STRONG UNIFORM EXPANSION IN $\mathrm{SL}(2,p)$

EMMANUEL BREUILLARD AND ALEX GAMBURD

Abstract. We show that there is an infinite set of primes $\mathcal{P}$ of density one, such that the family of *all* Cayley graphs of $\mathrm{SL}(2,p)$, $p \in \mathcal{P}$, is a family of expanders.

1. Introduction and statement of results

Expanders are highly-connected sparse graphs widely used in Computer Science; they also have found some remarkable applications in pure mathematics [10, 25]. 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 graphs $\mathcal{G}_n$ forms a family of c-expanders if there is $c > 0$, such that

$$\inf_{n\in\mathbb{N}} c(\mathcal{G}_n) \geq c. \tag{1}$$

Usually one takes the family of graphs to be d-regular, in which case the condition (1) has an alternative spectral interpretation. 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. Using the discrete analogue of Cheeger-Buser inequality, proved by Alon and Milman, condition (1) can be rewritten in terms of the second largest eigenvalue of the adjacency matrix $A(\mathcal{G})$ as follows:

$$\sup_{n\in\mathbb{N}} \lambda_1(A_{n,d}) < d. \tag{2}$$

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 $\sigma \in S$. The explicit constructions of expander graphs (by Margulis [20, 21] and Lubotzky, Phillips and Sarnak [17]) used deep tools (Kazhdan's property (T), Selberg's Theorem, proved Ramanujan conjectures) to construct families of Cayley graphs of finite groups as follows. Starting with an infinite group Γ (e.g. $\mathrm{SL}_2(\mathbb{Z})$) and a finite set of generators S, $\langle S\rangle = \Gamma$, one considers a family of Cayley graphs $\mathcal{G}_i = \mathcal{G}(G_i, S_i)$, where G_i is an infinite family of finite quotients (e.g. $\mathrm{SL}_2(\mathbb{F}_p)$)) and S_i is an image of S under the natural projection. On the other hand, as shown in [19], some families of groups, for example abelian groups or solvable groups of bounded derived length, cannot be made into families of expanders with respect to *any* choice of generators. A basic problem formulated by Lubotzky and Weiss in 1993 [19], (see also [15, 16]) is to what extent the expansion property is the property of the family of groups $\{G_i\}$ alone, independent of the choice of generators:

Date: October 2009.

The first author was supported in part by ERC starting grant GADA-20891. The second author was supported in part by DARPA, NSF, and the Sloan Foundation.

Independence Problem ([19]). Let $\{G_i\}$ be a family of finite groups, $\langle S_i\rangle = \langle S_i'\rangle = G_i$ and $|S_i| < k$, $|S_i'| < k$. Does the fact that $\{\mathcal{G}(G_i, S_i)\}$ is an expander family imply the same for $\{\mathcal{G}(G_i, S_i')\}$?

It turned out that in general the answer is negative. In 2001 Alon, Lubotzky and Wigderson [2], using the notion of zig-zag product introduced in the paper of Reingold, Vadhan and Wigderson [24], constructed a family of groups G_i which are expanders with respect to one choice of generators and not with respect to another such choice. The groups G_i are of the form $A_i \rtimes B_i$ where $B_i = \mathrm{SL}_2(\mathbb{F}_{p_i})$ and $A_i = \mathbb{F}_2^{P_i}$, with $P_i = \mathbb{F}_{p_i} \cup \{\infty\}$ for an infinite family of primes. In another breakthrough, Kassabov [12] proved that symmetric groups can be made expanders with respect to explicit sets of generators — it is easy to see that symmetric groups are not expanding with respect to $\{(12), (1, 2, \ldots, n)\}$.

In [5] it was proved 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 $\mathrm{SL}_2(\mathbb{F}_p)$. In this note we prove that Cayley graphs of $\mathrm{SL}_2(\mathbb{F}_p)$ are expanders with respect to all generators for infinitely many primes, thus obtaining a first example of an affirmative answer to the Lubotzky-Weiss problem. A related question, namely that of finding an infinite family of finite groups G_p all of whose Cayley graphs have diameter bounded by $O(log(|G_p|))$ was answered affirmatively by Abert and Babai in [1] who showed that the solvable groups $\mathbb{Z}/2\mathbb{Z} \wr \mathbb{Z}/p\mathbb{Z}$ have this property.

