Annals of Mathematics, **167** (2008), 625–642

Uniform expansion bounds for Cayley graphs of $\mathrm{SL}_2(\mathbb{F}_p)$

By Jean Bourgain and Alex Gamburd*

Abstract

We prove that Cayley graphs of $\mathrm{SL}_2(\mathbb{F}_p)$ are expanders with respect to the projection of any fixed elements in $\mathrm{SL}(2,\mathbb{Z})$ generating a non-elementary subgroup, and with respect to generators chosen at random in $\mathrm{SL}_2(\mathbb{F}_p)$.

1. Introduction

Expanders are highly-connected sparse graphs widely used in computer science, in areas ranging from parallel computation to complexity theory and cryptography; recently they also have found some remarkable applications in pure mathematics; see [5],[10], [15], [20], [21] and references therein. Given an undirected d-regular graph $\mathcal{G}$ and a subset X of V, the *expansion* of X, $c(X)$, is defined to be the ratio $|\partial(X)|/|X|$, where $\partial(X) = \{y \in \mathcal{G} : \text{distance}(y, X) = 1\}$. The *expansion coefficient* of a graph $\mathcal{G}$ is defined as follows:

$$c(\mathcal{G}) = \inf \left\{ c(X) \mid |X| < \frac{1}{2}|\mathcal{G}| \right\}.$$

A family of d-regular graphs $\mathcal{G}_{n,d}$ forms a family of C-expanders if there is a fixed positive constant C, such that

$$\liminf_{n\to\infty} c(\mathcal{G}_{n,d}) \geq C. \tag{1}$$

The *adjacency matrix* of $\mathcal{G}$, $A(\mathcal{G})$ is the $|\mathcal{G}|$ by $|\mathcal{G}|$ matrix, with rows and columns indexed by vertices of $\mathcal{G}$, such that the x, y entry is 1 if and only if x and y are adjacent and 0 otherwise.

By the discrete analogue of Cheeger-Buser inequality, proved by Alon and Milman, the condition (1) can be rewritten in terms of the second largest eigenvalue of the adjacency matrix $A(\mathcal{G})$ as follows:

$$\limsup_{n\to\infty} \lambda_1(A_{n,d}) < d. \tag{2}$$

*The first author was supported in part by NSF Grant DMS-0627882. The second author was supported in part by NSF Grants DMS-0111298 and DMS-0501245.

Given a finite group G with a symmetric set of generators S, the Cayley graph $\mathcal{G}(G, S)$, is a graph which has elements of G as vertices and which has an edge from x to y if and only if $x = \sigma y$ for some $\sigma \in S$. Let S be a set of elements in $\mathrm{SL}_2(\mathbb{Z})$. If $\langle S\rangle$, the group generated by S, is a finite index subgroup of $\mathrm{SL}_2(\mathbb{Z})$, Selberg's theorem [23] implies (see e.g. [15, Th. 4.3.2]) that $\mathcal{G}(\mathrm{SL}_2(\mathbb{F}_p), S_p)$ (where S_p is a natural projection of S modulo p) form a family of expanders as $p \to \infty$. A basic problem, posed by Lubotzky [15], [16] and Lubotzky and Weiss [17], is whether Cayley graphs of $\mathrm{SL}_2(\mathbb{F}_p)$ are expanders with respect to other generating sets. The challenge is neatly encapsulated in the following 1-2-3 question of Lubotzky [16]. For a prime $p \geq 5$ let us define

$$S_p^1 = \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\},$$

$$S_p^2 = \left\{ \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \right\},$$

$$S_p^3 = \left\{ \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix} \right\},$$

and for $i = 1, 2, 3$ let $\mathcal{G}_p^i = \mathcal{G}\left(\mathrm{SL}_2(\mathbb{F}_p), S_p^i\right)$, a Cayley graph of $\mathrm{SL}_2(\mathbb{F}_p)$ with respect to S_p^i. By Selberg's theorem $\mathcal{G}_p^1$ and $\mathcal{G}_p^2$ are families of expander graphs. However the group $\langle \left(\begin{smallmatrix} 1 & 3 \\ 0 & 1 \end{smallmatrix}\right), \langle \left(\begin{smallmatrix} 1 & 0 \\ 3 & 1 \end{smallmatrix}\right) \rangle$ has infinite index, and thus does not come under the purview of Selberg's theorem.

In [24] Shalom gave an example of infinite-index subgroup in $\mathrm{PSL}_2(\mathbb{Z}[\omega])$ (where ω is a primitive third root of unity) yielding a family of $\mathrm{SL}_2(\mathbb{F}_p)$ expanders. In [7] it is proved that if S is a set of elements in $\mathrm{SL}_2(\mathbb{Z})$ such that Hausdorff dimension of the limit set[1] of $\langle S\rangle$ is greater than $5/6$, then $\mathcal{G}(\mathrm{SL}_2(\mathbb{F}_p), S_p)$ form a family of expanders. Numerical experiments of Lafferty and Rockmore [12], [13], [14] indicated that Cayley graphs of $\mathrm{SL}_2(\mathbb{F}_p)$ are expanders with respect to projection of fixed elements of $\mathrm{SL}_2(\mathbb{Z})$, as well as with respect to random generators.

Our first result resolves the question completely for projections of fixed elements in $\mathrm{SL}_2(\mathbb{Z})$.

THEOREM 1. *Let S be a set of elements in* $\mathrm{SL}_2(\mathbb{Z})$. *Then the* $\mathcal{G}(\mathrm{SL}_2(\mathbb{F}_p), S_p)$ *form a family of expanders if and only if $\langle S\rangle$ is non-elementary*, *i.e. the limit set of $\langle S\rangle$ consists of more than two points* (*equivalently*, *$\langle S\rangle$ does not contain a solvable subgroup of finite index*).

[1]Let S be a finite set of elements in $\mathrm{SL}_2(\mathbb{Z})$ and let $\Lambda = \langle S\rangle$ act on the hyperbolic plane $\mathbb{H}$ by linear fractional transformations. The limit set of Λ is a subset of $\mathbb{R} \cup \infty$, the boundary of $\mathbb{H}$, consisting of points at which one (or every) orbit of Λ accumulates. If Λ is of infinite index in $\mathrm{SL}_2(\mathbb{Z})$ (and is not elementary), then its limit set has fractional Hausdorff dimension [1].

