Random Walks on $SL_2(\mathbb{F}_p) \times SL_2(\mathbb{F}_p)$

Based on joint work with Prof. Alireza Salehi Golsefidy

Srivatsa Srinivas

University of California, San Diego

December 2, 2024

What is an expander graph?

Definition: Expander Graph

A (c, k) **expander graph** is a graph $G = (V, E)$ such that for all v we have that $\deg(v) \leq k$ and for all $A \subset V$ such that $|A| < |V|/2$ we have that $\partial A \geq c|A|$, where

$$\partial A := \{y \in V \setminus A \,|\, \exists x \in A \text{ s.t } (x, y) \in E\}$$

Why do they matter?

- If $k \ll |V|$ then these graphs are sparse
- If $c > 0$, then these graphs are very well connected; the diameter of the graph is at most $\frac{2\log|V|}{\log(1+c)}$ They have many applications in

Example application of Expander Graphs

Using expander graphs as randomness-amplifiers:

- Suppose that (G, V) is a (c, k) expander graph (think of the vertices $v \in V$ being a random seed). Let X be a finite set and let $p : X \to \{T, F\}$ be a predicate
- We say that $f : X \times V \to \{T, F\}$ predicts p if for every $x \in X$ we have that $\mathbb{P}(f(x, U_V) \neq p(x)) \leq 1/3$, where U_V is the uniform random variable valued in V.
- Let f predict p. For any $d < |V|/2$ we have that there is a function $g : X \times V \to \{T, F\}$ that requires only $\Theta_{c,k}(d)$ computations of f such that
$$\mathbb{P}(g(x, U_v) \neq p(x)) \leq \Theta_{c,k}(1/d)$$
- Many more can be found in "Expander Graphs and Their Applications" by Wigderson, Linial and Hoory [HLW06]

Where is the linear algebra?

- Let $G = (V, E)$ be a k-regular graph, with adjacency matrix A. Let G be connected. We note that if $\frac{1}{k}A\phi = \phi$, where $\phi \in \mathbb{C}^{|V|}$, then $\phi = c1_V$, where 1_V is the constant vector with all entries being 1. (Hint: Consider the $v \in V$ at which ϕ has largest magintude and then use the fact that $\phi(v)$ is an average of ϕ across it's neighbours)
- Therefore 1 is the largest eigenvalue with unique eigenvector.

Definition: $\lambda(G)$

We define $\lambda(G)$ to be the second-largest eigenvalue of $\frac{1}{k}A$.

Here is the linear algebra

Definition: $h(G)$

For any graph $G = (V, E)$, we define

$$h(G) = \min_{\substack{S \subset V \\ |S| < |V|/2}} |\partial S| / |S|$$

- We have that

$$\frac{1 - \lambda(G)}{2} \leq h(G) \leq \sqrt{2(1 - \lambda(G))}$$

  The left-hand inequality follows from considering $\langle 1_S, \frac{1}{k} A 1_S \rangle$, and the right-hand side is non-trivial. There are four good proofs in [Fan Chung]

- Obviously, every k-regular graph, G, is a $(h(G), k)$ expander graph.
- We have successfully added linear algebra to expander graphs

What if I throw in groups?

Definition: Cayley Graph for the purposes of this talk

Given a group H and a generating S we define the Cayley Graph for the purpose of this talk to be the graph $\mathrm{Cay}(H, S) = (V, E)$ where

$$V = H, E = \{(x, gx) \mid (x, g) \in H \times (S \cup S^{-1})\}$$

- Basically it is the graph whose vertices are the group elements H and whose edges are pairs of elements that are only "one generator away".
- Note that $\mathrm{Cay}(H, S)$ is $|S \cup S^{-1}|$-regular
- Now we have the obvious question, what can we say about $h(G)$ when $G = \mathrm{Cay}(H, S)$?

