harald.helfgott@gmail.com

1. Expanders

1967. Kolmogorov & Barzdin 1973. Pinsker (??). Expanders

Combinatorial. spectral. probabilistic perspectives.

Directed graphs: $\Gamma = (V, E)$ (is symmetric. $(v,w) \in E \iff (w,v) \in E$)

For $S \subset V$, the outer-boundary / inner boundary are defined as:

$\partial_{out} S = \{v \in V \mid v \notin S. \exists w \in S \text{ s.t. } (v,w) \in E\}$ Similarly $\partial_{in} S$.

Def [ε-vertex expander] $\Gamma = (V, E)$ is an ε-v.e. if $|\partial_{out} S| \geq \varepsilon |S|$
$\forall S \subset V$ with $|S| < \frac{|V|}{2}$

Rmk One need ε to be large for it to make sense. e.g. every Γ connected is a $\frac{2}{|V|}$-expander graph.

Observation If the graph has deg $\leq d$, then $\text{diam}(\Gamma) > \frac{\log |V|}{\log d} - 1$

of course when $d=2$, this is worse. estimate $\text{diam} \leq 1 + d(1 + (d-1) + (d-1)^2 + \cdots (d-1)^{k-1})$
$= 1 + d\left(\frac{(d-1)^k - 1}{d-2}\right)$

Lemma If Γ is ε-v.e. then $\text{diam}(\Gamma) \ll \frac{1}{\varepsilon} \log |V|$

Pf: Take S_k the set of radius k. Then $S_{k+2} = S_k \cup \partial_{out} S_k$ as we know $|\partial_{out} S_k| \geq \varepsilon |S_k|$
then $|S_{k+1}| \geq (1+\varepsilon)^{k+2}$ (by induction) hence for any $k' \geq \frac{\log |V|}{\log 1+\varepsilon}$ $|S_{k'}| \geq \frac{|V|}{2}$

Hence we can find two copies of $S_{k'}$ s.t. ie diameter be made.

Conclusion: $\text{diam}(\Gamma) \leq 2\left(\frac{\log \frac{|V|}{2}}{\log 1+\varepsilon} + 1\right) \ll \frac{\log |V|}{\varepsilon}$ □

Remark. Show that if remove M vertices from V, the remaining graph still have a conn component with $\geq |V| - O(\frac{M}{\varepsilon})$

Also $|\partial_{edge} S| \geq |\partial_{out} S| \geq |\partial_{in} S|$ on the other hand, if max deg $\leq d$. then
$|\partial_{edge} S| \leq d|\partial_{in} S| \leq d|\partial_{out} S|$

1.2 Probablistic Viewpoint

How far is the probability distribution after k-steps from the unif dist $\frac{1}{|V|}$

$|f|_p = \ell^p(f) = \left(\sum_{v\in V} |f(v)|^p\right)^{1/p}$ $\quad L^p(f) = \left(\frac{\sum_{v\in V}|f(v)|^p}{|V|}\right)^{1/p}$ $\quad \ell^\infty = L^\infty = \max$

Def [mixing term] Given norm. the $t_{norm}(\varepsilon)$ the least const k s.t. after k-step

$$\left| f_k - \frac{1}{|V|}\mathbb{1} \right|_{norm} \le \varepsilon$$ ⇐ one need to specify.

$|f|_1 \overset{CS}{\le} |f|_2 \le |f|_\infty \Rightarrow \max_{L^1}(\varepsilon) \le \max_{L^2}(\varepsilon) \le \max_{L^\infty}(\varepsilon)$

f is random walk with $f(v) = \begin{cases} 1 & \text{if } v = v_0 \\ 0 & \text{otherwise} \end{cases}$

Ex Say $|f_k - \frac{\mathbb{1}}{|V|}|_2 \le \varepsilon$. Show that $|f_{2k} - \frac{\mathbb{1}}{|V|}|_\infty \le \varepsilon^2$

Ex If $|f_k - \frac{\mathbb{1}}{|V|}|_\infty < \frac{1}{|V|}$, then the $\operatorname{diam}(\Gamma) \le k$ $\quad (f_k = Ad_\Gamma^k f)$

cf. Lemma P3.

1.3 Spectral Viewpoint

Def [Adjacency operator] $Ad \curvearrowright f: V \to \mathbb{C}$ via: $Ad(f)(v) = \sum_{(v,w)\in E} f(w)$ and

$(Ad^2 f)(v) = \#$ paths of length 2 from v_0 to v. Hence we may write:

$\left(\left(\frac{1}{d} Ad^k\right)(f)\right)(v) =$ Prob of ending at v after a random walk of k-step.

Ex Ad is symm operator. it's hermitian w.r.t. the canonical metric

The gives the spectral viewpoint. i.e. per spectral thm. we have $\lambda_1 \ge \cdots \ge \lambda_N \in \mathbb{R}$ and if Γ is expander of deg d. then $\lambda_1 = d$ with eigenfct $f_1 = C$.

Def [spectral expander] Γ symm. reg of deg d. Γ is a **1-sided spec exp** if $\lambda_2 \le (1-\varepsilon)d$ and **2-sided spec exp** if $|\lambda_j| \le (1-\varepsilon)d \ \forall 2 \le j \le N$

Ex: Show $\lambda_2 = d$ if Γ non-connected. and $\lambda_N = -d$ if Γ is bipartite

Lemma: Let Γ be a 2-sided spec exp. then $\left|\left(\frac{1}{d}Ad_\Gamma\right)^k \delta_{v_0} - \frac{1}{|V|}\mathbb{1}\right|_{\ell^2} \le (1-\varepsilon)^k$

That is. our random walk starting at v_0 is exponentially converging to everywhere.

Pf For any f. write it by orthonormal decomp $f = \sum c_i f_i$ (where $Ad_\Gamma f_i = \lambda_i f_i$)

Note $f_1 = 1$ the const. Hence for any $f = \delta_{v_0} \Rightarrow c_1 = \langle f, 1\rangle = \frac{1}{|V|}\sum_{v\in V} f(v) = \frac{1}{|V|}$

Now: $\left(\frac{1}{d}Ad_\Gamma\right)^k \delta_{v_0} = c_1\left(\frac{1}{d}Ad_\Gamma\right)^k \mathbb{1} + c_2\left(\frac{1}{d}Ad_\Gamma\right)^k f_2 + \cdots = \frac{\mathbb{1}}{|V|} + \left(\frac{\lambda_2}{d}\right)^k c_2 f_2 + \cdots$

Hence the estimate $\left|\left(\frac{1}{d}Ad_\Gamma\right)^k \delta_{v_0} - \frac{\mathbb{1}}{|V|}\right|_2^2 = \left|\sum_{j=2}^{N}\left(\frac{\lambda_j}{d}\right)^k c_j f_j\right|_2^2 = \sum_{j=2}^{N}\left(\frac{\lambda_j}{d}\right)^k c_j^2$ (*)

Now (*) $\overset{\text{exp ppty}}{\leq} (1-\varepsilon)^{2k}\sum_{j=2}^{N} c_j^2 \leq \frac{(1-\varepsilon)^{2k}}{|V|}$ (as $\sum c_j^2 = |f|_{\ell^2}^2 = \frac{1}{|V|}$)

Rmk [ℓ^2, ℓ^∞] As $|\cdot|_1 \leq |\cdot|_2$ we have the trivial bound. For k suff small [e.g. $k \leq \frac{1}{2\varepsilon}\log|V|$] with $(1-\varepsilon)^k \gg \frac{1}{\sqrt{|V|}}$ we have the trivial bound.

On the other hand when k is large. (e.g. $k \geq \frac{2+\delta}{\log\frac{1}{1-\varepsilon}}\log|V| \sim \frac{2+\delta}{\varepsilon}\log|V|$)

we have $(1-\varepsilon)^k = \frac{1}{|V|^{2+\delta}}$, then $\left|\left(\frac{1}{d}Ad_\Gamma\right)^k \mathbb{1}_{v_0} - \frac{1}{|V|}\right|_\infty \leq \frac{1}{|V|^{\delta+1}}$ (By $|\cdot|_\infty \leq |\cdot|_1 = |V|\cdot|\cdot|_1$)

Lemma [$L_2 \Rightarrow \ell^\infty$] If $\left|\left(\frac{1}{d}Ad_\Gamma\right)^k \delta_{v_0} - \frac{\mathbb{1}}{|V|}\right|_{\ell^2} \leq \Delta$, then $\left|\left(\frac{1}{d}Ad_\Gamma\right)^k \delta_{v_0} - \frac{\mathbb{1}}{|V|}\right|_\infty \leq \Delta^2$

Pf [sketch] $\left\langle\left(\frac{1}{d}Ad_\Gamma\right)^k \delta_{v_0}, \delta_{v_1}\right\rangle \overset{\text{symm}}{=} \langle f_{k,v_0}, f_{k,v_1}\rangle$

$= \langle f_{k,v_0}, f_{k,v_1}\rangle = \langle f_{k,v_0} - \frac{\mathbb{1}}{|V|}, f_{k,v_1} - \frac{\mathbb{1}}{|V|}\rangle + \langle\frac{\mathbb{1}}{|V|}, f_{k,v_1}\rangle + \langle f_{k,v_0} - \frac{\mathbb{1}}{|V|}, \frac{\mathbb{1}}{|V|}\rangle$

(1) (2) (3)

(1) $\overset{C.S}{\leq} \left|f_{k,v_0} - \frac{\mathbb{1}}{|V|}\right|_2 \left|f_{k,v_1} - \frac{\mathbb{1}}{|V|}\right|_2 \leq \frac{\Delta^2}{|V|}$ (2) $= \frac{1}{|V|^2}$

(3) $= \frac{1}{|V|}\langle f_{k,v_0}, \mathbb{1}\rangle - \frac{1}{|V|}\langle\mathbb{1}, \mathbb{1}\rangle = \frac{1}{|V|}\sum_v f_{k,v_0}(v) - \frac{1}{|V|}$ ($= 1$ by prob dist)

$\Rightarrow \langle -, -\rangle \leq \frac{\Delta^2}{|V|}$ □

Cor For a 2-sided ε-exp. then $\left|\left(\frac{1}{d}Ad_\Gamma\right)^{2k}\delta_{v_0} - \frac{\mathbb{1}}{|V|}\right|_\infty \leq (1-\varepsilon)^{2k}$ e.g. $(1-\varepsilon)^{2k} \sim \frac{1}{|V|^2}$

Rmk: Sometimes we can prove/need something stronger than $|\lambda_j| \leq (1-\varepsilon)d$. But this cannot be stronger than

Prop (Alon-Boppana bound) Γ symm reg of deg d, then $\lambda_2 \geq 2\sqrt{d-1}\left(1 - O\left(\frac{1}{\text{diam}\,\Gamma)^2}\right)\right)$ $\approx \frac{1}{\sqrt{d}}$.

Lemma [Expander mixing Lemma] (Alon-Chung '88) Γ symm. reg graph. two-sided ε-expander $S_1, S_2 \subseteq V$. then

$$\left| \{(v,w) \in E : v \in S_1,\ w \in S_2\} - \frac{d|S_1||S_2|}{|V|} \right| \le (1-\varepsilon) d \sqrt{|S_1||S_2|}$$ here the trivial bound is $\le C(\max(|S_1|, |S_2|))$

The statement means # edges between any two large sets is what one expects in random d-reg graph

pf: Consider J the adjacency operator on complete graph. Then $Jf(v) = \sum_{v \in V} f(v)$ hence we have const fct. have eigenval $= |V|$ and other $\perp$ fct have eigenval 0. So:

$Ad_\Gamma - \frac{d}{|V|} J$ has eigfct $f_1, f_2, f_3 \cdots$ with eigenval $0, \lambda_2 \ge \lambda_3 \ge \cdots$

Note J commutes with everything. hence use eigenfct of Ad_Γ.

We see also Γ is 2-sided ε-spectral expander $\Leftrightarrow \left| Ad_\Gamma - \frac{d}{|V|} J \right| \le (1-\varepsilon) d$

On the other hand we can reinterpret $\{(v,w) \in E : v \in S_1, w \in S_2\}$ as:

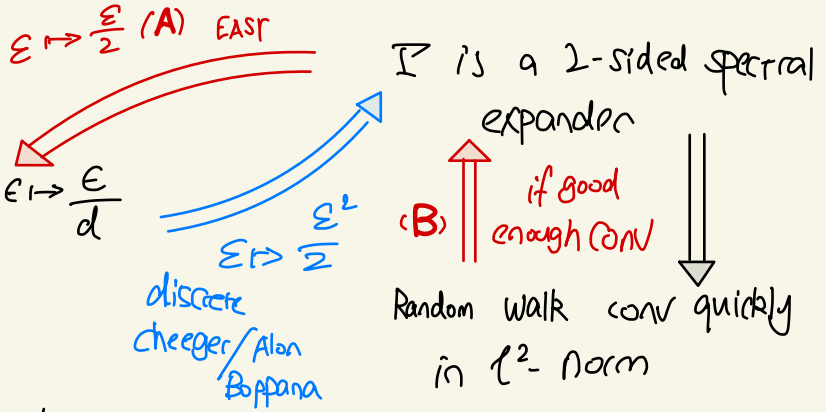
$$|V| \langle Ad_\Gamma \mathbb{1}_{S_1}, \mathbb{1}_{S_2} \rangle = |V| \langle \left(Ad_\Gamma - \frac{d}{|V|} J \right) \mathbb{1}_{S_1}, \mathbb{1}_{S_2} \rangle + d \langle J \mathbb{1}_{S_1}, \mathbb{1}_{S_2} \rangle$$

(a) (b)

whereas (a) $\overset{C.S}{\le} (1-\varepsilon) d \cdot |\mathbb{1}_{S_1}| |\mathbb{1}_{S_2}| = (1-\varepsilon) d \cdot \sqrt{|S_1||S_2|}/|V|$ $\Rightarrow$ the claimed bound $\square$

(b) $= \frac{d}{|V|} |S_1||S_2|$ Cancelled by leading term

Scholium



To prove (A): Estimate $S \subset V$

$f: \delta_S - \frac{|S|}{|V|} \mathbb{1}$. Note $|\langle Ad_\Gamma f, f \rangle| \le (1-\varepsilon) d \|f\|_2^2$. Expand the terms as previous.

$$LHS = \langle Ad_\Gamma \delta_S, \delta_S \rangle - \frac{|S|}{|V|} \langle Ad_\Gamma \mathbb{1}, \delta_S \rangle - \underbrace{\frac{|S|}{|V|} \langle Ad_\Gamma \left(\delta_S - \frac{|S|}{|V|} \right), \mathbb{1} \rangle}_{0}$$

Rmk [Converse of Expander mixing Lemma] Let G be a d-reg graph and supp

$$\left| |E(S,T)| - \frac{d|S||T|}{n} \right| \le \rho\sqrt{|S||T|}$$

holds for every disjoint sets S, T and for some positive ρ. Then

$$\lambda \le O(\rho \cdot (1+\log(d/\rho)))$$

The bound is tight.

In another words, EML can be seen as 'slight weaker equiv' of Expander.

For details, see Bilu, Linial 2006.

3. ∃ Expander

Prop: [∃ Expander, Pinsker '73, Kolmogorov-Barzdin '67] Expanders of bound deg (≥ 3) exist

Rmk [Prob method] One can choose X at random and show $\mathbb{P}(X \text{ is something}) > 0$ and therefore something exists. Also random surfaces?

Pf Let N be large and even. Create random symm graph of deg $d = 2\ell$ $\ell \geq 3$ as follows:

- $1 \leq i \leq \ell$, choose permutation $\pi_i : V \to V$ (independently) and uniformly at random
- Draw an edge from $v \to \pi_i(v)$ for all v, i.

WARNING There might be repeated edge (under transposition  )

Recall Γ is NOT an ε-expander $\iff \exists S$ with $|\partial_{out} S| \leq \varepsilon |S|$ (again $|S| \leq \frac{|V|}{2}$)

Given $S \subset S' \subset V$ with $|S'| = \lfloor (1+\delta)|S| \rfloor$. Now what is $\mathbb{P}(\partial_{out} S \subset S') \leq ?$

We want to know the $\mathbb{P}$ is tiny. Order S as $1, \dots, m = |S|$

Then $\mathbb{P}(\pi_1(1) \in S') = \frac{|S'|}{N}$ $\mathbb{P}(\pi_1(2) \in S' \mid \pi_1(1) \in S') = \frac{|S'|-1}{N-1} < \frac{|S'|}{|V|}$

and etc. $\Rightarrow \mathbb{P}(\pi_1(S) \subset S') < \left(\frac{|S'|}{|V|}\right)^{|S|}$ Recall conditional probability

$\mathbb{P}(A \cap B) = \mathbb{P}(B) \cdot \mathbb{P}(A|B)$

The same holds true for each π_i and $\mathbb{P}(\pi_i(S) \subset S')$ are independent/multiplicative hence

$$\mathbb{P}(\pi_i(S) \subset S' \ \forall 1 \leq i \leq \ell) < \left(\frac{|S'|}{|V|}\right)^{\ell |S|} \leq \left(\frac{1+\delta}{|V|}\right)^{\ell m}$$

(i.e. $\partial_{out}(S) \subset S'$; recall the setting of Γ)

note $\exists \binom{N}{m}$ many-choices of S and $\binom{N-m}{m'}$-many choices of $S' \setminus S$. where $m' = |S' \setminus S|$

$\mathbb{P}(\Gamma \text{ NOT a } \delta\text{-vertex exp}) = \mathbb{P}(\exists S, S', S \subset S' \text{ s.t. } \partial_{out} S \subset S' \text{ with } |S'| = \lfloor (1+\delta)|S| \rfloor \text{ and } |S| \leq \frac{|V|}{2})$

$$\leq \sum_{1 \leq m \leq \frac{N}{2}} \underbrace{\binom{N}{m}}_{(*)_m} \underbrace{\binom{N-m}{\lfloor \delta m \rfloor}}_{a_m} \left(\frac{(1+\delta)m}{N}\right)^{\ell m}$$

⇐ WANT TO SHOW THIS SUM IS SMALL. e.g. when $m=1 \rightsquigarrow \left(\frac{(1+\delta)}{N}\right)^{\ell-1}$

prove the claim by induction.: . from n to $n+1$. we use Stirling's formula:

$$n! = \left(\frac{n}{e}\right)^n \sqrt{2\pi n}\left(1 + O(n^{-1})\right)$$

Recall $\binom{N}{m} = \frac{N!}{m!(N-m)!}$

$$(*)_m \overset{\oplus}{=} \binom{N}{m, \lfloor \delta m \rfloor, N - \lfloor \delta m \rfloor - m} := \frac{N!}{m! \lfloor \delta m \rfloor ! c!} \ll \frac{N^N}{m^m \lfloor \delta m \rfloor^{\lfloor \delta m \rfloor} c^c} \leq \frac{N^N}{m^m (\delta m)^{\delta m} (N - (1+\delta)m)^{N-(1+\delta)m}} \quad (**)$$

Strategy of the proof

WANT TO SHOW:
$a_{m+1} \le \rho a_m$ for $\rho<1$ and $m+1 \le N/2$
Then our sum is geometric
$\sum a_m \le \frac{a_1}{1-\rho}$.

