Expanders and Related Results

Shotaro Makisumi

May 3, 2011

Abstract

This expository paper provides an overview of expanders and the various forms of the expansion property: graph edge expansion, spectral gap, rapid mixing, and connections to Property (T) and Selberg's $\frac{3}{16}$ Theorem. Some key ideas are also discussed from recent results on expansion in linear algebraic groups.

1 Introduction

Expanders are sparse graphs with strong connectivity properties. Although a simple combinatorial proof shows the existence of families of expanders, the first two known explicit constructions relied on deep results in representation theory and in the spectral theory of modular forms, respectively. Originally considered in computer science in the context of networks, expanders have found surprising connections to and applications in various branches of pure mathematics; see [22] and references therein.

This expository paper aims to present expanders in various forms and to discuss recent related results. The paper is organized as follows. Section 2 introduces expanders and looks at several equivalent reformulations of the expander property. Section 3 takes up the explicit constructions expanders using Property (T), Property (τ), and Selberg's $\frac{3}{16}$ Theorem. In particular, we will see that for every $n \geq 2$, Cayley graphs of $SL_n(\mathbb{Z}/p\mathbb{Z})$ with respect to projections of certain fixed generators of $SL_n(\mathbb{Z})$ form families of expanders. Much of the material in these sections is based on Lubotzky's exposition [22], omitting some technical proofs. Section 4 looks at recent results on expansion in certain linear algebraic groups, initiated by Helfgott's work in 2005. We discuss Sarnak and Xue's idea for exhibiting a spectral gap, as well as key components of Bourgain and Gamburd's characterization of expanders for certain Cayley graphs of $SL_2(\mathbb{Z}/p\mathbb{Z})$, and several generalizations of this result. Finally, Section 5 discusses the diameter of expanders and a related open problem.

Acknowledgment

I would like to thank my Junior Paper advisor, Alireza Salehi Golsefidy, for suggesting this topic to me and motivating me throughout the semester. I am very grateful for his careful guidance during our weekly meetings.

2 Expander Property and Equivalent Reformulations

This section introduces expanders and looks at various equivalent formulations of the expander property: edge expansion, the Cheeger constant, spectral gap of the Laplacian, and rapid mixing in random walks. These equivalences, together with a representation-theoretic reinterpretation, are summarized as Theorem 3.21 in Section 3.5.

Write $X = X(V, E)$ for a graph with vertex set V and edge set E. For $u, v \in V$, write $u \sim v$ to mean that u and v are adjacent, i.e. $\{u, v\} \in E$. For $A \subset V$, define $\partial A = \{x \in V : \mathrm{dist}(x, A) = 1\}$. For $A, B \subset V$, write $E(A, B)$ for the set of edges connecting vertices in A to vertices in B. Although much of the discussion in this section can be carried out more generally, we will only deal with regular graphs.

2.1 Edge Expansion

Expanders are graphs with uniform growth of small subsets to neighboring vertices under "expansion" through the edges, i.e. *edge expansion*.

Definition 2.1. *A k-regular graph $X = X(V, E)$ with n vertices is called an (n, k, c)-expander if $|\partial A| \geq c|A|$ for every $A \subset V$ with $1 \leq |A| \leq \frac{n}{2}$. The* expansion coefficient *of X is defined to be $c(X) = \inf\{\frac{|\partial A|}{|A|} : 1 \leq |A| \leq \frac{n}{2}\}$.*

Every finite connected k-regular graph with n vertices is trivially an (n, k, c)-expander for some $c > 0$ (also see Proposition 2.3 below). One therefore always considers *a family of expanders*, a family of (n, k, c)-expanders for fixed k and some fixed $c > 0$, with n going to infinity. Equivalently, k-regular graphs X_i form a family of expanders if $\liminf_{i\to\infty} c(X_i) > 0$.

Several alternative definitions of (n, k, c)-expanders exist in the literature, but with only at most a constant-factor change in c. For example, define an $(n, k, c)'$-expander by the condition that $|\partial A| \geq c(1 - \frac{|A|}{n})|A|$ for every $A \subset V$. Since $1 - \frac{|A|}{n} \geq \frac{1}{2}$ when $|A| \leq \frac{n}{2}$, an $(n, k, c)'$-expander is an $(n, k, \frac{c}{2})$-expander. Conversely, an (n, k, c)-expander is an $(n, k, \frac{c}{k})'$-expander: if $|A| \leq \frac{n}{2}$, then $|\partial A| \geq c|A| \geq c(1 - \frac{|A|}{n})|A|$; otherwise $B = V \setminus A$ expands, so $|\partial A| \geq \frac{1}{k}|E(A, B)| \geq \frac{1}{k}|\partial B| \geq \frac{c}{k}|B| \geq \frac{c}{k}(1 - \frac{|A|}{n})|A|$. The point is that c differ among various definitions by a constant factor independent of n, and hence the key notion of a family of expanders is consistently defined.

A short probabilistic argument shows the existence of families of expanders; see Proposition 1.2.1 in [22]. We will take up their explicit constructions, a much deeper result, in Section 3.

2.2 Cheeger Constant

For a connected compact Riemannian manifold, one defines its Cheeger isoperimetric constant. The discrete analogue provides an equivalent reformulation of the expander property.

Definition 2.2. *For a finite graph $X = X(V, E)$, define its* Cheeger constant *$h(X)$ by*

$$h(X) = \inf_{A,B\subset V} \frac{|E(A, B)|}{\min(|A|, |B|)},$$

where the infimum runs over all partitions $V = A \cup B$.

For any partition $V = A \cup B$, every edge in $E(A, B)$ connects a vertex in ∂A to a vertex in A. If X is k-regular, then there are between 1 and k edges in $E(A, B)$ for each vertex in ∂A, so $|\partial A| \leq |E(A, B)| \leq k|\partial A|$. This allows us to relate edge expansion to the Cheeger constant.

Proposition 2.3. *Let X be a k-regular graph with n vertices.*

(i) *If X is an (n, k, c)-expander, then $h(X) \geq c$.*

(ii) *X is an $(n, k, \frac{h(X)}{k})$-expander.*

Consequently, k-regular graphs X_i form a family of expanders if and only if $\liminf_{i\to\infty} h(X_i) > 0$.

Proof. **(i)** For any partition $V = A \cup B$ with say $|A| \leq |B|$, edge expansion implies $\frac{|E(A,B)|}{\min(|A|,|B|)} \geq \frac{|\partial A|}{|A|} \geq c$.

(ii) Let $A \subset V$ with $1 \leq |A| \leq \frac{n}{2}$. Taking $B = V \setminus A$, we have $|\partial A| \geq \frac{|E(A,B)|}{k|A|} \cdot |A| \geq \frac{h(X)}{k}|A|$. □

2.3 Spectral Gap

The Cheeger-Buser inequality relates the Cheeger constant of a connected compact Riemannian manifold to the first nontrivial eigenvalue of its Laplacian. The discrete analogue therefore provides another formulation of expansion, as a spectral gap for the combinatorial Laplacian.

Definition 2.4. *Let $X = X(V, E)$ be a connected k-regular graph with n vertices. Write $L^2(V)$ for the space of complex-valued functions on V. By fixing the basis of Dirac mass $\{\delta_v\}_{v\in V}$, i.e. $\delta_v(u) = 1$ if $u = v$ and 0 otherwise, we view an operator on $L^2(V)$ and its matrix interchangeably.*

Let A be the adjacency matrix of X, the $n \times n$ matrix indexed by $V \times V$ such that the (u, v) entry is 1 if $u \sim v$ and 0 otherwise. Then the Laplacian Δ on X is the operator on $L^2(V)$ defined by $\Delta = kI - A$.

