, and edges corresponding to Nielsen transformations. Most recently, graphs $\Gamma_k(G)$ became a subject of an intense investigation, prompted by the study of a commonly used 'practical' product replacement algorithm for generating random elements in finite groups, designed Leedham-Green and Soicher [LG]. This algorithm, based on the random walk on graphs $\Gamma_k(G)$, showed a remarkable performance, as reported in [C+]. It was suggested in [LP], and proved in several special cases, that the product replacement graphs $\Gamma_k(G)$ are expanders, for a fixed k, when $|G| \to \infty$.

The main result of this paper is Theorem 2, establishing the connection between the expansion coefficient of the product replacement graph $\Gamma_k(G)$ and the minimal expansion coefficient of a Cayley graph of group G with k generators. One can think of our result as of an additional evidence in favor of the speculation in [LP]. On the other hand, it gives an algorithmic motivation for study of the Independence Problem, in the aftermath of [ALW].

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

In a special case (see Theorem 1 below), we show that if one assumes that all Cayley graphs with at most four generators in $\mathrm{PSL}(2,p)$ have a universal lower bound on expansion, then the product replacement graphs $\Gamma_k(\mathrm{PSL}(2,p))$ form an expander family, when $k \geq 8$ is fixed, and $p \to \infty$.

The proof of the Theorems consists of two parts: probability on groups and graph theoretic. The latter is based on a new combinatorial result of independent interest (Lemmas 4, 5), which generalizes a classical lemma that the direct product of expanders is an expander (see e.g. [Ch]). We prove that if a graph Γ on a direct product of sets satisfies two conditions:

1) all 'row' subgraphs are expanders,

2) at least $(1-\epsilon)$ proportion of 'column' graphs are expanders,

then graph Γ is also an expander. We use a novel combinatorial technique based on graph decomposition, as opposed to path arguments used in previously in [CG,DS2,DS3,P4]. It is easy to see that such a technique can never prove that a certain family of graphs is an expander family (cf. [P3]).

0. Special case of $\mathrm{PSL}(2,p)$

Let Γ be a k-regular (oriented) graph with an adjacency matrix A. For the rest of the paper we assume that Γ is symmetric, i.e. that $A = A^T$. Consider a nearest neighbor random walk $\mathcal{W} = \mathcal{W}(\Gamma)$, with transition matrix $\mathrm{P} = A/k$. Denote by $1 = \lambda_0 > \lambda_1 \geq \lambda_2 \geq \dots$ the eigenvalues of P, and let $\beta(\Gamma) = 1 - \lambda_1$ be the *eigenvalue gap* of the graph Γ. We say that a sequence of k-regular graphs $\{\Gamma_n\}$ is an *expander family*, if for some $\epsilon > 0$, we have $\beta(\Gamma_n) > \epsilon$, for all $n \geq 1$. Among many properties of expanders are the bounds on the isoperimetric constant (see below), diameter of the graph $\mathrm{diam}(\Gamma_n) \leq C_1 \log|\Gamma_n|$, and the mixing time of the random walk $\mathrm{mix}\,\mathcal{W}(\Gamma_n) \leq C_2 \log|\Gamma_n|$, for some universal constants $C_1, C_2 > 0$.

Let G be a finite group, and let S be a generating set with k elements. We will always assume that S is symmetric : $S = S^{-1}$. Denote by $\mathcal{C} = \mathcal{C}(G,S)$ the corresponding *Cayley graph* on G. Consider a nearest neighbor random walk $\mathcal{W}(G,S) = \mathcal{W}(\mathcal{C})$. Denote by $\beta(G,S) = \beta\bigl(\mathcal{C}\bigr)$ the *eigenvalue gap* of $\mathcal{C}(G,S)$. As in case of general graphs, we say that a family of Cayley graphs $\{\mathcal{C}_n = \mathcal{C}(G_n,S_n)\}$ is an *expander*, if there exist $\varepsilon > 0$, such that $\beta(\mathcal{C}_n) > \varepsilon$ for all n.

For a fixed integer m, we say that a sequence of groups $\{G_n\}$ has *universal expansion* with m generators, if there exist $\epsilon > 0$, such that for every n and every $\langle S\rangle = G_n$, $|S| \leq m$, we have $\beta\bigl(\mathcal{C}(G_n,S_n)\bigr) > 0$. The positive answer to the Independence Problem for $\mathrm{PSL}(2,p)$ is the main assumption in this paper:

Conjecture 1. (A. Lubotzky [L]) *The sequence of groups* $\{\mathrm{PSL}(2,p),\ p-\text{prime}\}$ *has universal expansion with* $m \leq 4$ *generators.*[1]

An affirmative answer to Conjecture 1 is supported by numerical experiments [LR1,LR2] and some recent results [S1,Ga] (see comments in Appendix.)

Let us define the *product replacement graph* $\Gamma_k(G)$ as follows. Let vertices be all generating k-tuples of the group G, and let edges correspond to transformations

[1] In can be shown, in fact, that if conjecture holds, then $\{\mathrm{PSL}(2,p)\}$ has universal expansion for every fixed $m \geq 4$ (cf. Appendix.)

$L^{\pm}_{i,j}$ and $R^{\pm}_{i,j}$:

$$\begin{aligned} R^{\pm}_{i,j} \, &: \, (g_1, \dots, g_i, \dots, g_k) \to (g_1, \dots, g_i \cdot g_j^{\pm 1}, \dots, g_k), \\ L^{\pm}_{i,j} \, &: \, (g_1, \dots, g_i, \dots, g_k) \to (g_1, \dots, g_j^{\pm 1} \cdot g_i, \dots, g_k). \end{aligned}$$

These graphs were introduced in [C+], in connection with computing in finite groups. Note that graphs $\Gamma_k(G)$ are regular, of degree $D = 4\,k\,(k-1)$. Let $\{G_n\}$ be a sequence of finite groups, generated by at most d elements, and let $k \geq d$ be fixed. As before, we say that a sequence $\{\Gamma_k(G_n)\}$ is an *expander family*, if for some $\epsilon > 0$ we have $\beta\bigl(\Gamma_k(G_n)\bigr) > \epsilon$ for all n.

Theorem 1. *Conjecture 1 implies that the sequence of graphs* $\bigl\{\Gamma_k\bigl(\mathrm{PSL}(2,p)\bigr),\ p-\mathrm{prime}\bigr\}$ *forms an expander family , for any fixed* $k \geq 8$. ▶

Theorem 1 is a corollary of a general result we prove for every finite group G. We show that, under certain conditions, the Cheeger constant of $\Gamma_k(G)$ is bounded from below by the minimal Cheeger constant of the Cayley graph $\mathcal{C}(G,S)$, with $|S| \leq k$. This idea is similar in spirit to the paper [DS3], where the eigenvalue gap $\beta(\Gamma_k(G))$ was bounded in terms of maximal diameter of $\mathcal{C}(G,S)$ (cf. [P3]). For $k = \Omega(\log|G|)$, the dependence on diameter was later removed in [P4].

The rest of the paper is structured as follows. In section 1 we state the main results of the paper. Preliminary observations and lemmas are presented in sections 2, and 3. These follow with the proof of main results (section 4) and proof of the lemmas (see Appendix.) We conclude the Appendix with a collection of historical and mathematical remarks, and pointers to the literature.

Throughout the paper, $[n]$ will denote $\{1,2,\dots,n\}$. We use G to denote a finite group, and Γ to denote a connected regular graph.