Estimate of a_1: $a_1 \le \frac{N^N}{\delta^\delta (N-(1+\delta))^{N-(1+\delta)}} \left(\frac{1+\delta}{N}\right)^\ell \le \frac{(1+\delta)^\ell}{\delta^\delta e^{(1+\delta)}} \cdot \frac{1}{N^{\ell-(1+\delta)}}$

By $\frac{1}{\delta^\delta} \frac{N^{1+\delta}}{(1-\frac{1+\delta}{N})^{N-(1+\delta)}} \ll_{\delta,\ell} \frac{1}{\delta^\delta} \frac{1}{e^{(1+\delta)}} N^{1+\delta}$

one sees by easy manipulation that Const $(1-\frac{c}{N})^N \gg e^c$ for $c>1$

To show the claim, use **Entropy of Prob distribution**: $(P_1, \dots, P_n)_{\sum P_i = 1}$ is defined (a la Shannon) $H(P_1,\dots,P_n) = -\sum_{1\le i\le n} P_i \log P_i$. Rewrite (**) as:

$$e^{N\log N - m\log m - \delta m \log(\delta m) - (N-(1+\delta)m)\log(N-(1+\delta)m)}$$

$$= e^{-N\left(\frac{m}{N}\log\frac{m}{N} + \frac{\delta m}{N}\log\frac{\delta m}{N} + \frac{N-(1+\delta)m}{N}\log\frac{N-(1+\delta)m}{N}\right)}$$

$\left(\frac{m}{N}\log\frac{m}{N} + \frac{\delta m}{N}\log\frac{\delta m}{N} + \frac{N-(1+\delta)m}{N}\log\frac{N-(1+\delta)m}{N}\right) = H\left(\frac{m}{N}, \frac{\delta m}{N}, 1-\left(\frac{m}{N}+\frac{\delta m}{N}\right)\right) =: f\left(\frac{m}{N}\right) =: f(t)$

Note $\frac{m+\delta m + N-(1+\delta)m}{N} = 1$

Split $N\log N$ as $\frac{m}{N}\log N + \frac{\delta m}{N}\log N + \frac{N-(1+\delta)m}{N}\log N$

and then entropy shows up naturally

ATTENTION: f is convex up on $(0,1)$ (checking $f''(t)>0$ for $t<1$)

$$f'(t) = \frac{d}{dt}\left[t\log t + \delta t\log\delta t + \left(1-(1+\delta)t\right)\log\left(1-(1+\delta)t\right)\right]$$

$(f\log f)' = f'\log f + f'$.

$$= \log t + \delta\log\delta t - (1+\delta)\log(1-(1+\delta)t) = (1+\delta)\log t + \delta\log\delta - (1+\delta)\log(1-(1+\delta)t)$$

Note <0 and strictly increasing w.r.t. δ. and $(1+\delta)\log(1-(1+\delta)t)$ is strictly decreasing w.r.t. δ.

hence $f'(t) > f'(t)_{\delta=0}$ with the following ineq holds:

$$f\left(\frac{m+1}{N}\right) - f\left(\frac{m}{N}\right) \underset{\text{convexity}}{\ge} \frac{1}{N} f'\left(\frac{m}{N}\right) \ge \frac{1}{N}\left((1+\delta)\log\frac{m}{N} - \log\left(1-\frac{m}{N}\right) + \delta\log\delta\right) > 0 \quad (\star)$$

Recall strategy of proof we now want to show from a_m to a_{m+1} the increased amount is small.

deal with each term of a_{m+1}/a_m separately.

- $\left(\frac{(1+\delta)(m+1)}{N}\right)^{\ell(m+1)} \Big/ \left(\frac{(1+\delta)m}{N}\right)^{\ell m} = \left(1+\frac{1}{m}\right)^{\ell m} \cdot \left(\frac{(1+\delta)(m+1)}{N}\right)^\ell \le e^\ell \cdot \left(\frac{(1+\delta)(m+1)}{N}\right)^\ell$
- $(*_{m+1})/(*_m) \sim e^{-N\left(f\left(\frac{m+1}{N}\right) - f\left(\frac{m}{N}\right)\right)} \overset{(\star)}{\le} \left(\frac{N}{m}\right)^{1+\delta}\left(\frac{N-m}{N}\right) e^{-\delta\log\delta}$
- If f is convex-up fct attain maximum at $t=\frac{1}{2}$ (Recall $m \le \frac{N}{2}$). So

$$f\left(\tfrac{1}{2}\right) = \tfrac{1}{2}\log\tfrac{1}{2} + \tfrac{\delta}{2}\log\tfrac{\delta}{2} + \left(1-\tfrac{1+\delta}{2}\right)\log\left(1-\tfrac{1+\delta}{2}\right) = \log 2 - \left(\tfrac{\delta}{2}\log\tfrac{\delta}{2} + \tfrac{1-\delta}{2}\log\left(\tfrac{1-\delta}{2}\right)\right) = \log 2 + O(\delta\log\delta)$$

Estimate of a_{m+1}/a_m $\left(\frac{N}{m}\right)^{1+\delta}\left(\frac{N-m}{N}\right) e^{-\delta\log\delta} \cdot (1+\delta)^\ell \cdot \left(\frac{m+1}{N}\right)^\ell \underset{\text{at } m=\frac{N}{2}}{\le} \left(\frac{1}{2}\right)^{\ell-\delta} e^{-O(\delta(\log\delta+\ell))}$

Hence we see even when $\ell=2$, the term is still $\sim \frac{1}{2}$, as claimed in strategy of proof

Summing up, when N large $\sum_{1\le m\le N/2} a_m \sim$ Very small probability for large N.

It left to rule out anomalies. ie. those Γ with double edges ⚯ and loops ◌: we see their expectation are both indep of N.

(1) $\mathbb{E}(\Gamma \text{ has loops}) = \mathbb{E}(v \in V \mid \pi_i(v) = v \text{ for some } i \le \ell) = \ell$

$\mathbb{P}(\pi_i(1) = 1) = \frac{1}{N} \Rightarrow \mathbb{E}(v \in V : \pi_i(v) = v) = \frac{|V|}{N} = 1$

(2) $\mathbb{E}(\Gamma \text{ has mult-edges}) = \mathbb{E}(v \in V \mid \pi_i(v) = \pi_j(v) \text{ for some } i,j) = \binom{\ell}{2}$

as $\mathbb{P}(\pi_i(1) = \pi_j(1)) = \frac{1}{N}$, $\mathbb{E}(v \in V, \pi_i(v) = \pi_j(v)) = 1$

$\mathbb{P}(\Gamma \text{ has} \le 4\ell \text{ loops and} \le 2\ell^2 \text{ mult-edges}) \ge \frac{1}{2}$

as π_i are uniformly distributed

$\mathbb{P}(\text{loops} \ge 4\mathbb{E}(\text{loops})) \le 1/4$

similarly

$\mathbb{P}(\text{mult-edges} \le 4\mathbb{E}(\text{edges})) \le 1/2$

Conclusion: $\mathbb{P}(\Gamma \text{ } \delta\text{-expander} \le 4\ell \text{ loops} \le 2\ell^2 \text{ mult edges}) \ge \frac{1}{2}$ - very small Prob ≥ 0

□

Brilliant remark [entropy] Note the prob of a Γ being not a expander is per our argument corresponding to the case which entropy is small. (for large N vertices/particles). This resembles the physics intuition that choosing a N-particle system at random, the chance of hitting a low entropy system is small.

4. Cheeger's ineq (Discrete) Dodziuk'84, Alon-Milman'85

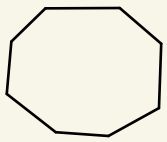
Γ is (n,d)-graph if Γ is n-vertices with deg d (regular). Now let $\Gamma \in (-,d)$-graph

Prop: Γ is δd-edge expander then $\frac{\delta^2}{4}$-spec exp. i.e. $\lambda_1 \le (1-\frac{\delta^2}{4})d$.

(Note 2- is possible) c.f. Tao's Expansion book

Example showing one can't do better than $\frac{\delta^2}{2}$. S = n-vertices at bottom of graph

$\partial_{edge} = 2$, $d = 2$ } this is $\frac{2}{n}$ edge-exp. here $\delta = \frac{1}{n}$



$2n$-vertices

Recall f on $\{e^{2\pi i \frac{k}{n}}\}$. Then $f(z) = z^k$ gives an eigenfcts. of

$Ad_\Gamma f(v_i) = \frac{1}{2}(f(v_{i+1}) + f(v_{i-1}))$ i.e $Ad_\Gamma f(v_i) = \cos(\frac{2\pi}{n}) f(v_i)$

Now $\lambda_0 = 1 \ge \lambda_1 = \cos(\frac{2\pi}{n}) \ge \lambda_2 = \cos(\frac{4\pi}{n}) \ge \dots$ Also $\cos\epsilon \underset{\epsilon\to 0}{\Rightarrow} 1-\frac{\epsilon^2}{2}$. So in this case the λ_1 is $\frac{\delta^2}{2}$ indeed. So the bound is tight.

Lemma: Let Γ be δd-edge exp. $f: V \to \mathbb{R}_{\ge 0}$ with $|\mathrm{supp}\, f| \le \frac{|V|}{2}$. Then

$$\langle Ad_\Gamma f, f\rangle \le d(1-\frac{\delta^2}{4})|f|_2^2$$

Pf of Prop assuming Lemma: Consider spectral decomposition of $L^2(\Gamma)$ $f_0 = id$. $f_1 \cdots$

Suff to show $\forall \phi \perp f_0$ $\langle Ad_\Gamma \phi, \phi\rangle \le d(1-\frac{\delta^2}{9})$. Also we can assume WLOG that f_i (hence ϕ) are real-valued. write:

$\phi = \phi_+ - \phi_- + t_0$ where $\phi_\pm$ non-neg. to const. WT shift t_0 so that $\phi_\pm$ are equally proportionate. i.e.

$\exists\, t_0$ s.t. $|\{v \mid \phi(v) \le t_0\}| \le \frac{|V|}{2}$ & $|\{v \mid \phi(v) > t_0\}| \le \frac{|V|}{2}$. Now

$\langle Ad(\phi - t_0\cdot \mathbb{1}), \phi - t_0\cdot\mathbb{1}\rangle = \langle Ad\,\phi, \phi\rangle + d\langle t_0\cdot\mathbb{1}, t_0\cdot\mathbb{1}\rangle = \langle Ad\,\phi,\phi\rangle + dt_0^2$ (*)

Now LHS $= \langle Ad(\phi_+ + \phi_-), \phi_+ + \phi_-\rangle \ge \langle Ad\,\phi, \phi\rangle$

Now $\langle Ad(\phi_+ + \phi_-), \phi_+ + \phi_-\rangle = \langle Ad\,\phi_+, \phi_+\rangle + \langle Ad\,\phi_-, \phi_-\rangle - 2\langle Ad\,\phi_+, \phi_-\rangle$ (≥ 0 by noneg)

Now by the Lemma we have $\langle Ad\,\phi_-, \phi_+\rangle \le d\left(1-\frac{\delta^2}{8}\right)\left(|\phi_+|^2+|\phi_-|^2\right)$

Now $|\phi_+|^2+|\phi_-|^2 = |\phi^{\subseteq \mathrm{supp}} - t_0 \mathbb{1}|^2 = |\phi|^2 + t_0^2$, But now (*) has extra.

dt_0^2 - factor cancels. Altogether $\langle Ad\,\phi_-, \phi_+\rangle \le \left(1-\frac{\delta^2}{4}\right)\cdot d \cdot 1$ □

Now we prove the **Lemma**.

Step 0: This is true for $f = \mathbb{1}_S$ $|S| \le \frac{|V|}{2}$. This is definition of vertex-expander

$\langle Ad(\mathbb{1}_S), \mathbb{1}_S\rangle = |\{(v,w)\in E,\ v,w\in S\}| = d|S| - |\{(v,w)\in E \mid v\in S,\ w\notin S\}| = d|S| - |\partial S|$

$\langle Ad(\mathbb{1}_S), \mathbb{1}_S\rangle \le (1-\delta)\, d\, |f|_2^2$ as $|f|_2^2 = |S|$.

Step 1: Decomp f as linear comb of fct $\mathbb{1}_S$ for $S_t = \{v \mid f(v)\ge t\}$

$f = \sum_t g(t)\,\mathbb{1}_{S_t}$ so by using discrete measure $d\delta_t$

$$\langle Ad\,f, f\rangle = \left\langle Ad \int_0^\infty \mathbb{1}_{S_t}\, d\delta_t, \int_0^\infty \mathbb{1}_{S_t}, d\delta_t \right\rangle = \int_0^\infty\int_0^\infty \langle Ad\,\mathbb{1}_{S_{t_0}}, \mathbb{1}_{S_{t_1}}\rangle d\delta_{t_0} d\delta_{t_1}$$

$$\overset{\text{symmetry}}{=} 2\int_0^\infty\int_0^{t_0} \langle Ad\,\mathbb{1}_{S_{t_0}}, \mathbb{1}_{S_{t_1}}\rangle dt_0\, dt_1 \qquad (\boxtimes)$$

Now $\langle Ad\,\mathbb{1}_{S_{t_0}}, \mathbb{1}_{S_{t_1}}\rangle \le d\min(|S_{t_0}|, |S_{t_1}|) = d|S_{t_0}|$ (bound 1)

also $\overset{\text{vertex-exp}}{\le} (1-\delta)\, d \max(|S_{t_0}|, |S_{t_1}|) = (1-\delta)\, d\, |S_{t_1}|$ (bound 2)

we use (bound 1) if $t_1 < (1-\epsilon)t_0$ Assuming $t_0 > t_1$

(bound 2) if $(1-\epsilon)t_0 \le t_1 \le t_0$

So $(\boxtimes) \le 2(1-\delta)d \int_0^\infty \int_{(1-\epsilon)t_0}^{t_0} |S_{t_1}|\, dt_1\, dt_0 + 2d\int_0^\infty\int_0^{(1-\epsilon)t_0} |S_{t_0}|\, dt_1\, dt_0$

$$= 2(1-\delta)d \int_0^\infty \left((1-\epsilon)^{-1}-1\right) t\, |S_{t_1}|\, dt_1 + 2d\int_0^\infty (1-\epsilon)\, t_0\, |S_{t_0}|\, dt_0$$

$$= 2d\,\underbrace{\left((1-\delta)\left((1-\epsilon)^{-1}-1\right)+(1-\epsilon)\right)}_{C_{\delta,\epsilon}} \int_0^\infty t\,|S_t|\, dt$$

choose $r = 1-\epsilon$ so that $(1-\delta)(r^{-1}-1)+r$ is minimal. take derivative.

$(-(1-\delta)r^{-2}+1 = 0$; i.e $r = \sqrt{1-\delta}$, $\epsilon = 1-\sqrt{1-\delta})$

So $C_{\epsilon,\delta} = 2\sqrt{1-\delta} - (1-\delta) \le 2\left(1 - \frac{\delta}{2} - \frac{\delta^2}{8}\right) - (1-\delta) = 1 - \frac{\delta^2}{4}$ □

Second pf (By Prob method): By contrapositive $\langle Ad f, f\rangle \ge d(1-\varepsilon)|f|_2$ for some $f \perp \mathbb{1}$.

we want to show $\exists$ set with small boundary

$$\frac{\sum_{(u,v)\in E}(f(u)-f(v))^2}{\sum f(v)^2} = \frac{d\sum f(u)^2 + \sum f(v)^2 - 2\sum_{(u,v)\in E} f(u)f(v)}{\sum f(v)^2} = 2d - \frac{2\langle f, Af\rangle}{|f|_2^2}$$

Hence this $\le 2\varepsilon d$.

On the other hand, $\otimes \ge \frac{\sum_{(u,v)\in E}(\phi_+(u)-\phi_+(v))^2 + \sum_{\epsilon E}(\phi_-(u)-\phi_-(v))^2}{|\phi_+|_2^2 + |\phi_-|_2^2 - t_0^2}$ Note the choice of ϕ_+, ϕ_- is the same as previous proof.

$\ge \frac{\text{same sum}}{|\phi_+|_2^2 + |\phi_-|_2^2} \ge \max\left(\frac{a}{b}, \frac{c}{d}\right) \ge \frac{a+c}{b+d}$ $\frac{\sum(\phi_+(u)-\phi_+(v))^2}{|\phi_+|_2^2}$ or $\frac{\sum(\phi_-(u)-\phi_-(v))^2}{|\phi_-|_2^2}$

Lemma: Let $f: V \to \mathbb{R}_{\ge 0}$ then $\exists S \subset \operatorname{supp} g$ s.t. $\partial_{\text{edge}}|S| \le \frac{\sum|f(u)-f(v)|}{\sum f(v)}|S|$

Pf: Assume WLOG $\max f(v) = 1$. Then choose t uniformly between 0 and 1

$$\mathbb{E}(|S_t|) = \sum_{v\in V}\mathbb{P}(v\in S_t) = \sum_{v\in V}\mathbb{P}(t\le f(v)) \overset{t \text{ is unif var}}{=\!=} \sum_{v\in V} f(v)$$

$$\mathbb{E}(|\partial_{\text{edge}} S_t|) = \sum_{v,w\in E}\mathbb{P}(v\in S_t, w\notin S_t) = \sum_{\substack{v,w\in E \\ f(w)\le f(v)}} f(v) - f(w)$$

So $\mathbb{E}\left[|S_t|\cdot\underbrace{\left(\sum_{\substack{v,w\in E \\ f(w)<f(v)}} f(v)-f(w)\right)}_{A_t} - \underbrace{|\partial_{\text{edge}} S_t|\cdot\sum_{v\in V} f(v)}_{B_t}\right] = 0 \Rightarrow A_t \ge B_t$ for some t □

Rmk: This part is what key part of proving Cheeger in discrete/cont case. namely bounding the Rayleigh Const ($\otimes$) by the "ℓ^1-Rayleigh const".

Apply **Lemma** to $g=\phi_+^2$ $\quad \frac{\sum|\phi_+^2(u)-\phi_+^2(v)|}{|\phi_+|_2^2} \overset{C.S}{\leq} \frac{\sqrt{\sum_E |\phi_+(u)-\phi_+(v)|^2}\sqrt{\sum_E|\phi_+(u)+\phi_+(v)|^2}}{\sqrt{|\phi_+|_2^2}\sqrt{|\phi_+|_2^2}}$

$\leq \sqrt{2\varepsilon d}\cdot 2\sqrt{d} = \sqrt{8\varepsilon}\cdot d$

$\leq\sqrt{2\varepsilon d} = R(Ad.f)$ by lemma $\qquad \leq\sqrt{d}$ $(a^2+b^2\leq 2(a^2+b^2))$

the same estimate for ϕ_- hence

$\exists S$ s.t. $|\partial_{edge} S| \leq \sqrt{2\varepsilon}\cdot d\cdot|S|$. But by assumption Γ is expander. some we have a contradiction if $\sqrt{2\varepsilon}<\delta$ i.e $\varepsilon=\frac{\delta^2}{2}$ the best spectral bound □

5. Weaker ALon-Boppana bound

Recall AB-bound gives $\lambda_2 \geq 2\sqrt{d-1}\left(1-O\left(\frac{1}{\Delta^2}\right)\right)$. we prove instead:

Prop: $\max_{i=2,\dots N}|\lambda_i| \geq 2\sqrt{d-1}\left(1-O\left(\frac{\log\Delta}{\Delta}\right)\right)$ $\quad \Delta=\text{diam}\,\Gamma. \gg \log_{d-1}|V|$

Rmk: This roughly means "no crazy-super expansion"

pf: Take $H=Ad^{2k}$ and $f\perp\mathbb{1}$. Then $|R(Ad^{2k}f.f)|\leq \max_{2\leq i\leq|V|}\lambda_i^{2k}$ where

$R(\Delta,f)=\frac{\langle\Delta f.f\rangle}{|f|_2^2}$ the Rayleigh quotient. So we want to find the largest f. Consider v_1, v_2 with $d(v_1,v_2)=\Delta$. Then $f=\mathbb{1}_{v_1}-\mathbb{1}_{v_2}$ Now let $k=\left\lfloor\frac{\Delta-1}{2}\right\rfloor$. Then

$$R(Ad^{2k}f,f)=\frac{\langle\mathbb{1}_{v_1},Ad^{2k}\mathbb{1}_{v_1}\rangle+\langle\mathbb{1}_{v_2},Ad^{2k}\mathbb{1}_{v_2}\rangle+0}{\geq|V|} \quad \leftarrow \text{as no path of length } 2k \text{ from } v_1 \text{ to } v_2$$

$$=\frac{1}{2}\sum_{i=1,2}\#\text{ of } 2k\text{ steps from } v_i \text{ to itself} \geq t_{d,2k}$$

$t_{d,2k}$: # trivial walks on trees of deg d and $2k$ steps!