Note that $\frac{1}{k}A$ is the averaging operator: if $f \in L^2(V)$, then $\frac{1}{k}Af(v) = \frac{1}{k}\sum_{u\sim v} f(u)$, the average value of f at the k vertices adjacent to v. Since $\frac{1}{k}A$ is symmetric, it is diagonalizable with n real eigenvalues. Since X is connected, 1 is a simple eigenvalue corresponding to the space of constant functions. Any other eigenfunction f of $\frac{1}{k}A$ lies in the orthogonal complement, $L^2_0(V) = \{f \in L^2(V) : \sum_{v\in V} f(v) = 0\}$. We may assume after rescaling that f is real-valued. By considering where f achieves its maximum, the averaging interpretation shows that f corresponds to an eigenvalue strictly less than 1. Moreover, a similar argument applied to $|f|$ shows that every eigenvalue is at most 1 in absolute value. Therefore $\Delta = k(I - \frac{1}{k}A)$ has spectrum $0 = \lambda_0(X) < \lambda_1(X) \leq \cdots \lambda_{n-1}(X) \leq 2k$. The difference $\lambda_1(X) - \lambda_0(X)$ is called the *spectral gap*.

For each $e \in E$, arbitrarily choose an orientation: a positive end e^+ and a negative end e^-. Define $d : L^2(V) \to L^2(E)$ by $df(e) = f(e^+) - f(e^-)$. Regardless of the choice of orientation, it can then be shown that $\Delta = d^*d$, or equivalently $\langle f, \Delta g\rangle = \langle df, dg\rangle$ for all $f, g \in L^2(V)$.

Proposition 2.5. *For a finite connected regular graph X, we have $\lambda_1(X) = \inf_{f \in L_0^2(V)} \frac{||df||^2}{||f||^2}$.*

Proof. By the discussion above, $\lambda_1(X)$ is the smallest eigenvalue of Δ on $L_0^2(V)$, so

$$\lambda_1(X) = \inf_{f \in L_0^2(V)} \frac{\langle \Delta f, f \rangle}{\langle f, f \rangle} = \inf_{f \in L_0^2(V)} \frac{\langle df, df \rangle}{\langle f, f \rangle}. \qquad \square$$

The following bounds for $h(X)$ are the discrete analogues of the Cheeger-Buser inequality. The upper bound is due to Dodziuk [14] and Alon [1]; see Propositions 4.2.4 in [22]. Here we only prove the lower bound, variously attributed to Tanner [30] and to Alon and Milman [2].

Proposition 2.6 (Discrete Cheeger-Buser Inequality)**.** *If X is a finite k-regular graph, then $\frac{h^2(X)}{2k} \leq \lambda_1(X)$ and $h(X) \geq \frac{\lambda_1(X)}{2}$. Consequently, finite k-regular graphs X_i form a family of expanders if and only if they have a uniform spectral gap, i.e. $\liminf_{i \to \infty} \lambda_1(X_i) > 0$.*

Proof of the second inequality. Let $X = X(V, E)$. For any partition $V = A \cup B$ with say $|A| \leq |B|$, define $f \in L_0^2(V)$ by $f(x) = |B|\chi_A - |A|\chi_B$. By Proposition 2.5,

$$\lambda_1(X) \leq \frac{||df||^2}{||f||^2} = \frac{|V|^2 |E(A,B)|}{|V||A||B|} \leq 2 \cdot \frac{|E(A,B)|}{|A|} = 2h(X). \qquad \square$$

2.4 Rapid Mixing in Random Walk

Spectral gap leads us to a further reinterpretation of expansion in terms of random walks.

Let $X = X(V, E)$ be a k-regular graph with n vertices. Consider a random walk on X in which one moves from a vertex to one of its adjacent vertices with equal probability $\frac{1}{k}$. Each step of the random walk can be characterized by a probability measure $\mu \in L^2(V)$ (i.e. $0 \leq \mu(v) \leq 1$ for all $v \in V$ and $\sum_{v \in V} \mu(v) = 1$), where $\mu(v)$ represents the probability of being at vertex v. Then the random walk defines the transition operator M on $L^2(V)$ that takes μ to the probability measure at the next step, $M\mu(v) = \frac{1}{k} \sum_{u \sim v} \mu(u)$.

Note that M is exactly the averaging operator $\frac{1}{k}A$ from the previous section. If X is connected, we saw that $\frac{1}{k}A$ has spectrum $1 = \lambda_0 > \lambda_1 \geq \cdots \geq \lambda_{n-1} \geq -1$, where now λ_1 denotes the largest nontrivial eigenvalue of $\frac{1}{k}A$, and that the expander property is equivalent to a uniform spectral gap $\lambda_1 \leq c < 1$. If in addition X is not bipartite, it can be shown that -1 is not an eigenvalue. Then $|\lambda_i| < |\lambda_0|$ for every $i \neq 0$, so iterating $\frac{1}{k}A$ brings every function close to the eigenspace of λ_0, i.e. the constants; that is, random walk converges to uniform distribution. The rate of convergence is controlled by the spectral gap (see Section 4.5 in [22]). In particular, expansion is related to *rapid mixing*, the rapid convergence of random walk to uniform distribution.

Families of expanders were first constructed as Cayley graphs of quotients of certain finitely generated groups. We now specialize to this setting.

Definition 2.7. *Let G be a group and S a finite symmetric (i.e. $S^{-1} = S$) generating set for G. The* Cayley graph *of G with respect to S, denoted $\mathcal{G}(G, S)$, is the graph with vertex set G and*

edge set $\{\{g, gs\} : g \in G, s \in S)\}$. *Define the probability measure* μ_S *on* G *by* $\mu_S = \frac{1}{|S|}\sum_{g\in S}\delta_g$, *where* δ_g *is the Dirac mass at* g. *For probability measures* $\mu, \nu \in L^2(G)$, *define their* convolution *by* $(\mu * \nu)(g) = \sum_{h\in G}\mu(gh^{-1})\nu(h)$. *One easily checks that convolution is symmetric and associative, and that the convolution of two probability measures is again a probability measure. Write* $\mu^{(k)}$ *for* μ *convolved with itself* k *times.*

For a random walk on the $|S|$-regular graph $\mathcal{G}(G, S)$, since each $g \in G$ is adjacent to gs^{-1}, $s \in S$, we have $M\mu(g) = \frac{1}{|S|}\sum_{s\in S}\mu(gs^{-1}) = \sum_{s\in G}\mu(gs^{-1})\mu_S(s) = (\mu * \mu_S)(g)$. The expander property is thus equivalent to a uniform spectral gap $\lambda_1 \leq c < 1$ in the convolution operator $M = *\mu_S$. We will revisit this interpretation in Section 4 in the context of expansion in certain linear algebraic groups.

3 Property (T), Property (τ), and Selberg's $\frac{3}{16}$ Theorem

As already mentioned, first explicit constructions of families of expanders came from Cayley graphs of quotients of certain finitely generated groups. This section introduces the Kazhdan Property (T), the related Property (τ), and Selberg's $\frac{3}{16}$ Theorem, and explain their connection to expanders.

3.1 Property (T) and the Explicit Construction of Expanders

The first construction of a family of expanders used the representation-theoretic Property (T), an idea due to Margulis [24]. We begin with a definition of Property (T) that more directly leads to expanders.

For the rest of this paper, G will denote a locally compact group. For a Hilbert space H, write $U(H)$ for the group of invertible unitary bounded linear operators on H. A *(unitary) representation* (H, ρ) of G is a group homomorphism $\rho : G \to U(H)$ such that $g \mapsto \rho(g)h$ is continuous for every $h \in H$.

Definition 3.1. *A group* G *is said to have* Property (T) *(or be a* Kazhdan group*) if there exists* $\epsilon > 0$ *and a compact subset* K *of* G *such that for every representation* (H, ρ) *of* G *with no non-trivial invariant vector and every* $v \in H$, $||\rho(k)v - v|| > \epsilon||v||$ *for some* $k \in K$. *The constant* ϵ *is called the* Kazhdan constant.

To put another way, a group G has Property (T) if every representation with no non-trivial invariant vector also has no *almost-invariant vector*. For finitely generated groups with Property (T), non-almost-invariance can be detected by any generating set. More precisely

Proposition 3.2 (Remark 3.2.5 in [22])**.** *Let* G *be a finitely generated discrete group with Property* (T). *For any finite symmetric* ($S^{-1} = S$) *generating set* S *of* G, *there exists* $\epsilon > 0$ *such that for every representation* (H, ρ) *with no non-trivial invariant vector and every* $v \in H$, $||\rho(s)v - v|| > \epsilon||v||$ *for some* $s \in S$.

