Random Walks on Group Extensions

Srivatsa Srinivas

University of California, San Diego

2025-06-12

Group Algebra

- Let G be a group
  - We can define
    $$\mathbb{C}[G] := \mathsf{Span}_{\mathbb{C}}\langle \delta_g \mid g \in G \rangle$$
    where the δ_g are formal symbols
  - We can define a multiplication $*$ on G given by $\delta_g * \delta_h = \delta_{gh}$
  - We can define a linear involution operation $\check{\delta}$ on $\mathbb{C}[G]$ given by $\widecheck{\delta_g} = \delta_{g^{-1}}$
  - We can define an inner product by
    $$\langle \delta_g, \delta_h \rangle = \begin{cases} 1 \text{ if } g = h \\ 0 \text{ else} \end{cases}$$

Group Algebra

- We note that the above inner product has the following properties. For all $f, g, h \in \mathbb{C}[G]$ we have that

$$\langle f * g, h \rangle = \langle g, \check{f} * h \rangle$$
$$\langle f, g * h \rangle = \langle f * \check{g}, h \rangle$$

- We note that for all $f, g \in \mathbb{C}[G]$ that

$$\widecheck{f * g} = \check{g} * \check{f}$$

Random Walks on Groups

- Given a group G and a finitely supported probability measure μ, we can identify μ as element of the group algebra $\mathbb{C}[G]$ by

$$\mu := \sum_{g \in G} \mu(g) \delta_g$$

- The l-step random walk on G is defined by

$$\mu^{*l} := \underbrace{\mu * \cdots * \mu}_{l}$$

Random Walks on Groups

- The semantic meaning of the previous definition is the probability distribution obtained by randomly choosing a group element via μ and multiplying it to the previous measure, staring with the measure δ_e and repeating this process l many times.
- The return probability after l steps is defined to be

$$p_l(\mu) := \langle \mu^{*l}, \delta_e \rangle$$

  i.e, the probability that the above process returns to the identity after l steps
- We say that $f \in \mathbb{C}[G]$ is symmetric if $\check{f} = f$

Random Walks on Groups

- For a symmetric measure $\mu \in \mathbb{C}[G]$ we have that

$$\begin{aligned}\langle \mu^{*2l}, \delta_e \rangle &= \langle \mu^{*l}, \breve{\mu^{*l}} * \delta_e \rangle \\ &= \langle \mu^{*l}, \mu^{*l} \rangle \\ &= \|\mu^{*l}\|_2^2\end{aligned}$$

- We note that if the random walk is "aperiodic", since the only stationary distribution of the markov process given by μ is the uniform distribution across G, we have that

$$\lim_{n\to\infty} p_n(\mu) \to \frac{1}{|G|}$$

Random Walks on Groups

- Given a finite symmetric set of generators S, i.e $S = S^{-1}$ we define

$$\mu_S \in \mathbb{C}[G] := \frac{1}{|S|} \sum_g 1_S(g)\delta_g$$

Random Walks on Infinite Groups

- Let G be an infinite group and let μ be a symmetric finitely supported measure whose support generates the group
- We know that

$$\lim_{n\to\infty} p_n(\mu) \to 0$$

and so the interesting question is how fast $p_n(\mu)$ goes to 0

Random Walks on Infinite Groups

- Let us look at the case of $\mathbb{Z} \times \mathbb{Z}$ with generators $S = \{(0,1),(1,0),(0,-1),(-1,0)\}$
- We have that

$$p_{2n}(\mu_S) = \Theta\left(\frac{1}{n}\right)$$

- Let us look at the case of $\mathbb{F}_2$ with generators $S = \{a, b, a^{-1}, b^{-1}\}$
- We have that

$$p_{2n}(\mu_S) = \Theta\left(\frac{1}{3^{2n}}\right)$$

Cayley Graphs and Relations

- Given a group G and a symmetric generating set S we define the Cayley Graph of a group G to be the graph $\mathsf{Cay}(G, S) := (V, E)$, where $V := G$ and $E := \{(x, sx) \mid s \in S, x \in G\}$

Cayley Graphs and Relations

- The reason why $p_n(\mu_S)$ was so different in the above two examples is the Cayley graph. Notice how the Cayley graph of $\mathbb{Z} \times \mathbb{Z}$ gives ample opportunity for a point to return to the identity, whereas the Cayley graph of $\mathbb{F}_2$ forces you to go back the way you came.
- Every loop starting at the identity in the Cayley graph represents a relation in the generators. The more relations, the more you return to the identity.
- Kesten's theorem: Given a group G and a generating set S, we have that G is amenable iff $(p_{2n}(\mu_S))^{\frac{1}{2n}} \to 1$ as $n \to \infty$
- Random walks reveal group structure!