For a finite group G generated by 2 elements let $g(G)$ be the smallest spectral gap of the averaging operator $\frac{1}{4}(a + a^{-1} + b + b^{-1})$ among all possible choices of a pair (a, b) in G which generates the group. We say that G has uniform spectral gap at least $g > 0$ if $g(G) \geq g$. We say that an infinite sequence $\{G_n\}_n$ of finite 2-generated groups has *strong uniform expansion* if $\inf_n g(G_n) > 0$. For k-generated Cayley graphs with fixed k a uniform lower bound on the spectral gap is equivalent to (2).

Theorem 1.1. *There is a function $\varepsilon(\delta) > 0$ with $\varepsilon(\delta) \to 0$ as $\delta \to 0$ such that for all $\delta > 0$ and all $X > 1$ the number of rational primes p less than X for which $\mathrm{SL}(2, p)$ has uniform spectral gap less than δ is at most $X^{\varepsilon(\delta)}$.*

We show furthermore that in our case the expansion property remains uniform as the number of generators increases, thus obtaining a result valid for all Cayley graphs regardless of the number of generators :

Corollary 1.1. *There is a function $\varepsilon(c) > 0$ with $\varepsilon(c) \to 0$ as $c \to 0$ such that for all $c > 0$ and all $X > 1$ the number of rational primes p less than X for which some Cayley graph of $\mathrm{SL}(2, p)$ fails to be a c-expander is at most $X^{\varepsilon(c)}$.*

According to the prime number theorem there are roughly $X/\log(X)$ primes less that X, hence Theorem 1.1 produces an infinite sequence of finite groups with strong uniform expansion. A well-known result about the distribution of primes (Hoheisel's theorem [9], see [14] §10.5) says that there is a constant $\beta_0 > 0$ such that for all large X, there is at least one prime between X and $X + X^{\beta_0}$ (one can take any $\beta_0 > \frac{7}{12}$ by [11]). Hence the following immediate consequence :

Corollary 1.2. *For any $\beta \in (\beta_0, 1)$, there is a constant $c = c(\beta) > 0$ and an infinite sequence of primes p_n with $p_{n+1} \leq p_n + p_n^{\beta}$ such that for every n every Cayley graph of $\mathrm{SL}(2, p_n)$ is a c-expander.*

We note that our method is effective in the sense that proofs give an explicit lower bound for the constant c in the last two corollaries.

Combining Corollary 1.2 with the main result of [7], we obtain an application to product replacement graphs [23]. Given a group G, the product replacement graph $\Gamma_k(G)$ introduced in [6] in connection with computing in finite groups is defined as follows. The vertices of $\Gamma_k(G)$ consist of all k-tuples of generators $(g_1, \dots, g_k)$ of the group G. For every (i, j), $1 \le i, j \le k, i \ne j$ there is an edge corresponding to transformations $L_{i,j}^{\pm}$ and $R_{i,j}^{\pm}$:

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

The graphs $\Gamma_k(G)$ are regular, of degree $4\,k\,(k-1)$, possibly with loops and multiple edges. Connectivity of $\Gamma_k(G)$ has been the subject of intensive recent investigations; for $G = \mathrm{SL}_2(p)$ and $k \ge 3$ it was established by Gilman in [8].

In the case of the free group F_k the moves $L_{i,j}^{\pm}$ and $R_{i,j}^{\pm}$ defined above correspond to Nielsen moves on $\Gamma_k(F_k)$. For every group G, the set $\Gamma_k(G)$ can be identified with $E = \mathrm{Epi}(F_k, G)$, the set of epimorphisms from F_k onto G, and the group $A = \mathrm{Aut}(F_k)$ acts on E in the following way: if $\alpha \in A$ and $\varphi \in E$, $\alpha(\varphi) = \varphi \cdot \alpha^{-1}$. A long-standing problem is whether $\mathrm{Aut}(F_k)$ has property T for $k \ge 4$; in [18] Lubotzky and Pak observed that a positive answer to this problem implies the expansion of $\Gamma_k(G)$ for all G and proved that $\Gamma_k(G)$ are expanders when G is nilpotent of class l and both k and l are fixed.