Now $t_{d,2k}\geq$ # correct expression with n-parenthesis $\cdot(d-1)^k$

Catalan no. $C_k=\frac{\binom{2k}{k}}{k+1}$

Hence $t_{d,2k}\geq\frac{1}{k+1}\binom{2k}{k}(d-1)^k \gg \frac{1}{k}\frac{2^{2k}}{\sqrt{k}}(d-1)^k$ □

pf of this equality:
$C_0=1$. $C_{n+1}=\sum_{i=0}^{n}C_iC_{n-i}$ and prove inductively

6. Construction of Expander Graph

Magulis's construction: $\mathbb{Z}^2 \rtimes SL_2(\mathbb{R})$ and any point is of the form $\begin{pmatrix} a & b & x \\ c & d & y \\ & & 1 \end{pmatrix}$.

where $SL_2(\mathbb{R})$ acts on $\mathbb{Z}^2$ by $\begin{pmatrix} a & b & x \\ c & d & y \\ & & 1 \end{pmatrix}\begin{pmatrix} m \\ n \\ 1 \end{pmatrix}$

Thm [Magulis] Let $G = SL_2(\mathbb{Z}) \ltimes \mathbb{Z}^2$ Let S be a symm gen set. For $n \geq 2$

$\pi_n : G \to SL_2(\mathbb{Z}/n\mathbb{Z}) \ltimes (\mathbb{Z}/n\mathbb{Z})^2$ the mod n-reduction.

Then $\exists \delta > 0$. s.t. the graphs $\Gamma(G(\mathbb{Z}/n\mathbb{Z}) \ltimes (\mathbb{Z}/n\mathbb{Z})^2, \pi_n(S))$ a δ-spectral expander. ← Schreier Graph

Lemma Let $S \subset SL_2(\mathbb{Z})$ a finite gen set. μ a probability measure on $\mathbb{Z}^2$.

Supp $|s*\mu - \mu| \leq \varepsilon \quad \forall s \in S$. then $\mu(\{0\}) = 1 - \mathcal{O}_S(\varepsilon)$

Pf: Consider $a = \begin{pmatrix} 1 & 2 \\ & 1 \end{pmatrix}$ and $b = \begin{pmatrix} 1 & \\ 2 & 1 \end{pmatrix}$. Then both a & b can be written as a word of length $\mathcal{O}_S(1)$ in S. Consider now the ping-pong Lemma (Schottky / Klein)

Let $A = \{(x,y) \in \mathbb{Z}^2 : |x| < |y|\}$ $\quad B = \{(x,y) \in \mathbb{Z}^2, \ |x| > |y|\}$

then $a^n A \subset B \ \forall n \neq 0$ as $\begin{pmatrix} 1 & 2 \\ & 1 \end{pmatrix}^n \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x+2ny \\ y \end{pmatrix}$

Similarly $b^n B \subset A$ for all $n \neq 0$

Scholium: [Use of ping-pong] One typical thing is to prove $\langle a, b \rangle$ gens a Free subgrp Prove any reduced word begin and end with a or a^{-1} is $\neq id$ (this is our A) And then the other are B. with the ping-pong action is conjugation by a.

Now since $|a*\mu - \mu| = \mathcal{O}_S(\varepsilon)$ by the assumption of Lemma. Now

$$\mu(B) \underset{aA \subset B}{\geq} \mu(aA) = \mu(A) + \mathcal{O}_S(\varepsilon)$$ ← in ε but not ε^n because of Δ-ineq

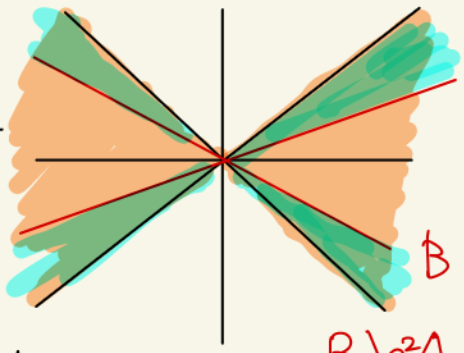
similarly $\mu(A) \geq \mu(bB) = \mu(B) + \mathcal{O}_S(\varepsilon)$

hence $\mu(B) = \mu(A) + \mathcal{O}_S(\varepsilon) = \mu(aA) + \mathcal{O}_S(\varepsilon) = \mu(a^2A) + \mathcal{O}_S(\varepsilon)$

Because $(a^2A \subset B) \quad \mu(B \setminus a^2A) = \mathcal{O}_S(\varepsilon)$

Ex: Can cover $\mathbb{Z}^2 \setminus \{0\}$ by a small ($< \infty$) no. of sets $\phi(B \setminus a^2A) \ \phi \in SL_2(\mathbb{Z})$

Therefore $\mu(\mathbb{Z}^2 \setminus \{0\}) = \mathcal{O}(\varepsilon)$ □



Pf of thm: Let e_1, e_2 be the generators of $\mathbb{Z}^2$. Prove by contradiction.

Assume $\exists\, 2 \le n_1 \le n_2 \le \dots$

and $f_i : (\mathbb{Z}/n_i\mathbb{Z})^2 \to \mathbb{R}$ with $\max_{s\in S} |S_* f_i - f_i|_2 \to 0$

Cassume also $f_i \in L^2_0(\mathbb{Z}/n_i\mathbb{Z})$ "cuspidal" i.e. the statement of thm is false.

Then: $|e_j \cdot f_i - f_i|_2 \longrightarrow o_S(1)\cdot \mathcal{O}_S(1) = o_S(1)$ for $j = 1, 2$ and $i \to \infty$.

as e_j are words of length $\mathcal{O}_S(1)$

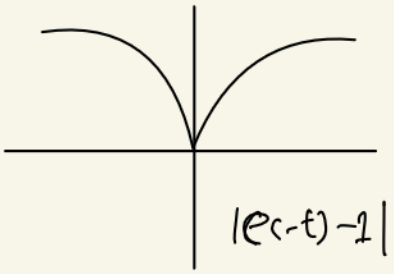
Now the Fourier transform $\hat{f}(\xi_1, \xi_2) = \frac{1}{n_i} \sum_{x_1, x_2 \in \mathbb{Z}/n_i\mathbb{Z}} f_{n_i}(x_1, x_2)\, e\left(\frac{-x_1\xi_1 - x_2\xi_2}{n_i}\right)$

Now

$$\widehat{|e_j \cdot f_i - f_i|}_2 = |e_j \hat{f}_i - \hat{f}_i|_2 = o_S(1) \quad \text{but}$$

$$\widehat{|e_j \cdot f_i - f_i|}_2 = |e(-\xi_j/n) \hat{f}_i - \hat{f}_i|_2 = |(e(-\xi_j/n) - 1)\hat{f}_i|_2 = o_S(1)$$

So almost all of the of $\hat{f}_i$ is concentrated on the origin.



i.e. $\forall \varepsilon, \exists N$ st. $\left|\widehat{e_j \cdot f_i} - \hat{f}_i\big|_{[-\frac{\varepsilon N_i}{2}, \frac{\varepsilon N_i}{2}]^2}\right|_2 \le \varepsilon$

for all $i \ge N$.

$B_{\varepsilon N_i}$

we can lift the function $\hat{f}_i|_{B_{\varepsilon N_i}}$ to a fct $g_i : \mathbb{Z}^2 \to \mathbb{C}$. that is supp on $B_{\varepsilon N_i} \cap \mathbb{Z}^2$.

For $s \in S$, $|\widehat{S_* f_i - f_i}|_2 = o(1) = |\hat{f}_i \circ s^t - \hat{f}_i|_2 = |(s^t)_* \hat{f}_i - \hat{f}_i|_2$

$$\sum (S_* f_{n_i}(x_1, x_2))\, e\left(\frac{-x_i\xi_i}{n_i}\right) = \sum f_n(s^{-1}(x_1, x_2))\, e\left(\frac{-x_i\xi_i}{n_i}\right) = \sum f_n(x_1, x_2)\, e\left(\frac{-x_i(s\xi_i)}{n_i}\right)$$

Then $|g_i \circ s^t - g_i|_2 = \mathcal{O}_S(1)$ provided that No overflow! i.e. $s^t \cdot B_{\varepsilon N_i} \subset B_{N_i}$ for ε small enough. so the reduction to $\mathbb{Z}/N\mathbb{Z}$ do not change the support

Now Lemma says $g_{(0,0)} = 1 - \mathcal{O}_S(1)$ However $g_i(0) = \hat{f}_i(0) + \varepsilon = \varepsilon$

But $f_i \perp 1$. ↯ □

§6.1. Expansion in $SL_3(\mathbb{Z}/n\mathbb{Z})$

Thm$^+$ (this is an extension/abstraction of Magulis' example) Recall for any n, the mod n reduction: $\pi: G \to G_n$ Take $G_n = \begin{pmatrix} * & * & * \\ * & * & * \\ & & 1 \end{pmatrix}$ and $H_n = \begin{pmatrix} 1 & & * \\ & 1 & * \\ & & 1 \end{pmatrix}$

if $v \in V$ unit vector satisfies $|\pi_n(s)v - v| < \varepsilon \quad \forall s \in S$.

(+) then $|hv - v| = O_S(\varepsilon) \quad \forall h \in H_n$

Furthermore, if (+) holds for $\varepsilon < c(S)$ a const. then $\exists$ H_n-invariant vector v_{fo} $\forall n$ (universally chosen)

This is known as Selberg ppty relative to H.

Example: [Thm$^+ \Rightarrow$ Thm] Take $V = L^2_0(\mathbb{Z}/n\mathbb{Z})$ But Selberg ppty tells $V \not\ni H_n$-inv. vector. (Because the only such vector is const. But $V \perp \mathbb{1}$) So (+) is false when ε is small w.r.t. S. and the proof by contradiction follows.

Recall a few facts about unitary rep:

(1) First we see $H_n \cong (\mathbb{Z}/n\mathbb{Z})^2$ then $hv = e\left(\frac{h_1\xi_1 + h_2\xi_2}{n}\right)v$ for H_n-rep $v \in V$. Now how $SL_2(\mathbb{Z})$ acts on V? $g = \begin{pmatrix} A & * \\ & 1 \end{pmatrix}$ claim $g: V_\xi \longmapsto V_{(A^{-1})^t\xi}$

bec. $hgv = g(g^{-1}hg)v = g\left(e\left(\frac{\langle g^{-1}hg, \xi\rangle}{n}\right)v\right) = e\left(\frac{\langle g^{-1}hg, \xi\rangle}{n}\right)gv$

But $g^{-1}hg = \begin{pmatrix} 1 & A^{-1}h \\ & 1 \end{pmatrix}$ so indeed the assertion is true.

Now the previous argument carries over to the rep theory setting,

$$\left|\sum_{\xi \in (\mathbb{Z}/n\mathbb{Z})^2} e\left(\frac{\xi_j}{n}\right)v_\xi - v_\xi\right|_2^2 = O_S(\xi) \Rightarrow \left|v - \sum_{\xi \in B_{e,n}} v_\xi\right| = O_S(\xi)$$

($e_j \cdot v$) and then lift the function as before, also apply the Lemma from yesterday $\square$

Now we prove there exists indeed a H_n-invariant vector v.

One create average vector $v_n = \frac{1}{|H_n|} \sum_{h_n \in H_n} h_n v$. Now we see

(1) $|v_n - v| \to O_S(\varepsilon)$ and (2) $|v|_2 = 1$ implies $\exists$ v_n conv to a nonzero vector v independent of n

Thm: [Selberg ppty of SL_3] $\Gamma(SL_3(\mathbb{Z}/n\mathbb{Z}), \pi_n(S))$ form expander family.

Lemma. Choose generator S to be elementary matrices $\left(\begin{pmatrix} 1 & 0 & 1 \\ & 1 & \\ & & 1 \end{pmatrix} \begin{pmatrix} 1 & & \\ & 1 & 0 \\ & 1 & 1 \end{pmatrix} \cdots\right)$. Then

Any $f_n : SL_3(\mathbb{Z}/n\mathbb{Z}) \to \mathbb{C}$ with $|f - g^* f|_2 < \varepsilon \quad \forall g \in \pi_n(S)$

Then $|f - g^* f|_2 = O(\varepsilon) \quad \forall g \in SL_3(\mathbb{Z}/n\mathbb{Z})$

Ex: $\exists$ abs const R (indep of n) such that every $g \in SL_3(\mathbb{Z}/n\mathbb{Z})$ can be written as a word of the form $g = s_1^{m_1} \cdots s_r^{m_r}$ $r = |R|$ with $s_i \in \pi_n(S)$

Claim $|f - g^* f|_2 = O(1)$ for $g = s^m$ for any $s \in \pi_n(S)$ and $m \in \mathbb{Z} \setminus \{0\}$

The reason of the claim is we can choose

$$S = \begin{pmatrix} 1 & 1 & 1 \\ & 1 & \\ & & 1 \end{pmatrix} \in \begin{pmatrix} 1 & 1 & * \\ & 1 & * \\ & & 1 \end{pmatrix} < SL_2(\mathbb{Z}/n\mathbb{Z}) \ltimes (\mathbb{Z}/n\mathbb{Z})^2 = G_n'$$

Note $\pi_n(S) \cap G_n'$ generates G_n'. So apply Thm$^+$ we see $|f - hf| = O(\varepsilon)$ for all $h \in H_n$ In particular $|f - s^m f| = O(\varepsilon)$ □

Pf of Thm: Supp Contrary. then $\exists f_1, f_2, \ldots$ on $SL_3(\mathbb{Z}/n_i\mathbb{Z})$ with $f_i \perp 1$ and We can always work with S = elementary. other generators gives $|f_i - s^* f_i| \le \varepsilon \ \forall s \in S$ a finite perturbation To the error term. Now the Lemma gives $|f_i - g^* f_i| = O_S(\varepsilon)$ Use the averaging argument as above. we get $\lightning$ □

7. Kazdhan's PPty (T)

[ppty T] $\mathbb{1}$ is isolated pt in $\hat{G}$. In other words, for generating set, that any unitary rep $G \curvearrowright \mathcal{H}$. Then $\forall v \in V$. either $|\pi(s)v - v| \geq \delta$ or $\exists$ nonzero G-inv vector.

For cont grp. replace S by cpt sets. and unitary rep by continuous unitary reps.

Ex/Nonex: $\mathbb{Z}$ does not have ppty (T). By finding $\xi \in S^1 \cong \hat{\mathbb{Z}}$ so that ξ^n is close to 1. Also infinite amenable groups does not have ppty (T)

Nomenklatur: (T) stands for open set and T stands for trivial :)

Lemma G discrete with ppty. (T). Then $\exists C$ G/N, $S \pmod N$ forms exp family for any finite gen set S.

Pf: Apply ppty (T) to $G \curvearrowright L^2_0(G/N)$. But nonconst fcn tells

$$|\pi(s)v - v| \geq \delta \quad \forall\, v \in L^2_0(G/N)$$ □

As proof of ppty (T) for infinite unitary rep resembles that of finite (mod FA).

Def [relative ppty (T)] $H < G$. So (G, H) has relative ppty (T) if $\exists S$ gen set $\ni G$.

either $|\pi(s)v - v| \geq \delta$ or $\exists$ H-invariant vector $\neq 0$.

Prop Let $G = SL_2(\mathbb{Z}) \ltimes \mathbb{Z}^2$, $H = \mathbb{Z}^2 \lhd G$ Then (G, H) has relative ppty (T)

Pf Given proof of Thm$^+$ in §G.1, we again by explicit understanding of the induction structure $\mathrm{ind}_{\mathbb{Z}^2}^{G} \chi$. $V_\xi \mapsto V_{(A^{-1})^t \xi}$ $v \mapsto gv$

$\|\pi(e_j)v - v\| \leq \varepsilon$ and $\|v - \sum_{\xi \in B_\xi'} v_\xi\| = \mathcal{O}(\varepsilon)$ Concentration of mass like Thm$^+$ for ε small enough w.r.t. S. i.e. $S \cdot [-\varepsilon, \varepsilon]^2 \subset [-\frac{1}{2}, \frac{1}{2}]^2$

e.g $S = \left[\begin{smallmatrix} 1 & 1 \\ 2 & 1 \end{smallmatrix}\right] \left[\begin{smallmatrix} 1 & 2 \\ 1 & 1 \end{smallmatrix}\right]$ and μ a prob-meas on $\mathbb{R}^2 \setminus \{0,0\}$. Then $\exists s \in S$ s.t. $|s^*\mu - \mu| > \delta$ by ping-pong phenomenon;

$A = \{(x,y) \in \mathbb{R}^2 \setminus \{0,0\} \mid |x| < |y|\}$ $B = \{(x,y) \in \mathbb{R}^2 \setminus \{0,0\} \mid |x| > |y|\}$

Thm: $SL_3(\mathbb{Z})$ has ppty T.

Pf: same as previous. Choose elementary matrices as gen. Then for V unitary.

$|v - sv|_2 < \varepsilon \ \forall s \in S$ then $|v - gv| = O(\varepsilon) \ \forall g \in G$

(By the Lemma in §6 1). But the question is how to do the averaging trick here. **Use the fact that any (small) bound set in unitary rep will have a unique center of mass**

Consider convex hull $\overline{C(Gv)}$. The claim is $0 \notin \overline{C(Gv)}$ as by our observation $\overline{C(Gv)} \subset \overline{C(B)} = B$. Now use

[Bruhat-Tits fixed pt thm] Γ grp of isometry on CAT(0)-space has fixed pt. i.e $G \curvearrowright V$ unitary. $C \subset V$ closed convex bdd non-empty. Then the stabilizer $\mathrm{Stab}_G C$ has a fixed pt action on C. Then define measure as distance to C.

ppty (T) does not hold for $SL_2(\mathbb{Z})$. first see easily ppty (T) are inherited by subgrp of finite index. Now it suff to see the $F_2 \cong \langle \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} \rangle$ (of index 12)

A free group does not have ppty (T). Consider:

$(x_1^{r_1} \cdots x_k^{r_k})(m) = m + \sum r_i$ induces isometry rep on $l^2(\mathbb{Z})$ w/o fixed vectors. but uniform distribution on $[0, M] \subset \mathbb{Z}$ for M big is almost fixed by $\{x_1, \ldots x_k\}$. □

Now How to show S gives $\Gamma(SL_2(\mathbb{Z}/N\mathbb{Z}), S \bmod N)$ is an expander graph.

proof 1: Use modular form: Selberg 3/16

2: Sarnak-Xue

3. Bourgain-Gamburd (We only need $\langle S \rangle$ to be Zariski-dense)

8. Ramanujan Graph

Recall Alon-Boppana told us the spectral bound is tight. First example in LPS. The proof used estimate of coeffs of modular form. A weaker form Sarnak-Davidoff-Valette used elementary proof.