Our second result shows that random Cayley graphs of $\mathrm{SL}_2(\mathbb{F}_p)$ are expanders. (Given a group G, a random $2k$-regular Cayley graph of G is the Cayley graph $\mathcal{G}(G, \Sigma \cup \Sigma^{-1})$, where Σ is a set of k elements from G, selected independently and uniformly at random.)

THEOREM 2. *Fix $k \geq 2$. Let $g_1, \ldots, g_k$ be chosen independently at random in $\mathrm{SL}_2(\mathbb{F}_p)$ and set $S_p^{\mathrm{rand}} = \{g_1, g_1^{-1}, \ldots, g_k, g_k^{-1}\}$. There is a constant $\kappa(k)$ independent of p such that as $p \to \infty$ asymptotically almost surely*

$$\lambda_1(A(\mathcal{G}(\mathrm{SL}_2(\mathbb{F}_p), S_p^{\mathrm{rand}})) \leq \kappa < 2k.$$

Theorem 1 and Theorem 2 are consequences of the following result (recall that the girth of a graph is a length of a shortest cycle):

THEOREM 3. *Fix $k \geq 2$ and suppose that $S_p = \{g_1, g_1^{-1}, \ldots, g_k, g_k^{-1}\}$ is a symmetric generating set for $\mathrm{SL}_2(\mathbb{F}_p)$ such that*

$$\mathrm{girth}(\mathcal{G}(\mathrm{SL}_2(\mathbb{F}_p), S_p)) \geq \tau \log_{2k} p, \tag{3}$$

where τ is a fixed constant independent of p. Then the $\mathcal{G}(\mathrm{SL}_2(\mathbb{F}_p), S_p)$ form a family of expanders.[2]

Indeed, Theorem 3 combined with Proposition 4 (see §4) implies Theorem 1 for S such that $\langle S \rangle$ is a free group. Now for arbitrary S generating a non-elementary subgroup of $\mathrm{SL}(2, \mathbb{Z})$ the result follows since $\langle S \rangle \cap \Gamma(2)$ (where $\Gamma(p) = \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod p\}$) is a free nonabelian group. Theorem 2 is an immediate consequence of Theorem 3 and the fact, proved in [8], that random Cayley graphs of $\mathrm{SL}_2(\mathbb{F}_p)$ have logarithmic girth (Proposition 5).

The proof of Theorem 3 consists of two crucial ingredients. The first one is the fact that nontrivial eigenvalues of $\mathcal{G}(\mathrm{SL}_2(\mathbb{F}_p), S)$ must appear with high multiplicity. This follows (as we explain in more detail in Section 2) from a result going back to Frobenius, asserting that the smallest dimension of a nontrivial irreducible representation of $\mathrm{SL}_2(\mathbb{F}_p)$ is $\frac{p-1}{2}$, which is large compared to the size of the group (which is of order p^3). The second crucial ingredient is an upper bound on the number of short closed cycles, or, equivalently, the number of returns to identity for random walks of length of order $\log |G|$.

The idea of obtaining spectral gap results by exploiting high multiplicity together with the upper bound on the number of short closed geodesics is due to Sarnak and Xue [22]; it was subsequently applied in [5] and [7]. In these works the upper bound was achieved by reduction to an appropriate

[2]In fact, our proof gives more than expansion (and this is important in applications [2]): if λ is an eigenvalue of $A(\mathcal{G}(\mathrm{SL}_2(\mathbb{F}_p), S_p))$, such that $\lambda \neq \pm 2k$, then $|\lambda| \leq \kappa < 2k$ where $\kappa = \kappa(\tau)$ is independent of p.

diophantine problem. The novelty of our approach is to derive the upper bound by utilizing the tools of additive combinatorics. In particular, we make crucial use (see §3) of the noncommutative product set estimates, obtained by Tao [26], [27] (Theorems 4 and 5); and of the result of Helfgott [9], asserting that subsets of $\mathrm{SL}_2(\mathbb{F}_p)$ grow rapidly under multiplication (Theorem 6). Helfgott's paper, which served as a starting point and an inspiration for our work, builds crucially on sum-product estimates in finite fields due to Bourgain, Glibichuk and Konyagin [3] and Bourgain, Katz, and Tao [4]. Our proof also exploits (see §4) the structure of proper subgroups of $\mathrm{SL}_2(\mathbb{F}_p)$ (Proposition 3) and a classical result of Kesten ([11, Prop. 7]), pertaining to random walks on a free group.

Acknowledgement. It is a pleasure to thank Enrico Bombieri, Alex Lubotzky and Peter Sarnak for inspiring discussions and penetrating remarks.

2. Proof of Theorem 3

For a Cayley graph $\mathcal{G}(G,S)$ with $S = \{g_1, g_1^{-1}, \dots, g_k, g_k^{-1}\}$ generating G, the adjacency matrix A can be written as

$$A(\mathcal{G}(G,S)) = \pi_R(g_1) + \pi_R(g_1^{-1}) + \ldots + \pi_R(g_k) + \pi_R(g_k^{-1}), \tag{4}$$

where π_R is a regular representation of G, given by the permutation action of G on itself. Every irreducible representation $\rho \in \hat{G}$ appears in π_R with the multiplicity equal to its dimension

$$\pi_R = \rho_0 \oplus \bigoplus_{\substack{\rho\in\hat{G}\\ \rho\neq\rho_0}} \underbrace{\rho \oplus \cdots \oplus \rho}_{d_\rho}, \tag{5}$$

where ρ_0 denotes the trivial representation, and d_ρ denotes the dimension of the irreducible representation ρ. A result going back to Frobenius [6], asserts that for $G = \mathrm{SL}_2(\mathbb{F}_p)$ (the case we consider from now on) we have

$$d_\rho \geq \frac{p-1}{2} \tag{6}$$

for all *nontrivial* irreducible representations.