Proof. Assuming that the Proposition fails for S, (H, ρ), and $v \in H$, we will obtain a contradiction to Property (T). Let $\epsilon > 0$ and a compact subset K of G be given. Since G is discrete, K is finite, so any $k \in K$ can be written as a word of length at most say l in elements of S; say $k = s_m \cdots s_1$, $s_i \in S$, $m \leq l$. Since $||\rho(s)v - v|| \leq \frac{\epsilon}{l}||v||$ for every $s \in S$,

$$||\rho(k)v - v|| \leq \sum_{i=1}^{m} ||\rho(s_i) \cdots \rho(s_1)v - \rho(s_{i-1}) \cdots \rho(s_1)v|| = \sum_{i=1}^{m} ||\rho(s_i)v - v|| \leq m\frac{\epsilon}{l}||v|| \leq \epsilon||v||. \quad \square$$

Expanders arise as Cayley graphs of quotients of finitely generated groups with Property (T).

Proposition 3.3 (Proposition 3.3.1 in [22])**.** *Let G be a finitely generated group with Property (T), $\mathcal{L}$ a family of finite-index normal subgroups of G, and S a finite symmetric generating set for G. For each $N \in \mathcal{L}$, write S_N for the natural projection of S to G/N. Then $\{\mathcal{G}(G/N, S_N)\}_{N \in \mathcal{L}}$ is a family of expanders.*

Proof. Take $\epsilon > 0$ as in Proposition 3.2. Fix $N \in \mathcal{L}$, and let $H = L^2(G/N)$. For $\alpha \in G$ and $f \in H$, define $\alpha \cdot f \in H$ by $(\alpha f)(x) = f(x\alpha)$. One easily checks that this is an action of G on H by linear operations. In fact, this gives a unitary representation of G since $||\alpha \cdot f||^2 = \sum_{x \in G/N} |f(x\alpha)|^2 = \sum_{x \in G/N} |f(x)|^2 = ||f||^2$. Further, $H_0 = \{f \in H : \sum_{x \in G/N} f(x) = 0\}$ is a subrepresentation with no non-trivial invariant function. Indeed, H_0 is clearly G-invariant, and since G acts transitively on G/N, the invariant functions in H are precisely the constant functions.

Write $n = |G/N|$. Let $G/N = A \cup B$ be a partition with $a = |A| \leq |B| = b$. Then $f := b\chi_A - a\chi_B \in H_0$, so by Proposition 3.2, $||sf - f|| > \epsilon||f||$ for some $s \in S$. We have $||f||^2 = ab^2 + ba^2 = nab$ and $||sf - f||^2 = \sum_{x \in V}(f(xs) - f(x))^2$. Non-zero contributions to the last sum come from $x \in V$ for which adjacent vertices xs and x lie in distinct subsets of the partition $V = A \cup B$. Each such x contributes $(a + b)^2 = n^2$, and $\{xs, x\} \in \partial A$ with each edge appearing at most twice in this way, so $||sf - f||^2 \leq 2|\partial A|n^2$. Hence

$$|\partial A| \geq \frac{||sf - f||^2}{2n^2} > \frac{\epsilon^2||f||^2}{2n^2} = \frac{\epsilon}{2} \cdot \frac{ab}{n} \geq \frac{\epsilon^2}{4}|A|.$$

Since $N \in \mathcal{L}$ was arbitrary, the Proposition is proved. $\square$

The key step of the proof was to translate non-almost-invariance from functions to sets. Since $||sf - f||$ measures the growth of A under multiplication by a single generator s, Proposition 3.2 says that every subset grows under multiplication by at least one of the generators. Note in particular that, having chosen S, the Kazhdan constant can be related to the expansion constant.

3.2 Fell Topology, Property (T), and Property (τ)

Here, we briefly discuss the original representation-theoretic definition of Property (T) and the related Property (τ). More details can be found in [3].

As in the finite-dimensional case, we may define notions of equivalence and irreducibility for unitary representations. Write $\hat{G}$ for the *unitary dual* of G, the space of equivalence classes of

irreducible unitary representations of G. For an adequate theory, the notion of subrepresentation from the finite-dimensional setting must be replaced by that of *weak containment*. The *Fell topology*, named after Fell for his work in the 1960s, provides a natural setting for this study.

Definition 3.4. *The* Fell topology *on $\hat{G}$ is generated by the following open neighborhoods for each $(H, \rho) \in \hat{G}$: for a compact subset K of G, $\epsilon > 0$, and $v \in H$ of norm one, $W(K, \epsilon, v)$ consists of $(H', \rho') \in \hat{G}$ for which there exists $v' \in H$ of norm one such that $|\langle v, \rho(g)v\rangle - \langle v', \rho'(g)v'\rangle| < \epsilon$ for all $g \in K$.*

Property (T) can be reformulated using the Fell topology, as in (3) below. This was Kazhdan's original definition of Property (T), which he defined in the mid-60s in the context of representations of semi-simple Lie groups [19].

Proposition 3.5. *The following are equivalent.*

(1) *G has Property (T), i.e. there exists $\epsilon > 0$ and a compact subset K of G such that for every representation (H, ρ) of G with no non-trivial invariant vector and every $v \in H$ of norm one, $||\rho(k)v - v|| > \epsilon$ for some $k \in K$.*

(2) *There exists $\epsilon > 0$ and a compact subset K of G such that for every non-trivial irreducible representation (H, ρ) of G and every $v \in H$ of norm one, $||\rho(k)v - v|| > \epsilon$ for some $k \in K$.*

(3) *The trivial representation ρ_0 is isolated in $\hat{G}$ in the Fell topology.*

Partial proof. Consider a neighborhood $W(K, \epsilon, v_0)$ of the trivial representation (H_0, ρ_0). Then $\langle v_0, \rho_0(g)v_0\rangle = 1$ for all $g \in G$, so for any $(\rho, H) \in \hat{G}$ and $v \in H$ of norm 1, $||\rho(g)v - v||^2 = ||\rho(g)v||^2 + ||v||^2 - 2\langle v, \rho(g)v\rangle = 2|\langle v_0, \rho_0(g)v_0\rangle - \langle v, \rho(g)v\rangle|$ for all $g \in G$. Hence $W(K, \epsilon, v_0)$ does not depend on v_0, and $(H, \rho) \in W(K, \epsilon, v_0)$ if and only if there exists $v \in H$ of norm 1 such that $||\rho(k)v - v|| < \sqrt{2\epsilon}$ for all $k \in K$.

Clearly (1) $\Rightarrow$ (2). The trivial representation ρ_0 is isolated exactly when some $W(K, \epsilon, v_0)$ contains only ρ_0, which by the previous paragraph is exactly (2). Thus (2) $\Leftrightarrow$ (3). We omit the proof of (3) $\Rightarrow$ (1), which uses further notions of unitary representations; see for example [34]. $\square$

Note that (3) lacks the Kazhdan constant, which we saw was related to the expansion constant. Expanders with explicit expansion constants are particularly desired in many applications.

Looking back to the construction of families of expanders, note that the proof of Theorem 3.3 only uses the defining condition of Property (T) for subrepresentations of the left-regular representations $L^2(G/N)$, and that N in each case acts trivially. This motivates a "relative" Property (T), called *Property (τ)*; an analogous proof shows the equivalence of the following two definitions.

Definition 3.6. *Let G be a finitely generated group and $\mathcal{L}$ a family of finitely-index normal subgroups of G. Let $R = \{\varphi \in \hat{G} : \ker\varphi \supset N \text{ for some } N \in \mathcal{L}\}$. We say that G has property (τ) with respect to $\mathcal{L}$ if the following equivalent conditions hold.*

(1) *The trivial representation ρ_0 is isolated in R in the Fell topology.*

(2) *For any finite generating set S of G, there exists $\epsilon > 0$ such that for every representation $(H, \rho) \in R$ with no non-trivial invariant vector and every $v \in H$, $||\rho(s)v - v|| > \epsilon||v||$ for some $s \in S$.*

We say that G has property (τ) if it has property (τ) with respect to the family of all finite-index normal subgroups.