Random Walks on Finite Groups

- In this case we know that if G does not have a subgroup of index two and that S is symmetric then we have that $p_{2n}(\mu_S) \to \frac{1}{|G|}$ as $n \to \infty$.
- The function $\rho = \frac{1_G}{|G|} \in \mathbb{C}[G]$ is very special.
  - $\rho^*\rho = \rho\rho^* = \rho$ and $\forall f \in \mathbb{C}[G], f * \rho = \rho * f$
  - We also note that for all $f \in \mathbb{C}[G]$

$$\rho * f = \left(\sum_{g \in G} f(g) \right) \rho$$

  - Therefore, $f \mapsto \rho * f$ is the orthogonal projection on to the space of "G-invariant" functions

Random Walks on Finite Groups

- This allows to have the following decomposition

$$\mathbb{C}[G] = \mathbb{C}[G]^{\circ} \oplus \mathbb{C} \cdot \rho$$

  where $\mathbb{C}[G]^{\circ}$ are φ such that $\rho * \varphi = 0$
- Set $T_\mu(f) := \mu * f$, and note that since μ commutes with ρ, T_μ preserves the above decompositon
- Given a measure μ we define

$$|\lambda|(\mu) = \max\{|\lambda| \mid T_\mu(\varphi) = \lambda\varphi, \rho * \varphi = 0\}$$

Random Walks on Finite Groups

- Note that

$$
\begin{aligned}
p_{2n}(\mu_S) - \frac{1}{|G|} &= \langle \mu_S^{*2l}, \delta_e \rangle - \langle \rho, \delta_e \rangle \\
&= \langle \mu_S^{*2l} - \rho, \delta_e \rangle \\
&= \langle \mu_S^{*2l} * (\delta_e - \rho), \delta_e \rangle \\
&= \langle \mu_S^{*2l} * (\delta_e - \rho), \delta_e - \rho \rangle \\
&\leq |\lambda|(\mu)^{2l}
\end{aligned}
$$

More about $|\lambda|$

- Suppose that $\mu * \varphi = \lambda\varphi$, where $|\lambda| = 1$. Then by using the fact that μ is a measure, considering the maximum value taken by φ, we deduce that either G has a subgroup of index two or that $\varphi = c\rho$
- Thus if G does not have a subgroup of index two we must have that $|\lambda|(\mu) < 1$

More about $|\lambda|(\mu)$

- If $G = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ with $S = \{(0,1),(0,-1),(1,0),(-1,0)\}$ then we have that

$$|\lambda|(\mu_S) = 1 - \Theta(1/n^2)$$

  With a bit of arguing, one can show that it takes $\Theta(n^2)$ steps to get within ε of the uniform distribution
- What is the analogue of $\mathbb{F}_2$ in the finite group setting?

More about $|\lambda|(\mu)$

- If $G = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ with $S = \{(0,1),(0,-1),(1,0),(-1,0)\}$ then we have that

$$|\lambda|(\mu_S) = 1 - \Theta(1/n^2)$$

  With a bit of arguing, one can show that it takes $\Theta(n^2)$ steps to get within ε of the uniform distribution
- What is the analogue of $\mathbb{F}_2$ in the finite group setting?
- There are many options, but one is $\mathsf{SL}_2(\mathbb{F}_p)$ with generating set

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

A look at the Cayley Graphs

- Note that the smallest relation satisfied by words in S has length $\Theta(\log p)$

Infinite Families of Finite groups

- Is there an infinite family of $(\mathsf{Group}, \mathsf{GenSet})$, $(G_i, S_i)_{i \in \mathcal{J}}$, such that $|\lambda|(\mu_S) < c_0 < 1$ for all $i \in \mathcal{J}$?
  - We will call such families, c_0-gap families
- By a theorem of Lubotzky and Weiss, if $(G_i, S_i)_{i \in \mathcal{J}}$ is a family of groups of bounded solvability index, then there is no $c_0 < 1$ for which they form a c_0-gap family [1]
- By Selberg's 3/16-theorem, we can deduce that $\left(\mathsf{SL}_2\left(\mathbb{F}_p\right), S_p\right)_{p \in \text{ Primes}}$ is a c_0-gap family for some $c_0 < 1$ [2]

Lubtozky's 1-2-3 problem

- Let

$$S_x = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -x \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ -x & 1 \end{pmatrix} \right\}$$