In [7] the second author and Pak established a connection between the expansion coefficient of the product replacement graph $\Gamma_k(G)$ and the minimal expansion coefficient of a Cayley graph of G with k generators, and in particular showed that the product replacement graphs $\Gamma_k(\mathrm{SL}(2, p))$ form an expander family under assumption of strong uniform expansion of $\mathrm{SL}(2, p)$ on k generators. Corollary 1.3 is an immediate consequence of Corollary 1.2 and Corollary 2 in [7].

Corollary 1.3. *Let $k \ge 4$. The family of product replacement graphs $\{\Gamma_k(\mathrm{SL}(2, p_n))\}_n$ forms a family of expanders.*

2. Proofs

First a few words about the strategy of proof. Roughly speaking Theorem 1.1 follows from the combination of the results of the second named author with Jean Bourgain on the spectral gap for $\mathrm{SL}(2, p)$ [5] with the Strong Tits Alternative proved by the first named author [3] together with a combinatorial argument based on the effective arithmetic Nullstellensatz which we explain here. We now give details.

2.1. Strong Tits.

Let $g(p) = g(\mathrm{SL}(2, p))$. We will in fact prove the following equivalent version of Theorem 1.1.

Theorem 2.1 (reformulation of the main theorem)**.** *For every $\varepsilon > 0$ and every $A > 1$ there is $\delta > 0$ such that for every $X > 1$, the number of primes p in the interval $[X, X^A]$ with $g(p) < \delta$ is at most X^{ε}.*

Recall the statement of the Strong Tits Alternative proved in [3] (see also [4] for a proof in the special case of $GL(2)$, which is enough for the purpose of this paper).

Theorem 2.2 ([3])**.** *There is a universal constant N such that any finite symmetric set S in $GL(2, \overline{\mathbb{Q}})$ which does not generate a virtually solvable group has the property that*

some words w_1 and w_2 of length at most N in the elements of S will generate a free subgroup.

Consider the set $\mathcal{C}_n$ of all assignments which assign 4 paths of length n starting at the identity in the free group F_2 to every pair $(w_1, w_2) \in B(N)^2$ ($B(N)$ is the ball of radius N in F_2). Observe that $|\mathcal{C}_n| = 4^{4Kn}$ where $K := |B(N)^2|$. Among those, consider the subset $\mathcal{D}_n \subset \mathcal{C}_n$ made of assignments all of whose 4 paths $W_1, ..., W_4$ satisfy $[[W_1, W_2], [W_3, W_4]] \neq 1$ (i.e. such that the associated reduced word is non trivial).

Lemma 2.1. *Let $S_n^{(i)}$ for $i = 1, ..., 4$ be 4 independent simple random walks on the free group F_2. Then $\mathbb{P}([[S_n^{(1)}, S_n^{(2)}], [S_n^{(3)}, S_n^{(4)}]] = 1) \leq e^{-\kappa n}$ for some explicit $\kappa > 0$.*

Proof. By Kesten's theorem [13] for every $x \in F_2$, the probability that the simple random walk on F_2 starting at 1 visits x at time n is at most $\left(\frac{\sqrt{3}}{2}\right)^n$. Observe also that the centralizer of a non trivial element in F_2 is a cyclic subgroup of F_2 and that any cyclic subgroup intersects $B(n)\backslash\{1\}$ in at most $2n$ elements. Thus if $[S_n^{(1)}, x] = 1$ for some given $x \neq 1$, then $S_n^{(1)}$ may take only $2n+1$ possible values in $B(n)$. We may now write

$$\mathbb{P}([S_n^{(1)}, S_n^{(2)}] = 1) \leq \max_{x \in B(n)\backslash\{1\}} \mathbb{P}([S_n^{(1)}, x] = 1) + \mathbb{P}(S_n^{(2)} = 1) \leq (2n+2) \cdot \left(\frac{\sqrt{3}}{2}\right)^n$$