It depends on the group and the generating set

- (Alon-Roichman) If G is any finite group and S is a uniform random subset of G of size $\Theta(\log |G|)$ then we have that $\lambda(\mathrm{Cay}(G, S)) < 1/2$ with high probability (around $1 - 1/|G|$). [LR04]
- If $G = \mathbb{Z}/q\mathbb{Z}^n$ and $|S| = n$ then

$$\lambda(\mathrm{Cay}(G, S)) = \cos(1/q)^n$$

- Using representation theory we can say that if $S = \left\{ \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \right\}$ then we have that for all $p > 0$

$$\lambda(\mathrm{Cay(G, S)}) \leq \frac{3}{4} + \frac{1}{4}\left(1 - \frac{1}{42\sqrt{2} + 480}\right)$$

[Kas05]

Expander families and why we like non-Abelian groups

Definition: Expander Family

We say that a family of graphs $(G_i)_{i \in I}$ is a (c, k) **expander family** of graphs if for all $i \in I$, G_i is a (c, k) expander graph.

- A theorem of Weiss and Lubotzky states the following. If $(G_i, S_i)_{i \in I}$ is an infinite family of $(\mathrm{Group}, \mathrm{GeneratingSet})$ where there exists n such that for all $i \in I$ we have that $\mathrm{SolvabilityIndex}(G_i) \leq n$ then $\mathrm{Cay}(G_i, S_i)$ is not a (c, k) expander family for any $c > 0$. [LW92]
- This is because there are too many relations in groups of bounded solvability index.

Lubotzky's 1-2-3

- Alexander Lubotzky in 1993 stated the following interesting problem. Let

$$S_l = \left\{ \begin{bmatrix} 1 & l \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ l & 1 \end{bmatrix} \right\}$$

and let

$$P(l) := \mathrm{Cay}(SL_2(\mathbb{Z}/p\mathbb{Z}), S_l)_{p \in \mathrm{Primes}} \text{ is an expander family}$$

We know that since S_1, S_2 generate finite index subgroups of $SL_2(\mathbb{Z})$, by representation theory, we have that $P(1), P(2)$ are true. S_3 does not generate a finite index subgroup of $SL_2(\mathbb{Z})$, is it true that $P(3)$? **[L1994]**

The Bourgain-Gamburd method

- This problem went unsolved for 12 years and stuck with Gamburd for that time, until him and Bourgain bumped into each other on the IAS campus at 3AM. Bourgain was working at methods in additive combinatorics at the time. And by just combining their joint knowledge of the problem, they solved the problem that night.
- The idea is the following. Consider the random variable X into $G_p = SL_2(\mathbb{F}_p)$ that takes values uniformly in the set $S \cup S^{-1}$ where S is a generating set. Let X_k be the product of k i.i.d copies of X.Then, if there exists a α, β such that for every subgroup $H \subset G_p$

$$\mathbb{P}(X_{\alpha \log p} \in H) \leq (|H|/|G|)^{\beta}$$

Then we have that $\lambda(\mathrm{Cay}(G, S)) = e^{-\Theta_{\alpha,\beta}(1)}$ [BG08a]

Is $SL_2(\mathbb{F}_p)$ special?

- After analyzing some group theory, we deduce that if X takes uniform random values in $S_3 \cup S_3^{-1}$ then X satisfies the above property with an α, β that does not depend on p and so $P(3)$ is true
- The above method depends heavily on two results for $G_p = SL_2(\mathbb{F}_p)$
    1. (Bounded Generation, Helfgott) If $A \subset G_p$ generates G_p and $|A| \geq |G_p|^\delta$ then $\prod_{\Theta(1/\delta)} A = G_p$ [Hel08]
    2. (Quasirandomness, Sarnak and Xue) Every non-trivial representation of G_p has dimension at least $|G_p|^{\Theta(1)}$ [SX91]
- The above two items in group theory speak mean that your group is far, far away from being Abelian.
- Okay, but there are actually a lot of groups that satisfy those two properties. [BGT11]

A Mantra

If X is a symmetric random variable into a sufficiently non-abelian group, G, then $\lambda(\mathrm{Cay}(G, \mathrm{Range}(X)))$ only depends on the rate at which the random walk induced by X escapes subgroups, i.e the α, β such that for all subgroups $H \subset G$

$$\mathbb{P}(X_{\alpha \log |G|} \in H) \leq (|H|/|G|)^{\beta}$$

A productive and lucrative industry

The following are all extremely non-trivial results that use the ideas of the Bourgain-Gamburd method on various groups to solve many problems in Algebra and Number Theory

[BG08a] Jean Bourgain and Alex Gamburd. "Uniform expansion bounds for Cayley graphs of". In: *Annals of Mathematics* (2008), pp. 625–642.