1. Main results

Let G be a finite group, $d = d(G)$ be the minimal number of generators of G. We say that the set of generators S is *minimal*, if no proper subset of S generates G. By $m(G)$ denote the maximal size of the minimal generating set of G. By $\ell(G)$ denote the length of the maximal subgroup chain of G. Clearly,

$$d(G) \leq m(G) \leq \ell(G) \leq \log_2 |G|.$$

Let $\varphi_k(G)$ denotes the probability that k random group elements generate G. Let $\theta_\epsilon(G)$ be the smallest k such that $\varphi_k(G) > 1-\epsilon$. It was shown in [P1] that $\theta_\epsilon(G) \leq \ell(G) + C\log(1/\epsilon)$, for a universal constant $C > 0$.

Let Γ be an (oriented, loops are allowed) graph. Denote by $\deg(\Gamma)$ the maximal in and out-degree of a vertex in Γ. We say that Γ is k-regular if every vertex has in and out-degree $k = \deg(\Gamma)$. Define *(edge) expansion* $e(\Gamma)$ as follows:

$$e(\Gamma) \, = \, \min\left\{ \frac{\bigl|E_\Gamma(X,\overline{X})\bigr|}{k\,|X|} \ : \ X \subset \Gamma,\ 1 \leq |X| \leq \frac{|\Gamma|}{2} \right\},$$

where $E_\Gamma(X,Y) = \{(x,y) \in \Gamma \, : \, x \in X, Y \in Y\}$ is the set of edges between X and Y, and $k = \deg(\Gamma)$. Note that $1 > e(\Gamma) > 0$. The *Cheeger inequality* (in this context, also known as *conductance* bound of Jerrum and Sinclair [JS]) gives:

$$e(\Gamma) \geq \beta(\Gamma) \geq \frac{e(\Gamma)^2}{8}.$$

Thus, a uniform lower bound on expansion $e(\Gamma_n) > \epsilon > 0$, for a family of k-regular graphs $\{\Gamma_n\}$, is an equivalent definition of expanders [Lu].

Let $\mathcal{C}(G,S)$ be an (oriented) Cayley graph on G, with a generating set S. Denote by $\rho_k(G)$ the smallest expansion of the Cayley graph on G with at most k generators:

$$\rho_k(G) \, = \, \min\bigl\{e\bigl(\mathcal{C}(G,S)\bigr) \ : \ \langle S\rangle = G, \, |S| \leq k\bigr\}.$$

Let $\Gamma_k(G)$ be the *product replacement graph*, defined as in the introduction Let $D = \deg(\Gamma_k(G)) = 4\,k\,(k-1)$.

Theorem 2. *Let G be a finite group. For every $k \geq 2\,m(G)$, there exist $\epsilon = \epsilon(k) > 0$, such that if $k \geq 2\,\theta_\epsilon(G)$, then*

$$e\bigl(\Gamma_k(G)\bigr) \, > \, c\,\rho_k(G),$$

where $c = c(k)$ is a constant, which depends only on k, and not on G. ▶

Note that the result in the theorem holds for every finite group G, not a family of groups. Recall that for any sequence $\{G_n\}$ of simple groups, with $|G_n| \to \infty$, we have $\varphi_2(G) \to 1$, as $n \to \infty$ (see section 2 below). Therefore, for every such sequence $\{G_n\}$, and $\epsilon > 0$, we have $\theta_\epsilon(G_n) \to 2$, as $n \to \infty$. The following corollaries follow from Main Theorem.

Corollary 1. *Let $\{G_n\}$ be a family of finite simple groups, such that $|G_n| \to \infty$, as $n \to \infty$. Suppose also that $m(G_n) \leq m$, and $\rho_m(G_n) \geq \rho > 0$, for all $n \geq 1$. Let $k \geq 2\,m$, $D = 4k(k-1)$. Then a family of D-regular graphs $\bigl\{\Gamma_k(G_n)\bigr\}$ is an expander family.* ▶

Corollary 2. *Let $\{G_n\}$ be a family of finite groups, such that $\ell(G_n) \leq \ell$, for all $n \to \infty$. Suppose also that $\rho_\ell(G_n) \geq \rho > 0$, for all $n \geq 1$. There exists a universal constant $C > 0$, such that for all $k \geq 2\,\ell + C\log\ell$, the family of $4k(k-1)$-regular graphs $\bigl\{\Gamma_k(G_n)\bigr\}$ is an expander family.* ▶

Theorems 1, 2 and the corollaries will be proved in section 4.

Remark 1. The product replacement graphs of simple groups, studied in Corollary 1, seem to complement the set of graphs $\Gamma_k(G)$ that are known to be expanders. Indeed, the only other cases, when $\Gamma_k(G)$ are shown to be expanders, are the abelian groups and nilpotent groups of bounded nilpotency class [LP]. But in these cases the Cayley graphs have large diameter and *cannot* be expanders (see appendix below.) Also, although Corollary 2 is stated in general terms, it can, in fact, be applied to variety of algebraic groups (see Appendix.)

2. Combinatorics and probability on finite groups

Let G be a finite group, and let

$$\varphi_k(G) \,=\, \mathbf{P}(\langle g_1, \dots, g_k\rangle = G) \,=\, \frac{|\Gamma_k(G)|}{|G|^k}$$

be the probability that k independent random elements in G generate the whole group. A major recent result in this direction was completed in a sequence of papers by Dixon [Dx] (see also [B1]), Kantor and Lubotzky [KL], Liebeck and Shalev [LS1,LS2]. Together, these papers prove that $\varphi_2(G_n) \to 1$, for any sequence of finite simple groups $\{G_n\}$, such that $|G_n| \to \infty$. While the overall result is based on classification of finite simple groups, the special cases $\varphi_2\bigl(\mathrm{PSL}(2,p)\bigr) \to 1$ as $p \to \infty$, and $\varphi_2(A_n) \to 1$ as $n \to \infty$, are completely elementary. In our notation, $\vartheta_\epsilon(\mathrm{PSL}(2,p) = \vartheta_\epsilon(A_n) = 2$ for all $\epsilon > 0$, and p, n large enough.

Note, that if $\vartheta_{1/2}(G) < r$ (i.e. $\varphi_r(G) < 1/2$), we easily have $\varphi_k(G_n) < \epsilon$, for $k > C\,r\,\log(1/\epsilon)$, and for some universal constant $C > 0$ (see [P2]). In this case $|\Gamma_k(G)| > (1-\epsilon)|G|^k$. It is also known that if $\ell = \ell(G)$, then for all $k > \ell + C\,\log(1/\epsilon)$ we have $\varphi_k(G_n) < \epsilon$, for some universal constant C [P2].

While the bound $m(G) \le \ell(G)$ is often sharp, there are examples when $m(G)$ is much smaller than $\ell(G)$ (see [W1,W2]). While the recent work [W2] calculates for a number of simple groups, we will use only result $m(\mathrm{PSL}(2,p)) \le 4$. There is little doubt that all our results can be generalized to all series of bounded rank. Note that this condition is crucial, since we trivially have $m(\mathrm{PSL}(n,p)) \ge n-1$.

We will also need the following probabilistic result (see Appendix)

Lemma 1. *Let $1 > \alpha > \epsilon > 0$. Consider a finite group G, and let $X \subset G$, such that $1 \le |X| \le (1-\alpha)|G|$. Then*

$$\mathbf{P}\bigl(|g\,X - X| > \epsilon|X|\bigr) \,>\, 1 \,-\, \frac{1-\alpha}{1-\epsilon},$$

where g is uniform in G. ▶

3. Edge expansion of graphs

In this section we present some known and some new results on edge expansion of graphs. The lemmas are arranged so that the level of generality roughly increases. Since at no point we need sharp bounds, we do not attempt to optimize the constants. Instead, we present simple proofs of (sometimes, known) lemmas so that their generalization can be obtained with no difficulty.