  The above is a subset of $\mathsf{SL}_2(R)$ for any ring R
- Then we know from Selberg's 3/16 theorem that $\left(\mathsf{SL}_2(\mathbb{F}_p), S_1\right)_{p \in \text{ Primes}}$ and $\left(\mathsf{SL}_2(\mathbb{F}_p), S_2\right)_{p \in \text{ Primes}}$ are both c_0-gap families for some $c_0 < 1$. The above capitalizes on the fact that S_1, S_2 generate finite index subgroups of $\mathsf{SL}_2(\mathbb{Z})$
- Lubotzky's 1-2-3 problem asks whether $\left(\mathsf{SL}_2(\mathbb{F}_p), S_{3,p}\right)_{p \in \text{ Primes}}$ is a c_0 -gap family for some $c_0 < 1$ [3]

It was difficult

- We know for a fact that S_3 generates an infinite index subgroup of $\mathsf{SL}_2(\mathbb{Z})$. So how do we deal with it???
- It was proposed in 1995 and was not solved all the way till late 2005

I met Jean in September 2005, six months after my daughter (who drew the pictures for this essay) was born, while visiting IAS for the program 'Lie Groups, Representations and Discrete Mathematics' led by Alex Lubotzky. I do not remember the precise date but do remember the hour: it was between 2 and 3 am. After changing my daughter's diapers I could not sleep, went to Simonyi Hall and ran into Jean walking to the Library. It was in this discombobulated state that I was free of fear to speak to him. By dawn, the problem which had been resisting my protracted attack for a decade was vanquished in Jean's office.[31]

Figure 1: An excerpt from Gamburd's article "Singular adventures of Baron Bourgain in the Labyrinth of the Continuum"

Using special properties of $\mathsf{SL}_2(\mathbb{F}_p)$

- Let $G_p = \mathsf{SL}_2(\mathbb{F}_p)$
- We know that since the smallest representation of $\mathsf{SL}_2(\mathbb{F}_p)$ is of dimension $\Theta(p)$ (a result of frobenius)
- Using non-abelian fourier analysis [4] one can show that there is a constant $q_0 < 1$ independent of p, such that for any $f \in \mathbb{C}[G_p]$, $g \in \mathbb{C}[G_p]^{\circ}$ we must have that

$$\|f * g\|_2^2 \leq |G|^{1-q_0} \|f\|_2^2 \|g\|_2^2$$

- Without the above property, the best you can get is

$$\|f * g\|_2^2 \leq |G| \|f\|_2^2 \|g\|_2^2$$

Using special properties of $\mathsf{SL}_2(\mathbb{F}_p)$

- (Quasirandomness Trick)[4], [5] If $|\lambda|(\mu) = e^{-\beta}$, with $\mu * \varphi = e^{-\beta}\varphi$. If we can show that there exists some l such that $\|\mu^{*l\log p}\|_2^2 \le \frac{1}{|G|^{1-\frac{q_0}{2}}}$, then

$$\begin{aligned} e^{-2\beta l \log p} &= \|\mu^{*l\log p} * \varphi\|_2^2 \\ &\le |G_p|^{1-q_0} \|\mu^{*l\log p}\|_2^2 \|\varphi\|_2^2 \\ &\le |G_p|^{1-q_0} |G_p|^{q_0/2-1} \\ &= |G_p|^{-q_0/2} \le e^{\frac{-3q_0\log p}{2}} \end{aligned}$$

Since $|G_p| \le p^3 = e^{3\log p}$. Thus we get a lower bound on β independent of p!

Using special properties of $\mathsf{SL}_2(\mathbb{F}_p)$

- So the goal has now been reduced to show that $\|\mu_{S_3}^{*l}\|_2^2$ is small enough after $l = \Theta(\log p)$ steps
- We know that since
  - $S_3 \subset \mathsf{SL}_2(\mathbb{Z})$ generates a free group
  - The elements in $\prod_{l \log p} S_3$ all have entries lesser than p, as long as $l \leq 1/6$
  - We get $\|\mu^{*\log p/6}\|_2 \leq \frac{1}{p^{\frac{\log 3}{6}}}$
- This is some, but not nearly enough "flatness"! We call this "initial entropy"

The Bourgain-Gamburd technique

- Okay, what if we multiplied a measure μ by itseld and dont gain much entropy, i.e

$$\|\mu * \mu\|_2^2 \geq \frac{1}{K}\|\mu\|_2^2$$

- If μ is uniformly distributed on the shift of an almost subgroup, a set $A \subset G$ such that

$$|A \cdot A \cdot A| \leq K|A|$$

then the above inequality holds

- Can we say the reverse?