General proof: counting non-backtracking random walk (Chebyshev polynomial)

Def [Ramanujan] $\Gamma(n,d)$ has all eigenval $|\lambda_i| \le 2\sqrt{d-1}$ indep of n

Consider a closed walk. A diagonalizable. then $\sum \lambda_i = \mathrm{Tr}\, A = \sum a_{ii}$

$\sum \lambda_i^n = \mathrm{Tr}(\mathrm{Ad}\,\Gamma)^n = \sum ((\mathrm{Ad}\,\Gamma)^n)_{ii}$:= # path of length n from i to i

General strategy: (n even) $\sum \lambda_i^n \ge \lambda_{i_0}^n$ So $\lambda_{i_0}^n \le$ # closed path of length n

If every nontrivial eigenval λ_i has multiplicity M, then

$\sum \lambda_i^n \ge M \lambda_{i_0}^n$ for every nontrivial n and

$\lambda_i^n \le \frac{1}{M}$ # closed walk of length n

problem of counting tree. gives you lower bound. known to physicists Re-invented by Sarnak

Refinement sometimes it's easier or more natural to count nonbacktracking walks. i.e $i_m i_2 \ne i_m \ \forall\, 0 \le m \le n-1$

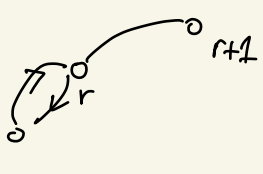
$\sum_{j \ge 0}$ #non-backtracking walks of length $n-2j$ = $\sum$ Chebyshev polynomials $\begin{cases} \text{if } |\lambda_j| \le \sqrt{d-1} \text{ very small} \\ \text{if } \lambda_j > 2\sqrt{d-1} \text{ +ve} \end{cases}$

A_r = non-backtracking matrix $(A_r)_{ij}$ # paths of length r from i to j without backtracking.

Lemma: For Γ deg d, $A_1^2 = A_2 + d \cdot I$ & $\forall r \ge 2$, $A_1 A_r = A_r A_1 = A_{r+1} + (d-1) A_{r-1}$

Pf: $(A_1^2)_{i,j}$: # paths from i to j $= \begin{cases} \#\text{ non-backtracking path of length 2 from } i \text{ to } j & (i \ne j) \\ |\#\text{ backtracking} = d| + \#\text{ nonbacktracking}. & (i = j) \end{cases}$

The second identity is proven in a similar way. The -1 comes from the backtracking already happen in $(r-1)$-step. □



Cor: from previous Lemma one can form recursive relation on the coeffs. namely:

$$\sum_{r=0}^{\infty} A_r t^r = \frac{1-t^2}{1-At+(d-1)t^2} \quad \text{i.e} \quad 1-t^2 = (1-A_1 t+(d-1)t^2)\sum_{r=0}^{\infty} A_r t^r \text{ formally}$$

$A = A_1 = Ad_I$

Sketch of pf: coef of t^0 : I on both sides

t^1 : 0 on the left, $-A_1 + A_1 = 0$

t^2 : $-I$ on left, $(d-1)\cdot I - A_1 A_1 + A_2 = 0$ by Lemma above.

And induction gives you all. □

Cor: [Chebyshev polynomials] $T_m := \sum_{0\le r\le m/2} A_{m-2r}$. Then $\sum_{m=0}^{\infty} T_m t^m = \frac{1}{I-At+(k-1)t^2\cdot I}$ (A)

By multiplying both sides $\sum_r A_r t^r$ □

Rmk: The chebyshev poly of 2nd kind given by $U_n(\cos\theta) = \frac{\sin(n+1)\theta}{\sin\theta}$ then by trigonometry: $U_{n+1}(x) = 2xU_n(x) - U_{n-1}(x)$. So we have

$$\sum_{m=0}^{\infty} U_m(x) t^m = \frac{1}{1-2xt+t^2} \xrightarrow{\text{c.o.v}} \sum_{m=0}^{\infty} (d-1)^{\frac{m}{2}} U_m\left(\frac{x}{2\sqrt{d-1}}\right) t^m = \frac{1}{1-xt+(d-1)t} \quad \text{(B)}$$

Hence we proved: (by comparing coeffs between (A) and (B)):

Prop For $m\ge 0$. $T_m = (d-1)^{m/2} U_m\left(\frac{A}{2\sqrt{d-1}}\right)$. i.e

Pf: $\operatorname{Tr} T_m = (d-1)^{m/2} \operatorname{Tr}\left[U_m\left(\frac{A}{2\sqrt{d-1}}\right) = (d-1)^{\frac{m}{2}} \sum_{i=0}^{n-1} U_m\left(\frac{\lambda_i}{2\sqrt{d-1}}\right)\right]$

Hence $T_m = \sum_{0\le r\le m/2}$ # closed non-backtracking walks of length $m-2r$

Now the analysis of Chebyshev polynomial gives desirable results:

For $|t|\le 1$, $|U_m(t)| \le m+1$. (One can do better for $U_m(t)$ neg) meaning $|\lambda_i| \le 2\sqrt{d-1}$

$|t|>1$, it will be the (hyp trigonometric fct)

8.1 Explicit Ramanujan Cayley LPS & Margulis)

We will black-box the following thm:

Thm [Jacobi] Let $n>0$ odd. Let $r_4(n) = |\{m_0, m_1, m_2, m_3) \in \mathbb{Z}^4 : n = \sum m_i^2\}|$

then $r_4(n) = 8 \sum_{d \mid n} d$ Proved by modular form or Davidoff-Sonak-Valette.

In particular. $p = 8(p+1)$ integral solns

Cor: $\exists$ $8(p+1)$ quaternions $\alpha = a_0 + a_1 i + a_2 j + a_3 k \in \mathbb{H}(\mathbb{Z})$ with norm $N\alpha = p$

Exc: If $N\alpha = p$. for p odd. then either one a_i is odd and all others are even or the other way around. if $i=0$. then we call such α distinguished.

This get rds of four equiv classes. we want eventually the distinguished class only contains $(p+1)$-many.

$S_p = \{$distinguished element in $\mathbb{H}(\mathbb{Z})$ with $N\alpha = p\} = \{\alpha_1, \bar{\alpha_1}, \dots, \alpha_s, \bar{\alpha_s}\}$

Thm: Let $k \geq 1$, $\alpha \in \mathbb{H}(\mathbb{Z})$ s.t. $N(\alpha) = p^k$. Then α admits unique factorization

$$\alpha = \varepsilon p^r \omega_m$$

ε unit in $\mathbb{H}(\mathbb{Z})$
ω_m reduced word in S_p
of length $m = k - 2r$

Def [reduced]
A word in S_p is reduced if it has no subword of form $\alpha_i \bar{\alpha_i}$, $\bar{\alpha_i} \alpha_i$, β_j^2

Sketch of pf: Prove $\mathbb{H}(\mathbb{Z})$ is ED and count soln using Jacobi

$$p^k = a_0^2 + \dots + a_3^2 \text{ with } 8 \sum_{d \mid p^k} p = 8 \cdot \frac{p^{k+1} - 1}{p - 1}$$

Now # reduced words of length $m = \begin{cases} 1 & m = 0 \\ (p-1)p^{m-1} & \text{if } m \geq 1 \end{cases}$ and $\varepsilon \in \pm\{1, j, i, k\}$ are 8. $\square$

$\mathbb{H}(\mathbb{Z}) \xrightarrow[\text{Red mod } q]{\pi_q} \mathbb{H}(\mathbb{F}_q) \xrightarrow[\text{isom}]{\psi_q} M_2(\mathbb{F}_q)$ where ψ_q defined via the following Lemma:

Lemma: $\exists$ $\mathbb{F}_q$-soln of $x^2+y^2+1=0$ (as there are $\frac{q+1}{2}$ squares., hence two set $\{-x^2 : x \in \mathbb{F}_q\}$ and $\{y^2+1 : y \in \mathbb{F}_q\}$ must have nontrivial intersection. and hence soln $\square$

($\{-x^2\}$: $q+1/2$-many; $\{y^2+1\}$: $q+1/2$-many)

Now: $\psi_q : i \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $j \mapsto \begin{pmatrix} x & y \\ y & -x \end{pmatrix}$ $k \mapsto \begin{pmatrix} -y & x \\ x & -y \end{pmatrix}$ is an isom

We work with $S_{p,q} := \varphi(\psi_q(\pi_q(S_p)))$ with φ the projectivization. The upshot is for q large enough, the composition is isomorphism

Lemma: For $q > 2\sqrt{p}$, $|S_{p,q}| = |S_p| = p+1$

Sketch: Two integers are not mod q congruent if both are smaller $\sqrt{p}$. $\square$

Fact: $S_{p,q}$ generates $PGL_2(\mathbb{F}_q)$ and $X_{p,q} = \Gamma(PGL_2(\mathbb{F}_q), S_{p,q})$ is our Cayley graphs

Prop: $X_{p,q}$ are connected. Ramanujan Graphs. Now:

$$S_Q(p^m) = \{(x_0, \dots, x_3) \in \mathbb{Z}^4 \mid Q(x_0, \dots, x_3) = p\} \qquad Q(x_0, \dots x_3) = x_0^2 + q^2(x_1^2 + \cdots x_3^2)$$

Claim: $S_Q(p^m) = 2\sum_{0 \le r \le m/2} f_{m-2r}$ where f_{m-2r} are closed walks of length $m-2r$ on $X_{p,q}$ without backtracking

Recall $S_Q(p^m) = \#$ quaternions in $\mathbb{H}(q) = a_0 + q(a_1 i + a_2 j + a_3 k) \subset \mathbb{H}$ with norm p^m (Note $\mathbb{H}(q)$ is really q-congruence of $\mathbb{H}$ (same as $SL_2(q)$ in SL_2!))

So $\mathbb{H}/\mathbb{H}(q) = \mathbb{H}(\mathbb{F}_q)$. Hence in this picture:

Reduced words	$\Longleftrightarrow$	words w/o backtracking
red words $\cup$ product in $\mathbb{H}(q)$		closed words w/o. b.t. $\cup$

Note $\alpha_p \bar{\alpha}_p$ gives precisely b.t. as this is a scalar. so projectivization kills it. as $\alpha_p \bar{\alpha}_p = p \cdot I$

quaternions of norm $p^m \underset{UFD}{=}$ products of irred quaternions (All p splits through $\mathbb{H}(\mathbb{Z})$)

Hence they can written as m-many products. they are in 1-1 correspondence with

$\mathcal{E} \cdot p^r$ (reduced words of length $m-2r$). Under such Correspondence.

Elements of $\mathbb{H}(q)$ of norm $p^m \xleftrightarrow[\text{for } r \le \frac{m}{2}]{1:1}$ reduced words of length $\le m-2r$ with products reduces to $\mathbb{H}(q)$

then these are vanish under mod q - reduction. i.e those are $\mathbb{H}(\mathbb{F}_q)$ with only a_0 entries. These reduced words (mod q, upon projectivization) gives you at origin/identity.

Summing up. # closed red. words of length $\le m-2r$ give upper spectral bound (c.f. §8) are now related to # Elements of $\mathbb{H}(q)$ of norm $p^m \cong \#\, S_Q(p^m)$

Now Spectral problem $\longleftrightarrow$ Counting problem. now

In the GL_2 - analog:

$\mathbb{H}(\mathbb{Z})$	$GL_2(\mathbb{Z})$
$\mathbb{H}(q)$	$GL_2(q)$
$a_0 \in \mathbb{H}(\mathbb{F}_q)$	$\begin{pmatrix} a_0 & \\ & a_0 \end{pmatrix} \in GL_2(\mathbb{F}_p)$
$\mathrm{Proj}(a_0) = 1$	$\mathrm{Proj}\begin{pmatrix} a_0 & \\ & a_0 \end{pmatrix} = id$

A crude bound on S_Q + mult count $\xrightarrow{\text{D.S.V.}}$ A Good bound on all λ_j

A better bound on S_Q (modular form) $\xrightarrow{\text{L.P.S.}}$ Ramanujan Bound

Note also the finite picture $X_{p,q}$ really corresp to the $\Gamma(q)\backslash G(\mathbb{Q}_p)/G(\mathbb{Z}_p)$ in the adic picture. (Cf Lubotzsky's book §5 - §7) The key is Hensel's Lemma. i.e $\mathbb{F}_p$-roots can be lifted to $\mathbb{Z}_p$-roots. and we are back to:

$$\sum_{0 \le r \le m/2} \#\text{ closed paths of } m-2r = p^{m/2} \sum_{j=0}^{n-1} U_n\left(\frac{\lambda_j}{2\sqrt{p}}\right) \quad \star$$

Now recall the dichotomy above in §8.:

(a) If $|\lambda_j| \le 2\sqrt{p}$, $\frac{\lambda_0}{2\sqrt{p}} = \cos\theta_j$, for θ_j are real. So $\left|U_m\left(\frac{\lambda_j}{2\sqrt{p}}\right)\right| = \left|\frac{\sin(m+1)\theta}{\sin\theta}\right| \le m+1$

so the contribution of small eigenval ($\Leftrightarrow$ large gaps) is $\le n \cdot p^{m/2} \cdot (m+1)$ to ☆

(b) If $|\lambda_j| \ge 2\sqrt{p}$, then $U_m\left(\frac{\lambda}{2\sqrt{p}}\right)$ will be larger $\lambda = 2\sqrt{p}\cos\theta$ with $\theta = \begin{cases} i\psi & \text{if } \lambda \text{ +ve} \\ \pi + i\psi & \text{if } \lambda \text{ -ve} \end{cases}$ so

$$U_m\left(\frac{\lambda}{2\sqrt{p}}\right) = \frac{\sin(m+1)\theta}{\sin\theta} = \frac{\sin(m+1)i\psi}{\sin i\psi} = \frac{\sinh(m+1)\psi}{\sinh\psi}.$$ Now for large eigenval $|\lambda| > 2\sqrt{p}$

$$\frac{n}{2} S_Q(p^m) = p^{m/2} \sum_{j=0}^{n-1} U_m\left(\frac{\lambda_j}{2\sqrt{p}}\right) \ge M(\lambda) \cdot p^{m/2} \frac{\sinh(m+1)\psi}{\sinh\psi} - np^{m/2}(m+1)$$

where $M(\lambda)$ mult of $\lambda = \lambda_i$

lower bound of $S_Q(p^m)$

Plan: show $M(\lambda)$ is large for non-trivial λ. and then bound S_Q from above.

Scholium: Why is $X_{p,q}$ connected ? i.e why $\varphi \circ \Psi_q \circ \pi_q(S_n)$ gen $PGL_2(\mathbb{F}_q)$

This dates back to Dickson ~1900 that computes all subgrps of $PGL_2(\mathbb{F}_q)$ that is either small ($\# \le 60$) or metabelian, i.e $([[g_1, g_2], [g_3, g_4]] = 1 \ \forall\ g_i)$

Hence one suffices to show the grp generated by such is neither small nor metabel.

Claim: For any nontrivial λ, $M(\lambda) \ge \frac{q-1}{2}$

Thm [Frobenius] Let $q \ge 5$. The deg of any nontrivial rep $PSL_2(\mathbb{F}_q) \ge \frac{q-1}{2}$.

Now the mult of eigen corresp to deg of rep that they are large.

Next we get crude upper bound of $S_Q(p^m)$ for m even. one sees:

- $|X_0| \le p^{m/2}$
- $X_0^2 \equiv p^m \bmod q^2$ and so $X_0 \equiv \pm p^{m/2} \bmod q$

  So by Hensel's Lemma $X_0 \equiv \pm p^{m/2} \bmod q^2$

So there are $\le 2 \cdot \frac{2p^{m/2}+1}{2q^2} + 1$ choices of X_0. Now for fixed X_0, there are ? sols to $X_1^2 + X_2^2 + X_3^2 = \frac{p^m - X_0^2}{4q^2}$ Recall $r_3(n) = \#$ sol'n to $X_1^2 + X_2^2 + X_3^2 = n$

Lemma: $r_3(n) \le n^{1/2+\varepsilon}$ (recall $r_2(n) \overset{\text{Fermat}}{=} 4(d_1(n) - d_3(n))$ for d_i # divisors of n that are $\equiv i \ (4)$. So r_3 have trivial bound $\sum_{1 \le X_2 \le \sqrt{n}} r_2(n - X_2^2) \le \frac{1}{n^{1/2+\varepsilon}}$

So $S_Q(p^m) \ll_\varepsilon \left(\frac{p^{m/2}}{q^2}+1\right)\cdot\left(\frac{p^m}{q^2}\right)^{\frac{1}{2}+\varepsilon} = \frac{p^{m(1+\varepsilon)}}{q^3} + \frac{p^{\frac{m}{2}(1+2\varepsilon)}}{q}$ upper bound of $S_Q(p^m)$

Conclusion: Lower bound of $S_Q(p^m) \ll$ Upper bound of $S_Q(p^m)$. i.e.

$$\frac{q-1}{2}\frac{\sinh(m+1)\psi}{\sinh\psi} \ll C_\varepsilon\left(p^{m(\frac{1}{2}+\varepsilon)} + q^2 p^{m\varepsilon}\right) + q^3(m+1)$$

$$\ll C_\varepsilon(q^{3+6\varepsilon}+q^{2+6\varepsilon}) + q^3(1+6\log_p 4) \quad \left(\begin{array}{l}\text{By taking } m \text{ the largest even integer}\\ \text{s.t. } p^{m/2}\le q^3\end{array}\right)$$

Hence $\frac{\sinh(m+1)\psi}{\sinh\psi} \ll_\varepsilon q^{2+6\varepsilon}$

$\left(\text{for } \psi \gg 1,\ \text{this} \sim \frac{e^{(m+1)\psi}}{e^\psi} = e^{m\psi} \gg e^{(6\log_p q-2)\psi} \gg \frac{1}{p} e^{(6\log_p q)\psi} = \frac{1}{p} e^{\left(\frac{6\psi}{\log p}\right)\log q}\right)$ $\psi \gg \log\sqrt{p}$

So $(2+6\varepsilon)\log q \ge \left(\frac{6\psi}{\log p}\right)\cdot\log q - \log p$ for $\boxed{q \gg_{p,\varepsilon} 1}$ $(2+6\varepsilon) \ge \frac{6\psi}{\log p} - \varepsilon$

So $\frac{6\psi}{\log p} \le 2+7\varepsilon$ i.e. $\psi = \left(\frac{1}{3}+\frac{7}{6}\varepsilon\right)\cdot\log p$. Now summing up:

$$\lambda \le 2\sqrt{p}\,(\cos\theta = \cosh\psi) \le 2\sqrt{p}\cdot p^{1/3+\varepsilon} \le 2p^{5/6+\varepsilon}$$ provided the q is large enough in terms of p & ε

Rmk [Modular form] Recall Eichler proved that

$$S_Q(p^m) = \frac{4}{q(q^2-1)}\frac{p^{m+1}-1}{p-1} + O_\varepsilon\left(p^{\frac{m}{2}(1+\varepsilon)}\right)$$ where LHS is really coeff of $\theta(\xi) = \sum_{k=0}^{\infty} r_Q(k) e^{2\pi i k\xi}$

Recall $(|PGL_2| = n)\cdot S_Q(p^m) = 2p^{m/2}\sum_{j=0}^{n-1}\frac{\sin(m+1)\theta_j}{\sin\theta_j}$

We complete the discussion by proving the thm of Frobenius. namely. no small rep. of $SL_2(\mathbb{F}_p)$. Recall every element is conj to unipotent part. Hence a nontrivial rep must not vanish U. but $\chi: \begin{pmatrix} 1 & * \\ & 1 \end{pmatrix} \to \mathbb{C}$ have eigenval λ with eigenvector v. Then $\rho\begin{pmatrix} a & \\ & a^{-1} \end{pmatrix} v$ are eigenval of $SL_2(\mathbb{F}_p)$ with eigenval λ^{a^2} Note λ is p^{th} r.o.u. So we have a space spanned by λ^{a^2} of dim $\geq \frac{p-1}{2}$.