With these definitions, Property (T) clearly implies Property (τ). By the observation above, Theorem 3.3 holds with Property (τ) with respect to $\mathcal{L}$. In fact, it can be shown that this is also necessary.

Theorem 3.7 (Theorem 4.3.2 in [22])**.** *Let G be a finitely generated group with a finite symmetric generating set S, and let $\mathcal{L}$ be a family of finite-index normal subgroups of G. Then G has Property (τ) with respect to $\mathcal{L}$ if and only if $\{\mathcal{G}(G/N, S_N)\}_{N \in \mathcal{L}}$ is a family of expanders.*

Thus Property (τ) provides yet another equivalent reformulation of the expander property, opening up the subject to the use of representation-theoretic notions such as Property (T).

3.3 Expanders from $SL_3(\mathbb{Z})$

We obtain our first example of a family of expanders by showing that $SL_3(\mathbb{Z})$ has Property (T). The proof below follows Lubotzky's treatment (Section 3.1 [22]) of Kazhdan's original proof.

Theorem 3.8 (Kazhdan, [19])**.** *$SL_3(\mathbb{Z})$ has Property (T).*

The proof relies on the following results, which use notions of induced representations and are beyond the scope of this paper. In particular, the first result arises from Kazhdan's original motivation for defining Property (T), to study properties of lattices in semi-simple Lie groups.

Theorem 3.9. *Let Γ be a lattice in G, i.e. a discrete subgroup of G such that G/Γ has finite measure in the Haar measure induced from G. Then G has Property (T) if and only if Γ has Property (T).*

Proposition 3.10. *The trivial representation of $G = \mathbb{R}^2 \rtimes SL_2(\mathbb{R})$ is isolated in $R = \{\rho \in \hat{G} : \rho|_{\mathbb{R}^2}$ is non-trivial$\}$. Equivalently, if a representation (H, ρ) of G has almost-invariant vectors, then (H, ρ) contains some representation not in R. In particular, some non-zero $v \in H$ is fixed by $\mathbb{R}^2$.*

With these in place, Theorem 3.8 follows from

Lemma 3.11. *Let $E = SL_2(\mathbb{R})$ and $N = \{\left(\begin{smallmatrix} 1 & t \\ 0 & 1 \end{smallmatrix}\right) : t \in \mathbb{R}\}$. For any representation ρ of E, every vector fixed by N is fixed by E.*

Proof. Fix $v \neq 0$ fixed by N. It suffices to show that $f(g) := \langle \rho(g)v, v \rangle$ is constant on E, for then $\langle \rho(g)v - v, v \rangle = f(g) - f(e) = 0$ and so $\rho(g)v = v$ for all $g \in E$.

Under the natural action of E on $\mathbb{R}^2$, $\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)$ has orbit $\mathbb{R}^2 \setminus \{0\}$ and stabilizer N, yielding the bijection

$$E/N \longrightarrow \mathbb{R}^2 \setminus \{0\}$$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} N \longmapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ c \end{pmatrix}.$$

Since $f(gn) = \langle \rho(g)\rho(n)v, v\rangle = \langle \rho(g)v, v\rangle = f(g)$ for all $n \in N$ and $g \in E$, we may define f on E/N by $f(gN) = f(g)$, then view it via the bijection above as a function on $\mathbb{R}^2 \setminus \{0\}$. Since $\left(\begin{smallmatrix}1 & t\\ 0 & 1\end{smallmatrix}\right)\left(\begin{smallmatrix}x & *\\ y & *\end{smallmatrix}\right) = \left(\begin{smallmatrix}x+ty & *\\ y & *\end{smallmatrix}\right)$, N acts on $\mathbb{R}^2 \setminus \{0\}$ like $\left(\begin{smallmatrix}1 & t\\ 0 & 1\end{smallmatrix}\right)\left(\begin{smallmatrix}x\\ y\end{smallmatrix}\right) = \left(\begin{smallmatrix}x+ty\\ y\end{smallmatrix}\right)$. Moreover, $f(ng) = f(g)$ for every $n \in N$, so f is constant on N-orbits, i.e. on every line parallel to the x-axis, and so by continuity also on the x-axis (minus the origin). As a function on E, f is constant on $P = \{\left(\begin{smallmatrix}a & b\\ 0 & d\end{smallmatrix}\right) \in E\}$, corresponding to the x-axis. Hence v is fixed by P.

Similarly, under the action of E on $\mathbb{P}^1(\mathbb{R})$ by $\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)(x : y) = (ax + by : cx + dy)$, $\infty = (1 : 0)$ has orbit $\mathbb{P}^1(\mathbb{R})$ and stabilizer P, yielding the bijection

$$E/P \longrightarrow \mathbb{P}^1(\mathbb{R})$$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} P \longmapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix} (1:0) = (a:c).$$

As before, f as a function on $\mathbb{P}^1(\mathbb{R})$ is constant on P-orbits $\mathbb{R}$ and $\{\infty\}$, hence on $\mathbb{P}^1(\mathbb{R})$ by continuity. Thus f is constant as a function on E. □

Proof of Theorem 3.8. It is well known that $SL_3(\mathbb{Z})$ is a lattice in $SL_3(\mathbb{R})$. By Theorem 3.9, it suffices to show that $SL_3(\mathbb{R})$ has Property (T).

Consider the following subgroups of $SL_3(\mathbb{R})$.

$$J = \left\{ \begin{pmatrix} 1 & & s \\ & 1 & t \\ & & 1 \end{pmatrix} : s,t \in \mathbb{R} \right\}, \quad E_0 = \left\{ \begin{pmatrix} a & b & \\ c & d & \\ & & 1 \end{pmatrix} \in SL_3(\mathbb{R}) \right\}$$
$$G = \left\{ \begin{pmatrix} a & b & s \\ c & d & t \\ & & 1 \end{pmatrix} \in SL_3(\mathbb{R}) \right\} \cong J \rtimes E_0 \cong \mathbb{R}^2 \rtimes SL_2(\mathbb{R}).$$

Suppose that a representation (H, ρ) of $SL_3(\mathbb{R})$ has almost-invariant vectors. Then so does its restriction to G, so by Proposition 3.10, some non-zero $v \in H$ is fixed by $\mathbb{R}^2 \cong J$. Now consider

$$E_1 = \left\{ \begin{pmatrix} a & & b \\ & 1 & \\ c & & d \end{pmatrix} \in SL_3(\mathbb{R}) \right\}, \quad N_1 = E_1 \cap J = \left\{ \begin{pmatrix} 1 & & s \\ & 1 & \\ & & 1 \end{pmatrix} : s \in \mathbb{R} \right\}$$
$$E_2 = \left\{ \begin{pmatrix} 1 & & \\ & a & b \\ & c & d \end{pmatrix} \in SL_3(\mathbb{R}) \right\}, \quad N_2 = E_2 \cap J = \left\{ \begin{pmatrix} 1 & & \\ & 1 & t \\ & & 1 \end{pmatrix} : t \in \mathbb{R} \right\}.$$

In the notation of Lemma 3.11, for $i = 1, 2$, the natural isomorphism of E_i to E takes N_i isomorphically to N. Since v is fixed by N_i, applying Lemma 3.11 to $\rho|_{E_i}$, v is fixed by E_i. Since E_1 and E_2 generate a dense subgroup of $SL_3(\mathbb{R})$, by continuity v is fixed by $SL_3(\mathbb{R})$. Thus every representation of $SL_3(\mathbb{R})$ with almost-invariant vectors has a non-zero invariant vector, i.e. $SL_3(\mathbb{R})$ has Property (T). □

Shortly after Kazhdan's original paper, it was shown by Wang [34] that the proof generalizes to all simple Lie groups of rank at least 2. In particular

Theorem 3.12. *$SL_n(\mathbb{Z})$, $n \geq 3$, has Property (T).*

This yields the following families of expanders.

Example 3.13 ([2])**.** *It is well known that*

$$A_n = \begin{pmatrix} 1 & 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix} \text{ and } B_n = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ (-1)^{n-1} & 0 & 0 & \dots & 0 \end{pmatrix}$$

generate $SL_n(\mathbb{Z})$. Consequently, for every $n \geq 3$, $\mathcal{G}(SL_n(\mathbb{F}_p), \{A_n, B_n\}_p)$ form a family of expanders as p runs through all primes.