Let $\Gamma = (V,E)$ be a finite (oriented) graph. A graph $\Gamma' = (V',E')$ is called a *subgraph* of Γ, if $V' \subset V$ and $E' \subset E$.

Let Γ be a k-regular graph, and let $e(\Gamma)$ be the (edge) *expansion* of Γ, defined as above. It is often convenient to work with the *Cheeger constant* of G is defined to be $h(\Gamma) = e(\Gamma)\,k$.

Lemma 2. *Let $\Gamma = (V, E)$ be a finite k-regular graph, $\Gamma_1 = (V_1, E_1), \dots,$ $\Gamma_n = (V_n, E_n)$ be the subgraphs of Γ, such that $V = \cup_i V_i$, and $|V_i| > (1-\epsilon)|V|$, for some $0 < \epsilon < \frac{1}{5}$ and all $i \in [n]$. Then*

$$h(\Gamma) \geq \frac{1}{\max\{n, 5\}} \, \min\bigl\{h(\Gamma_i) \, : \, i \in [n]\bigr\}. \quad \blacktriangleright$$

This lemma is probably well known, although we were unable to locate the precise reference. The proof are presented in the Appendix.

Lemma 3. *Let $X \subset [M] \times [N]$, $|X| \leq (M\,N/2)$. Denote $X_{i,*} = X \cap \{i\} \times [N]$, $X_{*,j} = X \cap [M] \times \{j\}$. Then, for some universal constants $\alpha, \delta > 0$, we have:*

$$(\circledast) \quad \begin{aligned} &\bigl|\bigl\{(i,j) \in X \, : \, X_{i,*} < (1-\alpha)\,N\bigr\}\bigr| \; + \; \bigl|\bigl\{(i,j) \in X \, : \, X_{*,j} < (1-\alpha)\,M\bigr\}\bigr| \\ &\quad > \; \delta\,|X|. \end{aligned}$$

Moreover, for all $\epsilon < \delta$ we have:

$$(\circledast\circledast) \quad \begin{aligned} &|\{(i,j) \in X \, : \, X_{i,*} < (1-\alpha)\,N, \; i \leq (1-\epsilon)\,M\}| \\ &\quad + \; |\{(i,j) \in X \, : \, X_{*,j} < (1-\alpha)\,M\}| \; > \; (\delta - \epsilon)\;|X|. \quad \blacktriangleright \end{aligned}$$

Versions of the first part of Lemma 3 seem to be known, with roughly the same elementary proof. Since we need the second part as well, we present the proof of lemma for values $\alpha = 1/10$ and $\delta = 31/90$. While these are probably not optimal, they suffice for our purposes.

For graphs $\Gamma_1 = (V_1, E_1)$ and $\Gamma_2 = (V_2, E_2)$, define the *cartesian product* $\Gamma = \Gamma_1 \times \Gamma_2$ to be the graph $\Gamma = (V, E)$, such that $V = V_1 \times V_2$ and

$$E = \bigl\{\bigl((v_1, v_2), (v_1', v_2')\bigr) \in V^2 : (v_1, v_1') \in E_1, \, v_2 = v_2' \text{ or } (v_2, v_2') \in E_2, \, v_1 = v_1'\bigr\}.$$

Let $k_1 = \deg(\Gamma_1)$ and $k_2 = \deg(\Gamma_2)$. Note that $\deg(\Gamma) = k_1 + k_2$.

Proposition 1. [CT,HT] *Let $\Gamma = \Gamma_1 \times \Gamma_2$ be the product of graphs Γ_1 and Γ_2. Let $h_1 = h(\Gamma_1)$, $h_2 = h(\Gamma_2)$. Then*

$$h(\Gamma) \geq \frac{1}{2} \, \min\bigl\{h_1, \, h_2\bigr\}. \quad \blacktriangleright$$

The proof is elementary, and follows from Lemma 3 (perhaps, with a different constant.) As we need an extension of the proposition, we include a proof with a constant $1/27$ instead of $1/2$. Let us also quote, without a proof, a known generalization of this result:

Proposition 2. [CT,HT] *Let* $\Gamma = \Gamma_1 \times \cdots \times \Gamma_m$ *be the product of graphs* $\Gamma_1, \ldots, \Gamma_m$. *Then*

$$h(\Gamma) \geq \frac{1}{2} \min \bigl\{ h(\Gamma_i) \ : \ i \in [m] \bigr\}. \quad \blacktriangleright$$

We say that $\Gamma' = (V', E')$ is a *restriction* of $\Gamma = (V, E)$, if $V' \subset V$, and $(v_1, v_2) \in E$, $v_1, v_2 \in V'$, implies that $(v_1, v_2) \in E'$.

Let $\Gamma = ([M] \times [N], E)$ be a k-regular graph. Define $\Gamma_{i,*} = \bigl(V_{i,*}, E_{i,*}\bigr)$, $\Gamma_{*,j} = \bigl(V_{*,j}, E_{*,j}\bigr)$, with $V_{i,*} = \{i\} \times [N]$, $V_{*,j} = [M] \times \{j\}$, to be restrictions of Γ.

Lemma 4. *There exist constants* $\alpha, \delta > 0$, *such that for all* $0 \leq \epsilon < \delta$ *the following holds. Let* $\Gamma = ([M] \times [N], E)$, $k = \deg(\Gamma)$. *Consider restrictions* $\Gamma_{i,*}$ *and* $\Gamma_{*,j}$, *defined as above. Define*

$$\begin{aligned} h_1 &= \min \bigl\{ h\bigl(\Gamma_{*,j}\bigr) \ : \ j \in [N] \bigr\}, \\ h_2 &= \min \bigl\{ \, h\bigl(\Gamma_{i,*}\bigr) \ : \ i \in [(1-\epsilon)M] \bigr\}. \end{aligned}$$

Then $h(\Gamma) \geq \alpha \min\{h_1, h_2\}$. $\blacktriangleright$

In section 5 we deduce the lemma from our proof of (a weaker version of) Proposition 1. Below we present a final extension of Lemma 3, tailored to our needs.

Let $\bigl\{\Gamma_i = (E_i, [N]),\, i \in [M]\bigr\}$ be a family of k-regular graphs on $[N]$. We say that $\{\Gamma_i\}$ has *ϵ-uniform expansion* with Cheeger constant $\widehat{h}$, if for all $X \subset [N]$, such that $1 \leq |X| \leq N/2$, we have $E_i(X, \overline{X}) \geq \widehat{h}_2 |X|$, for at least $(1-\epsilon)\, M$ different $i \in [M]$. Of course, if $h(\Gamma_i) \geq \widehat{h}$ for all $i \in [(1-\epsilon)M]$ (cf. Lemma 4), then $\{\Gamma_i\}$ has ϵ-uniform expansion with Cheeger constant $\widehat{h}$.

Lemma 5. *There exist constants* $\alpha, \delta > 0$, *such that for all* $0 \leq \epsilon < \delta$ *the following holds. Let* $\Gamma = ([M] \times [N], E)$, $k = \deg(\Gamma)$. *Consider restrictions* $\Gamma_{i,*}$ *and* $\Gamma_{*,j}$, *defined as above. Define*

$$h_1 = \min \bigl\{ h\bigl(\Gamma_{*,j}\bigr) \ : \ j \in [N] \bigr\},$$

and suppose $\bigl\{\Gamma_{i,*}\bigr\}$, $i \in [M]\bigr\}$ *is a family of k-regular graphs, which has ϵ-uniform expansion with Cheeger constant* $\widehat{h}_2$. *Then* $h(\Gamma) \geq \alpha \min\{h_1, \widehat{h}_2\}$. $\blacktriangleright$

Remark 2. Let us note that in Lemmas 3, 4 and 5, we cannot weaken the condition to have ϵ-error for both types of restrictions. For example, in Lemma 4, we cannot let $j \in [(1-\epsilon)N]$. Similarly, we cannot allow to have ϵ-uniform expansion for a family $\bigl\{\Gamma_{i,*}\bigr\}$ as well. Indeed, in these cases there can be very small sets $X \subset \Gamma$ which lie in the intersection of 'bad' directions.