[BGS10] Jean Bourgain, Alex Gamburd, and Peter Sarnak. "Affine linear sieve, expanders, and sum-product". In: *Inventiones mathematicae* 179.3 (2010), pp. 559–644.

[BG08b] Jean Bourgain and Alex Gamburd. "On the spectral gap for finitely-generated subgroups of SU (2)". In: *Inventiones mathematicae* 171 (2008), pp. 83–121.

A productive and lucrative industry

[BG12] Jean Bourgain and Alex Gamburd. "A spectral gap theorem in SU.(d).". In: *Journal of the European Mathematical Society (EMS Publishing)* 14.5 (2012).

[BV12] Jean Bourgain and Péter P Varjú. "Expansion in SL d (Z/q Z), q arbitrary". In: *Inventiones mathematicae* 188 (2012), pp. 151–173.

[GV12] Alireza Salehi Golsefidy and Péter P Varjú. "Expansion in perfect groups". In: *Geometric and functional analysis* 22.6 (2012), pp. 1832–1891.

[SS13] Alireza Salehi Golsefidy and Peter Sarnak. "The affine sieve". In: *Journal of the American Mathematical Society* 26.4 (2013), pp. 1085–1105.

[BK14] Jean Bourgain and Alex Kontorovich. "On Zaremba's conjecture". In: *Annals of Mathematics* (2014), pp. 137–196.

A productive and lucrative industry

[Gol19] Alireza Salehi Golsefidy. "Super-approximation, II: the p-adic case and the case of bounded powers of square-free integers.". In: *Journal of the European Mathematical Society (EMS Publishing)* 21.7 (2019).

The affine group

- We define $SL_n(\mathbb{F}_p) \ltimes \mathbb{F}_p^n$ as the group with the law

$$(A, v)(B, w) = (AB, Aw + v)$$

  We have that the map $\pi_\theta : SL_n(\mathbb{F}_p) \ltimes \mathbb{F}_p^n \to SL_n(\mathbb{F}_p)$ given by $(A, w) \mapsto A$ is a homomorphism
- We note that if $A \subset SL_n(\mathbb{F}_p) \ltimes \mathbb{F}_p^n$ is such that $\pi_\theta(A)$ generates $SL_n(\mathbb{F}_p)$, then either the group generated by A fixes a vector of $\mathbb{F}_p^n$ or the group generated by A is all of $SL_n(\mathbb{F}_p) \ltimes \mathbb{F}_p^n$

Expansion as a Algebraic Property

While solving a more difficult problem concerning random walks on $SO_n(\mathbb{R}) \ltimes \mathbb{R}^n$, Varju and Lindenstrauss proved the following theorem as a toy project:

Theorem 1 [LV16]

There exists a universal constant K_2 such that the following is true: Let S_p be a symmetric generating set of $G_p = SL_n(\mathbb{F}_p) \ltimes \mathbb{F}_p^n$. Let $H_p = SL_n(\mathbb{F}_p)$. Then we have that on setting $\alpha = (|S| - 1)/|S|$

$$-\log(\lambda(\mathrm{Cay}(G_p, S))) \geq \frac{1}{K_2} \min\left\{ \frac{-\log \lambda(\mathrm{Cay}(H_p, \pi_\theta(S))}{\min\{-\log(\alpha^{1/2} - \alpha), 100\}}, -\log \alpha \right\}$$

Algebraic Impetus

- The above result implies that $(\mathrm{Cay}(G_p, S_p))_{p \in \mathrm{Primes}}$ is an expander family if and only if $(\mathrm{Cay}(H_p, \pi_\theta(S_p)))_{p \in \mathrm{Primes}}$ is an expander family.
- The way they show this is by showing that if X is a uniform random variable into S_p, and v_0 is a vector in $\mathbb{F}_p^n$ then we there exists α, β that only depend on $|S_p|, \lambda(\mathrm{Cay}(H_p, \pi_\theta(S_p)))$ such that

$$\mathbb{P}(X_{\alpha \log p} \cdot v_0 = v_0) \leq \frac{1}{p^{n\beta}}$$

- By the Bourgain-Gamburd method, we are done; since we know that the projection of S_p to H_p escapes every subgroup of H_p quickly, we know that the only subgroups that X can "get stuck in" are those subgroups of G_p which fix a vector of $\mathbb{F}_p^n$. The previous point says that we escape such subgroups.