Furthermore, note that if a and b are fixed and not 1, then the set of x's such that $[a, x] = b$ coincides, if non empty, with a coset of the centralizer of a. In particular this set can intersect $B(n)$ in at most $4n+1$ elements. Using this we can now write:

$$\begin{aligned}
\mathbb{P}([[S_n^{(1)}, S_n^{(2)}], [S_n^{(3)}, S_n^{(4)}]] &= 1) \leq \max_{u \neq 1, a \in B(n)\backslash\{1\}} \mathbb{P}([u, [a, S_n^{(4)}]] = 1) + \mathbb{P}([S_n^{(1)}, S_n^{(2)}] = 1) + \mathbb{P}(S_n^{(3)} = 1) \\
&\leq (8n+1) \cdot \max_{a,b \neq 1} \mathbb{P}([a, S_n^{(4)}] = b) + (2n+3) \cdot \left(\frac{\sqrt{3}}{2}\right)^n \\
&\leq [(8n+1)(4n+1) + (2n+3)] \cdot \left(\frac{\sqrt{3}}{2}\right)^n \leq e^{-\kappa n}
\end{aligned}$$

for some explicit $\kappa > 0$.

Corollary 2.1. *There is an explicit number $\alpha > 0$ such that $|\mathcal{C}_n \backslash \mathcal{D}_n| \leq |\mathcal{C}_n|^{1-\alpha}$.*

Theorem 2.2 now implies that for every assignment $c \in \mathcal{D}_n$ the algebraic subvariety $\mathcal{W}_c$ of $(GL_2(\mathbb{C}))^2$ defined by the vanishing of the corresponding 4-fold commutators is contained in the subvariety $\mathcal{V}_{sol}$ in $(GL_2(\mathbb{C}))^2$ of pairs which generate a virtually solvable subgroup, because each commutator would give a non trivial relation for each of the pairs $(w_1, w_2) \in B(N)^2$. The subvariety $\mathcal{V}_{sol}$ coincides with the set of pairs that leave invariant a finite subset of at most M points on the projective line (for some constant M). Both varieties are defined over $\mathbb{Z}$ (see [4] §9 for more on this translation).

2.2. **Effective Nullstellensatz.** Observe further that $\mathcal{W}_c$ is defined by the vanishing of K words of length at most $4Nn$. Here K and N are fixed constants and n will grow. If $P_1(c), ..., P_{4K}(c)$ denote the polynomials (with integer coefficients) in the 8 standard variables of $(GL_2)^2$ (i.e. the matrix entries) whose vanishing define $\mathcal{W}_c$, and $Q_1, ..., Q_s$ the polynomials (also with integer coefficients) defining $\mathcal{V}_{sol}$, then the Nullstellensatz

asserts the existence of polynomials g_{ij} with integer coefficients and natural numbers $a_i(c)$ and $e_i(c)$ such that for each $i = 1, ..., s$

$$a_i(c)Q_i^{e_i(c)} = \sum_j g_{ij}P_j(c)$$

Moreover, standard versions of the effective arithmetic Nullstellensatz, based for instance on the classical Hermann method such as in Masser and Wusholtz's paper ([22], chapter 4), give bounds on the a_i's (and on the other parameters too, but we will only need the bound for a_i). In our context, the polynomials $P_j(c)$ have degree at most $4Nn$ and height (i.e. maximum modulus of coefficients) at most H^n for some constant H (see e.g. [4] §9). Then the Nullstellensatz bounds from [22] (Theorem 4.1.IV) give the existence of constants $C, r \geq 1$ such that $a_i(c) \leq e^{Cn^r}$.

We will denote by $a(c)$ the product $a_1(c) \cdot ... \cdot a_s(c)$, which is again bounded above by e^{Cn^r} (for some other constant C, since s is a constant).

$$a(c) \leq e^{Cn^r} \tag{3}$$

We need the following lemma.

Lemma 2.2. *There is $p_0 > 0$ such that for all primes $p > p_0$ we have : for all $(a, b) \in \mathrm{SL}(2, p)^2$ if $Q_i(a, b) = 0$ for all $i = 1, ..., s$ then (a, b) does not generate $\mathrm{SL}(2, p)$.*

Proof. This follows from [4] §9 : the variety $\mathcal{V}_{sol}$ coincides with the $\mathbb{Z}$-scheme of pairs (a, b) that leave invariant a finite set of at most M points on the projective line $\mathbb{P}^1$ (for some constant M). This condition is given by the vanishing of one of finitely many resultant polynomials, the product of which must lie in the ideal generated by the Q_i's. Thus if the $Q_i(a, b)$ vanish in $\mathbb{F}_p$, for p large enough, the group generated by $(a, b) \in \mathrm{SL}(2, p)^2$ must have a subgroup of index at most M which fixes a point in $\mathbb{P}^1(\overline{\mathbb{F}_p})$, hence does not generate $\mathrm{SL}(2, p)$ when p is $> M$ say. □

Thus if p is a prime not dividing $a(c)$, then for every generating pair $(a, b) \in \mathrm{SL}(2, p)$ there must be some j such that $P_j(c) \neq 0$, i.e. there must be 4 paths of length n and two words w_1, w_2 in a, b such that the resulting commutator word does not vanish.