The Bourgain-Gamburd technique

- The Bourgain-Gamburd lemma says that if the inequality in the previous slide holds, then there exists a symmetric subset $A \subset G$ such that
  - $$\frac{K^{\Theta(1)}}{\|\mu\|_2^2} \geq |A| \geq \frac{1}{K^{\Theta(1)}\ \|\mu\|_2^2}$$
  - $$|A \cdot A \cdot A| \leq K^{\Theta(1)}\ |A|$$
  - $$\forall a \in A, \mu * \check{\mu}(a) \geq \frac{1}{K^{\Theta(1)}|A|}$$
- The proof uses Tao's non-commutative Balog-Gowers-Szemeredi and the dyadic pigeonhole technique

The Bourgain-Gamburd technique

- We now ask what happens when

$$\|\mu_{S_3}^{*l\log p} * \mu_{S_3}^{*l\log p}\|_2^2 \leq \frac{1}{|G_p|^\delta}\|\mu_{S_3}^{*l\log p}\|_2^2$$

- We get that there is a $\Theta(\delta)$ almost subgroup A of size greater than $|G_p|^{\frac{\log 3}{3}-\Theta(\delta)}$
- (Helfgott) [6] For all $\gamma > 0$, $\exists\delta > 0$ such that if A generates G_p then $|A \cdot A \cdot A| \geq |A|^{1+\delta}$.
- The above result means that the only almost subgroups in G_p are actual subgroups

The Bourgain-Gamburd technique

- Thus there is some sugroup $H \leq G$

$$\mu_{S_3}^{*l \log p}(H) \geq \frac{1}{|G_p|^{\delta}}$$

- This was proven not to be the case in [7] finite group theory; all proper subgroups of G_p have a bounded relation, but S_3 has no relation of length lesser than $\log p/6$.
- A more elegant method relating to the algebraic geometry of $\mathsf{SL}_2(-)$ was developed in [8].
- Thus $|\lambda|\left(\mu_{S_3}\right) < c_0 < 1$, where c_0 is independent of p

Can this be done for other groups?

- If we are to apply the above technique to a family of groups G_i we need two ingredients.
  - (Large enough almost subgroups are groups): For all $\gamma > 0$, there is a $\delta > 0$, for all $i \in \mathcal{I}$, the only δ-almost subgroups of G_i which are of size at least $|G_i|^\gamma$, are actual subgroups
  - (Non-Trivial representations are large): There exists a q_0 such that for all $i \in \mathcal{I}$, for all non-trivial irreducible representations $\rho : G_i \to \mathsf{GL}(V_\rho)$, we have that $\dim V_\rho \geq |G_i|^{q_0}$
- The above two assumptions hold for groups which look like $\mathsf{AlgGrp}(\mathbb{F}_q)$. The first requirement took quite a while (2004-2010) [9], [10] solve and the second requirement was known since the 1970s [11]

Can this be done for other groups?

- Bourgain and Gamburd led the charge in finding an anlogue to the above technique in $\mathsf{SU}(2)$
- The above technique is now used in a lot of different groups!
- Since $|\lambda|(\mu)$ is such refined information, we get a lot of corollaries in number theory due to group actions!

A lucrative idea

[7] J. Bourgain and A. Gamburd, "Uniform expansion bounds for Cayley graphs of," *Annals of Mathematics*, pp. 625–642, 2008.

[12] R. Boutonnet, A. Ioana, and A. Golsefidy, "Local spectral gap in simple Lie Groups and applications," *Inventiones mathematicae*, vol. 208, no. 3, 2017.

[13] J. Bourgain, A. Gamburd, and P. Sarnak, "Affine linear sieve, expanders, and sum-product," *Inventiones mathematicae*, vol. 179, no. 3, pp. 559–644, 2010.

[14] J. Bourgain and A. Gamburd, "On the spectral gap for finitely-generated subgroups of SU (2)," *Inventiones mathematicae*, vol. 171, pp. 83–121, 2008.

A lucrative idea

[15] J. Bourgain and A. Gamburd, “A spectral gap theorem in SU.(d).,” *Journal of the European Mathematical Society (EMS Publishing)*, vol. 14, no. 5, 2012.

[16] J. Bourgain and P. P. Varjú, “Expansion in SL d (Z/q Z), q arbitrary,” *Inventiones mathematicae*, vol. 188, pp. 151–173, 2012.