A conjecture

- Along similar lines, Lindenstrauss and Varju conjectured that the following should be true too

Open Problem 1.1 [LV16]

Let $G_p = H_p \times H_p$ where $H_p = SL_2(\mathbb{F}_p)$. Then we have that $(\mathrm{Cay}(G_p, S_p))_{p \in \mathrm{Primes}}$ is an expander family if and only if $(\mathrm{Cay}(H_p, \pi_L(S_p)))_{p \in \mathrm{Primes}}$ and $(\mathrm{Cay}(H_p, \pi_R(S_p)))_{p \in \mathrm{Primes}}$ are expander families.

- We know the following. If $A \subset G_p$ is a subset such that $\pi_L(A) = \pi_R(A) = H_p$ then either the subgroup generated by the A is all of G_p or is the graph of an automorphism from H_p to H_p
- By the Bourgain-Gamburd method all we have to prove in order to show the above conjecture is that random variables into G_p that escape $1 \times H_p$, $H_p \times 1$ quickly and generate G_p, also escape every graph quickly.

A Solution

Theorem 1, [GS24]

There exists a universal constant K_2 such that the following is true: Let S_p be a symmetric generating set of $G_p = SL_2(\mathbb{F}_p) \times SL_2(\mathbb{F}_p)$, $H_p = SL_2(\mathbb{F}_p)$ and let $\pi_L, \pi_R : SL_2(\mathbb{F}_p) \to SL_2(\mathbb{F}_p)$ be the projections onto the left and right factors of G_p. Then we have that on setting $\alpha = (|S| - 1)/|S|$

$$-\log(\lambda(\mathrm{Cay}(G_p, S)))) \geq \frac{1}{K_2} \min \left\{ \frac{-\log \lambda(\mathrm{Cay}(H_p, \pi_L(S))}{\min\{-\log(\alpha^{1/2} - \alpha), 100\}}, \right. \\ \left. -\log \alpha, \frac{-\log \lambda(\mathrm{Cay}(H_p, \pi_R(S)))}{\min\{-\log(\alpha^{1/2} - \alpha), 100\}} \right\}$$

Renyi Entropy

Definition: Renyi Entropy

Given a random variable X into a finite group G, with distribution μ we define the Renyi entropy of X as

$$H_2(X) = -\log\left(\sum_{g\in G}\mu(g)^2\right)$$

The special ingredient

The special ingredient that we brought to the table was the following: Let G be a finite group that acts on another finite group H. Let X be a random variable into G and Y a random variable into H. If $X^{(j)}$ are i.i.d and $Y^{(j)}$ are i.i.d where $i \in \{1, 2\}$ then we have that

$$H_2((X^{(1)} \cdot Y^{(1)})(X^{(2)} \cdot Y^{(2)})^{-1}) \geq H_2((X^{(1)} \cdot Y^{(1)})(X^{(1)} \cdot Y^{(2)})^{-1})$$

Lindenstrauss and Varju, implicitly used the above inequality in their work, but their proof only proved the inequality in the case that H was Abelian. Luckily enough, the above inequality boiled down to a clever application of Cauchy-Schwarz.

The recipe

We let $G_p = SL_2(\mathbb{F}_p) \times SL_2(\mathbb{F}_p)$ act on $H_p = SL_2(\mathbb{F}_p)$ by $(x, y) \cdot g = xgy^{-1}$. We note that the subgroup of G_p that fixes an element h of H_p is exactly the graph (g, hgh^{-1}). Let $X = (X_L, X_R)$ be a random variable into G_p. Let Y be a random variable into H_p. Then we have that

$$
\begin{aligned}
& H_2((X^{(1)} \cdot Y^{(1)})(X^{(2)} \cdot Y^{(2)})^{-1}) \geq H_2((X^{(1)} \cdot Y^{(1)})(X^{(1)} \cdot Y^{(2)})^{-1}) \\
& = H_2((X_L^{(1)} Y^{(1)} X_R^{(1)})(X_L^{(1)} Y^{(2)} X_R^{(1)}))^{-1}) \\
& = H_2(X_L^{(1)} Y^{(1)} (Y^{(2)})^{-1} (X_L^{(1)})^{-1})
\end{aligned}
$$

But we actually have a lot of information about the random variable $X_L^{(1)}$; namely we know that it's range generates the group with a bounded second-largest eigenvalue. We use this information, along with the above inequality to prove that you cannot get stuck in a graph