9. A short survey on automorphic forms

Recall the basics of autom forms from Zagier 1-2-3 of Mod form.

Note expansion/non-expansion does not change if we replace generators by their powers (i.e. can replace the generating set by a smaller one so long as they lie in a ball)

I omit the discussion on the fundamental domain and Selberg's 3/16-thm here. Interested reader can consult either Lubotzsky's book or many other literatures on this classic theme. The idea is not unlike the graph case.

10. Zig-Zag Product

Another way to construct a infinite family of expanders is due to Reynold-Vardhan-Widgerson.

Thm [RVW] Let G be regular graph $I(n, m)$ with $|\lambda| \leq \alpha m$. In short (n, m, α)-graph

Then we can define $G \textcircled{z} H$ for H a (m, d, β)-expander s.t. (same m)

$G \textcircled{z} H$ is an $(nm, d^2, \beta + \max(\alpha, \beta^2))$-expander

Application: we start with $(d^4, d, 1/4)$-expander H. for some d (which one can find by brute forcing). then define $G = H^2$ (in the sense $Ad_G = Ad_H^2$, with weight in G = # paths of length 2 from v to w in H.

Ex: If H is an (n, d, α)-graph, then H^2 is an (n, d^2, α^2)-graph

Prop: Define G_n a family inductively: $G_1 = H^2$, $G_{n+1} = (G_n)^2 \textcircled{z} H$. Then.

G_n is an $(d^{4n}, d^2, 1/2)$-expander

Pf: If $n=1$, this is true by Ex. Then from $n \to n+1$, we have

(1) G_n^2 is a $(d^{4n}, d^4, 1/4)$-expander by ind hyp. But then using Thm [RVW].

(2) $G_n^2 \textcircled{z} H$ is a $(d^{4n}, d^2, \frac{1}{4} + \max(\frac{1}{4}, \frac{1}{16}))$-expander □

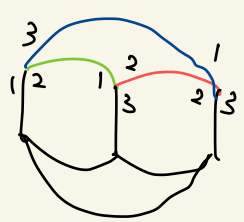
10.1. So what is Zig-Zag product?

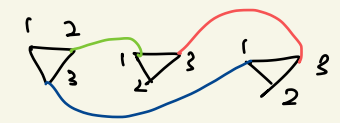
Step 1: Define replacement graph $G \textcircled{r} H$. with:

$V(G \textcircled{r} H) = V(G) \times V(H)$. label the edges from each vertex of G from 1 to m.

Think it as replacing vertices of G by cloud of vertices. i.e. replacing all $V(G)$ by H. with m^{th}-edge from v to w (which is l^{th}-edge from w to v) becomes an edge from (v, m) to (w, l). This behaves somewhat like resolving singularity by blowing-up.

Ex: $H =$ 

$G =$ 

$G \textcircled{r} H$ 

etc.

Step 2: Define $G \textcircled{z} H$ from $G \textcircled{r} H$ with

Vertice set $= V(G \textcircled{r} H) = V(G) \times V(H)$ with

edge set: (v, i) ——— (w, j) iff $\exists\, k, l \in \{1, \dots, m\}$ s.t. $(i, k), (l, j) \in E(H)$

Ex: Recall the previous example. in such case an edge in $G \textcircled{z} H$ means $\exists$ path of length 3 between respective points

One verifies the degree of $G \textcircled{z} H$ as claimed. So we prove the eigenval as claimed. Write $Z = \mathrm{Ad}_{G \textcircled{z} H}$ as BPB with permutation matrix $P_{(v,k),(w,l)} = \begin{cases} 1 & \text{if } k^{th}\text{-edge of } v \text{ is } l^{th} \text{edge of } w \\ 0 & \text{otherwise} \end{cases}$

Let $f \in L^2_0(G \textcircled{z} H)$. Write f'' as average on labeling. i.e. $f''(x, i) = \frac{1}{m} \sum_j f(x, j)$

and $f^\perp = f - f''$. Then $\langle f, Zf \rangle = \langle f'', Zf'' \rangle + \langle f'', Zf^\perp \rangle + \langle f^\perp, Zf'' \rangle + \langle f^\perp, Zf^\perp \rangle$

Now claim $Bf'' = mf''$. By assumption $|Bf^\perp|_2 \le m\beta |f^\perp|_2$ Moreover.

$\langle f'', Pf'' \rangle \le \alpha |f''|^2$. Also note $\frac{1}{m}B$ are so called Stochastic that they are contracting in L^2-norm. i.e. $|(\frac{1}{m}B) f|_2 \le |f|_2$. $|Pf|_2 \le |f|_2$ Now

$$\langle f, Zf \rangle \underset{\substack{B.P \\ \text{contracting} \\ C\text{-}S}}{\le} m^2 \alpha |f''|_2^2 + \beta m^2 |f''|_2 |f^\perp|_2 + \beta^2 m^2 |f^\perp|_2^2 \quad \longleftrightarrow \quad |f|_2^2 = |f^\perp|_2^2 + |f''|_2^2$$

$M = \begin{pmatrix} \alpha & \beta \\ \beta & \beta^2 \end{pmatrix}$. Again by Minmax Largest eigenval of M is $\frac{\langle v, Mv \rangle}{|v|_2^2}$ Now

$\mathrm{char.poly}(M) = (\alpha - \lambda)(\beta^2 - \lambda) - \beta^2$ for $\lambda = \beta + \max(\alpha, \beta^2)$ This is ≥ 0

So the conclusion is $\langle f, Zf \rangle \le m^2 \left\langle \begin{pmatrix} f'' \\ f^\perp \end{pmatrix}, M \begin{pmatrix} f'' \\ f^\perp \end{pmatrix} \right\rangle \le m^2 \cdot$ largest eigenval of M.

$\le m^2(\beta + \max(\alpha, \beta^2))$ as claimed. □

11 Growth & Expansion

11.1. State of knowledge (before 2005) $\Gamma\backslash SL_2(\mathbb{Z}/p\mathbb{Z})$. A mod $p\}$ was known for $\{\begin{pmatrix}1&1\\1&1\end{pmatrix}\begin{pmatrix}1&1\\1&1\end{pmatrix}\}$ and $\{\begin{pmatrix}1&2\\1&1\end{pmatrix}\begin{pmatrix}1&2\\2&1\end{pmatrix}\}$. Then Lubotzky's 1-2-3 problem (after Gamburd) asks if $\{\begin{pmatrix}1&1\\3&1\end{pmatrix}\begin{pmatrix}1&3\\1&1\end{pmatrix}\}$ also forms expander family for any $\# \geq 3$ due to infinite-index in $SL_2(\mathbb{Z})$

Another perspective (additive combinatorics) One basic question: Let $A \subseteq \mathbb{Z}$ finite. then $|A+A|$ is bounded between $[2|A|-1, \frac{1}{2}(|A|^2+|A|)]$. for instance for any 2^n+1 they are distinct pairwise

when is $|A+A|$ close to $|A|$ or $|A|^2$ or $|A|^{3/2}$?

(1) For the first case it's much known (Freiman-Rigusa(?) thm) $|A+A| \leq K|A| \Rightarrow A$ has +ve density in the union of a few segments of (possibly higher-dim) arithm progressions e.g. $\{5+3m+7n \;\; m \in \{m_0, m_0+1, \dots\}, n \in \{n_0, n_0+1, \dots\}\}$

(2) Other cases are not well-understood. Similar things for G abelian and G nilpotent

(3) For $A \subseteq G$. for G nonabelian. Consider $SL_2(\mathbb{Z}/p\mathbb{Z})$. nonabelian. almost simple. when is A^k much larger than A.

Yet another perspective (Cayley graph of simple finite grps) diameter of Cayley graph.

[Folklore Conj] $\exists C_i > 0$ s.t. $G = Alt(n)$ or $Sym(n)$ with gen set A. Then $diam(\Gamma(G,A)) \leq C(\log|G|)^{C_2}$

[Babai Conj] $\exists C, C > 0$ Let G be fin simple grp $\langle A \rangle = G$ then $diam(\Gamma(G,A)) \leq C_1(\log|G|)^{C_2}$

Thm [H^2, 2005-2008] Let $G = SL_2(\mathbb{F}_p)$ Then $|A|^3 \geq |A|^{1+\delta}$ or $A^3 = G$

This directly implies Babai conjecture for $SL_2(\mathbb{F}_p)$ In fact one can choose $r_2 \sim O(1/\delta)$ i.e $(1+\delta)^k > \frac{\log|G|}{\log|A|} \rightsquigarrow |A|^{(1+\delta)^k} > |G|$ Take log log then one finds this gives $k \sim 1/\delta$.

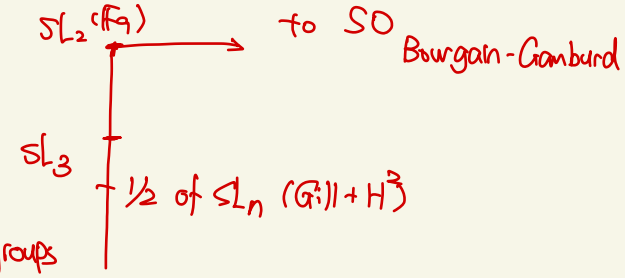
Note $C = \log_{\frac{3}{2}} 8 \approx 5.13$

Much better dependence on the rank. (Rudnev-Shkredov)

(Bajpai-Dona-H^2)

($C = 1000n^3$ say) for SL_n. But for SO_n, SO_{2n+1} Sp_{2n} things can also be done.

Landmap of thm



All groups of Lie type with implied exponent depends on the rank by (Pyber-Szabo, Breuillard-Green-Tao) $C = 3^{3^{\cdot^{\cdot^{3}}}}\}$ rank-many

Rmk: One cannot reach similar result for $Alt(n)$ or $Sym(n)$. The counterexample given by Pyber-Szabo

Let $1<m\le n$. with H the permutation of m. $Sym(m)\subset Sym(n)$ with $\sigma=(1,\dots,n)$

$A=H\cup\{\sigma,\sigma^{-1}\}$. Then $|A^3|=|\{\sigma,\sigma^{-1},*\}H\{\sigma,\sigma^{-1},*\}\cup H\sigma^{\pm1}H|\le 9m!+2(m+1)!$

$\le (2m+1)|A|$ linearly!

Thm: [Bourgain-Gamburd] Using growth estimate. one may prove $A\subset SL_2(\mathbb{Z})$ not contained in an algebraic subgrp ($\sim$ not contained in Borel subgrps) Then:

$\{\Gamma(SL_2(\mathbb{Z}/p\mathbb{Z}),\ A \bmod p\}$ is a family of expanders (ϵ,C implied const by A)

Rmk: This is not easy to prove. On the other hand. a direct consequence from growth estimate (+ ping pong Lemma) is the diameter estimate.

Namely find a $\mathbb{F}_2$ free grp in $\langle A\rangle$. (by Tit's alternative) Then work with $A=\{g_1,g_2,g_1^2,g_2^{-1}\}$. we see entries of A^k are bounded by $(2C)^k$ $\begin{pmatrix}c&c\\c&c\end{pmatrix}\begin{pmatrix}c&c\\c&c\end{pmatrix}=\begin{pmatrix}2c^2&\cdot\\\cdot&2c^2\end{pmatrix}$

So only if at least one of two elements in $\mathbb{Z}/p\mathbb{Z}$ is $\ge p/2$ can two elements p-cong

so now at $\#=L\epsilon\log p$ - step $|A|^{\#}\ge 2^{L\epsilon\log p}\ge\frac{1}{2}p^{\epsilon}$. New growth estimate applies to A showing that we can improve $\frac{1}{2}p^{\epsilon}$ to $|G|\sim p^3$ so the diameter

$$\text{diam}\ll 3^{\log_{1+\delta}3/\epsilon}\,\epsilon\log p$$

Note (A mod p) gen $SL_2(\mathbb{F}_q)$ really comes from either General results (Weisfeiler etal)

(Main ideas of growth thm) These methods also holds for general groups of Lie type

- Dimensional estimate
  - statements generalizing group theory
  - Orbit-Stabilizer thm
  - growth in a subgrp $\Rightarrow$ growth in the grp
- Escape from Subvarieties
  - Given var $V_t=\{A\in SL_2\mid \text{tr}\,A=t\}$ one can prove $|V_t\cap A|\le C|A|^{\frac{\dim V}{\dim G}=\frac{2}{3}}$
  - pivoting argument
  - Final step: no small-dim cplx dim of $SL_2(\mathbb{F}_q)\Rightarrow$ every nontrivial eigenval has high mult

In the end want to apply to $\mathbb{R}$-split tori.

12. Göbel: Additive Combinatorics

Abelian grp + comb $|A^2| < K|A| \Rightarrow |A^k| < K^{O(k)}|A|$ For abelian groups take

$A = N \cup \begin{pmatrix} 1 & \\ 1 & 1 \end{pmatrix}$ but now $\begin{pmatrix} 1 & b \\ & 1 \end{pmatrix}\begin{pmatrix} 1 & \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1+b & b \\ & 1 \end{pmatrix}$ so $|A|^2 \le 2|A|$

on the other hand NgN is much larger than A $\begin{pmatrix} 1+b & c+bc+b \\ 1 & c+1 \end{pmatrix}$

Lemma: (Ruzsa's Δ-ineq) A, B, C finite subset of a grp. then $\boxed{|AC^{-1}||B| \le |AB^{-1}||BC^{-1}|}$

Pf: Construct inj map $AC^{-1} \times B \xrightarrow{i} AB^{-1} \times BC^{-1}$ choose $(f_1(d), f_2(d)) \in A \times C$

for $d \in AC^{-1}$ s.t. $d = f_1(d) f_2(d)^{-1}$. Now set

$i : (d, b) \mapsto (f_1(d) b^{-1}, b f_2(d)^{-1})$ so $i(d, b) \mapsto (x, y) \Rightarrow \begin{matrix} xy = d \\ y f_2(xy) = b \end{matrix}$

Prop: Let G be a group and A finite. Then:

$$\frac{|(A \cup A^{-1} \cup \{e\})^3|}{|A|} \le \left(3\frac{|A^3|}{|A|}\right)^3 \qquad \frac{|(A \cup A^{-1} \cup e)^k|}{|A|} \le \left(3\frac{|A^3|}{|A|}\right)^{3(k-2)} \quad \forall k \ge 3 \quad (\star)$$

if $A = A^{-1}$, then $\frac{|A|^k}{|A|} \le \left(\frac{|A^3|}{|A|}\right)^{k-2} \quad \forall k \le 3$

Pf: Take the Lemma with A, B, C being A^{-1}, A^2, A respectively

$|A^{-1}A^2||A| \le |A^{-1}A^{-1}||AAA||A| \le |A^3|^3$ whereas

taking A, B, C to be $A, A^{-1}, A^{-1}A$ gives

$|AA^{-1}A||A^{-1}|^2 \le |A||A^{-1}A^{-1}A||A| \le |A^2||A^2||A^3| \le |A^3|^3$

$|(A \cup A^{-1} \cup e)^3||A|^2 \le 3(|A^3|)^3$ with the claim

LHS of $(\star) = \frac{|(A \cup A^{-1} \cup e)^k|}{|A \cup A^{-1} \cup e|} \frac{|A \cup A^{-1} \cup e|}{|A|} \le \left(\frac{|\sim^3|}{|\sim|}\right)^{k-2} \frac{|\sim|}{|A|} \le \left(3\frac{|A|^3}{|A|}\right)^{3(k-2)}$

Recall now orbit-stab thm: $|H \cap \mathrm{Stab}(x)| = \frac{|H|}{|Hx|}$ This can be extended to sets

Thm: Let G be a grp acting on X. with $A \subseteq G$ finite set. Then:

$$|(A^{-1}A) \cap \mathrm{Stab}(x)| \geq \frac{|A|}{|Ax|}$$ with $B \subseteq G$. then $|BA| \geq |A|\,|\mathrm{Stab}(x)|\,|Bx|$

Pf: Piegeonhole: d elements into k sets For each $x^i \in Ax$ define $\mathrm{Stab}^A_{x^i} = \{a \in A \mid ax \in x^i\}$ and dist $|A|$ elements into $|Ax|$ sets. Then PH is just saying $\exists x^j \in Ax$ st $|\mathrm{Stab}^A_{x^j}| \geq \frac{|A|}{|Ax|}$. Now:

$$|(AA^{-1}) \cap \mathrm{Stab}(x)| \geq |\mathrm{Stab}^A_{x'}\,\mathrm{Stab}^A_{x'}| \geq |\mathrm{Stab}_{x'}| \geq \frac{|A|}{|Ax|} \quad (\square)$$

(if $a, b \in \mathrm{Stab}^A_{x'}$. then $b^{-1}ax = b^{-1}x' = x'$). Now

For $a, a' \in A \cap \mathrm{Stab}(x)$ and $b_i a = b_j a'$ then $b_i x = b_i ax = b_j x$

hence $b_i a = b_j a' \Rightarrow b_i = b_j \;\; a = a'$. hence

$$|BA| \geq |\{b_i : 1 \leq i \leq |Bx|\} \cdot (A \cap \mathrm{Stab}(x))| = |Bx|\,|A \cap \mathrm{Stab}(x)| \quad (\triangle)$$

Now consider $G \curvearrowright G$ conj. Now $\mathrm{Stab}(g) = $ Centralizer $C(g)$ orbit. $\mathcal{O}_g$.

Lemma: $A \subseteq G$ nonempty and $A = A^{-1}$ Then every $g \in A^l$ $l \geq 1$.

$$|A^2 \cap C(g)| \geq \frac{|A|}{|A^{l+2} \cap \mathcal{O}_g|}$$

Pf: $|A^2 \cap C(g)| = |(A^{-1}A) \cap \mathrm{Stab}(g)| \geq \frac{|A|}{|Ag|} \geq \frac{|A|}{|A^{l+2} \cap \mathcal{O}_g|}$ as $Ag \subseteq A^{l+2} \cap \mathcal{O}_g$ $(\square)$

Also let G acts on G/H by canonical action.

Lemma: $A \subset G$ symm, then $|A^2 \cap H| \geq \frac{|A|}{r}$ $\quad r = \#\{gH \cap A \neq \phi\}$

Pf: for $xeH \in eH$, $\mathrm{Stab}(eH) = H$ $|A^2 \cap H| = |(A^{-1}A) \cap \mathrm{Stab}(eH)| \geq \frac{|A|}{|AeH|} = \frac{|A|}{r}$

Lemma: Let $A \subseteq G$ symm. Then for every $k>0$, $|A^{k+1}| \geq \frac{|A^k \cap H|}{|A^2 \cap H|} |A|$

Pf: $|A^{k+1}| \geq |A^k \cap \mathrm{Stab}(x)| |Ax| = \frac{|B^k|}{|B^2|} \cdot |B^2||Ax|$ (Δ), $|A^k \cap \mathrm{Stab}(x)| := B^k$, $|B^2||Ax| \geq |A|$

This says growth in subgrp quickly ⇒ growth in whole grp quickly

Lemma: $\pi: G \to G/H$ Let $A \subseteq G$ symm. then for $k>0$, $|A^{k+2}| \geq \frac{|\pi(A^k)|}{|\pi(A)|} |A|$

This says growth in quotient ⇒ growth in whole grp quickly

In more panoramic words we enlarge set/rate of subgrps to set/rate of approx subgrps and proving certain nice pptys can be extended likewise. and then prove that such pptys only hold when {approx subgrps} \ {subgrps} can only be the whole group

Now the main ideas of thm 1 in Helfgott 08 paper.