We will show in subsection 4.1 (see Proposition 6) that logarithmic girth assumption (3) implies that for p large enough, the set S_p generates all of $\mathrm{SL}_2(\mathbb{F}_p)$. Let $N = |\mathrm{SL}_2(\mathbb{F}_p)|$. The adjacency matrix A is a symmetric matrix having N real eigenvalues which we can list in decreasing order:

$$2k = \lambda_0 > \lambda_1 \geq \ldots \geq \lambda_{N-1} \geq -2k.$$

The eigenvalue $2k$ corresponds to the trivial representation in the decomposition (5); the strict inequality

$$2k = \lambda_0 > \lambda_1$$

is a consequence of our graph being connected (that is, of S_p generating all of $\mathrm{SL}_2(\mathbb{F}_p)$). The smallest eigenvalue λ_{N-1} is equal to $-2k$ if and only if the graph is bipartite, in the latter case it occurs with multiplicity one. Denoting by W_{2m} the number of closed walks from identity to itself of length $2m$, the trace formula takes form

$$\sum_{j=0}^{N-1} \lambda_j^{2m} = N W_{2m}. \tag{7}$$

Denote by μ_S the probability measure on G, supported on the generating set S,

$$\mu_S(x) = \frac{1}{|S|} \sum_{g \in S} \delta_g(x),$$

where

$$\delta_g(x) = \begin{cases} 1 & \text{if } x = g \\ 0 & \text{if } x \neq g; \end{cases}$$

when it is clear which S is meant we will omit the subscript S. Let $\mu^{(l)}$ denote the l-fold convolution of μ:

$$\mu^{(l)} = \underbrace{\mu * \cdots * \mu}_{l},$$

where

$$\mu * \nu(x) = \sum_{g \in G} \mu(xg^{-1})\nu(g). \tag{8}$$

Note that we have

$$\mu_S^{(2l)}(1) = \frac{W_{2l}}{(2k)^{2l}}. \tag{9}$$

For a measure ν on G we let

$$\|\nu\|_2 = \left(\sum_{g \in G} \nu^2(g) \right)^{1/2},$$

and

$$\|\nu\|_\infty = \max_{g \in G} \nu(g).$$

PROPOSITION 1. *Suppose $\mathcal{G}(\mathrm{SL}_2(\mathbb{F}_p), S_p)$ with $|S_p| = 2k$ satisfies logarithmic girth condition* (3); *that is,*

$$\mathrm{girth}(\mathcal{G}(\mathrm{SL}_2(\mathbb{F}_p), S_p)) \geq \tau \log_{2k} p.$$

Then for any $\varepsilon > 0$ there is $C(\varepsilon, \tau)$ such that for $l > C(\varepsilon, \tau) \log_{2k} p$

$$\|\mu_{S_p}^{(l)}\|_2 < p^{-\frac{3}{2} + \varepsilon}. \tag{10}$$

Now observe that since S is a symmetric generating set, we have

$$\mu^{(2l)}(1) = \sum_{g \in G} \mu^{(l)}(g)\mu^{(l)}(g^{-1}) = \sum_{g \in G} (\mu^{(l)}(g))^2 = \|\mu^{(l)}\|_2^2;$$

therefore, keeping in mind (9), we conclude that (10) implies that for

$$l > C(\varepsilon) \log_{2k} p$$

we have

$$W_{2l} < \frac{(2k)^{2l}}{p^{3-2\varepsilon}}. \tag{11}$$

Let λ be the largest eigenvalue of A such that $\lambda < 2k$. Denoting by $m_p(\lambda)$ the multiplicity of λ, we clearly have

$$\sum_{j=0}^{N-1} \lambda_j^{2l} > m_p(\lambda)\lambda^{2l}, \tag{12}$$

since the other terms on the left-hand side of (7) are positive.

Combining (12) with the bound on multiplicity (6), and the bound on the number of closed paths (11), we obtain that for $l > C(\varepsilon) \log p$,

$$\frac{p-1}{2}\lambda^{2l} < |\mathrm{SL}_2(\mathbb{F}_p)| \frac{(2k)^{2l}}{p^{3-2\varepsilon}}. \tag{13}$$

Since $|\mathrm{SL}_2(\mathbb{F}_p)| = p(p^2-1) < p^3$, this implies that

$$\lambda^{2l} \ll \frac{(2k)^{2l}}{p^{1-2\varepsilon}}, \tag{14}$$

and therefore, taking $l = C(\varepsilon, \tau) \log p$, we have

$$\lambda_1 \leq \lambda < (2k)^{1-\frac{(1-2\varepsilon)}{C(\varepsilon)}} < 2k, \tag{15}$$

establishing Theorem 3.

Proposition 1 will be proved in Section 4; a crucial ingredient in the proof is furnished by Proposition 2, established in Section 3.

3. Property of probability measures on $\mathrm{SL}_2(\mathbb{F}_p)$

PROPOSITION 2. *Suppose $\nu \in \mathcal{P}(G)$ is a symmetric probability measure on G; that is,*

$$\nu(g) = \nu(g^{-1}), \tag{16}$$

satisfying the following three properties for fixed positive γ, $0 < \gamma < \frac{3}{4}$:

$$\|\nu\|_\infty < p^{-\gamma}, \tag{17}$$

$$\|\nu\|_2 > p^{-\frac{3}{2}+\gamma}, \tag{18}$$

$$\nu^{(2)}[G_0] < p^{-\gamma} \textit{ for every proper subgroup } G_0 \ . \tag{19}$$

Then for some $\varepsilon = \varepsilon(\gamma) > 0$, *for all sufficiently large* p:

$$\|\nu * \nu\|_2 < p^{-\varepsilon}\|\nu\|_2. \tag{20}$$

Proof of Proposition 2. Assume that (20) fails; that is, suppose that for any $\varepsilon > 0$,

$$\|\nu * \nu\|_2 > p^{-\varepsilon}\|\nu\|_2. \tag{21}$$

We will prove that by choosing ε sufficiently small (depending on γ), property (19) fails for some subgroup. More precisely, we will show that for some $a \in G$ and some proper subgroup G_0 we have that

$$\nu[aG_0] > p^{-\gamma/2}, \tag{22}$$

and this in turn will imply that $\nu^{(2)}(G_0) > p^{-\gamma}$.