A lot of bounty

- The above result was published in the Journal of the European Mathematical Society this year, with a generalization getting into TAMS.
- Using analogues of the above inequality, along with other recent progress in the field [HD22] we have (hopefully), as a corollary, solved the Super-Strong Approximation conjecture for $\mathbb{N}$, which was one of the main problems posited at an MSRI meeting whose results were published in 2014 called Thin Groups and Super-Strong Approximation. The conjecture had been floating around since the early 2000's.
- The above work is very technical and has taken a lot of non-trivial ideas (including coming up with a new-inequality) in order to complete. We should finish typing it up by the end of the academic year.

References

[HLW06] Shlomo Hoory, Nathan Linial, and Avi Wigderson. "Expander graphs and their applications". In: *Bulletin of the American Mathematical Society* 43.4 (2006), pp. 439–561.

[LR04] Zeph Landau and Alexander Russell. "Random Cayley graphs are expanders: a simple proof of the Alon–Roichman theorem". In: *the electronic journal of combinatorics* 11.1 (2004), R62.

[Kas05] Martin Kassabov. "Kazhdan constants for SL n (Z)". In: *International Journal of Algebra and Computation* 15.05n06 (2005), pp. 971–995.

[LW92] Alexander Lubotzky and Benjamin Weiss. "Groups and expanders.". In: (1992), pp. 95–109.

[BG08a] Jean Bourgain and Alex Gamburd. "Uniform expansion bounds for Cayley graphs of". In: *Annals of Mathematics* (2008), pp. 625–642.

References

[Hel08] Harald Andrés Helfgott. "Growth and generation in". In: *Annals of Mathematics* (2008), pp. 601–623.

[SX91] Peter Sarnak and Xiaoxi Xue. "Bounds for multiplicities of automorphic representations". In: (1991).

[BGT11] Emmanuel Breuillard, Ben Green, and Terence Tao. "Approximate subgroups of linear groups". In: *Geometric and Functional Analysis* 21.4 (2011), pp. 774–819.

[HD22] Weikun He and Nicolas De Saxce. "Linear random walks on the torus". In: *Duke Mathematical Journal* 171.5 (2022), pp. 1061–1133.

[BGS10] Jean Bourgain, Alex Gamburd, and Peter Sarnak. "Affine linear sieve, expanders, and sum-product". In: *Inventiones mathematicae* 179.3 (2010), pp. 559–644.

References

[BG08b] Jean Bourgain and Alex Gamburd. "On the spectral gap for finitely-generated subgroups of SU (2)". In: *Inventiones mathematicae* 171 (2008), pp. 83–121.

[BG12] Jean Bourgain and Alex Gamburd. "A spectral gap theorem in SU.(d).". In: *Journal of the European Mathematical Society (EMS Publishing)* 14.5 (2012).

[BV12] Jean Bourgain and Péter P Varjú. "Expansion in SL d (Z/q Z), q arbitrary". In: *Inventiones mathematicae* 188 (2012), pp. 151–173.

[GV12] Alireza Salehi Golsefidy and Péter P Varjú. "Expansion in perfect groups". In: *Geometric and functional analysis* 22.6 (2012), pp. 1832–1891.

References

[SS13] Alireza Salehi Golsefidy and Peter Sarnak. "The affine sieve". In: *Journal of the American Mathematical Society* 26.4 (2013), pp. 1085–1105.

[BK14] Jean Bourgain and Alex Kontorovich. "On Zaremba's conjecture". In: *Annals of Mathematics* (2014), pp. 137–196.

[GS24] Alireza Salehi Golsefidy and Srivatsa Srinivas. "Random walks on direct products of groups". In: *Journal of the European Mathematical Society* (2024).

[Gol19] Alireza Salehi Golsefidy. "Super-approximation, II: the p-adic case and the case of bounded powers of square-free integers.". In: *Journal of the European Mathematical Society (EMS Publishing)* 21.7 (2019).

References

[LV16] Elon Lindenstrauss and Péter P Varjú. "Spectral gap in the group of affine transformations over prime fields". In: 25.5 (2016), pp. 969–993.

[BO14] Emmanuel Breuillard and Hee Oh. *Thin groups and superstrong approximation*. Vol. 61. Cambridge University Press, 2014.