Let V be irred variety. then $|A \cap V(k)| \leq c|A^k|^{\frac{\dim(V)}{\dim(G)}}$ with implied const depending on $\dim(V)$ and $\deg(V)$

This result has been proved for A a subgrp by Larsen-Pink for classifying grps of SL_n

Let G acts on $\mathbb{A}^n$ affine. $A \subset G$ symm gen set. $W \subsetneq \mathbb{A}^n$ with $Gx \not\subseteq W$ for some x.

Thm: $\exists k$ (depend only on # components of W and their deg, dim) s.t. $\exists g \in A^k$ s.t. $gx \notin W$

This is the (Escaping from Subvariety)

sketch of pf: There has to $a \in A$ s.t. $W \cap a^{-1}W \subsetneq W$ By induction you can escape from this subset. i.e. $\exists a_1, \dots a_{k-1}$, with $a_1 \cdots a_{k-1} x \notin W \cap a^{-1}W$ for $a_i \in A$ hence either $a_1 \cdots a_{k-1} \notin W$ or $a a_1 a_2 \cdots a_{k-1} \notin W$

Ex: Consider $\{Tr = \pm 2\} = W \subsetneq SL_2(\mathbb{R})$ why is this bad. $\exists g \in A^k$ not on W i.e. g is diagonalizable

13. Escape from subvariety (Shi)

This is the Chapter 4.2 from Helfgott Arizona Lecture. We add some remark/rephrasing of the arguments. For most of the times we restrict our attention to rk-1 (SL_2) case. and remark when necessary if generalization is different.

Most of arguments goes over to arbitrary field. But keep $K = \mathbb{Z}/p\mathbb{Z}$

Prop: [4.2] $G \curvearrowright \mathbb{A}^n / K$. $W \subsetneq \mathbb{A}^n$ affine subvar. A symm gen set. and $x \in \mathbb{A}^n$ (not necessarily in W) s.t. $G.x \not\subset W$.

Then $\exists \geq \max(1, c|A|)$ elements $g \in A^k$ s.t. $gx \notin W$ when

k.c. = k.c.(#. dim. deg of irred components of W)

Pf: Prove by induction on $\dim W$. Assume W is irred to begin with (i.e. W is sbv of an irred pdy / K). If reader is uncomfortable with AG, just take some $W = \{x^2 + 1 = 0\} \subset (\mathbb{Z}/p\mathbb{Z})$ for $p \neq 2$ and take statements against this example to make-believe.

Step 0: $\dim W = 0$. Then $W = \{x\}$. Then for any $x \in \mathbb{A}^n$. $\exists\, ax \neq x$ for some $a \in A$. even if $\exists < |A|/2$ elements moving x. pick $a_0 x \neq x$. then

$$\#\{a^{-1}a_0 \mid ax = x,\ a^{-1}a_0 x \neq x\} > |A|/2. \quad (c = \tfrac{1}{2}) \qquad \checkmark$$

Inductive step: Assume Statements hold for all W' with $\dim(W') < \dim(W)$

Case 1: $aW = W$ $\forall a \in A$. Then:

Case 1.1: $Ax \cap W = \emptyset$ hence the claim

Case 1.2: $Ax \subset W$ Then $G.x \subset W$. Contradicting the claim.

Case 2: $aW \neq W$ for some a. then $W' = aW \cap W$ is a subvar of $\dim W' < \dim W$ by IH. $\exists\, c'|A|$-many elements $g' \in A^{k'}$ s.t. $g'x \notin W'$ again by Step 0 argument either $g^{-1}g'x$ or $g'x \notin W$ hence the statement holds for $c = c'/2$ $k = k'+1$ □

Rmk [Generalization of argument to arbitrary subvariety] Assume $W = \bigcup_r W_r$ r-many components. Similarly $W' = gW \cap W$ have several components. Note by Bezout's thm. $\#(W') \leq r^2$. now let $d = \max \dim \{V \subset W' \text{ irred}\}$ Then applying induction on both r and d:

either (1) $d < \max \dim W$ hence induction on d works

or (2) $d = \max \dim W$. but $r' < r$, then induction on r works

or (3) $x \notin W_r^d := \{\text{all } W_r \text{ with } \dim = d\}$ Then we can remove all $W \setminus \bigcup_r W_r^d$.

This push the induction argument to general case.

Rmk: This argument works event for arbitrary variety. Instead keeping track of $\#_\cdot = \sum 1$ we keep track of $\sum \deg$ of each. □

Now the escape result + the discussion on approx subgrps together should give the the dimension estimate. i.e. $\min_{\max} \dim (A^k \cap V)$ for some subvar $V \subset G$. This estimate is only meaningful if A grows relatively slow.

Thm [4.4] $G < GL_n$ simple algebraic linear subgrp / k finite field (No reductiveness is assumed) Then for A symm gen set. Then:

$$|A \cap V(k)| \ll |A^k|^{\frac{\dim V}{\dim G}}$$

With k and implied const $\sim n$ and $\deg V$.

Rmk: If K finiteness is dropped, then Pyber-Szabo gives a similar statement for which the A replaces by $\langle A \rangle$ generates "Zariski-dense enough" sets i.e not contain in union of $\leq C(n, \deg(V))$-many varieties

Rmk: In the SL_2-case. much language of AG can be reduced. Also in original paper of Helfgott, these estimate were computed directly

Lemma 4.5: $G = SL_2$, $V = T$. $e \in A$. $|A \cap T(k)| \ll |A^k|^{1/3}$ with k and implied const are both absolute (in this case $n=2$, $\deg V = 1$)

Pf of Lemma: WLOG. let $|k|, |A| > C$. Again by $SL_2(\bar{k})$-conjugation assume T is k-split tori. (But even anisotropic ones the argument works!) Then consider

$$\phi_g = \phi_{g,\bar{k}} : T \times T \times T \to G \qquad x.y.z \mapsto x \cdot y^g \cdot z$$

we will see this map is almost injective. (Such an idea is prevalent in following discussion. The pivot in the incoming discussion is one such example).

Assuming almost inj. the result is immediate:

$$|A \cap T(k)|^3 \approx |\phi(A \cap T(k)^3)| \le |AA^{\ell}AA^{-\ell}A| = |A^{2\ell+3}|$$

The injectivity is, note for $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \subset SL_2(\bar{k})$ s.t. $abcd \neq 0$

$$\phi(r,s,t) = \begin{pmatrix} rt(sad - s^{-1}bc) & rt^{-1}(s^{-1} - s)ab \\ r^{-1}t(s - s^{-1})cd & r^{-1}t^{-1}(s^{-1}ad - sbc) \end{pmatrix} = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

In general. $r.s.t \in \bar{K}$. Consider $s \in \bar{K}$ s.t. $s^{-1} - s \neq 0$ and $sad - s^{-1}bc \neq 0$ Now $\phi^{-1}\phi\{(r,s,t)\}$ has almost 16-elents: see first $BC = -(s - s^{-1})^2 abcd$

So for $abcd \neq 0$, so $-(s-s^{-1})^2 abcd$ is only the same for $\pm s^{\pm 1}$ (≤ 4)

Fix such s. then consider AB and $\frac{A}{B}$. note then (we fix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ a priori) that these gives expression $C_1(s) \cdot C_2\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot r^2$, and $C_3(s) \cdot C_4\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot t^2$. each of which have 2-possibilities. Altogether $\exists \le 16$-many

On the other hand at ramified place (s det $g = 0$) $\exists$ 4 possibility of s. Altogether

$$\phi((A \cap T(k))^3) \ge \frac{1}{16} |A \cap T(k)| (|A \cap T(k)| - 4) \cdot |A \cap T(k)| \quad (\star)$$

i.e $\phi(\text{Set}) \ge \text{Set}^3$ ramified part.

with $\phi((A \cap T(k))^3) \subset A^{3+2\ell}$ as above. Now for $A \cap T(k)$ suff large. (small ≤ 8 is trivial). we see:

$$|A \cap T(k)|^3 \le 2(\star) \le 32 |A^{2\ell+3}|$$

Now it suff to see $\exists\, abcd \neq 0$ In $\mathbb{F}_p$-case this is straightforward. In general case. might $abcd=0$ defines subvar of $\mathbb{A}^4$ of lower dim. Now the definability of ϕ_g /k can be dropped by noting $\mathbb{A}^4 \setminus \{abcd=0\} \neq \phi$. Here take $\{abcd=0\} = W$ and $x = e$ with $G \curvearrowright \mathbb{A}^4$ by left mult. then $\exists\, A^\ell$ s.t. $g \cdot e = g \notin W(K)$. hence we see for such $g \in A^\ell \subset G(K)$ This is already possible. $\square$

Rmk [Generalization] Again for general case Consider V variety of dim 1. Consider the map

$$\phi: V^r \to G \qquad (v_1, \dots, v_r) \mapsto v_1 g_1 v_2 g_2 \dots v_r g_r$$

Again for generic points of V, the preimage of $\phi(v)$ is dim 0. In this case one needs the full power of escape argument to take care of everything

To extend the result to higher rank case, we need the following auxillary Lemma. See for example Tao's Expansion book Prop 5.5.3.

Lemma 4.6: Let $G < SL_n$ simple alg /k. Given V, V' subvar of G with $\dim(V) < \dim(G)$, $\dim(V') > 0$. Then $\forall g \in G(\bar{k})$ outside a subvar $W(V,V') \subsetneq G$, then $\dim \overline{VgV'} > \dim(V)$

Moreover. $\#\{W_r \subset W : \deg W_r < C\} \sim C(C, \deg V, \deg V')$

Pf of ϕ_g simple: By possible translation by $G(\bar{k})$ assume $V, V' \ni e$ and e is not singular

Also $k = \bar{k}$ (of course dim of polynomial do not change when passing over alg closure)

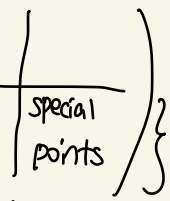
Next consider $\mathfrak{a}$ and $\mathfrak{a}'$ the tangent space of V, V' at e. (Recall these are derivations $\mathrm{Der}_k(k[X], k_x)$ with $k_x = k[X]/\{f(x)=0\}$ the germ at x. Replacing $k=\mathbb{C}$ should give the "diff-geom intuition of what is going on) see also Springer Chapter 4 for rigorous elaboration. Now the tangent space $T_e \overline{VgV'g^{-1}}$ is the derivation at there. so $\mathfrak{a} + \mathrm{Ad}_g \mathfrak{a}'$. It suff to prove $\dim(\mathfrak{a} + \mathrm{Ad}_g \mathfrak{a}') > \dim(\mathfrak{a})$

Supp not. $\forall g \in G$. Then consider $\mathfrak{n} = \langle \bigcup_g \mathrm{Ad}_g \mathfrak{a}' \rangle \subset \mathfrak{a}$ Since $\dim(V) < \dim(G)$ by assumption. $\mathfrak{a} \neq \mathfrak{g}$. hence $\mathfrak{n} \neq 0$ and $\mathfrak{n}$ invariant under G-action hence an ideal

But we assume $\mathfrak{g}$ is simple ($\mathfrak{a}$ will corespond to a normal subgrp). $\lightning$.

So generically g should make $\dim(\mathfrak{a} + \mathrm{Ad}_g \mathfrak{a}') > \dim r(\mathfrak{a})$. Special points (i.e. those $f \in k[X_1, \dots X_{n^2}]$ with $f(G) = 0$). are those which do not happen. Now the claim on # and deg are controlled by Bézout's thm. □

$M_n[f_{11} \dots f_{nn}]$ with $f_{ij} \in k[X_1 \dots X_n]$



Now 4.5+4.6 will extend the result to first 1-dim tori in higher rank grp (Prop 4.8) and second general tori in higher rank grp (Exe 4.12)

Before proving 4.8, first get an estimate of counting points in W.

Exe: $W \subset \mathbb{A}^n/k$. with $\dim W \leq d$. S a finite set of K. Then $\#S^n \cap W \ll |S|^d$ with implied Const can be chosen to depend only on n, #, degs of components of W

Intuitively this is clear. I do not show it in a rigorous way. One can verify it over $k = \mathbb{Z}$. and W some irred poly $/\mathbb{Z}$.

Prop 4.8. [Estimate of 1-dim var in higher rank] $G \subset SL_n$ simple alg $/k$. fin. Assume $|G(k)| \geq c|k|^{\dim G}$

$Z \subset G$ dim-1 var. $A \subset G(k)$ Symm gen set. Then

$$|A \cap Z(k)| \ll |A^k|^{\frac{1}{\dim G}} \qquad (\dim G \text{ arbitrary}, \dim V = 1)$$

In particular. $G = SL_n$ works

Pf: Repeatedly use 4.6. First begin with $V = V' = Z$. then applying 4.6 gives

(1) Subvariety $W \subsetneq G$ s.t. $\forall g \notin W$. $\dim V_2 = \overline{VgV'} > \dim V$

(2) Every W_r has $\dim < G$ by irreducibility of G.

(3) (+ Exe($S=k$) + $G(k) \gg |k|^{\dim G}$) hence $\exists$ points of $G(k) \notin W$. now escape 4.2 works

To summarize, we have found $g_1 \in A^{l=l(\#W, \deg W)}$ s.t. $gx \notin W$. But now $\overline{Zg_1Z}$ has dim $=2$ so induction starts! Next apply $V = V_2$, $V' = Z$, we get for some $g_2 \in A^{l_2}$

$V_3 = \overline{V_2 g_2 Z}$ of dim 3 so altogether:

$\exists\, g_i \in (A)^{\max(l_i)}$ (this is possible by assuming $e \in A$), we see $\overline{Zg_1Z \cdots g_{r-1}Z} = V_{r-1}$

our desired dimension r. Now consider the following algebraic map:

$$\phi: Z^r \longrightarrow G \quad (\leftrightarrow \phi_g \text{ in } Z=T,\ r=2 \text{ case}) \quad (z_1 \cdots z_r) \mapsto z_1 g_1 z_2 \cdots g_{r-1} z_r$$

Now Z^r pdt of irred var is irred, and cont map preserves irred. (Springer Lemma 1.2.3)

also $\max \dim W < \dim V_{r-1}$ so this time apply 4.7 to $S = A \cap Z(K)$, we get almost $O(|S|^{r-1})$ points in S^r that are in W. So.

$\#\{* \in S^r \mid * \notin W\} \sim \deg\phi \cdot \#\phi(S^r)$ for $S^r \subseteq A^k$ for $k = r + (r-1)\cdot\max(l_i)$

(Recall these are in $Zg_1Z \cdots g_{r-1}Z$. where $g_i \in A^{\max l_i}$)

Summing up. We have:

$$|A \cap Z(K)|^r \leq \deg(\phi) \cdot |A^R| + O(|A \cap Z(K)|^{r-1}) \qquad \square$$

Next to extend V to arbitrary dim. We begin with baby example in SL_2 (a result which will be used in proving general V for SL_n-case)

Consider the following variety of dim 2: $V_t = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \subset SL_2 \;\middle|\; a+d = t \right\}$ for $t \neq 2$ Note conjugacy class of any regular semisimple $g \subset V_{tr(g)}$.

Prop [4.9] $G = SL_2$. A as above, then $|A \cap V_t(K)| \ll |A^k|^{2/3}$ $\quad \dim G = 3$, $\dim V = 2$

Pf: This time choose ϕ to be slightly different:

$$\phi: V_t \times V_t \longrightarrow G \qquad (y_1, y_2) \mapsto y_1 y_2^{-1}$$

In contrast with the Torus case, this time ϕ_t is not even nearly injective. Consider

$$\phi^{-1}(h) = \{(w, h^{-1}w) : tr(w) = t = tr(h^{-1}w)\} \quad \text{for } h \in SL_2(K)$$

So consider now subvar $Z_{t,h} \subset SL_2$ be the points of form (w, hw). This has dim-1 for h generic, with # & deg $Z_{t,h} < C$ Now 4.7 immediately gives a bound for such 1-dim subvar:

$$|A \cap Z_{t,h}(K)| \ll |A^{k'}|^{1/3}$$

To lift from $Z_{t,h}$ to V_t note: (A^2-many possible h $\mapsto$ # $\phi^{-1}(h = y_1 y_2^{-1})$)

$$|A \cap V_t(K)|(|A \cap V_t(K)| - 2) \leq |A^2| \cdot \max_{g \neq \pm e} |A \cap Z_{t,h}(K)| \leq |A^2| \cdot |A^{k'}|^{1/3}$$

(# $(y_1, y_2) \in A \cap V_t$. $y_1 y_2^{-1} \neq \pm e$)

because any $y_1 \in V_t$ has at least $|V_t| - 2$ many y_2 s.t. $y_1 y_2^{-1} \neq \pm e$.

Now assuming $A \cap V_t$ suff large (≥ 3). we see $|A \cap V_t(K)| \ll |A^k|^{2/3}$ □

Combining with results from approximate sets we also get lower bound of dimension estimate:

Cor 4.10 $g \in A^\ell$ reg. s.s. $G = SL_2$. Then $|A^2 \cap C_G(g)| \gg \frac{|A|}{|A^{k\ell}|^{2/3}}$. In particular, if $|A^3| \leq |A|^{1+\delta}$, then:

$$|A^2 \cap C_G(g)| \gg_\ell |A|^{\frac{1}{3} - O(\delta)}$$ with implied const both abs.

Pf: Recall $|A^2 \cap C_G(g)| \geq \frac{|A|}{|A^{\ell+2} \cap \text{conj}(g)|}$. Now the denominator is controlled by conj $< V_t$ that $|A^{(\ell+2)k}|^{2/3}$. Hence the claim. The second is really from the estimate:

$$\frac{|A^k|}{|A|} \leq 3^{k-2} \left(\frac{|A^3|}{|A|}\right)^{3(k-2)}$$ again from previous chapter □

Rmk (Induction on dim V) Now the Prop 4.9 gives us an idea how to induction on dim V that is, to eventually prove Thm 4.4 However, one possible pitfall here is $\exists$ tori of smaller dim. Nonetheless the main idea should be clear from previous discussion.

Summing up. we see now: first conjugacy gives transversality between $C_G(g)$ and $\overline{Conj(g)}$. i.e

$$\dim G = \dim C_G(g) + \dim \overline{Conj(g)}$$

Now by 4.10 we can bound $|A^2 \cap C_G(g)| \gg |A|^{\frac{\dim C_G(g)}{\dim G} - O(\delta)}$ if $|A^2| \leq |A|^{1+\delta}$

This is the result we strive to contradict eventually.

14. Kistos: Growth and diameter in $SL_2(K)$. K arbitrary

This is chapter 5 of Arizona Lecture. Instead of following original agument of Helfgott 08, it uses a pivoting argument in Pyber-Szabo. 16. Original treatment use sum-product thm. instead of using the thm as a whole, we recycle some ideas in proving the thm: namely pivoting.

Thm [5.1] $G = SL_2(K)$. A as above. Then either $|A^3| \geq |A|^{1+\delta}$ with δ abs const. or $A^3 = G$.