Set

$$J = 10\log p \tag{23}$$

and let

$$\tilde{\nu} = \sum_{j=1}^{J} 2^{-j}\chi_{A_j}, \tag{24}$$

where A_j are the level sets of the measure ν: for $1 \le j \le J$,

$$A_j = \{x \,|\, 2^{-j} < \nu(x) \le 2^{-j+1}\}. \tag{25}$$

Setting

$$A_{J+1} = \{x \,|\, 0 < \nu(x) \le 2^{-J}\},$$

we have, for any $x \in G$,

$$\tilde{\nu}(x) \le \nu(x) \le 2\tilde{\nu}(x) + \frac{1}{2^J}\chi_{A_{J+1}}(x);$$

hence, keeping in mind (23) we obtain

$$\tilde{\nu}(x) \le \nu(x) \le 2\tilde{\nu}(x) + \frac{1}{p^{10}}. \tag{26}$$

Note also, that for any j satisfying $1 \le j \le J$, we have

$$|A_j| \le 2^j. \tag{27}$$

By our assumption, (21) holds for arbitrarily small ε; consequently, in light of (26), so does

$$\|\tilde{\nu} * \tilde{\nu}\|_2 > p^{-\varepsilon}\|\tilde{\nu}\|_2. \tag{28}$$

Using the triangle inequality

$$\|f+g\|_2 \le \|f\|_2 + \|g\|_2,$$

we obtain

$$\|\tilde{\nu} * \tilde{\nu}\|_2 = \| \sum_{1 \le j_1, j_2 \le J} 2^{-j_1-j_2} \chi_{A_{j_1}} * \chi_{A_{j_2}} \|_2 \le \sum_{1 \le j_1, j_2 \le J} 2^{-j_1-j_2} \|\chi_{A_{j_1}} * \chi_{A_{j_2}}\|_2.$$

Thus by the pigeonhole principle, for some j_1, j_2, satisfying $J \ge j_1 \ge j_2 \ge 1$, we have

$$J^2 2^{-j_1-j_2} \|\chi_{A_{j_1}} * \chi_{A_{j_2}}\|_2 \ge \|\tilde{\nu} * \tilde{\nu}\|_2. \tag{29}$$

On the other hand,

$$\|\tilde{\nu}\|_2 = \left(\sum_{j=1}^{J} \frac{1}{2^{2j}} |\chi_{A_j}| \right)^{1/2} \ge \left(\frac{1}{2^{2j_1}} |A_{j_1}| + \frac{1}{2^{2j_2}} |A_{j_2}| \right)^{1/2}$$
$$\ge \left(2^{-j_1-j_2} |A_{j_1}|^{1/2} |A_{j_2}|^{1/2} \right)^{1/2};$$

therefore

$$\|\tilde{\nu}\|_2 \ge 2^{-j_1/2} 2^{-j_2/2} |A_{j_1}|^{1/4} |A_{j_2}|^{1/4}. \tag{30}$$

Note that we also have

$$J^2 2^{-j_1-j_2} \|\chi_{A_{j_1}} * \chi_{A_{j_2}}\|_2 \ge p^{-\varepsilon} \max(2^{-j_1} |A_{j_1}|^{\frac{1}{2}}, 2^{-j_2} |A_{j_2}|^{\frac{1}{2}}),$$

and since

$$|A_{j_1}|^{\frac{1}{2}} |A_{j_2}|^{\frac{1}{2}} \min(|A_{j_1}|^{\frac{1}{2}}, |A_{j_2}|^{\frac{1}{2}}) \ge \|\chi_{A_{j_1}} * \chi_{A_{j_2}}\|_2,$$

we obtain

$$\min(2^{-j_1} |A_{j_1}|, 2^{-j_2} |A_{j_2}|) \ge \frac{p^{-\varepsilon}}{J^2}. \tag{31}$$

Now combining (28), (29) and (30) we have

$$J^2 2^{-j_1-j_2} \|\chi_{A_{j_1}} * \chi_{A_{j_2}}\|_2 \ge \|\tilde{\nu} * \tilde{\nu}\|_2 \ge p^{-\varepsilon} 2^{-j_1/2} 2^{-j_2/2} |A_{j_1}|^{1/4} |A_{j_2}|^{1/4},$$

yielding

$$\|\chi_{A_{j_1}} * \chi_{A_{j_2}}\|_2 \ge \frac{p^{-\varepsilon}}{J^2} 2^{j_1/2} 2^{j_2/2} |A_{j_1}|^{1/4} |A_{j_2}|^{1/4};$$

recalling (23) and (27), we obtain

$$\|\chi_{A_{j_1}} * \chi_{A_{j_2}}\|_2 \ge p^{-2\varepsilon} |A_{j_1}|^{3/4} |A_{j_2}|^{3/4}. \tag{32}$$

Let

$$A = A_{j_1} \text{ and } B = A_{j_2}. \tag{33}$$

Given two multiplicative sets A and B in an ambient group G, their *multiplicative energy* is given by

$$E(A,B) = |\{(x_1,x_2,y_1,y_2) \in A^2 \times B^2 | x_1y_1 = x_2y_2\}| = \|\chi_A * \chi_B\|_2^2. \tag{34}$$

Inequality (32) means that for the sets A and B, defined in (33),

$$E(A,B) \geq p^{-4\varepsilon}|A|^{3/2}|B|^{3/2}. \tag{35}$$

We are ready to apply the following noncommutative version of Balog-Szemerédi-Gowers theorem, established by Tao [26]:

THEOREM 4 ([27, Cor. 2.46]). *Let A, B be multiplicative sets in an ambient group G such that $E(A,B) \geq |A|^{3/2}|B|^{3/2}/K$ for some $K > 1$. Then there exists a subset $A' \subset A$ such that $|A'| = \Omega(K^{-O(1)}|A|)$ and $|A' \cdot (A')^{-1}| = O(K^{O(1)}|A|)$ for some absolute C.*

Theorem 4 implies that there exists $A_1 \subset A$ such that

$$|A_1| > p^{-\varepsilon_1}|A|, \tag{36}$$

where

$$\varepsilon_1 = 4C_1\varepsilon \text{ with an absolute constant } C_1, \tag{37}$$

such that

$$|A_1(A_1)^{-1}| < p^{\varepsilon_1}|A_1|, \tag{38}$$

which means that

$$d(A_1, A_1^{-1}) < \varepsilon_1 \log p, \tag{39}$$

where

$$d(A,B) = \log \frac{|A \cdot B^{-1}|}{|A|^{1/2}|B|^{1/2}}$$

is *Ruzsa distance* between two multiplicative sets.