3.4 Expanders from $SL_2(\mathbb{Z})$ and Selberg's $\frac{3}{16}$ Theorem

Cayley graphs of certain quotients of $SL_2(\mathbb{Z})$ also form a family of expanders, but for a reason fundamentally different from that for $SL_n(\mathbb{Z})$, $n \geq 3$. In fact, we have

Proposition 3.14. *$SL_2(\mathbb{Z})$ does not have property (T).*

Proof. It is well known that $SL_2(\mathbb{Z})$ contains a free subgroup of finite index (e.g. $\langle \left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 2 & 1 \end{smallmatrix}\right) \rangle$), which surjects to $\mathbb{Z}$. The Proposition therefore follows from Theorem 3.9 and the following Lemmata. □

Lemma 3.15. *$\mathbb{Z}$ does not have Property (T).*

Proof. Consider the irreducible representations $\rho_n : \mathbb{Z} \to \mathbb{C}^\times = U(\mathbb{C})$ defined by $\rho_n(x) = e^{2\pi i x/n}$. Since $\rho_n(\pm 1) = e^{\pm 2\pi i/n}$ is rotation by angle $\pm\frac{2\pi}{n}$, for any $\epsilon > 0$ and $v \in \mathbb{C}$, we have $||\rho_n(\pm 1)v - v|| \leq \epsilon||v||$ for all large n. Since $\{\pm 1\}$ generates $\mathbb{Z}$, the Lemma follows by Proposition 3.2. □

Lemma 3.16. *Any homomorphic image of a Kazhdan group is Kazhdan.*

Proof. If $\varphi : G \to \varphi(G)$ is a continuous homorphism, any representation (H, ρ) of $\varphi(G)$ pulls back to a representation $(H, \rho \circ \varphi)$ of G. If G is Kazhdan with $\epsilon > 0$ and $K \subset G$, then since $\varphi(K)$ is again compact, $\varphi(G)$ is Kazhdan with the same ϵ and $\varphi(K)$. □

One nevertheless obtains expanders from $SL_2(\mathbb{Z})$ through Selberg's $\frac{3}{16}$ Theorem. We have already mentioned the analogy between compact Riemannian manifolds and finite graphs in the contexts of the Cheeger constant and the Laplacian. To understand how Selberg's $\frac{3}{16}$ Theorem relates to expanders, we must first make this connection more precise. The following rough treatment will suffice for our purpose; for more details, see [12].

As in the set-up of Property (τ), let G be a finitely generated group and $\mathcal{L} = \{N_i\}$ a family of finite-index normal subgroups of G. Suppose $G = \pi_1(M)$ for some compact Riemannian manifold M. Then G acts on the universal cover U of M, and $M = U/G$. Fix a compact fundamental domain D. It can be shown that we may choose a generating set S for G such that for every $s \in S$, D and $s \cdot D$ intersect in a "face" of D. For each $N_i \in \mathcal{L}$, there is a covering map $\varphi_i : U \to M/(G/N_i) = U/N_i$ to the corresponding finite-sheeted cover of M, and G/N_i acts on U/N_i with fundamental domain $\varphi_i(D)$. Let S_i be the natural projection of S to G/N_i. Then $\mathcal{G}(G/N_i, S_i)$ can be viewed naturally as a finite approximation of U/N_i: vertex gN_i corresponds to the translate $gN_i \cdot \varphi_i(D)$ of the fundamental domain, and two translates are connected if and only if they share a face. The following easy example should clarify the matter.

Example 3.17. *Consider $\mathbb{Z} = \pi(S^1)$. Then $\mathbb{Z}$ acts on the universal cover $\mathbb{R}$ by translation, with fundamental domain $[0, 1]$ and corresponding generators $\{\pm 1\}$. For every finite-index subgroup $n\mathbb{Z}$, the quotient $\mathbb{Z}/n\mathbb{Z}$ acts on the corresponding cover $\mathbb{R}/n\mathbb{Z}$ of $S^1 = \mathbb{R}/\mathbb{Z}$ by translation, with fundamental domain $[0, 1]/n\mathbb{Z}$. Then $\mathcal{G}(\mathbb{Z}/n\mathbb{Z}, \{\pm 1\})$ can be realized by associating each $a + n\mathbb{Z}$ with the translate $[a, a+1]/n\mathbb{Z}$ of the fundamental domain. Each $a+n\mathbb{Z}$ is adjacent to $(a \pm 1)+n\mathbb{Z}$; correspondingly, $[a, a + 1]/n\mathbb{Z}$ is connected to $[a + 1, a + 2]/n\mathbb{Z}$ and $[a - 1, a]/n\mathbb{Z}$, which share a "face" (endpoint) with $[a, a + 1]/n\mathbb{Z}$.*

This partition of the compact manifold U/N_i into translates of $\varphi_i(D)$ allows one to relate the Cheeger constant of U/N_i to that of its approximating Cayley graph. In particular

Theorem 3.18. *In the set-up above,* $\liminf_{i\to\infty} h(U/N_i) > 0$ *if and only if* $\liminf_{i\to\infty} h(\mathcal{G}(G/N_i, S_i)) > 0$. *Consequently, $\mathcal{G}(G/N_i, S_i))$ form a family of expanders if and only if* $\liminf_{i\to\infty} h(U/N) > 0$.

We apply this to the action of the modular group $SL_2(\mathbb{Z})$ on the (hyperbolic) upper half plane $\mathbb{H}$ by fractional linear transformations. It can be shown that the Laplacian $\Delta = -y^2(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2})$ is well defined on any quotient $\Gamma\backslash\mathbb{H}$ for a subgroup Γ of $SL_2(\mathbb{Z})$. Selberg proved a lower bound for $\lambda_1(\Gamma\backslash\mathbb{H})$ when Γ is a *congruence subgroup*, a finite-index subgroup of $SL_2(\mathbb{Z})$ containing $\ker(SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/m\mathbb{Z}))$ for some $m > 0$.

Theorem 3.19 (Selberg's $\frac{3}{16}$ Theorem [28])**.** *If Γ is a congruence subgroup of $SL_2(\mathbb{Z})$, then $\lambda_1(\Gamma\backslash\mathbb{H}) \geq \frac{3}{16}$.*

Selberg's proof relates the eigenvalues λ_j to *Kloosterman sums*, certain exponential sums that arise as the Fourier coefficients of modular forms. He then uses a bound by Weil on Kloosterman sums, which itself comes from the Riemann hypothesis for curves over a finite field, also proved by Weil. More specifically, Selberg forms a Dirichlet series Z whose coefficients are Kloosterman sums,

then cusp forms U_m with Fourier coefficients related to Z. Considering the Hilbert space of cusp forms in $L^2(\mathbb{H}, \frac{dxdy}{y^2})$ (the hyperbolic measure), Selberg rewrites U_m in the basis of eigenvectors for the self-adjoint operator Δ. The poles of these coefficients can be expressed in terms of the corresponding eigenvalues, thus relating λ_j to poles of U_m, and in turn to poles of Z. Now, Weil's result bounds the possible poles of Z, and hence bounds λ_j.

As an aside, Selberg's conjecture that the lower bound $\frac{1}{4}$ holds remains a fundamental open problem in the theory of the modular forms.

Selberg's $\frac{3}{16}$ Theorem together with Theorem 3.18 prove that $\mathcal{G}(SL_2(\mathbb{F}_p), S_p)$ form a family of expanders for any fixed finite generating set S of $SL_2(\mathbb{F}_p)$. In fact, similar considerations apply when $\langle S \rangle$ is merely a finite-index subgroup of $SL_2(\mathbb{F}_p)$. We therefore have

Theorem 3.20. *Let S be a finite subset of $SL_2(\mathbb{Z})$. If S generates a finite-index subgroup of $SL_2(\mathbb{Z})$, then $\mathcal{G}(SL_2(\mathbb{F}_p), S_p)$ form a family of expanders as p runs through all primes.*

3.5 Summary of Expander Property

The following theorem summarizes the equivalences among the various formulations of the expander property for Cayley graphs of quotients of finitely generated groups.