Rmk [Generalization] Statement holds for K infinite. by dropping $|A| < |G|^{1-\epsilon}$. Note char 0 - case is easier to prove than char p case (heuristically easy to see, as no extra condition $pk=0$ to worry about). For applications though, one estimate $\#\{a,b \in A \ d(a,b) \text{ small}\}$ and $\#\{a,b \in A^3 \ d(a,b) \text{ small}\}$ using the same technique of Helfgott 08. This is BG08 - Invention.

Pf idea: Use the escape idea, we first escape from some tori (using 4.10). This is case (a) in the following. The pivoting is essentially what we had in the tori case (c.f 4.5) where ϕ is almost injective. Next the non-pivoting case corresp to (4.9) whee ϕ is not nearly injective. This is case (b) Last the transition step from case (a) to case (b) is case (c). We derive estimate in each case separately

pf: Again assume A is large than an abs const. WLOG. Fix $G = SL_2$ throughout. Supp to the contrary $|A^3| < |A|^{1+\delta}$. Fix $g_0 \in A$ regular s.s. i.e $\mathrm{tr}(g_0) \neq \pm 2$ Then the centralizer is a maximal torus T. Define $\xi \in G(k)$ a pivot if:

$$\phi_\xi : A \times T \to G(k) \qquad (a, t) \mapsto a\xi t \xi^{-1}$$

is almost inj (i.e. an inj map from $A \times T \to G(k)$ (mod $\pm e$) now:

Beginning case (a): $\exists$ a pivot $\xi \in A$ Then 4.10 gives a lower bound of $A^2 \cap (C_G(g) = T)$ ($\gg |A|^{1/3 - O(\delta)}$). Now inj of ϕ_ξ gives

$$\phi_\xi(A, A^2 \cap T) \geq \frac{1}{4} |A|(A^2 \cap T| \gg |A|^{\frac{4}{3} - O(\delta)} \qquad (\bigcirc)$$

(Note $\frac{1}{4}$ factor comes from at most the $\pm e$ at both factor) On the other hand. $\phi_\xi(A, A^2 \cap T) \subset A^5$ has size $\gg |A|^{\frac{4}{3} - O(\delta)}$. Now for A large enough, then: $\frac{|A^k|}{|A|} \leq \left(\frac{|A^3|}{|A|}\right)^{k-2}$ again by previous estimate of last chapter. Hence we reach a contradiction if $|A^3| < |A|^{1+\delta}$ i.e pivoting $\Rightarrow A^3$ exponentially large.

Ending case (b) $\nexists$ pivot ξ in $G(k)$. Say $(a_1, t_1), (a_2, t_2)$ is the pt of non-inj. Then:

$$a_1 \xi t_1 \xi^{-1} = \pm a_2 \xi t_2 \xi^{-1} \quad \Rightarrow \quad a_2^{-1} a_1 = \pm \xi t_2 t_1^{-1} \xi^{-1}$$

This gives some combinatorial non-transversality between A^2 and $\xi T \xi^{-1}$ i.e $\forall \xi$ $A^2 \cap \xi T \xi^{-1} \neq \{\pm e\}$ (In particular, this means case (b) should never happen in ∞-field. as for instance by considering K-split torus T, then $\mathrm{tr}\, t \in T \geq 2$. but now we can always choose A gen set with very small trace that they are disjoint.

Now $C_G(g) = \xi T \xi^{-1}$ (because $C_G(g) \cap \xi T \xi^{-1}$ nontrivial) Hence again apply 4.10 gives:

$$|A^2 \cap \xi T \xi^{-1}| \geq c' |A|^{1/3 - O(\delta)} \qquad (\triangle)$$

again the C' and implied const are absolute.

Next choose $g \in A^2 \cap \xi T \xi^{-1}$ regular s.s. (This part need generalization in higher-rank case due to existence of non-reg s.s elmts e.g $\begin{pmatrix} a & & \\ & a^{-2} & \\ & & \end{pmatrix}$)

Now the tori counting gives $\leq \frac{1}{2} \frac{|G(k)|}{|T|}$ - many max tori of the form $\xi T \xi^{-1}$ hence

$$|A^2| \geq \frac{1}{2} \frac{|G(k)|}{|T|} (c|A|^{\frac{1}{3} - O(\delta)} - 2) \gg |G(k)|^{2/3} |A|^{1/3 - O(\delta)} \qquad (*)$$

(# tori) (by $(\triangle)$)

Now as $|G| > |A|$ we see in this case either $|A| \geq |G|^{1/3-O(\delta)}$ or $|A^2| > |A|^{1+2\delta}$ by either use $|A^2| < |G|$ or $|A^2| > |A|$ of the (*) in previous page. Now the $|A^2|$ too large case contradicts our assumption. whereas $|A|$ too large case implied $A^3 = G$ already

(Rmk: This result will be proven below indep of pivoting argument!)

Transition case (C) Now there are some intermediate case where $\exists$ pivots & nonpivots of $G(k)$

i.e $\exists\ \xi \in G$ nonpivot s.t. $a \in A$ with $a\xi$ is pivot. (Easy argument as otherwise all nonpivot are mapped to nonpivot hence falling into case (b)). Now:

ξ nonpivot $\underset{\text{Case (b)}}{\Rightarrow} |A^2 \cap \xi T \xi^{-1} = C_G(g)| >> |A|^{1/3-O(\delta)} \xrightarrow[s \in A^k]{\text{Take}} |A^k| \gg |A|^{1/3-O(\delta)}$

$a\xi$ pivot $\Rightarrow |A^s| \geq |\phi_{a\xi}(A, \xi^{-1}(A^2 \cap \xi T \xi^{-1})\xi)| \underset{\text{Replace } T \text{ by } \xi T \xi^{-1}}{\overset{(0)}{=}} \frac{1}{4}|A|^{\frac{4}{3}-O(\delta)}$ and

But now recall again $\frac{|A^k|}{|A|} \leq \left(\frac{|A^3|}{|A|}\right)^{k-2}$. Now this contradicts the assumption $|A^3| \leq |A|^{1+\delta}$ for δ smaller than a const

???

It left to show the remaning part in (case (b)) where A is large implies already $A^2 = G$. This uses an argument of Gowers, adapted by Nikolov-Pyber.

Recall Ad_Γ is G-equivariant, i.e. $Ad_\Gamma \curvearrowright L^2(\Gamma) = \bigoplus_{\lambda_i} V_{\lambda_i}$ into G-representations with $V_\lambda := \{ f \in L^2(\Gamma) : Ad_\Gamma f = f \}$ is a G-representation $\xrightarrow[G = SL_3(\mathbb{F}_q)]{\text{Frobenius}}$ $\dim V_\lambda \geq \frac{q-1}{2}$

The idea is to obtain an upper bound of $\lambda_i < 1$. Recall

$$\operatorname{tr} Ad_\Gamma^2 := \frac{1}{|A|^2} \#\{ \text{cycle of length 2 in } \Gamma \} = \sum_i \lambda_i^2 \Rightarrow \sum_i \lambda_i^2 = \frac{|G||A|}{|A|^2} \geq \frac{q-1}{2} \lambda_i^2 \text{ So.}$$

(each vertice have A-many closed paths; proj to V_λ.)

$$|\lambda_i| \leq \sqrt{\frac{|G|}{|A| \cdot \frac{q-1}{2}}} \xrightarrow{|A| \text{ large}} |\lambda_i| \text{ is small}$$

Prop: [Nikolov-Pyber 11] $G = SL(\mathbb{F}_{p^\alpha})$ $A \subset G$ symm $|A| \geq 2|G|^{8/9} \Rightarrow A^3 = G$

Rmk: $A = A^{-1}$ can be dropped by appealing to Gowers 08, following essentially same argument

Pf: Supp $a \in G \setminus A^3$ Then $\langle Ad_\Gamma \mathbb{1}_A, \mathbb{1}_{gA} \rangle = \frac{1}{|A|} \sum_{x \in G} \sum_{a \in G} \mathbb{1}_A(ax) \cdot \mathbb{1}_{gA}(x) = 0$. for otherwise there exists $x \in gA$ and $ax \in A \Rightarrow g \in A^{-1} A A^{-1} = A^3$ ↯

Take λ_i with eigenvector v_i. then: decompose $L^2(\Gamma)$ with v_0 const fct

$$\langle Ad_\Gamma \mathbb{1}_A, \mathbb{1}_{gA} \rangle = \lambda_0 \langle \mathbb{1}_A, v_0 \rangle \langle v_0, \mathbb{1}_{gA} \rangle + \sum_{j>0} \lambda_j \langle \mathbb{1}_A, v_j \rangle \langle v_j, \mathbb{1}_{gA} \rangle$$

$\langle \mathbb{1}_A, v_0 \rangle = \frac{|A|}{\sqrt{|G|}}$, $\langle \mathbb{1}_{gA}, v_0 \rangle = \frac{|gA|}{\sqrt{|G|}} = \frac{|A|}{|G|}$, $\lambda_0 = 1$ (+)

where $(+) \underset{C.S}{\leq} \sqrt{\frac{|G|}{|A| \cdot \frac{q-1}{2}}} \left(\sum \langle \mathbb{1}_A, v_j \rangle^2 \right)^{1/2} \left(\sum \langle v_j, \mathbb{1}_{gA} \rangle^2 \right)^{1/2} \underset{C.S}{\leq} \sqrt{\frac{|G|}{|A| \cdot \frac{q-1}{2}}} \| \mathbb{1}_A \|_2 \| \mathbb{1}_{gA} \|_2 \leq \left(\frac{2|G||A|}{q-1} \right)^{1/2}$

But now $|G| = q(q^2-1)$ $|A| \geq 2|G|^{8/9}$ implies $\frac{|A|^2}{|G|} > \left(\frac{2|G||A|}{q-1} \right)^{1/2} \Rightarrow \operatorname{Tr} Ad_\Gamma \neq 0$ ↯

Rmk: This result would be recycled in the next section when finishing the pf of Bourgain-Gamburd.

This method was already implemented when discussing D.S.V. approach to Ramanujan Graph.

15. Han: Expansion in SL_2. Bourgain-Gamburd

Recall in previous classes we have seen quite a few constructions of expander families. In particular for $SL_2(\mathbb{Z})$ case. we see $A = \{\begin{pmatrix}1&1\\0&1\end{pmatrix}, \begin{pmatrix}1&0\\1&1\end{pmatrix}\}$, the corresponding mod-p families $\{SL_2(\mathbb{Z}/p\mathbb{Z}), A \bmod p\}$ gives the desired family. In this section. the choice of A is enlarged to much larger class. i.e. A is only asks to generates a Zariski-dense subgrp of $SL_2(\mathbb{Z})$. The main result is the following:

Thm [Bourgain-Gamburd '08 Ann] $\langle A\rangle$ zariski-dense in G, then $\{SL_2(\mathbb{Z}/p\mathbb{Z}), A \bmod p\}$ forms family of expanders.

Key-ingredient: Helfgott '08 + ℓ^2-flattening Lemma The main idea of the proof can be listed in the following steps:

Given μ a prob measure on G (concentrated on A) Convolution of measure is:

$$\mu*\mu(f) = \int_{G\times G} f(xy)\,\mu(dx)\mu(dy) = \int_{A\times A} f(ab)\,\mu(da)\mu(db)$$

roughly captures the probabilistic measure of A^2. (Discretely this is $\mu*\nu(x) = \sum_{y\in G}\mu(xy^{-1})\nu(y)$)

Consider the probability measure concentrated in A. and one shows a mixing result at small steps due to freeness (which is possible in SL_2). For intermediate steps. Helfgott's growth result gives further decrease. Eventually. when $|\mu^{(k)}|_2$ is small enough. The previous high mult estimate give the expansion.

Final step: First one sees why $|\mu^{(k)}|_2$ small implies expansion. Recall the beginning of lecture says

$$|\mu^{(k)}|_2^2 \ll 1/|G|^{1-\delta} < \left|\mu^{(k)} - \frac{\mathbb{1}}{|G|}\right|_2^2 \ll \frac{\epsilon}{|G|} < \text{Spectral expansion}$$

(our result; ℓ^2-mixing of R.W.; "converse" of Expander-mixing)

However. if we have high mult of each λ_i, one can get from LHS to RHS (merit: Sarnak-Xue 1991)

Again write $\mathrm{Tr}\,\mathrm{Ad}_I^{2\ell}$ in two ways: (Geom) $|G||\mu^\ell|_2^2 : \mathbb{P}(x\to x \text{ after } 2\ell \text{ steps})\cdot \#\text{vertices}$

(Spec) $\sum\lambda_i^{2\ell}$

Now mult $\lambda_1\cdot\lambda_1^{2\ell} \le \sum\lambda_i^{2\ell} = |G||\mu^\ell|_2^2 \ll \frac{|G|}{|G|^{1-\delta}} = |G|^\delta$. Now $|G|^{1/3} = |PGL(\mathbb{F}_p)|^{1/3} \sim p$ (? is it enough?) in the meantime $\dim V_{\lambda_1}$ by estimate of previous section $> \frac{p-1}{2}$. Hence $\lambda_1^{2\ell} \gg |G|^{\delta-1/3}$. Now choose δ small enough (say $1/6$) gives upper bound $\lambda_1 \le 1-\epsilon$ where ϵ indep of p. □

Hence the goal is to prove the decay of $|\mu^{(2k)}|_2^2 = \mathbb{P}(x \to x \text{ after } 2k\text{-steps of RW})$ with respect to $|G|$. The steps are as follows:

Step 0: Red to $\langle A \rangle$ free. $G = SL_2$, $H = \Gamma(2) = \{g \equiv I \bmod 2\} \subseteq SL_2(\mathbb{Z})$ free of index 12. Hence $\langle A \rangle \cap H$ free by Nielsen-Schreier (if $H < F$ free $\Rightarrow H$ free), $\mathbb{Z}$-dense, and gen by $A' \subset \langle A \rangle$. Replacing A by A' completes the reduction.

Rmk [Generalization] Gelfeidy-Varjú extends to higher-rank groups. as current H is insufficient.

Step 1: For small steps ($k \ll \log|G|$), $|\mu^{(k)}|_2$ decrease due to freeness. $\langle A \rangle$ free grp on ≥ 2 elmts. Then two words w_1, w_2 of A with length $w_i = k \leq c_A \log p$ reduces to same word in $G(\mathbb{Z}/p\mathbb{Z})$ only when they are the same words in $G(\mathbb{Z})$. (Reason: To see this consider $a_1 a_2 \equiv a_3 a_4 \pmod p$ then: By the diameter estimate $a_3^{-2} a_1 a_2 a_4^{-1} = e$ implies $a_3 = a_1$, $a_4 = a_2$ for otherwise we have a nontrivial cycle But $\operatorname{diam} G_p = O(\log|G|)^C$ for some abs const C

But now using $\langle A \rangle$ free this means two elmts must have same reduction. Now

$$\mu^{(k)}(e) = \text{probabilities of words reducing to } e = \frac{|\text{words of length } k \text{ reducing to } e|}{r^k} \qquad (A)$$

Now Kesten's bound gives # numerator: i.e. $\mu^k(e) \ll_\epsilon \left(\sqrt{\frac{2r-1}{r}} + \epsilon\right)^k$ with now:

$k = \lfloor C \log p \rfloor$ say $\mu^{(k)}(e) \ll p^{-\eta_C}$ $\left(\left(\sqrt{\frac{2r-1}{r}}\right)^{C \log p} \sim p^{C \cdot \log \sqrt{\frac{2r-1}{r}}}\right)$

From e to G': Assume A is free, then $\mu^{(k)}(G')$ for any subgrp $G' < G$ (This easy in SL_2. as every proper subgrp $G' \supset G''$ soluable with $[G' : G''] < C$ indep of p. (This can be seen directly from classification of subgrps of $SL_2(\mathbb{F}_p)$ for $p \geq 5$, due to Dickson:

(a) D_2 of size $2\left(\frac{p \pm 1}{2}\right)$ with their subgrps

(b) Borel groups $P\left(\frac{p-1}{2}\right)$ and its subgrps

(c) A_4, S_4 or A_5

It's enough now to show $\mu^{(2k)}(G'')$ is small ($\Rightarrow \mu^{(k)}(G')$ is small) **Escape from proper subgrp.**

Now G'' is 2-step soluable as $G'' < SL_2$ i.e. $[[g_1, g_2], [g_3, g_4]] = e$. For same reason as above this implies $[[g_1, g_2], [g_3, g_4]] \equiv e \pmod p$, then the claim is (c.f BG Prop 8)

$$\#S := \{g \in F^r \mid \text{length } g < \ell \quad g \in G''\} < \ell^6 \sim \ell^{O(1)} \qquad (B)$$

To prove the previous claim. Note if $|S| > \ell^6$ then $|[S,S]| > \ell^3$ (Lemma 3 BG). then since $[[S,S],[S,S]] = 1 \Rightarrow [S,S]$ is cyclic. which contains elmts of at most 8ℓ. hence $|[S,S]| = O(\ell)$ ↯

Now we have established the condition

$$\mu^{(k)}(G') \ll \mu^{(k)}(G'') \overset{(A)+(B)}{\ll} \frac{(2k)^{O(1)}}{\nu^{2k}} \ll p^{-\eta} \quad \text{for } \eta = \eta_c > 0$$

$\ell = 2k$

Now it suff to bridge the gap that $\mu^{(k)}$ is small when k intermediate. This is the main innovation of this paper. It's also known as

Lemma (ℓ^2-flattening lemma) μ symmetric prob measure on G finite grp ($\mu(g) = \mu(g^{-1})$). Supp

$$|\mu * \mu|_2 \geq K^{-1} |\mu|_2 \qquad (\ell^2)$$

for some $K > 0$. Then $\exists$ a $K^{O(1)}$-approximate subgrp $H \subset G$ of size $\ll \frac{K^{O(1)}}{|\mu|_2^2}$ and an elmt $g \in G$ s.t. $\mu(Hg) \gg K^{-O(1)}$

This mean a symm prob measure μ on G that is not substantially flatter than μ can only concentrate on an approx subgrp (in fact here says nonflattening $\Rightarrow$ concentration in coset of approx subgp)

Consequence: $\mu(Hg) \gg K^{-O(1)} \Rightarrow (\mu * \mu)(H^2) \geq \mu(Hg)\mu(g^{-1}H) \overset{\text{symm}}{\gg} K^{-O(1)}$

Now ℓ^2-flattening + $|A^3| \geq |A|^{1+\delta} \Rightarrow \mu^{(k)}$ small for medium size μ. namely consider $|\mu^{(k)}|, |\mu^{(2k)}| \cdots$ At each step apply ℓ^2-flattening to $K = p^{\delta'}$ $\delta' > 0$ set later. if flattening. i.e Not (ℓ^2), then $|\mu^{(2^r k)}|_2^2 \leq \frac{1}{K^r} |\mu|_2^2 = \frac{1}{p^{r\delta'}} |\mu|_2^2 < \frac{1}{|G|}$ after $r = O_{\delta',\eta}(1)$ steps

then we are already at final step. WIN! $(\not\ell)$

Supp Not. then $\exists\, k' = 2^j k$ for $j \ll_{\delta,\eta} 1$. $\overset{\ell^2\text{-flattening}}{\Longrightarrow}$ $\exists\, p^{O(\delta')}$-approx subgrp $H \subset G$ s.t

(F1) $|H| \ll \frac{p^{O(\delta')}}{|\mu^{(k')}|_2^2}$

(F2) $\exists g \in G$ s.t. $\mu^{(k')}(Hg) \gg p^{-O(\delta')}$ $\Bigg\} \Rightarrow |H^3| < |H|^{1+O(\delta'/\eta)}$

as $H \cdot H \subset H \cdot x$, $H \cdot H \subset x \cdot H$ $\Rightarrow$ $|H^3| = |H \cdot H^2| \leq |H^2 \cdot x| < |H \cdot x^2| < K^2 |H|$

$\Rightarrow |H^3| < p^{2O(\delta')} |H|$

But $|H| \underset{(k)}{\geq} p^{\eta - O(\delta')}$ hence $p^{2O(\delta')} |H| < |H|^{1+O(\delta'/\eta)}$ hence the claim.