[8] A. S. Golsefidy and P. P. Varjú, “Expansion in perfect groups,” *Geometric and functional analysis*, vol. 22, no. 6, pp. 1832–1891, 2012.

[17] A. Golsefidy and P. Sarnak, “The affine sieve,” *Journal of the American Mathematical Society*, vol. 26, no. 4, pp. 1085–1105, 2013.

A lucrative idea

[18] J. Bourgain and A. Kontorovich, “On Zaremba's conjecture,” *Annals of Mathematics*, pp. 137–196, 2014.

[19] A. S. Golsefidy, “Super-approximation, II: the p-adic case and the case of bounded powers of square-free integers.,” *Journal of the European Mathematical Society (EMS Publishing)*, vol. 21, no. 7, 2019.

[20] A. Mohammadi and E. Lindenstrauss, “Polynomial effective density in quotients of $\mathbb{H}^3$ and $\mathbb{H}^2 \times \mathbb{H}^2$”, *Inventiones Mathematicae*, 2023.

The Bourgain-Gamburd mantra

- Suppose a group G is "Bourgain-Gamburdable". Let μ be any measure on G
  - If we have that for all subgroups H of G that

$$\mu^{*l \log|G|}(H) \le e^{-\beta \log|G:H|}$$

then we have that $-\log|\lambda|(\mu) > \Theta_{l,\beta,\mathrm{params}(G)}(1) > 0$

where $\mathrm{params}(G)$ is a set of numbers only to do with the representation theory and almost subgroups of G

- Therefore the refined information of the spectral gap, can be deduced from the crude information of escaping subgroups

Group Actions and Homomorphims

- Given a group G acting on a set X, we can define a bilinear map

$$\boxtimes : \mathbb{C}[G] \times \mathbb{C}[X] \to \mathbb{C}[X]$$

  given by $\delta_g \boxtimes \delta_x := \delta_{g \cdot x}$
- Given two groups G, H and a homomorphism $\varphi : G \to H$, there is an algebra homomorphism $\varphi[-] : \mathbb{C}[G] \to \mathbb{C}[H]$ given by $\delta_g \mapsto \delta_{\varphi(g)}$

Affine Actions

- Let $H_p = \mathsf{SL}_2(\mathbb{F}_p)$ and let $V_p = \mathbb{F}_p^2$. Let $A_p = \mathsf{SL}_2(\mathbb{F}_p) \ltimes V_p$ and let $\pi_\theta : A_p \to H_p$ be the projection homomorphism
- Suppose that A' is a subgroup of A_p such that $\pi_\theta(A') = H_p$. Then we note that if $\{1\} \times W := A' \cap \{1\} \times V_p$, then W is an H_p submodule of V_p. Therefore, it is either V_p or $\{0\}$. Thus A' is either all of A_p or there is a cocycle ρ such that

$$A = \{(g, \rho(g))\}$$

Since we know that all cocycles of the above group are coboundaries, there exists v_0 such that $A' \cdot v_0 = v_0$

Bourgain-Gamburd applied to Affine Actions

- Therefore, we can expect the following theorem: Let S be a symmetric generating set of A_p. We have that

$$-\log|\lambda|(\mu_S) \geq \Theta_{|S|}(1)(-\log|\lambda|(\pi_\theta[\mu_S])) \tag{1}$$

- Which is exactly what was proved in in 2014, by Lindenstrauss and Varju in [21]
- We know that $A_p \curvearrowright V_p$ by affine actions and so we can define $\boxtimes : \mathbb{C}[A_p] \times \mathbb{C}[V_p] \to \mathbb{C}[V_p]$

Bourgain-Gamburd applied to Affine Actions

- They prove that there exists an $l, \beta = \Theta_{|S|}\left(-\log|\lambda|\left(\pi_{\theta[\mu_S]}\right)\right) > 0$ such that for all $v \in \mathbb{F}_p$

$$\|\mu_S^{*l\log|A_p|} \boxtimes v_0\|_2^2 \leq e^{-\beta\log[A_p:H_p]}$$

- In other words, we have shown that the probability of fixing a vector is very small. Since the escaping properties of the projection of μ_S onto the H_p has a spectral gap, the only subgroups that μ_S can possible get stuck in, are exactly those subgroups which fix a vector. Thus, by the Bourgain-Gamburd mantra we have shown Equation 1