The following result, connecting Ruzsa distance with the notion of an approximate group in a noncommutative setting was established by Tao [26].

THEOREM 5 ([27, Th. 2.43]). *Let A, B be multiplicative sets in a group G, and let $K \geq 1$. Then the following statements are equivalent up to constants, in the sense that if the j-th property holds for some absolute constant C_j, then the k-th property will also hold for some absolute constant C_k depending on C_j:*

(1) *$d(A,B) \leq C_1 \log K$ where $d(A,B) = \log \frac{|A \cdot B^{-1}|}{|A|^{1/2}|B|^{1/2}}$ is Ruzsa distance between two multiplicative sets.*

(2) *There exist a $C_2K^{C_2}$-approximate group H such that $|H| \leq C_2K^{C_2}|A|$, $A \subset X \cdot H$ and $B \subset Y \cdot H$ for some multiplicative sets X, Y of cardinality at most $C_2K^{C_2}$.*

By definition, a *multiplicative K-approximate group* is any multiplicative set H which is symmetric;

$$H = H^{-1} \tag{40}$$

contains the identity, and is such that there exists a set X of cardinality

$$|X| \leq K, \tag{41}$$

such that we have the inclusions

$$H \cdot H \subseteq X \cdot H \subseteq H \cdot X \cdot X; \tag{42}$$

$$H \cdot H \subseteq H \cdot X \subseteq X \cdot X \cdot H. \tag{43}$$

Note, that equations (41), (42), (43) imply

$$|H^3| = |H \cdot H^2| \leq |H^2 \cdot X| < |H \cdot X^2| < K^2|H|. \tag{44}$$

By Theorem 5, (39) implies that there exists a p^{ε_2}- approximative group H, where

$$\varepsilon_2 = C_2\varepsilon_1 \text{ with an absolute constant } C_2, \tag{45}$$

satisfying the following properties:

$$|H| < p^{\varepsilon_2}|A_1| \tag{46}$$

and

$$A_1 \subset XH,\ A_1 \subset HY \text{ with } |X||Y| < p^{\varepsilon_2}. \tag{47}$$

Now since $A_1 \subset \bigcup_{x \in X} xH$ and $|X| < p^{\varepsilon_2}$, there is $x_0 \in X$ such that

$$|A_1 \cap x_0H| > p^{-\varepsilon_2}|A_1|. \tag{48}$$

Since $A_1 \subset A = A_{j_1}$, by definition (25) of A_j, we have

$$\nu(x_0H) > \nu(A_1 \cap x_0H) > \frac{1}{2^{j_1}}|A_1 \cap x_0H| \overset{(48)}{>} \frac{1}{2^{j_1}}p^{-\varepsilon_2}|A_1| \overset{(36)}{>} \frac{1}{2^{j_1}}p^{-\varepsilon_2}p^{-\varepsilon_1}|A_{j_1}|,$$

and consequently, keeping in mind (31), we have

$$\nu(x_0H) > p^{-\varepsilon_3} \tag{49}$$

with

$$\varepsilon_3 = \varepsilon_1 + \varepsilon_2 + 2\varepsilon. \tag{50}$$

Now (46) combined with $A_1 \subset A_{j_1}$ and (27) implies that

$$|H| \leq p^{\varepsilon_2}2^{j_1}. \tag{51}$$

Using Young's inequality

$$\|f * g\|_2 \leq \|f\|_1 \|g\|_2, \tag{52}$$

we have

$$\|\chi_{A_{j_1}} * \chi_{A_{j_2}}\|_2 \leq |A_{j_2}||A_{j_1}|^{1/2};$$

therefore

$$2^{j_2}|A_{j_1}|^{1/2} \geq |A_{j_2}||A_{j_1}|^{1/2} \geq \|\chi_{A_{j_1}} * \chi_{A_{j_2}}\|_2$$

and

$$2^{-j_1}|A_{j_1}|^{1/2} \geq 2^{-j_1-j_2}\|\chi_{A_{j_1}} * \chi_{A_{j_2}}\|_2. \tag{53}$$

Since by (27)

$$2^{-j_1/2} \geq 2^{-j_1}|A_{j_1}|^{1/2}$$

and since by (23), (26), (28), (29),

$$2^{-j_1-j_2}\|\chi_{A_{j_1}} * \chi_{A_{j_2}}\|_2 \geq p^{-2\varepsilon}\|\nu\|_2,$$

equation (53) implies that

$$2^{-j_1/2} \geq p^{-2\varepsilon}\|\nu\|_2,$$

which combined with (18) yields

$$2^{j_1} \leq p^{4\varepsilon}\|\nu\|_2^{-2} \leq p^{3-2\gamma+4\varepsilon}. \tag{54}$$

Therefore, recalling (51), we have

$$|H| \leq p^{\varepsilon_2}2^{j_1} \leq p^{3-2\gamma+4\varepsilon+\varepsilon_2}. \tag{55}$$

On the other hand, combining equation (49) with (17) we have

$$|H| > p^{\gamma-\varepsilon_3}. \tag{56}$$

Since H is a p^{ε_2}-approximate group, it follows from (44) that

$$|H \cdot H \cdot H| < p^{2\varepsilon_2}|H|, \tag{57}$$

and, therefore, using (56), we have

$$|H \cdot H \cdot H| < |H|^{1+\frac{2\varepsilon_2}{\gamma-\varepsilon_3}}. \tag{58}$$

Recalling (55), we now apply to H the following product theorem in $\mathrm{SL}_2(\mathbb{F}_p)$, due to Helfgott [9].