2.3. **Pigeonhole principle.** We can split $\mathcal{D}_n$ into $\mathcal{D}_n(p)$'s where $\mathcal{D}_n(p)$ is the set of c's such that p divides $a(c)$. But (3) implies that no more than n^r primes bigger than e^{Cn} can divide a single $a(c)$. In particular for every finite set $\mathcal{P}$ of primes larger that e^{Cn} we have

$$|\mathcal{P}| \cdot \min_{p \in \mathcal{P}} |\mathcal{D}_n(p)| \leq \sum_{p \in \mathcal{P}} |\mathcal{D}_n(p)| \leq n^r \cdot |\cup \mathcal{D}_n(p)| \leq n^r |\mathcal{D}_n|$$

Thus, given $\varepsilon > 0$, if $|\mathcal{P}| \geq |\mathcal{D}_n|^{2\varepsilon}$, there must be a prime $p \in \mathcal{P}$ with $|\mathcal{D}_n(p)| < |\mathcal{D}_n|^{1-\varepsilon}$.

Now we pass to the second part of the proof: namely it remains to show that if a prime p satisfies $|\mathcal{D}_n(p)| \leq |\mathcal{D}_n|^{1-\varepsilon}$ then a lower bound on $g(p)$ can be deduced. This is of course the place where we will use the results of [5].

2.4. **Modified** [5]**: subgroup non-concentration implies gap.** In fact, rather than the main statement of [5], which gave a lower bound on $g(a, b)$ in terms of the girth of the pair (a, b), we are going to explain how the proof of [5] allows to obtain a similar lower bound out of the weaker hypothesis that the simple random walk on $< a, b >$ at time *constant* $\times$ *log*(p) gives a weight of at most $1/p^{constant}$ to every proper subgroup $\mathrm{SL}(2, p)$. Namely, writing $\mu_{(a,b)} = \frac{1}{4}(\delta_a + \delta_{a^{-1}} + \delta_b + \delta_{b^{-1}})$,

Theorem 2.3 (Modified [5]). *There is a function $\delta = \delta(\tau, \gamma) > 0$ such that for every $\tau, \gamma > 0$, every large prime p, and every generating pair (a, b) in $\mathrm{SL}(2, p)$ such that*

$$\sup_H \mu_{(a,b)}^{(\tau \log_3 p)}(H) \leq p^{-\gamma} \tag{4}$$

(where the sup is taken over all proper subgroups H of $SL(2, p)$), we have $g(a, b) > \delta$.

Let $2l = \tau \log_3 p$ and let $\nu = \mu_{(a,b)}^{(l)}$. In [5] the logarithmic girth condition is used to verify that ν satisfies the two conditions of the l^2 flattening lemma (Proposition 2 in [5]), namely: (a) $\|\nu\|_\infty < p^{-\gamma}$ and (b) $\nu^{(2)}(H) < p^{-\gamma}$ for all proper subgroups H of $SL(2, p)$. Condition (b) follows immediately from (4); condition (a) also easily follows by applying (4) with the trivial subgroup $H = \{e\}$. Indeed, we have $\mu_{(a,b)}^{(2l)}(e) = \|\mu_{(a,b)}^{(l)}\|_2^2$ and $\|\mu_{(a,b)}^{(l)}\|_\infty \leq \|\mu_{(a,b)}^{(l)}\|_2$, thus we obtain $\|\mu_{(a,b)}^{(l)}\|_\infty < p^{-\gamma}$.