This is the main reason why we cannot weaken our assumption 1) to a weaker version of it, with *all* Cayley graphs of $\mathrm{PSL}(2,p)$ substituted by *random* Cayley graphs.

4. Proof of the Theorems and Corollaries

Proof of Theorem 2.

Fix $1/2 > \epsilon > 0$, and let $n = \max\{m(G), \theta_\epsilon(G)\}$, $r = k - n$. Since $k \geq 2\theta_\epsilon(G)$ and $k \geq 2\,m(G)$, we obtain $r \geq \max\{\theta_\epsilon(G), m(G)\}$.

Define an action of S_k on $\Gamma_k(G)$ as follows : $\sigma(g_1, \dots, g_k) = (g_{\sigma(1)}, \dots, g_{\sigma(k)})$, for $\sigma \in S_k$. Consider a subgraph Γ' with vertices all generating k-tuples $(g_1, \dots, g_k) \in \Gamma = \Gamma_k(G)$, such that $\langle g_1, \dots, g_n \rangle = G$, and edges corresponding to transformations $R^{\pm}_{i,j}$, $L^{\pm}_{i,j}$, such that $1 \leq j \leq n < i \leq k$, or $1 \leq i \leq n < j \leq k$. Consider also $\sigma\,\Gamma'$, defined as above, for each coset representative $\sigma \in \Sigma(k, n) = S_k/\big(S_n \times S_r\big)$. Clearly, $\sigma\Gamma' \simeq \Gamma'$ for all $\sigma \in S_k$.

We have $|\Gamma'| > (1 - \epsilon)\,|\Gamma|$, since, by definition, $n \geq \theta_\epsilon(G)$. Also, for every $(g) = (g_1, \dots, g_k) \in \Gamma_k(G)$, there exists $\sigma' \in \Sigma(k, n)$, such that $(g) \in \sigma'\Gamma'$ (this follows from $n \geq m(G)$). From Lemma 2, we obtain:

$$h(\Gamma) \geq \frac{1}{\binom{k}{n}} \min\{h(\sigma\Gamma') : \sigma \in \Sigma(k, n)\} = C\,h(\Gamma'),$$

for some constant $C = C(n, k)$.

Now let us prove that $h(\Gamma') > c\rho_n(G)$. Think of Γ' as a graph on $\Gamma_n(G) \times G^r$. For every fixed $(g) = (g_1, \dots, g_n) \in \Gamma_n(G)$, consider $\Gamma'_{(g),*} \subset \Gamma'$, the subgraph of Γ' with vertices $\big((g), (h)\big)$, where $(h) \in G^r$ is any r-tuple of elements. Define $\Gamma'_{*,(h)} \subset \Gamma'$ analogously, for every $(h) \in G^r$. We have $k' = \deg \Gamma'_{*,(h)} = \deg \Gamma'_{(g),*} = 4\,n\,r$.

Define $\overline{\mathcal{C}}(G, S) = \mathcal{C}(G, S) \cup \mathcal{C}^{-1}(G, S)$ to be a union of two isomorphic Cayley graphs corresponding to multiplication on the left and on the right: $\overline{\mathcal{C}} = \big\{(g, g\,s^{\pm 1}), (g, s^{\pm 1}\,g) \,:\, g \in G,\, s \in S\big\}$. Clearly, $h(\overline{\mathcal{C}}) = 2\,h(\mathcal{C})$. Now, by definition, $\Gamma'_{(g),*} = \mathcal{C}\big(G, \{g_1, \dots, g_n\}\big)^r$, and by Proposition 2, we have $h\big(\Gamma'_{(g),*}\big) \geq \frac{1}{2}\,h(\overline{\mathcal{C}}) > k'\,\rho_n(G)$.

We cannot prove that $h\big(\Gamma'_{*,(h)}\big) > \delta > 0$ for two reasons. First, not all elements $(h) \in G^r$ are generating sets (although there are $> (1 - \epsilon)|G|^r$ of them). The graphs $\Gamma_{*,(h)}$ are disconnected when $(h) \notin \Gamma_r(G)$. Thus, we cannot conclude that Cayley graphs on these r-tuples are expanders. Second, graphs $\Gamma'_{*,(h)} = \overline{\mathcal{C}}\big(G, \{h_1, \dots, h_r\}\big)^n$ are not products of (union of) Cayley graphs $\overline{\mathcal{C}}$, but their intersection with $\Gamma_k(G)$. Thus we cannot use Proposition 2 to bound Cheeger constant. In fact, we cannot do this for any fixed $(h) \in G^r$. Instead, we use Lemma 5 to establish ε-uniform expansion of the family $\big\{\Gamma'_{*,(h)}\big\}$ on $\Gamma_n(G)$, for $(h) \in G^r$.

Indeed, consider first $H = G^n$ and any subset $X \subset H$, $1 \leq |X| \leq |H|/2$. Now apply Lemma 1 to the group H (taking $\alpha = 1/2$ and $\epsilon = 1/4$). We obtain that the difference in the lemma is $> |X|/4$, for $> |X|/3$ different $g \in H$. Now observe that for uniform $(h) \in G^r$, the first n components $(h)' = (h_1, \dots, h_n)$ in (h) are uniform in H. Multiplication of (g) by $(h)'$ is a composition of transformations $L_{1,n+1} \circ L_{2,n+2} \circ \dots \circ L_{n,2n}$. By the symmetry, if the composition has expansion $> \alpha$, at least one of the transformations $L_{i,n+i}$ has expansion $> \alpha/n$ (cf. [B2]). Since $|\Gamma_n(G)| > (1 - \epsilon)|H|$, this gives $|g\,X - X| \cap \Gamma_n(G)| > (1/4n - \epsilon)|X| = \delta\,|X|$

for at least $|X|/3$ different $g \in H$. This proves the 1/3-uniform expansion for the family of graphs $\left\{\Gamma'_{*,(h)}\right\}$, with Cheeger constant $> \delta$.

Now take $\epsilon = \min\{1/4 \cdot 1/90, 1/8n\}$, so as to satisfy the lemmas. From Lemma 5 we conclude that $h(\Gamma') > C(n,k)\rho_n(G)$. Now the theorem follows from the observations above. □

Proof of Corollary 1. Since $\varphi_2(G_n) \to 1$, and $d(G_n) = 2$, the second condition $k \geq 2\theta_\epsilon(G_n) = 4$ is trivial. The corollary now follows immediately from Theorem 2. □

Proof of Theorem 1. This is a special case of Corollary 1. Recall that $m(\mathrm{PSL}(2,p)) \leq 4$, and the result follows. □

Proof of Corollary 2. Recall that $m(G) \leq \ell(G)$, and $\varphi_{\ell+t} = 1 - O(1/2^t)$ [P2]. Finally, observe that $\rho_k(G) \geq (k/\ell)\rho_\ell$ (this follows by removing extra edges). In the proof of Theorem 2 we need to find k and ϵ, such that $\varphi(k/2) \geq 1-\epsilon$, and $\epsilon = O(1/k)$. Since $\ell(G_n)$ is bounded, we can solve these two equations by taking $t = O(\log k)$. We omit the easy calculation. □

Acknowledgements

We are grateful to Noga Alon, Persi Diaconis, Alex Lubotzky, Andrew Odlyzko, Prasad Tetali, Jan Saxl, and Avi Widgerson for interesting remarks help with the references. Both authors were MSRI Fellows when the paper was written.