Theorem 3.21 (Theorem 4.3.2 in [22])**.** *Let G be a finitely generated group with a finite generating set S. Let $\mathcal{L} = \{N_i\}$ be a family of finite-index normal subgroups of G. Write S_i for the natural projection of S to G/N_i. The following are equivalent.*

(1) *$\mathcal{G}(G/N_i, S_i)$ form a family of expanders.*

(2) $\liminf_{i\to\infty} h(\mathcal{G}(G/N_i, S_i))$.

(3) $\liminf_{i\to\infty} \lambda_1(\mathcal{G}(G/N_i, S_i))$.

(4) *G has Property (τ) with respect to $\mathcal{L}$.*

If in addition $G = \pi(M)$ for a compact Riemannian manifold M with universal cover U, then the following are also equivalent to the conditions above.

(5) $\liminf_{i\to\infty} h(U/N_i) > 0$.

(6) $\liminf_{i\to\infty} \lambda_1(U/N_i) > 0$.

Proof. We have already proved or mentioned all the implications. (1) $\Leftrightarrow$ (2) was Proposition 2.3, a trivial consequence of the definitions of edge expansion and the Cheeger constant. (2) $\Leftrightarrow$ (3) and (5) $\Leftrightarrow$ (6) were the Cheeger-Buser inequality and its discrete analogue (Proposition 2.6). Extending this analogy between finite graphs and compact manifolds, we viewed the Cayley graphs $\mathcal{G}(G/N_i, S_i)$ as finite approximations of compact manifolds U/N_i and indicated that this leads to (2) $\Leftrightarrow$ (5) (Theorem 3.18). Finally, we recorded (1) $\Leftrightarrow$ (4) as Theorem 3.7, noting that the proof of the reverse implication for Property (T) (Theorem 3.3) in fact only required Property (τ). $\square$

4 Expansion in Linear Algebraic Groups

Given Theorem 3.20, a natural question, considered by Lubotzky and Weiss by the early 90s [22], is to determine the condition on a subset S of $SL_2(\mathbb{Z})$ under which $\mathcal{G}(SL_2(\mathbb{F}_p), S_p)$ form a family of expanders. Lubotzky captured the challenge in his "1-2-3 problem" [23]: do $\mathcal{G}(SL_2(\mathbb{F}_p), \{\left(\begin{smallmatrix}1 & i\\ 0 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}1 & 0\\ i & 1\end{smallmatrix}\right)\})$ form a family of expanders for $i = 1, 2, 3$? Selberg's theorem only applies to $i = 1, 2$; the subgroup $\langle \left(\begin{smallmatrix}1 & 3\\ 0 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}1 & 0\\ 3 & 1\end{smallmatrix}\right)\rangle$ does not have finite index in $SL_2(\mathbb{Z})$.

Although the 90s saw encouraging partial results towards this question, a breakthrough only began in 2005 with Helfgott's work [16], which incorporated tools of arithmetic combinatorics. In this section, we briefly discuss Helfgott's Triple Product result, summarize the key components of Bourgain and Gamburd's complete resolution of the question for $SL_2(\mathbb{F}_p)$ [4], and give a brief survey of recent generalizations.

4.1 Sum-Product Phenomenon and Helfgott's Triple Product Result

We have already noted that the expander property for Cayley graphs amounts to uniform growth of small subsets under multiplication by the generators. We therefore begin with a discussion of general results on such growth.

Arithmetic combinatorics studies combinatorial estimates associated with arithmetic operations such as addition and multiplication. A typical question is the following: For a finite subset A of some ring, what can be said about the sizes of $A+A := \{a+b : a, b \in A\}$ and $A \cdot A := \{ab : a, b \in A\}$? The last decade saw a number of developments in this field; for further details, see [32].

Of particular relevance to expanders is the so-called *sum-product phenomenon*. The earliest result of this type is the following, proved in 2004.

Theorem 4.1 (Sum-Product Phenomenon in $\mathbb{F}_p$, Bourgain, Katz, and Tao [9])**.** *Let A be a subset of a finite field $\mathbb{F}_p$, where p is prime. If $p^\delta < |A| < p^{1-\delta}$ for some $\delta > 0$, then $|A+A|+|A\cdot A| > c|A|^{1+\epsilon}$, where $c > 0$ and $\epsilon > 0$ depend only on δ.*

The condition $|A| > p^\delta$ was subsequently dropped by Bourgain, Glibichuk, and Konyagin [8]. Thus every subset of $\mathbb{F}_p$ that is not too large grows under either addition or multiplication with itself. Among other tools of arithmetic combinatorics, Helfgott's result uses a generalization of this sum-product phenomenon to arbitrary finite fields.

The following is Helfgott's main result, Triple Product expansion in $SL_2(\mathbb{F}_p)$.

Theorem 4.2 (Triple Product expansion in $SL_2(\mathbb{F}_p)$, Helfgott [16])**.** *Let p be a prime. Let A be a subset of $SL_2(\mathbb{F}_p)$ not contained in any proper subgroup. If $|A| < p^{3-\delta}$ for some fixed $\delta > 0$, then $|A \cdot A \cdot A| > c|A|^{1+\epsilon}$, where $c > 0$ and $\epsilon > 0$ depend only on δ.*

Helfgott's idea is to relate the growth of A to that of its trace set $\mathrm{tr}(A) = \{\mathrm{tr}(a) : a \in A\}$, then apply a sum-product result to $\mathrm{tr}(A)$. Very roughly, his argument proceeds as follows. If some A violates the theorem, then A must have high "multiplicative structure." In particular, A intersects many conjugacy classes, from which it can be shown that it contains many simultaneously diagonalizable elements. Non-expansion then yields a contradiction with a sum-product theorem.

4.2 Expansion in $SL_2(\mathbb{F}_p)$

Starting with Helfgott's result, Bourgain and Gamburd provided a necessary and sufficient condition on a finite symmetric subset S of $SL_2(\mathbb{Z})$ under which $\mathcal{G}(SL_2(\mathbb{F}_p), S_p)$ form a family of expanders: that S generates a Zariski-dense subgroup of $SL_2(\mathbb{Z})$, a much weaker condition than generating a finite-index subgroup [4]. They deduced this as a result of the following quantitative result.

Theorem 4.3 (Bourgain and Gamburd, Theorem 3 in [4])**.** *Fix $k \geq 2$ and $\tau > 0$. For each prime p, suppose that S_p with $|S_p| = 2k$ is a symmetric generating set for $SL_2(\mathbb{F}_p)$ such that*

$$\operatorname{girth}(\mathcal{G}(SL_2(\mathbb{F}_p), S_p)) \geq \tau \log_{2k} p.$$

Then $\mathcal{G}(SL_2(\mathbb{F}_p), S_p)$ form a family of expanders as p runs through all primes.

The *girth* of a graph is the length of a shortest closed path.