2.5. **Proof of Theorem 2.1.** Since $|\mathcal{C}_n| = 4^{4Kn}$ is an exponential function of n, observe that it is enough to prove the theorem for X of the form $X = |\mathcal{C}_n|$ for some n. If there are less that $X^{2\varepsilon}$ primes between X and X^A there is nothing to prove. Otherwise §2.3 implies that there is a prime p between X and X^A such that $|\mathcal{D}_n(p)| < |\mathcal{D}_n|^{1-\varepsilon}$. Let $(a, b) \in \mathrm{SL}(2, p)^2$ a generating pair. Note that Lemma 2.2 implies that for every $c \in \mathcal{D}_n \backslash \mathcal{D}_n(p)$ there is w_1, w_2 in $B(N)^2$ such that the corresponding commutator of length $4n$ in w_1, w_2 is not 1. Suppose that for every w_1, w_2 in $B(N)^2$ there is a proper subgroup H of $\mathrm{SL}(2, p)$ such that $\mu_{(w_1,w_2)}^{*n}(H) \geq 4^{-\varepsilon n/2}$. Recall the subgroup structure of $\mathrm{SL}(2, p)$: every proper subgroup either has cardinality at most 60, or must be solvable of solvability class at most 2 (see [26]). Let $S_n^{(i)}$ be four independent simple random walks starting at 1 on the subgroup of $\mathrm{SL}(2, p)$ generated by (w_1, w_2). Then if H has cardinality at most 60, $\mu_{(w_1,w_2)}^{*n}(H) \leq 60 \cdot \mathbb{P}(S_n^{(1)} = 1)$, while if H is solvable, $\mu_{(w_1,w_2)}^{*n}(H)^4 \leq \mathbb{P}([[S_n^{(1)}, S_n^{(2)}], [S_n^{(3)}, S_n^{(4)}]] = 1)$. It follows in both cases that are at least $4^{4(1-\varepsilon/2)n}$ quadruples of paths of length n whose 4-fold commutator vanishes. Then we can count at least $4^{4(1-\varepsilon/2)nK} = |\mathcal{C}_n|^{1-\varepsilon/2}$ assignments $c \in \mathcal{C}_n$ for which all corresponding words vanish at (a, b) ; hence at least $|\mathcal{C}_n|^{1-\varepsilon}$ assignments $c \in \mathcal{D}_n$ for which all corresponding commutator words vanish at (a, b) (recall $|\mathcal{C}_n \backslash \mathcal{D}_n| \leq |\mathcal{C}_n|^{1-\alpha}$ for some explicit $\alpha > \varepsilon/2 > 0$ by Corollary 2.1). By the preceding remark, those must belong to $\mathcal{D}_n(p)$. Hence $|\mathcal{D}_n(p)| \geq |\mathcal{C}_n|^{1-\varepsilon}$ a contradiction. Therefore, there must exist w_1, w_2 such that $\mu_{(w_1,w_2)}^{*n}(H) \leq 4^{-\varepsilon n/2}$ for all proper subgroups H in $SL(2, p)$. But $p \in [X, X^A]$ and $X = 4^{Kn}$. Hence we may apply Theorem 2.3 and deduce that $g(w_1, w_2) > \delta$. But this readily implies that $g(a, b) > \delta/N$, which ends the proof of Theorem 2.1.

2.6. **Proof of Corollary 1.1.** For a Cayley graph of a finite group G generated by a symmetric set S containing 1 to be a c-expander, it is sufficient that for every $f \in \ell_0^2(G)$ (functions with zero average on G) there is an $s \in S$ such that $||s \cdot f - f||_2 \geq 2\sqrt{c} \cdot ||f||_2$. Indeed take $f = a\mathbf{1}_A - b\mathbf{1}_{A^c}$ with a choice of a and b such that $a|A| = b|A^c|$. Then, since $|A^c| \geq |A|$, we have $a \geq b$ and $||f||_2^2 = (a+b)a|A| \geq \frac{(a+b)^2}{2}|A|$, while $||s \cdot f - f||_2^2 = (a+b)^2|sA\Delta A|$. Thus $|\partial A| \geq |sA \backslash A| = \frac{1}{2}|sA\Delta A| \geq c \cdot |A|$.