THEOREM 6 ([9]). *Let H be a subset of $\mathrm{SL}_2(\mathbb{F}_p)$. Assume that $|H| < p^{3-\delta}$ for $\delta > 0$ and H is not contained in any proper subgroup of $\mathrm{SL}_2(\mathbb{F}_p)$. Then*

$$|H \cdot H \cdot H| > c|H|^{1+\kappa},$$

where $c > 0$ and $\kappa > 0$ depends only on δ.

It follows, that by choosing ε sufficiently small (depending on γ) we can conclude that H is contained in some proper subgroup G_0 of $\mathrm{SL}_2(\mathbb{F}_p)$; consequently (by (49), with $a = x_0$ and $\varepsilon_3 < \gamma/2$), it follows that (22) is satisfied. We have thus obtained a desired contradiction and completed the proof of Proposition 2.

4. Proof of Proposition 1

4.1. *Preliminary results on* $\mathrm{SL}_2(\mathbb{F}_p)$.

4.1.1. *Structure of subgroups.* We recall the classification of subgroups of $\mathrm{SL}_2(\mathbb{F}_p)$ [25].

THEOREM 7 (Dickson). *Let p be a prime with $p \geq 5$. Then any subgroup of $\mathrm{SL}_2(\mathbb{F}_p)$ is isomorphic to one of the following subgroups*:

(1) *The dihedral groups of order $2(\frac{p\pm 1}{2})$ and their subgroups.*

(2) *A Borel group of order $p(\frac{p-1}{2})$ and its subgroups.*

(3) *A_4, S_4, or A_5.*

The following proposition easily follows:

PROPOSITION 3. *If G_0 is a proper subgroup of G and $|G_0| > 60$ then G_0 has trivial second commutators*; *that is*, *for all g_1, g_2, g_3, g_4 in G_0*,

$$[[g_1, g_2], [g_3, g_4]] = 1. \tag{59}$$

4.1.2. *Girth.* Proposition 4 is proved in [7, §2], following closely the method of Margulis [19].

PROPOSITION 4. *Let S be a symmetric set of elements in $\mathrm{SL}_2(\mathbb{Z})$ such that $\langle S \rangle$ is a free group. For a matrix L define its norm by*

$$\|L\| = \sup_{x \neq 0} \frac{\|Lx\|}{\|x\|},$$

where the norm of $x = (x_1, x_2)$ is the standard Euclidean norm $\|x\| = \sqrt{x_1^2 + x_2^2}$; let

$$\alpha(S) = \max_{L \in S} \|L\|.$$

The girth of Cayley graphs $\mathcal{G}_p = \mathcal{G}(\mathrm{SL}_2(\mathbb{F}_p), S_p)$ is greater than $2 \log_\alpha(p/2)$.

Proposition 5 is proved in [8].

Proposition 5 ([8]). *Let d be a fixed integer greater than 2. As $p \to \infty$, asymptotically almost surely the girth of the d-regular random Cayley graph of $G = \mathrm{SL}_2(\mathbb{F}_p)$ is at least*

$$(1/3 - o(1)) \cdot \log_{d-1} |G|.$$

Logarithmic girth implies connectivity for sufficiently large p:

Proposition 6. *Fix $d \geq 2$ and suppose S_p, $|S_p| = d$ is a set of elements in $\mathrm{SL}_2(\mathbb{F}_p)$ such that*

$$\mathrm{girth}(\mathcal{G}(\mathrm{SL}_2(\mathbb{F}_p), S_p)) \geq \tau \log_d p.$$

Then for $p > d^{17/\tau}$ the graphs $\mathcal{G}(\mathrm{SL}_2(\mathbb{F}_p), S_p)$ are connected.

Proof. Let G_p be a subgroup of $\mathrm{SL}_2(\mathbb{F}_p)$ generated by S_p. We want to show that $G_p = \mathrm{SL}_2(\mathbb{F}_p)$ for p large enough. Suppose not. Then G_p is a certain proper subgroup listed in Theorem 7. The subgroups of order less than 60 can be eliminated as possibilities for G_p since they contain elements of small order which clearly violate the girth bound. For the remaining subgroups, we have by Proposition 3, that for all $x_1, x_2, y_1, y_2 \in G_p$ the following relation holds:

$$(x_1 y_1 x_1^{-1} y_1^{-1})(x_2 y_2 x_2^{-1} y_2^{-1})(y_1 x_1 y_1^{-1} x_1^{-1})(y_2 x_2 y_2^{-1} x_2^{-1}) = 1.$$

If we take x_1, y_1, x_2, y_2 to be any generators in S_p, then we see that this condition provides a closed cycle of length 16. However, such a cycle also violates the girth bound, whenever $\tau \log_d p \geq 17$.

4.2. *Preliminary results on F_k.* Let F_k denote the free group on k generators $\{\tilde{g}_1, \ldots, \tilde{g}_k\}$. Denote by $\tilde{\mu}$ the probability measure on F_k supported on $\tilde{g}_i$'s and their inverses,

$$\tilde{\mu} = \frac{1}{2k} \sum_{i=1}^{k} (\delta_{\tilde{g}_i} + \delta_{\tilde{g}_i^{-1}}). \tag{60}$$

Denote by $\tilde{p}^{(l)}(x, y)$ the probability of being at y after starting at x and performing a random walk according to $\tilde{\mu}$ for l steps. We will make use of the following classical result of Kesten.

Proposition 7 (Kesten [11]). *Notation being as above,*

$$\limsup_{l \to \infty} \tilde{p}^{(l)}(x, x)^{1/l} = \frac{\sqrt{2k-1}}{k}. \tag{61}$$

In particular, this implies (see, e.g. [28, Lemma (1.9)]) that

$$\tilde{p}^{(l)}(x, y) \leq \tilde{p}^{(l)}(x, x) \leq \left(\frac{\sqrt{2k-1}}{k} \right)^l. \tag{62}$$

We will also need the following elementary results pertaining to the free group.