References

[AKS] M. Ajtai, J. Komlos, E. Szemeredi, *Sorting in $c \log n$ parallel steps*, Combinatorica **3** (1983), 1–19.

[ALW] N. Alon, A. Lubotzky, A. Widgerson, *manuscript, 2001.*

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

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

[Ch] F. R. K. Chung, *Spectral Graph Theory*, AMS, Providence, RI, 1994.

[CG] F. R. K. Chung, R. L. Graham, *Random walks on generating sets for finite groups*, Electronic J. of Comb. **4:2** (1997), #R7.

[CT] F. R. K. Chung, P. Tetali, *Isoperimetric inequalities for cartesian products of graphs*, Combin. Probab. Comput. **7** (1998), 141–148.

[DS2] P. Diaconis, L. Saloff-Coste, *Walks on generating sets of abelian groups*, Probability Theory and Related Fields **105** (1996), 393–421.

[DS3] P. Diaconis, L. Saloff-Coste, *Walks on generating sets of groups*, Invent. Math. **134** (1998), 251–199.

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

[GG] O. Gabber, Z. Galil, *Explicit constructions of linear size superconcentrators*, Proc. 20th IEEE FOCS, 1979, 364–370.

[Ga] A. Gamburd, *Spectral gap for infinite index "congruence" subgroups*, Israel Journal of Mathematics, to appear.

[G+] O. Goldreich, R. Impagliazzo, L. A. Levin, R. Venkatesan, D. Zuckerman, *Security Preserving Amplification of Hardness*, Proc. 31^{st} IEEE FOCS, 1990, 318–326.

[HT] C. Houdré, P. Tetali, *Isoperimetric invariants for product Markov chains and graph products,* preprint, Georgia Tech, 1996.

[JS] M. Jerrum, A. Sinclair, *Approximating the permanent*, SIAM J. Comput. **18** (1989), 1149–1178.

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

[LR1] J. Lafferty, D. Rockmore, *Fast Fourier analysis for* SL_2 *over a finite field and related numerical experiments*, Experimental Mathematics **1** (1992), 115-139.

[LR2] J. Lafferty, D. Rockmore, *Numerical investigation of the spectrum for certain families of Cayley graphs*, DIMACS Series in Disc. Math. and Theor. Comp. Sci. **10** (1993), 63-73.

[LG] C. R. 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.

[L] A. Lubotzky, Durham Symposium talk (July, 2001).

[Lu] A. Lubotzky, *Discrete Groups, Expanding Graphs and Invariant Measures*, Birkhauser, Boston, 1994.

[LP] A. Lubotzky, I. Pak, *The product replacement algorithm and Kazhdan's property (T)*, Journal of AMS **52** (2000), 5525–5561.

[LPS] A. Lubotzky, R. Phillips, P. Sarnak, *Ramanujan graphs*, Combinatorica **8** (1988), 261–277.

[LW] A. Lubotzky, B. Weiss, *Groups and expanders,* in Expanding graphs (Princeton, NJ, 1992), 95–109, DIMACS Ser., **10**, AMS, Providence, RI, 1993.

[M1] G. A. Margulis, *Explicit constructions of expanders*, Problems of Information Transmission **9** (1973), 325–332.

[M2] G. A. Margulis, *Explicit group theoretic constructions of combinatorial schemes, and their applications for construction of expanders and concentrators*, Problems of Information Transmission **24** (1988), 39–46.

[P1] I. Pak, *Random walks on finite groups with few random generators*, Electr. J. Prob. **4** (1999), 1–11.

[P2] I. Pak, *The probability of generating a finite group,* preprint (1999).

[P3] I. Pak, *What do we know about the product replacement algorithm?,* in "Groups and Computation III" (W. Kantor, A. Seress, eds.), Berlin, 2000, 301–347.

[P4] I. Pak, *The product replacement algorithm is polynomial*, Proc. 41^{st} IEEE FOCS, 2000.

[RVW] O. Reingold, S. Vadhan, A. Wigderson, *Entropy Waves, The Zig-Zag Graph Product, and New Constant-Degree Expanders and Extractors*, Proc. 41^{st} IEEE FOCS, 2000.

[S1] Y. Shalom, *Expanding graphs and invariant means*, Combinatorica **17** (1997), 555–575.

[SS] M. Sipser, D. A. Spielman,, *Expander Codes*, IEEE Transactions on Information Theory **42(6)** (1996), 1710–1722.

[V] L. Valiant, *Graph theoretic properties in computational complexity*, Jour. Comp. Sys. Sci. **13** (1976), 278–285.

[W1] J. Whiston, *Maximal independent generating sets of the symmetric group*, J. Algebra **232** (2000), 255–268.

[W2] J. Whiston, Ph.D. Thesis, Cambridge University, 2001.

[WZ] A. Wigderson, D. Zuckerman, *Expanders that Beat the Eigenvalue Bound, Explicit Construction and Applications*, Proc. of the 25th STOC, 1993, 245–251.

Appendix

1. Proofs of Lemmas.

Proof of Lemma 1. Note that

$$\mathbf{E}\big(|g\,X \cap X|\big) \,=\, \sum_{x,x' \in X} \mathbf{P}(gx = x') \,=\, |X|^2 \cdot \frac{1}{|G|} \,\le\, (1-\alpha)|X|.$$

Markov inequality gives

$$\mathbf{P}\big(|g\,X - X| \,<\, \epsilon\,|X|\big) \,=\, \mathbf{P}\big(|g\,X \cap X| > (1-\epsilon)|X|\big) \,<\, \frac{1-\alpha}{1-\epsilon}.$$

This implies the result. □

Proof of Lemma 2. Let $X \subset V$, $1 \le |X| \le |V|/2$. Consider subsets $X_i = X \cap V$. Denote $E_i(X,Y) = E_{\Gamma_i}(X,Y)$, for $X, Y \subset V_i$, and let $e_i = e(\Gamma_i)$. Also, let $k_i = \deg(\Gamma_i)$, $k = \deg(\Gamma)$. Fix a constant $\delta = (1-\epsilon)/2 > 0$. Note that $\frac{2}{5} < \delta < \frac{1}{2}$.

There are two possible cases. Either $|X| \le \delta\,|V|$, or $|X| > \delta\,|V|$. We consider them separately. In the first case, $|X_i| < \frac{\delta}{1-\epsilon}\,|V_i| = |V_i|/2$. Therefore $|E_i(X_i, V_i - X_i)| > e_i\,|X_i|\,k_i$. Since $X \subset \cup_i X_i$, there is always $i \in [n]$, such that $|X_i| \ge |X|/n$. Therefore, for this i we have:

$$E_\Gamma(X,\overline{X}) \ge |E_i(X_i, V_i - X_i)| \ge (e_i\,k_i)\frac{|X|}{n}.$$

We conclude:

$$e(\Gamma) \,=\, \min_{X:\,1\le|X|\le|V|/2} \frac{E_\Gamma(X,\overline{X})}{k\,|X|} \,\ge\, \frac{1}{k\,n}\,\min_i\, e_i\,k_i.$$