Direct Products

- Let $G_p = H_p \times H_p$, with $\pi_L, \pi_R : G_p \to H_p$ being the left and right projections respectively. Let G' be a subroup of G_p such that $\pi_L(G_p), \pi_R(G_p) = H_p$. Then, we know that if $\{I\} \times L := G' \cap \{1\} \times H_p$ then L is a normal subroup of H_p. Thus we have that

$$L = \{I\}, \{+I, -I\}, H_p$$

On setting $\pi_Z : H_p \to H_p/Z(H_p)$, we have that, either $G' = G_p$ or there exists an automorphism $\varphi : H_p/Z(H_p) \to H_p/Z(H_p)$ such that $\pi_Z \times \pi_Z(G') \subset \mathrm{Graph}(\varphi)$

Direct Products

- Therefore in [21] Lindenstrauss and Varju conjectured that if S is a symmetric generating set of G_p, then we must have that

$$-\log|\lambda|(\mu_S) \geq \Theta_{|S|}(1) \min(-\log|\lambda|(\pi_L[\mu_S]), -\log|\lambda|(\pi_R[\mu_S])) \quad (2)$$

- Let us find a group action that allows us to find if we are “trapped in a graph or not”. Define $G_p \underset{\varphi}{\curvearrowright} \frac{H_p}{Z(H_p)}$ by

$$(x, y) \cdot_\varphi z = \pi_Z(x) z \pi_Z(\varphi(y)^{-1})$$

- We note that $(x, y) \cdot_\varphi I = I$ iff $(\pi_Z(x), \pi_Z(y)) \in \mathrm{Graph}(\varphi)$

Direct Products

- Can we somehow show that that there are l, β linearly dependent on $\min(-\log|\lambda|(\pi_L[\mu_S]), -\log|\lambda|(\pi_R[\mu_S]))$ such that

$$\|\mu_S^{*l \log|G_p|} \boxtimes_\varphi I\|_2^2 \leq e^{-\beta \log[G_p : H_p]}$$

- Can we say that the probability of being trapped in a graph is small? A statement like the above would immediately imply Equation 2 by the Bourgain-Gamburd mantra

Lindenstrauss and Varju's technique

- Lindenstrauss and Varju used the following inequality: Let $G = H \ltimes A$, where A is abelian and let $\mu \in \mathbb{C}[G], \alpha \in \mathbb{C}[A]$ with μ being a probability measure. Let $\boxtimes$ come from the affine action.
- There is also the linear action of $H \underset{\theta}{\curvearrowright} A$ which induces

$$\boxtimes_\theta : \mathbb{C}[H] \times \mathbb{C}[A] \to \mathbb{C}[A]$$

- Since for any $(\theta_0, v) \in G, \alpha \in \mathbb{C}[A]$

$$\delta_g \boxtimes \alpha = \left(\delta_{\theta_0} \boxtimes_\theta \alpha\right) * \delta_v$$

We note that

$$\left(\delta_g \boxtimes \alpha\right) * \left(\widetilde{\delta_g \boxtimes \alpha}\right) = \pi_\theta(g) \boxtimes_\theta \left(\alpha * \check{\alpha}\right)$$

Lindenstrauss and Varju's technique

- Lindenstrauss and Varju prove the following inequality

$$\|(\mu \boxtimes \alpha) * (\widecheck{\mu \boxtimes \alpha})\|_2^2 \leq \left\| \sum_g \left(\delta_g \boxtimes \alpha\right) * \left(\widecheck{\delta_g \boxtimes \alpha}\right) \mu(g) \right\|_2^2$$

$$= \|\pi_\theta[\mu] \boxtimes_\theta (\alpha * \check{\alpha})\|_2^2$$

- And use it to derive information about $\mu \boxtimes -$ using $\pi_\theta[\mu] \boxtimes_\theta -$

Our Technique

- We take a group $G = H \times H$ and a homomorphism $\pi_Z : H \to \tilde{H}$, where $\tilde{H} = H/Z(H)$. Let $\varphi : H \to H$ be a homomorphism. We have $\boxtimes_\varphi$ from before, but now we define $\boxtimes_\theta$ as the map we get from the action $H \curvearrowright \tilde{H}$

$$x \cdot_\theta z = \pi_Z(x) z \pi_Z(x^{-1})$$

- We note that since

$$\delta_{(x,y)} \boxtimes_\varphi \alpha = \delta_{\pi_Z(x)} * \alpha * \delta_{\pi_Z(\varphi(y)^{-1})}$$

we have that

$$\left(\delta_g \boxtimes \alpha\right) * \left(\widecheck{\delta_g \boxtimes \alpha}\right) = \pi_L(g) \boxtimes_\theta \left(\alpha * \check{\alpha}\right)$$