Let $\mu_{S_p} = \frac{1}{|S_p|} \sum_{g \in S_p} \delta_g$. Then as we saw in Section 2.4, the expander property is equivalent to a spectral gap $\lambda_1 \leq c < 1$, uniform in p, for the convolution operator $*\mu_{S_p}$ on $L^2(SL_2(\mathbb{F}_p))$. Bourgain and Gamburd exhibit this spectral gap using an idea of Sarnak and Xue [27], by bounding the trace of $*\mu_{S_p}^{(2l)}$. More precisely, recall that $*\mu_{S_p}$ is the averaging operator $\frac{1}{2k}A$, where A is the adjacency matrix of $\mathcal{G}(SL_2(\mathbb{F}_p), S_p)$. Since A is given as the sum of the values of the regular representation of $SL_2(\mathbb{F}_p)$ at the generators, a result of Frobenius, which states that non-trivial irreducible representations of $SL_2(\mathbb{F}_p)$ have dimension at least $\frac{p-1}{2}$, provides a lower bound for the multiplicity of λ_1. In particular, $\frac{p-1}{2}\lambda_1^{2l} \leq \sum \lambda_j^{2l}$. On the other hand, the trace equals $|SL_2(\mathbb{F}_p)|\mu_{S_p}^{(2l)}(1)$ and, by the symmetry of μ_{S_p}, $\mu_{S_p}^{(2l)}(1) = \sum_{g \in G} \mu_{S_p}^{(l)}(g)\mu_{S_p}^{(l)}(g^{-1}) = \sum_{g \in G}(\mu_{S_p}^{(l)}(g))^2 = ||\mu_{S_p}^{(l)}||_2^2$. Thus

$$\frac{p-1}{2}\lambda_1^{2l} < |SL_2(\mathbb{F}_p)|||\mu_{S_p}^{(l)}||_2^2.$$

This reduces the problem to showing that for any $\epsilon > 0$, there exists $C(\epsilon, \tau) > 0$ such that $||\mu_{S_p}^{(l)}||_2 < |SL_2(\mathbb{F}_p)|^{-1/2+\epsilon}$ for all $l \geq C(\epsilon, \tau) \log_{2k} p$. Indeed, then $\lambda_1^{2l} \ll p^{-1}|SL_2(\mathbb{F}_p)|^{2\epsilon}$, and taking $l = C(\epsilon, \tau) \log_{2k} p$ yields a spectral gap independent of p.

For any probability measure μ on $SL_2(\mathbb{F}_p)$, we have $||\mu||_2 \geq |SL_2(\mathbb{F}_p)|^{-1/2}$, with equality when μ is uniform. Thus the goal is to show that μ_{S_p} convolved with itself approaches uniform distribution at a fast enough rate independent of p. Bourgain and Gamburd showed this in two steps: *escape from proper subgroups* and *ℓ^2-flattening*.

Proposition 4.4 (Escape from proper subgroups, Bourgain and Gamburd [4])**.** *In the situation of Theorem 4.3, let $l_0 = \lfloor \frac{1}{2}\tau \log_{2k} p \rfloor - 1$. Then there exists some $\epsilon < \frac{3\tau}{16}$ such that the following holds: For all $l \geq l_0$,*

$$\mu^{(l)}(gH) < [SL_2(\mathbb{F}_p) : H]^{-\epsilon}$$

for any $g \in SL_2(\mathbb{F}_p)$ and proper subgroup $H < SL_2(\mathbb{F}_p)$.

That is, after l_0 steps, the random walk does not accumulate in any coset of any proper subgroup.

The proof makes use of two observations. First, the girth condition implies that, for words of length up to l_0, the Cayley graph $\mathcal{G}(SL_2(\mathbb{F}_p), S_p)$ is isomorphic to that of the free group on k letters. Kesten's classical result on random walk on a regular tree [20] then gives an upper bound on the value of $\mu^{(l_0)}$ at any vertex. Second, by the classification of subgroups of $SL_2(\mathbb{F}_p)$, due to Dickson [29], if H is a proper subgroup of $SL_2(\mathbb{F}_p)$ and $|H| > 60$, then H is solvable: in fact, $[[g_1, g_2], [g_3, g_4]] = 1$ for all $g_i \in H$.

The proof proceeds by contradiction. If the condition fails for some l, then it follows that in fact $\mu_S^{(l_0)}(g_0 H) > p^{-\epsilon/2}$ for some $g_0 \in SL_2(\mathbb{F}_p)$ and so $\mu_S^{(2l_0)}(H) > p^{-\epsilon}$. Combined with Kesten's result, this implies that the number of words in H of length l_0 is exponential in l_0. Meanwhile, the vanishing of the second commutators implies, by a combinatorial argument, that this number is in fact at most polynomial in l_0, providing the desired contradiction.

Proposition 4.5 (ℓ^2-flattening, Bourgain and Gamburd [4]; treatment by Varjú [33])**.** *For any $\epsilon > 0$, there is some $\delta > 0$ such that the following holds: If μ is a probability measure on $SL_2(\mathbb{F}_p)$ satisfying*

$$||\mu||_2 > |SL_2(\mathbb{F}_p)|^{-1/2+\epsilon} \text{ and } \mu(gH) < [SL_2(\mathbb{F}_p) : H]^{-\epsilon}$$

for any $g \in SL_2(\mathbb{F}_p)$ and proper subgroup $H < SL_2(\mathbb{F}_p)$, then for any probability measure ν,

$$||\mu * \nu||_2 < ||\mu||_2^{1/2+\delta} ||\nu||_2^{1/2}.$$

This is exactly what we wanted: assuming escape from proper subgroups, convolution with μ brings any measure closer to uniform distribution at a rapid rate independent of p. The proof assumes that $||\mu * \nu||_2 > ||\mu||_2^{1/2+\delta} ||\nu||_2$ for any $\delta > 0$ and obtains a lower bound on some $\mu(gH)$, contradicting escape. By proving the same inequality for dyadic level-set approximations $\tilde{\mu}$, $\tilde{\nu}$ of μ, ν, one produces level sets A and B with high *multiplicative energy*, roughly indicating common multiplicative structure. By an arithmetic combinatorial result of Tao [31], this implies that some symmetric set S close to both A and B is an *approximate group*; although not closed like an actual group, S grows under multiplication in a controlled way. Then $S \cdot S \cdot S$ does not grow, hence lies in a proper subgroup H by Helfgott's Triple Product expansion. The inequality $||\mu * \nu||_2 > ||\mu||_2^{1/2+\delta} ||\nu||_2$ then provides a lower bound on some $\mu(gS)$, and hence on $\mu(gH)$, as desired.

Theorem 4.3 now follows as a consequence of these Propositions. Given $\epsilon > 0$, we are done if $||\mu_{S_p}^{(l)}|| < |SL_2(\mathbb{F}_p)|^{-1/2+\epsilon}$ already for $l = l_0$, i.e. if $\mu_{S_p}^{(l_0)}$ is already close to uniform distribution. Otherwise, since escape holds for $l \geq l_0$, convolving $\mu_{S_p}^{(l)}$ with itself rapidly decreases the norm, reaching $|SL_2(\mathbb{F}_p)|^{-1/2+\epsilon}$ in finitely many steps independent of p.

4.3 Survey of Recent Results

Several generalizations followed Bourgain and Gamburd's result for $SL_2(\mathbb{Z}/p\mathbb{Z})$: for $SL_2(\mathbb{Z}/n\mathbb{Z})$, n square-free, by Bourgain, Gamburd, and Sarnak [7], and $SL_2(\mathbb{Z}/p^n\mathbb{Z})$ by Bourgain and Gamburd [5]. In each case, the necessary and sufficient condition is that S generates a Zariski-dense subgroup.

These generalizations all required a suitable Triple Product result. In this direction, the case $SL_3(\mathbb{F}_p)$ was handled by Helfgott himself [17], and in 2010, Breuillard, Green, and Tao [11] and Pyber and Szabó [25] independently proved a Triple Product result for all finite simple groups of Lie type.

As in $SL_2(\mathbb{F}_p)$, this Triple Product result has led to correspondingly general results on expanders. Sufficient conditions for expanders were obtained for $SL_d(\mathbb{Z}/q\mathbb{Z})$, q arbitrary, by Bourgain and Varjú [10], and for square-free quotients of $SL_n(\mathcal{O}_K)$, K any number field, by Varjú [33]. Salehi Golsefidy and Varjú [26] recovered an exact characterization for square-free quotients: for a finite subset $S \subset GL_n(\mathbb{Q})$, Cayley graphs of square-free quotients of $\langle S \rangle$ form a family of expanders if and only if the connected component of the Zariski closure of $\langle S \rangle$ is perfect, i.e. equals its own commutator subgroup. Such expanders arising from square-free quotients have applications to affine sieve methods in number theory; see [7] by Bourgain, Gamburd, and Sarnak for the case $SL_2(\mathbb{Z}/n\mathbb{Z})$, n square-free.

The proofs of these generalizations still use Sarnak and Xue's idea and bound the trace from above using escape from proper subgroups and ℓ_2-flattening. For the latter, the argument for $SL_2(\mathbb{F}_p)$ generalizes given a corresponding Triple Product result. However, the original argument for escape relied crucially on the structure of $SL_2(\mathbb{F}_p)$, and generalizations have required completely new approaches.