In the second case, we have :

$$\begin{aligned} |X_i| \,&>\, (\delta-\epsilon)\,|V| \,\ge\, (\delta-\epsilon)\,2\,|X| \,>\, \frac{2}{5}\,|X|, \\ |X_i| \,&\le\, |X| \,\le\, \frac{1}{2}|V| \,<\, \frac{1}{2(1-\epsilon)}\,|V_i| \,<\, \frac{5}{8}\,|V_i|, \end{aligned}$$

and therefore $|V_i - X_i|/|X_i| < \frac{1-5/8}{5/8} = \frac{3}{5}$. For every $i \in [n]$, we have :

$$\begin{aligned} E_\Gamma(X,\overline{X}) \,&\ge\, E_i(X_i, V_i - X_i) \,\ge\, e_i\,k_i\,\min\{|X_i|, |V_i - X_i|\} \\ &>\, \frac{3}{5}\,e_i\,k_i\,|X_i| \,>\, \frac{3}{5}\,e_i\,k_i \cdot \frac{2}{5}\,|X| \,>\, \frac{1}{5}\,e_i\,k_i\,|X|. \end{aligned}$$

We conclude:

$$e(\Gamma) \,=\, \min_{X:\,1\le|X|\le|V|/2} \frac{E_\Gamma(X,\overline{X})}{k\,|X|} \,\ge\, \frac{1}{5\,k}\,\min_i\, e_i\,k_i.$$

This completes the second case and proves Lemma 2. □

Proof of Lemma 3. Let $\alpha = 1/10$ and $\delta = 31/90$. Denote $I = \{i \in [M] : |X_{i,*}| < \frac{9}{10}N\}$, $J = \{j \in [N] : |X_{*,j}| < \frac{9}{10}M\}$. Since $|X| \le MN/2$, we have

$$\frac{9}{10}N \cdot (M - |I|) < |X| \le \frac{M\,N}{2},$$

which gives $|I| > \frac{4}{9}M$. Therefore, for every $j \in J$, we have

$$|X_{*,j} - \overline{I} \times \{j\}| > \frac{9}{10}M - \frac{5}{9}M = \frac{31}{90}M \ge \frac{31}{90}X_{*,j}.$$

Now

$$P = \left|\cup_{i\in I} X_{i,*}\right| + \left|\cup_{j\in J} X_{*,j}\right| = \sum_{j\in J}\left|X_{*,j}\right| + \sum_{j\notin J}\left|X_{*,j} - \overline{I}\times\{j\}\right|$$
$$> (1-\gamma)\,|X| + \sum_{j\notin J}\frac{31}{90}\left|X_{*,j}\right| = (1-\gamma)\,|X| + \frac{31}{90}\gamma\,|X| \ge \frac{31}{90}\,|X|,$$

where P is equal to the l.h.s. of $(\circledast)$ in the lemma, and

$$\gamma = \frac{\sum_{j\notin J}|X_{*,j}|}{|X|} \ge 0.$$

This proves the first part $(\circledast)$.

The second part follows verbatim, except for a substitution of I by $I' = I \cap [(1-\epsilon)M]$, and the constant $31/90$ is replaced by $(31/90 - \epsilon)$, as in $(\circledast\circledast)$. □

Proof of Proposition 1. Recall that we prove only a weaker version of the proposition, with constant $1/27$ instead of $1/2$, as in the claim.

Suppose $\Gamma_1 = ([M], E_1)$, $\Gamma_2 = ([N], E_2)$. Let $\Gamma_{i,*} = \{i\} \times \Gamma_2$, $\Gamma_{*,j} = \Gamma_1 \times \{j\}$, for all $i \in [M]$, $j \in [N]$.

Let $X \subset \Gamma$, $1 \le |X| \le |\Gamma|/2$. As in Lemma 3, let $X_{i,*} = \Gamma_{i,*} \cap X$, $X_{*,j} = \Gamma_{*,j} \cap X$. Consider

$$I = \left\{i \in [M] : \left|X_{i,*}\right| < \frac{9}{10}N\right\}, \quad J = \left\{j \in [N] : \left|X_{*,j}\right| < \frac{9}{10}M\right\}.$$

Also, let

$$E_{i,*} = E_1\big(X_{i,*}, \Gamma_{i,*} - X_{i,*}\big), \quad E_{*,j} = E_2\big(X_{*,j}, \Gamma_{*,j} - X_{*,j}\big).$$

By definition of I and J, for all $i \in I$, $j \in J$ we have:

$$\min\left\{\left|X_{i,*}\right|, \left|\Gamma_{i,*} - X_{i,*}\right|\right\} > \frac{1}{9}\left|X_{i,*}\right|, \quad \min\left\{\left|X_{*,j}\right|, \left|\Gamma_{*,j} - X_{*,j}\right|\right\} > \frac{1}{9}\left|X_{*,j}\right|.$$

By Lemma 3, we have:

$$
\begin{aligned}
\bigl|E(X,\Gamma - X)\bigr| \, &\geq \, \sum_{i\in I} \bigl|E_{i,*}\bigr| + \sum_{j \in J} \bigl|E_{*,j}\bigr| \, \geq \, \sum_{i\in I} e_2\, k_2\, \frac{\bigl|X_{i,*}\bigr|}{9} + \sum_{j\in J} e_1\, k_1\, \frac{\bigl|X_{*,j}\bigr|}{9} \\
&\geq \, \frac{\min\{e_1\, k_1,\, e_2\, k_2\}}{9} \cdot \left(\sum_{i\in I} \bigl|X_{i,*}\bigr| + \sum_{j\in J} \bigl|X_{*,j}\bigr| \right) \\
&\geq \, \frac{1}{9}\, \min\{e_1\, k_1,\, e_2\, k_2\} \cdot \frac{31}{90}\, |X| \, \geq \, \frac{|X|}{27}\, \min\{e_1\, k_1,\, e_2\, k_2\}.
\end{aligned}
$$

We conclude:

$$
e(\Gamma) \, = \, \min_{X:\, 1 \leq |X| \leq MN/2} \, \frac{\bigl|E(X,\Gamma - X)\bigr|}{k\, |X|} \, \geq \, \frac{1}{27\, k}\, \min\{e_1\, k_1,\, e_2\, k_2\}. \; \square
$$

Proof of Lemma 4. Let $\alpha = 1/27$, and $\delta = 1/90$. Use the second part of Lemma 3. Substitute $\epsilon = \frac{1}{90}$ to obtain that the r.h.s. of $(\circledast\circledast)$ is at least $\frac{31-1}{90} = \frac{1}{3}$. Now note that we never used in the proof of Proposition 1 the fact that $\Gamma_{i,*}$ (and, similarly, graphs $\Gamma_{*,j}$) are isomorphic to each other. Now the proof of the lemma follows verbatim the proof of Proposition 1, with the only difference that we use $(\circledast\circledast)$ instead of $(\circledast)$, with $\epsilon = 1/90$, as above. $\square$

Proof of Lemma 5. Follows verbatim the proof of Lemma 4. Indeed, notice again that in the proof of Proposition 1 we never used the fact that i is always in the same subset of size $(1-\epsilon)M$ in $[M]$. Similarly, for every $X \subset [N]$ we never used the full expansion of $\Gamma_{i,*}$, but rather $E_{i,*} = E_i(X, \overline{X})$. The rest of the proof remains unchanged. $\square$

2. Final Remarks.

Let us note here that $\ell(G)$ is bounded for a large number of algebraic groups, which extends the Corollary 3 beyond simple groups. Indeed, for a series of algebraic groups $\{G(p)\}$ of the same rank, over $\mathbb{F}_p$ (such as $\{\mathrm{PSL}(n,p)\}$, when n is fixed), the order $f(p) = \mathrm{ord}(G(p))$ is a polynomial in $p \geq 3$ of a fixed degree $\leq n^2$ [Bo]. Thus, the sieve methods in number theory imply that $f(p)$ has at most a bounded number of prime factors for infinitely many primes p (see [HR], chapter 8,9.) Therefore, $\ell(G_p) < C$ for infinitely many prime p, where $C = C(n)$ is a fixed constant. In particular, for $G(p) = \mathrm{PSL}(2,p)$, we have $f(p) = \mathrm{ord}(G(p)) = \frac{1}{2}p(p-1)(p+1)$. It is believed [O] that there are infinitely many primes q, such that $6q+1$ and $12q+1$ are also primes. Taking $p = 12q+1$, this gives $f(p) = 12p(6p+1)(12p+1)$, so that $\ell(\mathrm{PSL}(2,p)) \leq 6$ for infinitely many primes p. On the other hand, one can deduce from [HR] that $\ell(\mathrm{PSL}(2,p)) \leq 13$ for infinitely many primes p.