Our Technique

- We prove the inequality

$$\|(\mu \boxtimes_\varphi \alpha) * (\widecheck{\mu \boxtimes_\varphi \alpha})\|_2^2 \leq \left\|\sum_g (\delta_g \boxtimes_\varphi \alpha) * (\widecheck{\delta_g \boxtimes_\varphi \alpha})\mu(g)\right\|_2^2$$

$$= \|\pi_L[\mu] \boxtimes_\theta (\alpha * \check{\alpha})\|_2^2$$

- And use it to derive information about $\mu \boxtimes_\varphi -$ using $\pi_L[\mu] \boxtimes_\theta -$

I don't know what to name this inequality

- Our inequality follows from the following more general inequality: Let $\mathcal{H}$ be a Hilbert algebra and let $\mathcal{A}, \mathcal{B}$ be two subalgebras such that $[\mathcal{A}, \mathcal{B}] = 0$. Let (Ω, μ) be a measure space $\mathcal{H}$ and let $f : \Omega \to \mathcal{A}$ $g : \Omega \to \mathcal{B}$ be square integrable. Then we have that

$$\left\| \left(\int_\Omega f(\omega) g(\omega)^* d\mu(\omega) \right) \left(\int_\Omega f(\omega) g(\omega)^* d\mu(\omega) \right)^* \right\|_2^2$$

$$\leq \left\| \int_\Omega f(\omega) f(\omega)^* d\mu(\omega) \right\|_2^2 \left\| \int_\Omega g(\omega) g(\omega)^* d\mu(\omega) \right\|_2^2$$

I don't know what to name this inequality

- The proof is relatively simple: We set $\alpha(\omega_1, \omega_2) = f(\omega_1)^* f(\omega_2)$ $\beta(\omega_1, \omega_2) = g(\omega_1)^* g(\omega_2)$ and note that

$$\int_{\Omega^4} (\alpha(\boldsymbol{\omega}_1)\beta(\boldsymbol{\omega}_2) - \alpha(\boldsymbol{\omega}_2)\beta(\boldsymbol{\omega}_1))(\alpha(\boldsymbol{\omega}_1)\beta(\boldsymbol{\omega}_2) - \alpha(\boldsymbol{\omega}_2)\beta(\boldsymbol{\omega}_1))^* d\mu^4(\boldsymbol{\omega_1}, \boldsymbol{\omega_2})$$

is a positive element of $\mathcal{H}$. The inequality follows from taking the inner product of the above with $1_{\mathcal{H}}$

- In the case of the problem Lindenstrauss and Varju solved, we can take $\mathcal{H}$ to be $\mathbb{C}$ and then it just becomes Cauchy-Schwarz
- In our case we take $\mathcal{H}$ to be $\mathbb{C}[G]$ and $\mathcal{B}$ to be $\mathbb{C}$

Pushing the inequality to its limit

- My thesis is based on joint work of Prof. Alireza Golsefidy and mine, titled Random Walk on Group Extensions.
- The extremely nerfed 🔫 🔫 🔫 version of the main theorem is the following, which encapsulates the above two theorems:

Let $\mathsf{G} = \left(\prod_i \mathsf{G}_i\right) \ltimes \mathsf{U}$ be a perfect algebraic group defined over $\mathbb{Z}$, where G_i are quasi-simple and U are unipotent all defined over $\mathbb{Z}$. Then there exists a constant $K > 0$ such that for all $p \in \mathsf{Primes}$ such that for any measure μ on $\mathsf{G}(\mathbb{Z}/p\mathbb{Z})$, we have that

$$-\log(|\lambda|(\mu)) \geq K \max_i(-\log|\lambda|(\pi_i[\mu]))$$

where $\pi_i : \mathsf{G} \to \mathsf{G}_i$ is the projection map

Pushing the inequality to its limit

- In my opinion the above theorem will be a foundation in the field, as it moves towards proving that all generating sets of particular group have a spectral gap. One of the biggest problems in the field is finding "initial entropy", which is usually done by choosing special generating sets.
- The above theorem should be thought of as a "result booster"; any result about spectral gaps that you can cook up about finite simple groups of Lie Type immediately apply towards the $\mathbb{F}_q$ points of perfect algebraic groups. You don't have to waste time dealing with annoying "$\times$" and "$\ltimes$". One can "Keep It Simple Stupid"
- It has already found uses in [22] and future work communicated to me by Prof. Breuillard

Future Directions of this Idea

- The analogous result for the $\prod_{p \in \mathsf{Primes}} \mathbb{Z}_p$ points of perfect algebraic groups is under completion and we hope to publish it in this summer
- The ideas are analogous, but the technical details took a lot of new ideas, both in the algebra and the analysis.