Now observe (by the triangle inequality) that if there is a constant N such that for any $f \in \ell_0^2(G)$ there is $\gamma \in S^N$ such that $||\gamma \cdot f - f||_2 \geq 2N\sqrt{c} \cdot ||f||_2$, then there must also be some $s \in S$ such that $||s \cdot f - f||_2 \geq 2\sqrt{c} \cdot ||f||_2$. Therefore Corollary 1.1 will follow from Theorem 1.1 if we can show that there is a constant N independent of S and p such that S^N contains two elements $\{a, b\}$ that generate $\mathrm{SL}(2, p)$. As in the last

paragraph, observe that every proper subgroup either has cardinality at most 60, or must be solvable of solvability class at most 2, therefore for $\{a, b\}$ to generate $\mathrm{SL}(2, p)$ it is enough that a and b have no relation of length at most 60 say. The existence of such a constant N is an immediate consequence of the strong Tits alternative, i.e. Theorem 2.2 (see [4] for more details on this derivation). This ends the proof of Corollary 1.1.

Acknowledgement: We are grateful to Harald Helfgott for pointing out [9] and to Ben Green for a useful comment.

References

[1] M. Abert, L. Babai, Finite groups of uniform logarithmic diameter, Israel J. Math. 158 (2007), 193–203.

[2] N. Alon, A. Lubotzky, A. Wigderson, *Semi-direct product in groups and zig-zag product in graphs: Connections and applications*, Proc. of the 42nd FOCS, 2001.

[3] E. Breuillard, *A strong Tits alternative*, preprint 2008, arXiv:0804.1395

[4] E. Breuillard, *Heights on SL(2) and free subgroups*, to appear in Zimmer's festschrift, Chicago Univ. Press.

[5] J. Bourgain and A. Gamburd, *Uniform expansion bounds for Cayley graphs of* $\mathrm{SL}_2(\mathbb{F}_p)$, Annals of Mathematics, **167**, 2008, 625-642.

[6] 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.

[7] A. Gamburd and I. Pak, *Expansion of product replacement graphs*, Combinatorica, **26**, 2006, 411-429.

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

[9] Hoheisel, *Primzahlprobleme in der analysis*, S-B Preuss. Akad. Wiss. Phys.-Math. Kl 1930, 580-588.

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

[11] M. N. Huxley, *On the difference between consecutive primes*, Invent. Math. **15**, 1972, 164-170.

[12] M. Kassabov, *Symmetric groups and expander graphs*, Invent. Math. **170**, 2007, 327–354.

[13] H. Kesten, *Symmetric random walks on groups*, Trans. AMS **92**, (1959), 336–354.

[14] E. Kowalski, H. Iwaniec, *Analytic number theory*, AMS Colloquium Publication, volume 53.

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

[16] A. Lubotzky, *Cayley graphs: eigenvalues, expanders and random walks*, Surveys in Combinatorics, (P. Rowbinson ed.), London Math. Soc. Lecture Note Ser. 218, Cambridge Univ. Press, 1995, 155-189.

[17] A. Lubotzky, R. Phillips, P. Sarnak, *Ramanujan Graphs*, Combinatorica **8** 1988, 261-277.

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

[19] 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.

[20] G.A. Margulis, *Explicit constructions of concentrators*, Probl. of Inform. Transm., **10**, 1975, 325-332.

[21] G.A. Margulis, *Explicit group-theoretic constructions of combinatorial schemes and their applications in the construction of expanders and concentrators*, Probl. of Inform. Trans., **24**, 1988, 39-46.

[22] Masser, Wustholz, *Fields of large transcendence degree generated by values of elliptic functions*, Invent. Math., 1983.

[23] 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.

[24] O. Reingold, S. Vadhan, A. Wigderson, *Entropy waves, the zig-zag graph product, and new constant-degree expanders*, Annals of Mathematics, **155**, No.1, pp. 157-187, 2002.

[25] P. Sarnak, *What is an expander?*, Notices of the American Mathematical Society **51**, 2004, 762-763.

[26] M. Suzuki, *Group Theory I*, Springer-Verlag, Berlin-Heidelberg-New York, (1982).

Laboratoire de Mathématiques, Université Paris-Sud 11, 91405 Orsay cedex, France
E-mail address: Emmanuel.Breuillard@math.u-psud.fr

Department of Mathematics, University of California at Santa Cruz, 1156 High Street, Santa Cruz, CA 95064, USA
E-mail address: agamburd@ucsc.edu