LEMMA 1 ([18, Ex. 2, p. 41]). *If u and v are elements in a free group and $u^k = v^k$, then $u = v$.*

LEMMA 2 ([18, Ex. 6, p. 42]). *Two elements of a free group commute if and only if they are powers of the same element.*

4.3. *Proof of Proposition* 1. We now apply Proposition 2 to $\nu = \mu_{S_p}^{(l)}$ with $l \sim \log p$, for a symmetric set of generators S_p, $|S_p| = 2k$, such that the associated Cayley graphs, $\mathcal{G}_p = \mathcal{G}(\mathrm{SL}_2(\mathbb{F}_p), S_p)$ satisfy the large girth condition,

$$\mathrm{girth}(\mathcal{G}(\mathrm{SL}_2(\mathbb{F}_p), S_p)) > \tau \log_{2k} p. \tag{63}$$

The assumption (63) implies that for walks of length up to l_0 given by

$$l_0 = \lfloor \frac{1}{2}\tau \log_{2k} p \rfloor - 1, \tag{64}$$

the part of $\mathcal{G}_p$ visited by the random walk performed according to μ_{S_p} is isomorphic to a part of a $2k$-regular tree (which is Cayley graph of a free group F_k) visited by the random walk associated with the measure $\tilde{\mu}$, defined in Section 4.2. In particular, denoting by support(ν) the set of those elements x for which $\nu(x) > 0$, we have

$$|\mathrm{support}(\mu^{(l_0)})| = |\mathrm{support}(\tilde{\mu}^{(l_0)})| > (2k-1)^{l_0},$$

where the latter inequality follows from the elementary fact that the number of points on a $2k$-regular tree whose distance to a given vertex is at most l_0 is equal to

$$\frac{(2k-1)^{l_0} k - 1}{k-1}.$$

Consequently,

$$|\mathrm{support}(\mu^{(l_0)})| > (2k-1)^{\tau/2 \log_{2k} p} = p^{\gamma_1}$$

with

$$\gamma_1 = \frac{\tau}{2} \log_{2k}(2k-1), \tag{65}$$

and, therefore, since

$$\|\mu^{(l_0)}\|_\infty |\mathrm{support}(\mu^{(l_0)})| \leq 1,$$

we obtain that $\mu^{(l_0)}$ satisfies condition (17) with $\gamma = \gamma_1$, as given in (65). Further, using Young's inequality

$$\|f * g\|_\infty \leq \|f\|_\infty \|g\|_1,$$

we conclude that (17) will also hold for $\mu^{(l)}$ with $l \geq l_0$.

We now show that for $l \geq l_0$ the measure $\nu = \mu^{(2l)}$ satisfies (19) with

$$\gamma < \frac{3\tau}{16}. \tag{66}$$

Assume that ν violates (19); more precisely, assume that it satisfies (22) for some proper subgroup G_0. We first show that under this assumption $\mu^{(2l_0)}$ will also violate (19); more precisely, we will show that there is $b \in G$ such that

$$\mu^{(l_0)}(bG_0) > p^{-\gamma/2}, \tag{67}$$

which would imply that

$$\mu^{(2l_0)}(G_0) > p^{-\gamma}. \tag{68}$$

To prove (67), observe that

$$p^{-\gamma/2} < \mu^{(l)}(aG_0) = \sum_{y \in G} \mu^{(l-l_0)}(y)\mu^{(l_0)}(yaG_0) \leq \max_b \mu^{(l_0)}(bG_0).$$

It remains to rule out (68).

Denote by $W_S(L)$ the set of words of length L in generators S, and let

$$\Sigma(S, l_0) = \{g \in G_0 \cap W_S(2l_0)\}. \tag{69}$$

Keeping in mind (63) and (64), and applying Kesten's result (62) we have that

$$|\Sigma(S,l_0)| \geq \frac{\mu^{(2l_0)}(G_0)}{\|\mu^{(2l_0)}\|_\infty} > \frac{p^{-\gamma}}{\|\tilde{\mu}^{(2l_0)}\|_\infty} > p^{-\gamma}\left(\sqrt{\frac{2k-1}{k^2}}\right)^{-2l_0} > \left(\frac{k^2}{2k-1}\right)^{\frac{l_0}{4}}, \tag{70}$$

where in the last inequality we used (66).

Now the following proposition, combined with Proposition 3 and the logarithmic girth property, will imply a contradiction to (70), and consequently a contradiction with the assumption given in (22), completing the proof of Proposition 1.

Proposition 8. *Denote by $\tilde{W}_k(L)$ the set of words in a free group F_k of length L. Let $\tilde{\Sigma}(k, l_0)$ be a subset of elements of F_k lying in $\tilde{W}_k(2l_0)$ and satisfying the following property*: $\forall\, g_1, g_2, g_3, g_4 \in \tilde{\Sigma}$

$$[[g_1, g_2], [g_3, g_4]] = 1.$$

Then

$$|\tilde{\Sigma}(k, l_0)| < l_0^6. \tag{71}$$

Proposition 8, in turn, follows from the following lemma.

LEMMA 3. *Let* $T = \{[g_1, g_2] \mid g_1, g_2 \in \tilde{\Sigma}\}$ *and assume that*

$$|\tilde{\Sigma}(k, l_0)| > l_0^6.$$

Then

$$|T| > l_0^3. \tag{72}$$

To show that Lemma 3 implies Proposition 8, we note that since $[x_1, x_2] = 1$ for all $x_1, x_2 \in T$, by Lemma 2, T is contained in a cyclic group; further, since it lies in $\tilde{W}_k(8l_0)$, we have that $|T| = O(l_0)$, establishing a contradiction with the conclusion of Lemma 3 and thus proving Proposition 8.