5 Diameter of Cayley Graphs of $SL_2(\mathbb{F}_p)$

We end with an open problem that may be approached separately from the rest of the theory.

Proposition 5.1. *If k-regular graphs X_i form a family of expanders, then* $\operatorname{diam}(X_i) = \Theta(\log |X_i|)$, *where the constants depend only on k and the expansion constant c.*

Proof. Fix some $X = X(V, E)$ in this family, and let $a, b \in V$. Let A_d be the set of vertices with distance at most d from a, and let $d(a)$ be the smallest positive integer for which $|A_{d(a)}| > \frac{|X|}{2}$. The choice of $d(a)$ and edge expansion imply $\frac{|X|}{2} \geq |A_{d(a)-1}| \geq \cdots \geq (c+1)^{d(a)-1}|A_0| = (c+1)^{d(a)-1}$, so $d(a) \leq \log_{c+1} \frac{|X|}{2} + 1$. If we similarly define B_d and $d(b)$ for b, then $A_{d(a)}$ and $B_{d(b)}$ must overlap, so $\operatorname{dist}(a, b) \leq d(a) + d(b) \leq 2(\log_{c+1} \frac{|X|}{2} + 1)$. Since a and b were arbitrary, this shows $\operatorname{diam}(X) = O(\log |X|)$.

On the other hand, there is 1 vertex at distance 0 from a, k at distance 1, and at most $k(k-1)^{d-1} < k^d$ at distance d. Hence $|X| < \sum_{d=0}^{\operatorname{diam}(X)} k^d < k^{\operatorname{diam}(X)+1}$, so $\operatorname{diam}(X) > \log_k |X| - 1$. □

For fixed $n \geq 2$, if $\mathcal{G}(SL_n(\mathbb{F}_p), S_p)$ form a family of expanders as p runs through all primes, then this Proposition implies that $\operatorname{diam}(\mathcal{G}(SL_n(\mathbb{F}_p), S_p)) = \Theta(\log |SL_n(\mathbb{F}_p)|) = \Theta(\log p)$. However, the proof provides no fast algorithm (say polynomial time in $\log p$) that expresses a given element as word of length $O(\log p)$ in the generators. For $n \geq 3$, Kassabov and Riley have shown the even stronger result that $\operatorname{diam}(SL_n(\mathbb{Z}/k\mathbb{Z})) = O(n^2 \log k)$ by exhibiting such an algorithm [18]. However, there is no known analogue for $SL_2(\mathbb{F}_p)$.

Problem 5.2. *Does there exist a polynomial-time (in* $\log p$*) algorithm that expresses a given element of* $SL_2(\mathbb{F}_p)$ *as a word of length* $O(\log p)$ *in* $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$ *and* $\left(\begin{smallmatrix}1 & 0\\ 1 & 1\end{smallmatrix}\right)$*?*

The best known result is a probabilistic algorithm due to Larson, with the following property.

Theorem 5.3 (Larsen [21])**.** *There exist absolute constants* $c_1, c_2 > 0$ *such that the following holds: for any* $\epsilon > 0$*, there exists* $c(\epsilon) > 0$ *such that for any element of* $SL_2(\mathbb{F}_p)$ *for any prime* p*, the algorithm will find a word of length* $\leq c_1 \log p \log\log p$ *in time* $\leq c(\epsilon)\log^{c_2} p$ *with probability* $\geq 1-\epsilon$*.*

There is no fast deterministic algorithm in the literature, even for expressing an element as a word of polylogarithmic length.

References

[1] N. Alon, *Eigenvalues and expanders*, Combinatorica **6** (1986), 83–96.

[2] N. Alon and V. D. Milman, λ_1*, isoperimetric inequalities for graphs and superconcentrators*, J. Comb. Th. **B 38** (1985), 78–88.

[3] B. Bekka, P. de la Harpe, and A. Valette, *Kazhdan's Property (T)*, *New Mathematical Monographs* **11**, Cambridge Univ. Press, Cambridge, 2008.

[4] J. Bourgain and A. Gamburd, *Uniform expansion bounds for Caley graphs of* $SL_2(\mathbb{F}_p)$, Ann. of Math. **167** (2008), 625–642.

[5] ———, *Expansion and random walks in* $SL_d(\mathbb{Z}/p^n\mathbb{Z})$*:I*, J. Eur. Math. Soc. **10** (2008), 987–1011.

[6] ———, *Expansion and random walks in* $SL_d(\mathbb{Z}/p^n\mathbb{Z})$*:II* with an appendix by J. Bourgain, J. Eur. Math. Soc. **11** (2009), 1057–1103.

[7] J. Bourgain, A. Gamburd, and P. Sarnak, *Affine linear sieve, expanders, and sum-product*, Invent. Math. to appear.

[8] J. Bourgain, A. Glibichuk, and S. Konyagin, *Estimates for the number of sums and products and for exponential sums in elds of prime order*, J. London Math. Soc. (2) **73** (2006), no. 2, 380–398.

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

[10] J. Bourgain, P. P. Varjú, *Expansion in* $SL_d(\mathbb{Z}/q\mathbb{Z})$*, q arbitrary*, preprint.

[11] E. Breuillard, B. Green, and T. Tao, *Approximate subgroups of linear groups*, preprint.

[12] R. Brooks, *The spectral geometry of a tower of coverings*, J. of Diff. Geom. **23** (1986), 97–107.

[13] P. Buser, *A note on the isoperimetric constant*, Ann. Sci. École Norm. Sup. (4) **15** (1982), no. 2, 213–230.

[14] J. Dodziuk, *Difference equations, Isoperimetric inequality and transcience of certain random walks*, Trans. A.M.S. **284** No. 2. (1984), 787–794.

[15] J. M. G. Fell, *Weak containment and induced representations of groups*, Canadian J. Math. **14** (1962), 237–268.

[16] H. Helfgott, *Growth and generation in $SL_2(\mathbb{Z}/p\mathbb{Z})$*, Ann. of Math. **167** (2008), 601–23.

[17] ———, *Growth in $SL_3(\mathbb{Z}/p\mathbb{Z})$*, J. Eur. Math. Soc. **13** (2009), no. 3, 651–851.

[18] M. Kassabov and T. R. Riley, *Diameters of Cayley Graphs of $SL_n(\mathbb{Z}/k\mathbb{Z})$*, preprint.

[19] D. A. Kazhdan, *On the connection of the dual space of a group with the structure of its closed subgroups*, Funct. Anal. Appl. **1** (1967): 63-65.

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

[21] M. Larsen, *Navigating the Cayley Graphs of $SL_2(\mathbb{F}_p)$*, International Mathematics Research Notices (2003), No. 27, 1465–1471.

[22] A. Lubotzky, *Discrete Groups, Expanding Graphs and Invariant Measures*, *Progress in Math.* **125**, Birkhäuser, Basel, 1994.

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

[24] G. A. Margulis, *Explicit constructions of concentrators*, Probl. of Inform. Transm. **10** (1975), 325–332.

[25] L. Pyber and E. Szabó, *Growth in finite simple groups of Lie type of bounded rank*, preprint.

[26] A. Salehi Golsefidy and P. P. Varjú, *Expansion in perfect groups*, preprint.

[27] P. Sarnak and X. X. Xue, *Bounds for multiplicities of automorphic representations*, Duke Math. J. **64** no. 1, (1991), 207–227.

[28] A. Selberg, *On the Estimation of Fourier Coefficients of Modular Forms*, Proc. Symp. Pure Math., VIII, Amer. Math. Soc. (1965), 1-15.

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

[30] R. M. Tanner, *Explicit concentrators from generalized N-gons*, SIAM J. Alg. Discr. Meth. **5** (1984), 287–294.

[31] T. Tao, *Product set estimates for non-commutative groups*, Combinatorica **28** (5) (2008), 547–594.

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

[33] P. P. Varjú, *Expansion in $SL_d(\mathcal{O}_K/I)$, I square-free*, preprint: http://arxiv.org/abs/1001.3664

[34] S. P. Wang, *The dual space of semi-simple Lie groups*, Amer. J. Math. **91** (1969), 921–937.