Let us now elaborate on the rich history of the problem and known results, related to the following questions 1) and 2) :

1) *Does the sequence of groups* $\{G_n\}$ *have universal expansion with bounded number of generators?*

2) *Does the sequence of graphs* $\{\Gamma_k(G_n)\}$ *form an expander family , for some bounded number of generators* k *?*

It is well known that, in a certain precise sense, "random" k-regular graphs are expanders. Only a much weaker result is known for Cayley graphs, when k is allowed to grow with $|G|$. The best known bound for all finite group is the case when $k = \Omega(\log |G|)$ [AR] (see also [P1]). While this bound cannot be improved for abelian groups, no better result is known for other classes of groups (cf. [B3]).

The first explicit constructions of expanders were found by Margulis [M1], who used Kazhdan's property (T) from representation theory to prove the expansion. The next breakthrough came in papers [LPS,M2], where the authors used harmonic analysis and number theory to obtain the explicit constructions of so called *Ramanujan graphs*, the expanders with the largest possible eigenvalue gap (when k is fixed). Both approaches use Cayley graphs of linear groups, and neither of them is elementary, although an effort to simplify the technique has been made (see [GG,Lu,DaS].) Most recently, combinatorial constructions of expanders has been introduced in [RVW], which led to [ALW]. One can think of our results as providing a new approach to constructing large expanders from smaller ones.

In case of Cayley graphs, only very special generators has been used, although recent improvements increase the variety of such sets (see [Ga,GJS,S1,S2]). These results support an affirmative answer to the Conjecture 1 (the Independence Problem 1) for $\mathrm{PSL}(2,p)$), i.e. that *all* Cayley graphs of $\mathrm{PSL}(2,p)$ form an expander family (see [LW]). Further support is given by numerical evidence [LR1,LR2]. Our results indicate the importance of this problem for computational group theory.

Let us note Independence Problem remains open even for "random" generating sets [B+,Lu], and there seem to be little hope of proving 1) with existing techniques. On the other hand, it was speculated in [LW] that universal expansion property must hold *for all* group sequences, which admit some expanding family of Cayley graphs. If true, this would allow us to prove expansion for a large family of product replacement graphs.

As we mentioned above, the product replacement graphs $\Gamma_k(G)$ in this form were introduced recently in connection with the 'practical' algorithm for generating random elements [C+]. On the other hand, a related family of graphs $\widetilde{\Gamma}_k(G)$ was studied back in the sixties by B.H. Neumann, M. Dunwoody, and others, in connection with the so called T-systems (see [P3] for the references). Many basic questions about these graphs remain unanswered, such as the connectivity of $\Gamma_k(G)$, for general finite groups G. In our running example, it was proved by Gilman that graphs $\Gamma_k(\mathrm{PSL}(2,p))$ are connected, for $k \geq 3$, and $p \geq 5$ [Gi]. In general, it is known that $\Gamma_k(G)$ is connected for all $k > m(G) + d(G)$ [DS3,P3].

Now, a rigorous study of convergence of random walks on the product replacement graphs $\Gamma_k(G)$, for general finite groups G and in special cases, was undertaken in a number of recent papers [B4,CG,DS2,DS3,LP,P3]. In the latest paper [P4], the second author showed that the random walk mixes in time polynomial in k and $\log |G|$, for $k = \Omega^*(\log |G|)$. Still, for small k, the nature of the practical rapid mixing remains unclear. One possible explanation came in [LP], where the authors showed that $\Gamma_k(G)$ are always expanders, provided a known open problem 3) has positive solution:

3) *Does group* $\mathrm{Aut}(F_k)$ *have Kazhdan's property (T) ?*

The problem 3) remains open; an indirect evidence in favor of it is the fact proved in [CV] the it has property (FA) of Serre. It is also known that $\mathrm{Aut}(F_k)$ are hyperbolic and thus nonamenable [G1]. There are also some negative indications: $\mathrm{Aut}(F_2)$ and $\mathrm{Aut}(F_3)$ are shown *not* to have (T) [Mc], and $\mathrm{Aut}(F_k)$ do not have bounded generation [Su], a property closely related to (T) [S3]. Now, since the authors in [C+] test the product replacement algorithm on a number of simple and quasisimple groups, one can think of this work as an alternative explanation of the algorithm performance.

Let us mention here that it was proved (unconditionally) in [LP], that graphs $\Gamma_k(G)$ are expanders, when G is nilpotent of class ℓ, and both k and ℓ are fixed. It is entirely possible that any family of graphs $\bigl\{\Gamma_k(G)\bigr\}$, for a fixed k, is an expander. While a counterexample to this claim would give a negative answer to 3), a proof of this would not, however, imply 3). We refer to an extensive survey article [P3] for references and details.

Let us note that the main theorem is inapplicable to a family of alternating groups $\{A_n\}$, where $n \geq 5$. Not all Cayley graphs of A_n are expanders (see below), and also $m(A_n) = n - 2$ [W1], which contradicts the assumptions in Corollary 1. Let us present here an important closely related open problem [B+,Lu,LW]:

4) *Is there any sequence of Cayley graphs* $\bigl\{\mathcal{C}(S_n, R_n)\bigr\}$*, which is an expander (for some generating sets* $\langle R_n\rangle = S_n$*.)*

Not unlike question 1), question 4) remains difficult if not unapproachable. Only recently, a sequence of bounded generating sets $\langle R_n\rangle = S_n$, with $\operatorname{diam}\mathcal{C}(S_n, R_n) = O(n \log n)$, has been constructed [BKL,Q]. It was widely speculated that the answer to 4) is negative, i.e. that there are no expanders on S_n [LW]. At the moment, not even generating sets with $\operatorname{mix}\mathcal{W} = O(n \log n)$ are known. The sets R_n, as above, come close with $\operatorname{mix}\mathcal{W}(S_n, R_n) = O(n \log^3 n)$ [DS1]. To add to a confusion, let us mention here a conjecture that *all* Cayley graphs on S_n have diameter at most $O(n^2)$ [B3,Di], while for "random" Cayley graphs the diameter is believed to be $O(n \log n)$ [K1]. The best bounds in both cases are $\exp\bigl(O(\sqrt{n})\bigr)$ and $\exp\bigl(O(\log^2 n)\bigr)$, respectively [B+,BH]. It is easy to find a non-expanding family in S_n, i.e. $R_n = \{(1,2); (1,2,\ldots,n)^{\pm 1}\}$, such that $\operatorname{diam}\mathcal{C}(S_n, R_n) = \Omega(n^2)$ (see [Di,DS1,Lu]). Still, for all we know, "random" Cayley graphs on S_n can be expanders [B3,BH].

Let us conclude with an interesting observation in [LP], which connects all questions 1) − 4). First, consider a diagonal action of $\mathrm{Aut}(G)$, defined as follows : $\alpha(g_1, \ldots, g_k) = (\alpha(g_1), \ldots, \alpha(g_k))$, for $\alpha \in \mathrm{Aut}(G)$. Define a graph $\widetilde{\Gamma}_k(G)$ with vertices corresponding to orbits of action of $\mathrm{Aut}(G)$ and edges corresponding to $L^{\pm}_{i,j}$ and $R^{\pm}_{i,j}$ (see [Gi,P3]). Clearly, if $\Gamma_k(G)$ is connected, then $\widetilde{\Gamma}_k(G)$ is also connected [P3].