Proof of Lemma 3. Assume that (72) is not satisfied. Then there is $a \in T$ such that

$$|\{g_1, g_2\} \in \tilde{\Sigma} \mid [g_1, g_2] = a| > |\tilde{\Sigma}|^2 l_0^{-3}. \tag{73}$$

Consequently, there is $b \in \tilde{\Sigma}$, $b \neq 1$, such that

$$|\{g \in \tilde{\Sigma} \mid [b, g] = a\}| > |\tilde{\Sigma}| l_0^{-3} > l_0^3. \tag{74}$$

Let $\tilde{\Sigma}_1 = \{g \in \tilde{\Sigma} \mid [b, g] = a\}$.

Taking g and h in $\tilde{\Sigma}_1$, we have

$$gb^{-1}g^{-1} = b^{-1}a,$$

and

$$hb^{-1}h^{-1} = b^{-1}a.$$

Consequently,

$$gb^{-1}g^{-1}hbh^{-1} = 1,$$

and, therefore

$$bh^{-1}g = h^{-1}gb,$$

implying that b and $h^{-1}g$ commute.

By Lemma 2, there are $x \in F_k$ and positive integers m, n such that $x^m = b$ and $x^n = h^{-1}g$; hence

$$b^n = (h^{-1}g)^m. \tag{75}$$

Observe that since $x^m \in \tilde{W}_k(2l_0)$, we have $m < 2l_0$ and, similarly, $n < 2l_0$. Therefore we have at most $4l_0^2$ possibilities for m, n.

We also note that in light of Lemma 1, equation (75) determines $h^{-1}g$ uniquely in terms of b.

We therefore have

$$|\tilde{\Sigma_1}|^2 < 4l_0^2 |\tilde{\Sigma_1}|;$$

hence

$$|\tilde{\Sigma_1}| < 4l_0^2,$$

and we have obtained a contradiction, completing the proof of Lemma 3 and Proposition 1.

Institute for Advanced Study, Princeton, NJ
E-mail address: bourgain@math.ias.edu

University of California at Santa Cruz, Santa Cruz, CA
E-mail address: agamburd@ucsc.edu

References

[1] A. F. Beardon, *The Geometry of Discrete Groups*, Springer-Verlag, New York, 1983.

[2] J. Bourgain, A. Gamburd, and P. Sarnak, Sieving and expanders, *Comptes Rendus Acad. Sci. Paris*, *Ser*. I **343** (2006), 155–159.

[3] J. Bourgain, A. Glibichuk, and S. Konyagin, Estimate for the number of sums and products and for exponential sums in fields of prime order, *J. London Math. Soc.* **73** (2006), 380–398.

[4] J. Bourgain, N. Katz, and T. Tao, A sum-product estimate in finite fields and applications, *GAFA* **14** (2004), 27–57.

[5] G. Davidoff, P. Sarnak, and A. Valette, *Elementary Number Theory*, *Group Theory*, *and Ramanujan Graphs*, Cambridge Univ. Press, Cambridge, 2003.

[6] G. Frobenius, Über Gruppencharaktere, Sitzungsberichte der Königlich Preußischen Akademie der Wissenschaften zu Berlin, 1896, 985–1021.

[7] A. Gamburd, Spectral gap for infinite index "congruence" subgroups of $\mathrm{SL}_2(\mathbb{Z})$, *Israel J. Math*. **127** (2002), 157–200.

[8] A. Gamburd, S. Hoory, M. Shahshahani, A. Shalev, and B. Virág, On the girth of random Cayley graphs, *Random Structures and Algorithms*, to appear.

[9] H. Helfgott, Growth and generation in $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, *Ann. of Math*. **167** (2008), 000–000.

[10] S. Hoory, N. Linial, and A. Wigderson, Expander graphs and their application, *Bull. Amer. Math. Soc*. **43** (2006), 439–561.

[11] H. Kesten, Symmetric random walks on groups, *Trans. Amer. Math. Soc*. **92** (1959), 336–354.

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

[13] ———, Numerical investigation of the spectrum for certain families of Cayley graphs, in *DIMACS Series in Disc. Math. and Theor. Comp. Sci.* Vol. 10 (J. Friedman, ed.) (1993), 63–73.

[14] ———, Level spacings for Cayley graphs, in *IMA Vol. Math. Appl*. **109** (1999), 373–387.

[15] A. Lubotzky, *Discrete Groups Expanding Graphs and Invariant Measures*, *Progress in Math*. **195**, Birkhäuser, Basel, 1994.

[16] ———, Cayley graphs: eigenvalues, expanders and random walks, in *Surveys in Combinatorics* (P. Rowbinson ed.), *London Math. Soc. Lecture Note Ser*. **18**, 155–189, Cambridge Univ. Press, Cambridge, 1995.

[17] A. Lubotzky and B. Weiss, Groups and expanders, in *DIMACS Series in Disc. Math. and Theor. Comp. Sci*. Vol. 10 (J. Friedman, ed.) (1993), 95–109.

[18] W. Magnus, A. Karrass, and D. Solitar, *Combinatorial Group Theory*, Interscience Publishers, New York, 1966.

[19] G. A. Margulis, Explicit construction of graphs without short cycles and low density codes, *Combinatorica* **2** (1982), 71–78.

[20] O. Reingold, S. Vadhan, and A. Wigderson, Entropy waves, the zig-zag graph product, and new constant-degree expanders, *Ann. of Math.* **155** (2002), 157–187.

[21] P. Sarnak, What is an expander?, *Notices of the Amer. Math. Soc.* **51** (2004), 762–763.

[22] P. Sarnak and X. Xue, Bounds for multiplicities of automorphic representations, *Duke Math. J.* **64** (1991), 207–227.

[23] A. Selberg, On the estimation of Fourier coefficients of modular forms, *Proc. Sympos. Pure Math.* **VII** (1965), 1–15.

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

[25] M. Suzuki, *Group Theory I*, Springer-Verlag, New York, 1982.

[26] T. Tao, Product sets estimates for non-commutative groups, preprint, 2005.

[27] T. Tao and V. Vu, *Additive Combinatorics*, Cambridge Univ. Press, Cambridge, 2006.

[28] W. Woess, *Random Walks on Infinite Graphs and Groups*, Cambridge Univ. Press, Cambridge, 2000.

(Received November 3, 2005)