Thanks for being on my committee

- I would like to thank the members of my commitee for being on my committee
- "Solving an open problem problem using Non-Commutative Cauchy-Schwarz" is a pipe-dream for a PhD thesis, but I would like to thank my advisor for making it possible!

Bibliography

[1] A. Lubotzky and B. Weiss, "Groups and expanders.," pp. 95–109, 1992.

[2] T. Tao, "254B, Notes 3: Quasirandom groups, expansion, and Selberg's 3/16 theorem." [Online]. Available: https://terrytao.wordpress.com/2011/12/16/254b-notes-3-quasirandom-groups-expansion-and-selbergs-316-theorem/

[3] A. Lubotzky, "Cayley graphs: eigenvalues, expanders and random walks," *London Math. Soc. Lecture Note*, 1995.

[4] W. T. GOWERS, “Quasirandom Groups,” *Combinatorics, Probability and Computing*, vol. 17, no. 3, pp. 363–387, 2008, doi: 10.1017/S0963548307008826.

[5] P. Sarnak and X. Xue, “Bounds for multiplicities of automorphic representations,” 1991.

[6] H. A. Helfgott, “Growth and generation in,” *Annals of Mathematics*, pp. 601–623, 2008.

[7] J. Bourgain and A. Gamburd, “Uniform expansion bounds for Cayley graphs of,” *Annals of Mathematics*, pp. 625–642, 2008.

[8] A. S. Golsefidy and P. P. Varjú, "Expansion in perfect groups," *Geometric and functional analysis*, vol. 22, no. 6, pp. 1832–1891, 2012.

[9] E. Breuillard, B. Green, and T. Tao, "Approximate subgroups of linear groups," *Geometric and Functional Analysis*, vol. 21, no. 4, pp. 774–819, 2011.

[10] L. Pyber and E. Szabo, "Growth in finite simple groups of Lie type," *Journal of the American Mathematical Society*, 2016.

[11] V. Landazuri and G. M. Seitz, "On the minimal degrees of projective representations of the finite Chevalley groups," *Journal*

of Algebra, vol. 32, no. 2, pp. 418–443, 1974, doi: https://doi.org/10.1016/0021-8693(74)90150-1.

[12] R. Boutonnet, A. Ioana, and A. Golsefidy, "Local spectral gap in simple Lie Groups and applications," *Inventiones mathematicae*, vol. 208, no. 3, 2017.

[13] J. Bourgain, A. Gamburd, and P. Sarnak, "Affine linear sieve, expanders, and sum-product," *Inventiones mathematicae*, vol. 179, no. 3, pp. 559–644, 2010.

[14] J. Bourgain and A. Gamburd, "On the spectral gap for finitely-generated subgroups of SU (2)," *Inventiones mathematicae*, vol. 171, pp. 83–121, 2008.

[15] J. Bourgain and A. Gamburd, "A spectral gap theorem in SU.(d).," *Journal of the European Mathematical Society (EMS Publishing)*, vol. 14, no. 5, 2012.

[16] J. Bourgain and P. P. Varjú, "Expansion in SL d (Z/q Z), q arbitrary," *Inventiones mathematicae*, vol. 188, pp. 151–173, 2012.

[17] A. Golsefidy and P. Sarnak, "The affine sieve," *Journal of the American Mathematical Society*, vol. 26, no. 4, pp. 1085–1105, 2013.

[18] J. Bourgain and A. Kontorovich, "On Zaremba's conjecture," *Annals of Mathematics*, pp. 137–196, 2014.

[19] A. S. Golsefidy, “Super-approximation, II: the p-adic case and the case of bounded powers of square-free integers.,” *Journal of the European Mathematical Society (EMS Publishing)*, vol. 21, no. 7, 2019.

[20] A. Mohammadi and E. Lindenstrauss, “Polynomial effective density in quotients of $\mathbb{H}^3$ and $\mathbb{H}^2 \times \mathbb{H}^2$”, *Inventiones Mathematicae*, 2023.

[21] E. Lindenstrauss and P. P. Varjú, “Spectral gap in the group of affine transformations over prime fields,” vol. 25, no. 5, pp. 969–993, 2016.

[22] L. Bary-Soroker, D. Garzoni, and S. Sodin, "Irreducibility of the characteristic polynomials of random tridiagonal matrices." [Online]. Available: https://arxiv.org/abs/2502.17218