Now, let F_k be a free group on k generators. One can think of $L^{\pm}_{i,j}$ and $R^{\pm}_{i,j}$ as of (special[2]) Nielsen generators in $\mathrm{Aut}(F_k)$. Let $\mathrm{Aut}^{+}(F_k) = \langle L^{\pm}_{i,j}, R^{\pm}_{i,j}\rangle \subset \mathrm{Aut}(F_k)$.

[2] Transpositions and inversions of elements are the remaining Nielsen generators [MKS]

It is easy to see that $\mathrm{Aut}^+(F_k)$ is a subgroup of index 2 in $\mathrm{Aut}(F_k)$ [LP,P3].

One can think of graphs $\Gamma_k(G)$ and $\widetilde{\Gamma}_k(G)$ as of Schreier graphs of $\mathrm{Aut}^+(F_k)$. It was shown by Gilman [Gi] that $\mathrm{Aut}(F_k)$ acts on $\widetilde{\Gamma}_k(G)$ as A_{N} or S_{N}, where $\mathrm{N} = |\widetilde{\Gamma}_k(G)|$, provided that graph $\Gamma_k(G)$ is connected and G is simple.

Consider the case $G = \mathrm{PSL}(2,p)$. It is known that $\Gamma_k(\mathrm{PSL}(2,p))$ is connected for $k \geq 3$ [Gi]. Now, if the question 1) above has a positive answer, the Corollary 2 implies that $\{\Gamma_k(p) = \Gamma_k(\mathrm{PSL}(2,p))\}$ is an expander, for $k \geq 8$. On the other hand, Gilman's result (see above) shows that a quotient graph $\widetilde{\Gamma}_k(p) = \Gamma_k(p)/\mathrm{GL}(2,p)$ is a Schreier graph of A_{N} or S_{N}, each of them infinitely often. Therefore, if 4) has a negative answer, then $\{\widetilde{\Gamma}_k(p)\}$ cannot be an expander, which contradicts 1). In a different direction, since $\mathrm{Aut}(F_k)$ is mapped onto S_N, the positive answer to question 3) implies that for 4).

Finally, let us show here that if $\left\{\widehat{\Gamma}_k(p) = \Gamma_k(\mathrm{PSL}(2,p)^N)/\mathrm{GL}(2,p)^N\right\}$, where $N = N(k,p) = |\Gamma_k(\mathrm{PSL}(2,p)|/|\mathrm{GL}(2,p)|$, are expanders for some fixed $k \geq 3$, then the positive answer to 4) follows. This is a weaker condition than 3) (see above). Indeed, Gilman's result implies that $\mathrm{Aut}^+(F_k)$ acts transitively on $\widehat{\Gamma}_k(p)$ for infinitely many primes p. But in fact, Hall's result [Ha] (see also [KL]) gives that vertices in $\widehat{\Gamma}_k(p)$ are exactly permutations of all vertices in $\widetilde{\Gamma}_k(p)$. Therefore, $\widehat{\Gamma}_k(p)$ is a *Cayley graph* of S_N. This implies the claim.

References

[AM] N. Alon, V. D. Milman, λ_1, *isoperimetric inequalities for graphs, and superconcentrators*, J. Comb. Theory, Ser. B **38** (1985), 73-88.

[AR] N. Alon, Y. Roichman, *Random Cayley graphs and expanders*, Random Structures and Algorithms **5** (1994), 271–284.

[B2] L. Babai, *Local expansion of vertex-transitive graphs and random generation in finite groups*, in Proc. 23rd ACM STOC, 1991, 164–174.

[B3] L. Babai, *Automorphism groups, isomorphism, reconstruction*, in Handbook of Combinatorics (R. L. Graham, M. Groetschel, and L. Lovasz, eds.), Elsevier, 1996.

[B4] 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, AMS, Providence, 1997.

[BH] L. Babai, G. L. Hetyei, *On the diameter of random Cayley graphs of the symmetric group*, Combin. Probab. Comput. **1** (1992), 201–208.

[B+] L. Babai, G. Hetyei, W. M. Kantor, A. Lubotzky, Á. Seress, *On the diameter of finite groups*, Proc. 31st IEEE FOCS, 1990, 857–865.

[BKL] L. Babai, W. M. Kantor, A. Lubotzky, *Small-diameter Cayley graphs for finite simple groups*, European J. Combin. **10** (1989), 507–522.

[BP] L. Babai, I. Pak, *Strong bias of group generators: an obstacle to the "product replacement algorithm"*, Proc. 11th ACM-SIAM Symposium on Discrete Algorithms, 2000, 627–635.

[Bo] A. Borel, *Linear Algebraic Groups*, (Second edition), Springer, 1991.

[CV] M. Culler, K. Vogtmann, *A group theoretic criterion for property FA*, Proc. Amer. Math. Soc **124** (1996), 677-683.

[DaS] G. Davidoff, P. Sarnak, *An elementary approach to Ramanujan graphs* unpublished monograph.

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

[DS1] P. Diaconis, L. Saloff–Coste, *Comarison techniques for random walk on finite groups*, Annals of Probability **21** (1993), 2131–2156.

[GJS] A. Gamburd, D. Jakobson, P. Sarnak, *Spectra of elements in the group ring of* SU(2), J. European Math. Soc. **1** (1999), 51–85.

[Gi] R. Gilman, *Finite quotients of the automorphism group of a free group*, Canad. J. Math. **29** (1977), 541–551.

[G1] M. Gromov, *Hyperbolic groups*, Math. Sci. Res. Inst. Publ., 8, Springer, New York, 1987.

[G2] M. Gromov, *Spaces and Questions*, GAFA (2000 Special Volume, Part I), 118–161.

[HR] H. Halberstam, H.-E. Richert, *Sieve Methods*, LMS Monographs, Academic Press, London, 1974.

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

[K1] W. M. Kantor, *Some topics in asymptotic group theory,* in Groups, Combinatorics & Geometry (Durham, 1990), Cambridge Univ. Press, Cambridge, 1992, pp. 403–421.

[K2] W. M. Kantor, *Simple groups in computational group theory,* in Proc. ICM Berlin, Vol. II (1998), 77–86.

[MKS] W. Magnus, A. Karrass, D. Solitar, *Combinatorial group theory. Presentations of groups in terms of generators and relations* (Second edition), Dover, New York, 1976.

[Mc] J. McCool, *A faithful polynomial representation of* $\mathrm{Out}\,F_3$, Math. Proc. Cambridge Philos. Soc. **106** (1989), 207–213.

[O] A. Odlyzko, personal communication.

[PB] I. Pak, S. Bratus, *On sampling generating sets of finite groups and the product replacement algorithm*, Proc. 11th ISSAC, 1999, 91–96.

[PZ] I. Pak, A. Zuk, *Two Kazhdan constants and mixing of random walks,* preprint (2001).

[Q] J.-J. Quisquater, unpublished manuscript.

[S2] Y. Shalom, *Expander graphs and amenable quotients,* in: Emerging applications of number theory, 571–581, IMA Vol. Math. Appl., 109, Springer, New York, 1999.

[S3] Y. Shalom, *Bounded generation and Kazhdan's property* (T) **90** (1999), Publ. Math. IHES, 145–168.

[Su] B. Sury, *Bounded generation does not imply finite presentation*, Comm. Algebra **25** (1997), 1673–1683.