To see: $|H| \overset{(*)}{\gg} p^{\eta - O(\delta')}$ for some $\eta = \eta_c$. Note first $|\mu^{(k')}|_2 \ll p^{-\eta_c}$ for otherwise Cauchy-Schwarz really gives $|\mu^{(\frac{k'}{2})}|_2 \gg p^{-\eta_c}$ a contradiction. But now $\nu(Hg) \gg p^{-O(\delta')}$ hence another C.S gives

$$p^{-O(\delta)} \ll \Big(\sum_{x \in Hg} \mu^{(k)}(x)\Big)^2 \underset{CS}{\leq} |Hg| \sum_{x \in Hg} \mu^{(k')}(x)^2 \ll p^{-\eta} |H| \Rightarrow |H| \gg p^{\eta - O(\delta')}$$

But this contradicts $|A^3| \geq |A|^{1+\delta}$ by choosing δ' small, unless

(A) $|H| \geq |G|^{1-O(\delta)}$ for δ arb small. Now (F1) $\Rightarrow |\mu^{(k')}|_2^2 \ll \frac{1}{|G|^{1-\delta-\delta'}}$ WIN.

(B) $H < G'$ proper subgrp. Then (F2) $\Rightarrow \mu^{(k')}(G'g) \gg |G|^{-O(\delta')}$ But this implies already $\mu^{(k)}(G'g) \geq |G|^{-O(\delta')}$ (By writing $\mu^{(k')}(G'g) = \mu^{(k)} * \mu^{(k'-k)}(G'g)$)

This means in turn $\mu^{(k)}$ is concentrated in a subgrp G'. But this contradicts our observation in Stage 1

This concludes the proof (modulo the L^2-flattening lemma. which is our next focus.) □

Consequence of methods Later the method of Bourgain-Gamburd was expanded by Salehi-Golsefidy & Varjú to much more general scenario. here is the theorem

Thm [Expansion in algebraic Groups. SGV.'12] A symm subset of $GL_n(\mathbb{Z}_S)$ and $\Gamma = \langle A \rangle$. let G be the Zariski-closure and G° identity component. Then Cayley graph $(\pi_q(\Gamma), \pi_q(A))$ forms a family of expanders as q runs through square-free S-integers iff G° is perfect.

This is a fundamental tool in affine sieve.

Scholium [Approximate subgrp] We have seen this essentially in previous text. $A \subset G$ is K-approx subgrp if $A = A^{-1}$ and with $|X| \le K$ s.t. $A^2 \subset K \cdot A$ set that do not grow too fast

Lemma 3.3: [Tao] $A \subset G$ finite with $|A \cdot A| \le K|A|$ or $|A \cdot A^{-1}| \le K|A|$. then A lies in union of at most $O(K^{O(1)})$-cosets of an $O(K^{O(1)})$ approx subgrps H of size $|H| \ll K^{O(1)}|A|$.

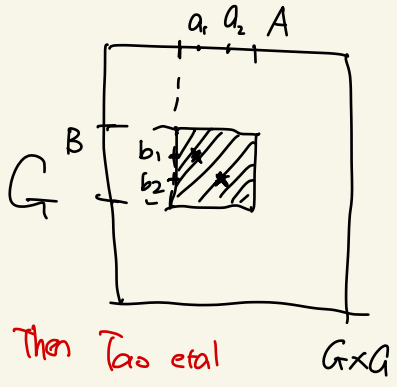
A with small doubling are covered by $O(K^{O(1)})$ approx subgrp of bounded (by $|A|$) size

This use Ruzsa Covering Lemma & we omit it here.

Prop [Noncommutative Balog-Szemerédi-Gowers, Tao 08] $A, B \subset G$ finite. define mult energy

$$E(A,B) := \sum_{g \in G} |(1_A * 1_B)(g)|^2 = |\{(a_1, a_2, b_1, b_2) \in A \times A \times B \times B,\ a_1 b_1 = a_2 b_2\}|$$

if $E(A,B) \ge \frac{|A|^{3/2}|B|^{3/2}}{K}$ (⇐) then $\exists A', B' \subset A, B$ s.t. $|A'| \gg \frac{|A|}{K}$ and $|B'| \gg \frac{|B|}{K}$ with $|A' \cdot B'| \ll K^8 \sqrt{|A| \cdot |B|}$



History: BS uses Szemeredi's regularity Lemma: (with towers of (log bound)

Then G proved much stronger version (abelian) with polynomial dependence. Then Tao etal extends this to ⇔ case (seamlessly)

If we write $w(x) = |\{(a,b) : ab = x\}|$ Then $\sum w(x) = |A||B|$. and $\sum w(x)^2 = \sum_x |ab=x||ab=x| = E(A,B)$

Note $E(A,B) \le |A|^2|B|$ or $|A||B|^2$ for trivial reasons

Rmk: A and B cannot be too different in size. for example. the energy lower bound (⇐) do not hold if $K < \sqrt{\frac{\max(|A|,|B|)}{\min(|A|,|B|)}}$. (because it contradicts the trivial upper bound)

The theorem is proven from the following stronger result

Prop [⇔ BSG, version 2] $A, B \subset G$ with $|A|, |B| = n$ $S = A \times B$ with $|S| \ge \delta^2 n$ and $|P := \{a \cdot b \mid (a,b) \in S\}| = cn$ (with δ, n are deemed to be small). Then:

$\exists A' \subset A$, $B' \subset B$, $|A'|, |B'| \ge \frac{\delta^2 n}{16}$ and $|A'B'| \le \frac{2^{15} c^3}{\delta^5} n$

Cor to BGS2: For the same condition of BGS2. we have $|A'(A')^{-1}| \le \frac{2^{38}}{\delta^{14}c^6}|A|$

Pf: Remember Ruzsa's Δ-ineq (from Göbel's talk. first lemma). that

if one may $\delta(A,B] = \log \frac{|AB^{-1}|}{\sqrt{|A||B|}}$. then $\delta(A,B) \le \delta(A,C) + \delta(C,B)$

Hence $\delta(A',A') \le \delta(A',(B')^{-1}) + \delta((B')^{-1},A') = 2\delta(A',(B')^{-1})$ i.e. $\frac{|A'(A')^{-1}|}{|A'|} \le \frac{|A'B'|^2}{|A'||B'|}$

Pf of BGS 1 from BGS 2: Let $X = \{x \in A\cdot B : w(x) \ge \frac{\sqrt{|A||B|}}{2K}\}$ ← popular values $w(x)$ as before

$$\sum_{x\notin X} w^2(x) \le \frac{\sqrt{|A|\cdot|B|}}{2K}\cdot\sum w(x) = \frac{(|A||B|)^{3/2}}{2K} \quad \text{hence} \quad \sum_{x\in X} w^2(x) \ge \frac{(|A||B|)^{3/2}}{K} - \frac{(|A||B|)^{3/2}}{2K}$$

Now $\sum_{x\in X} w(x) \le \sum_x w(x) = |A||B|$. we see $|X| \le \frac{|A||B|}{\sqrt{|A||B|}/2K} \le 2K\sqrt{|A||B|}$

On the other hand. Since $w(x) \le \min(|A|,|B|)$, then

$$\sum_{x\in X} w(x) \ge \sum_{x\in X} w(x)^2 \ge \frac{(|A||B|)^{3/2}}{2K\cdot\min(|A|,|B|)}$$

if $|A| = |B|$ This is done from BGS.2 : $S = \{(a,b) \in A\times B,\ a\cdot b \in X\}$ with $|P| = |X|$ and

$|S| = \sum_{x\in X} w(x) \ge \frac{(|A||B|)^{3/2}}{\min(|A|,|B|)}$.

So consider $|A| \ne |B|$. use Cor. BGS 2 choose B' $(=|A|)$ that is "most popular on S"

That is order all $b\in B$ on decreasing order of $\eta(b) := \{a\in A, a\cdot b \in X\}$. Now let

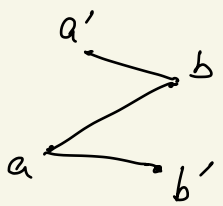
$S' = \{(a,b) \in A\times B',\ ab \in X\}$. Then $|S| \ge \frac{|B'|}{|B|}\cdot\frac{(|A||B|)^{3/2}}{K|A|} \ge \frac{|A|^2}{K}$ with

$|\{(a,b)\ ab\in P\}| \le |X| \le 2K\sqrt{|A|\cdot|B|} \le 2K^2|A|$ and now applying BGS 2 . □

Graph Theory prop: Let $G = (V \sqcup W, E)$ bipartite. graph. with $|V| = |W| = n$ $|E| = \delta n^2$ $\delta > 0$

Then $\exists V' \subset V$, $W' \subset W$ with $|V'|, |W'| \ge \frac{\delta^2 n}{16}$ s.t. $\forall v', w' \in V'\times W'$, there exists more than $2^{-12}\delta^5 n^2$ paths of length 3 from v' to w' in G

Pf of BGS 2 from Graph prop Let $V, W, E = A, B, S$ Apply Graph-prop Then $\exists V' \subset V, W' \subset W$ s.t. $\forall a' \in V', b \in W', \exists \geq 2^{-12}\delta^5 n^2$ values of $(a,b) \in V \times W$. i.e. P are the edges: $(a'b \in P, ab' \in P, ab \in P)$. Now:



$(a'b') = (a'b)\cdot(ab)^{-1}(ab') = a'b'$. So $\forall a' \in V', b' \in W'$ and $a'b' = xyz$ has $\geq 2^{-12}\delta^5 n^2$ solns $(x,y,z) \in P^3$. Yet $|P| \leq cn$

Hence $|\{a'b' : a' \in V', b' \in W'\}| \leq \frac{(cn)^3}{2^{-12}\delta^5 n^2} = \frac{2^{12}c^3}{\delta^5} n$ □

To prove the BSG graph prop, based on Gowers, quantitively much stronger than BS.

Graph Lemma (Length 2) Let $G = (V \sqcup W, E)$ bipartite with $|E| \geq \delta|V||W|$. Then: $\forall \varepsilon > 0$:

$\exists V' \subset V$ with $|V'| \geq \frac{\delta}{2}|V|$ s.t. for $\geq |1-\varepsilon|\cdot|V'|^2$ pairs $(v,v') \in V' \times V'$. There are $\geq \frac{\varepsilon\delta^2}{2}|W|$ - paths of length 2 from v to v'

Pf idea: Choose V' to be nbd $N(w)$ of a random elmt w of W.

In full, choose $w \in W$ uniformly in W. Let $V' = N(w) \subset V$. (by bipartiteness). Then:

$$\mathbb{E}(|V'|) \geq \frac{|E|}{|W|} \geq \frac{\delta|V||W|}{|W|} = \delta|V|$$ Hence by CS. $\mathbb{E}(|V|^2) \geq \delta^2|V|^2$

Now $\mathbb{E}(|V'|^2)$ = expected # of pairs $(v,v') \in V' \times V'$. Let $B \subset V' \times V'$ be the set of BAD pairs $(v,v') \in V' \times V$, i.e those $\exists < \frac{\varepsilon\delta^2}{2}|W|$ paths of length 2 from v to v'. aka. $\exists <$ $\frac{\varepsilon\delta^2}{2}|W|$ - many elmts in W s.t. $N(w) \cap \{v, v'\} = \emptyset$. We want to show this B is small.

Now $\mathbb{E}(|B|) = \int_{\substack{(v,v') \\ \text{bad}}} \mathbb{P}\{(v,v') \in V' \times V'\} < \frac{\varepsilon\delta^2}{2}|$

Lemma (ℓ^2-flattening lemma) μ symmetric prob measure on G finite grp ($\mu(g)=\mu(g^{-1})$). Supp

$$\|\mu*\mu\|_2 \geq K^{-1}\|\mu\|_2 \qquad (\ell^2)$$

for some $K>0$. Then $\exists$ a $K^{O(1)}$-approximate subgrp $H\subset G$ of size $\ll \frac{K^{O(1)}}{\|\mu\|_2^2}$ and an elmt $g\in G$ s.t. $\mu(Hg)\gg K^{-O(1)}$

Recap on ℓ^2-flattening

Sketch of ℓ^2-flattening Lemma: The sketch of the Lemma can be seen as follows:
First Establish the claim of lemma for $\mu=\mu_A$ char function. on A. then try to reduce the proof of general measure to the characteristic fct by "chopping off the tail part" and measure the median part by Char fct of some suitably choosing A. we first recall some preliminaries here on approx subgps.

Pf of ℓ^2: Assume the $\not\Leftrightarrow$ BSG. Consider the Ansatz ($\mu=\mu_A$): Then $\|\mu*\mu\|_2^2 = \frac{1}{|A|^4}E(A,A)$ and $\|\mu\|_2^2=\frac{1}{|A|}$. Then: $(\ell^2)\Rightarrow E(A,A)\geq K^{-2}|A|^3$

But $\not\Leftrightarrow$ BSG $\Rightarrow \exists A_1', A_2'$ of size $\geq |A|/K^2$ and $|A_1'A_2'|\leq K^{18}\sqrt{|A_1'||A_2'|}\Rightarrow |A_1'A_1'|\leq K^{36}|A_1'|$

by Ruzsa's Δ-ineq $\boxed{|AC^{-1}||B|\leq |AB^{-1}||BC^{-1}|}$ By taking $A=A_1, B=A_2^{-1}, C=A_1$

Thus by another Lemma 3.3 [Tao] A_i' lies in union of $\leq K^{O(1)}$-many cosets of H. Pigeon hole tells at least one of coset $Hg \supset K^{-O(1)}|A_1'|$ elements of $A_1' \Rightarrow \mu(Hg)\gg K^{-O(1)}$

Now the proof for general μ follows in the same as Ansatz: i.e bulk of μ have $\mu(g)$ not too large nor too small then ℓ^2-norm:

Procedure: Take $a=\|\mu\|_2^2$, Note here onwards $\mu\neq\mu_A$ anymore

$$A=\left\{g\in G \mid \mu(g)\geq \frac{a}{Ck^c}\right\}$$ with μ_A. this is the case to which we degenerate.

Easy consequences:
(1) $a=\|\mu\|_2^2 \geq |A|\min_{g\in A}|\mu(g)|^2 \geq |A|\cdot\frac{a^2}{C^2K^{2c}} \Rightarrow \frac{1}{|A|}\geq \frac{a}{C^2K^{2c}}$

(2) as $\mu_A=\frac{1}{|A|}1_A$ $\|\mu_A\|_2=\frac{1}{\sqrt{|A|}}$ as a probability measure.

(Rmk $\frac{1}{a}$ is intuitively the "width" of probability measure)

Now write $\mu = \mu_< + \mu_\sim + \mu_>$ with $\mu_< = \mu < \frac{a}{CK^c}$ $\mu_> = \mu > CK^c a$ and $\mu_\sim$ the rest

Now Young's ineq: $|f*g|_2 \le \|f\|_2 \|f\|_1$. using this let's see $|\mu * \mu| \sim |\mu_\sim * \mu_\sim|$.

Note $\|\mu_<\|_2^2 \le \|\mu_<\|_\infty \|\mu\|_1 \overset{\mu \text{ prob}}{=} \frac{a}{CK^c}$, hence:

$\|\mu_< * \mu\|_2 \le \|\mu\|_1 \|\mu_<\|_2 = \sqrt{\frac{a}{CK^c}}$ similarly we get

(Young's ineq)

$\|\mu_>\|_1 \le \frac{\|\mu_>\|_2^2}{\min_{g\in G} |\mu_>(g)|} \overset{\|\mu\|_2^2 = a}{\le} \frac{a}{CK^c a} = \frac{1}{CK^c}$ hence:

$\|\mu_> * \mu\|_2 \overset{\text{Young}}{\le} \|\mu\|_2 \|\mu_>\|_1 \le \frac{\sqrt{a}}{\sqrt{CK^c}}$

$$
\begin{aligned}
&|\mu_\sim * \mu_\sim|_2 \\
&\ge |\mu*\mu|_2 - 2|\mu_< * \mu|_2 - 2|\mu_> * \mu| \\
&\overset{(\ell^2)}{\ge} K^{-1}\sqrt{a} - \frac{4\sqrt{a}}{\sqrt{CK^c}} \\
&\overset{C=2}{\ge} \frac{1}{5} K^{-1}\sqrt{a} \qquad (>) \\
&\overset{C=5}{}
\end{aligned}
$$

Recall

Now one suff to bound $\mu_\sim$ by genuine μ_A that we descend into Ansatz case. $A = \text{supp}\, \mu_\sim + \mu_>$

$$|\mu_A * \mu_A|_2 \overset{(+1)}{\ge} \frac{1/|A|}{|\mu_\sim|_\infty} |\mu_\sim * \mu_\sim|_2 \overset{(>)}{\ge} \frac{1/|A|}{CK^c a} \cdot \frac{1}{5} K^{-1}\sqrt{a} = \frac{1}{25K^3} \frac{1/|A|}{\sqrt{a}} \qquad (\ell)$$

(+): because $\mu_\sim \le |\mu_\sim|_\infty$ on A whereas $\mu_A = \frac{1}{|A|}$ on A

Next as $\frac{1}{|A|} \overset{\text{Easy Consq (1)}}{\ge} \frac{a}{C^2 K^{2C}} = \frac{a}{25K^4}$ (Q2) and $|\mu_A * \mu_A|_2^2 \overset{\text{def}}{=} \frac{E(A,A)}{|A|^4} \le \frac{1}{|A|}$ from trivial bound $E(A,B) \le \min(|A|^2|B|, |A||B|^2)$

then this implies:

$$|\mu_A * \mu_A|_2 \overset{(Q)}{>} \frac{1/|A|}{25K^3} \cdot \underbrace{\frac{\sqrt{|A|}}{5K^2}}_{(\&Q)} = \frac{1/\sqrt{|A|}}{5^3 K^5} = \frac{|\mu_A|_2}{5K^2} \quad \text{with } |A| \ge \frac{1/a}{5^4 K^6} \text{ Rewriting } (Q,Q)$$

Now proceeding as Ansatz, we have

$\exists K^{O(1)}$-approx subgrp $H < K$ s.t. $\mu_A(Hg) \gg K^{-O(1)}$ for some $g \in G$. So

$$\mu(Hg) \ge \frac{a}{5K^2} \mathbb{1}_A(Hg) = \frac{a|A|}{5K^2} \mu_A(Hg) \gg K^{-O(1)}$$

□

16. Higher Expanders

A motivating example: $\lambda(p_1 \cdots p_k) = (-1)^k$. Then p a set of primes in a fixed interval

$$\frac{1}{\log X}\sum_{n\le X}\frac{\lambda(n)\lambda(n+1)}{n} = O\left(\frac{1}{\sqrt{\log\log X}}\right)$$

Tao proved: $O\left(\frac{1}{\sqrt{(\log\log\log\log X)^a}}\right)\cdots$

This implies a certain graph is a strongly local Expander

Note (*) from the following fact that given bounded f.

(*)

(a) $$\sum_{\substack{N<n\le 2N\\ p\mid n\\ p\in P}} f(n)f(n+p) - \sum_{\substack{N<n\le 2N\\ p\mid n\\ p\in P}} \frac{f(n)f(n+p)}{p} = O(NL)$$ with $L = \sum_{p}\frac{1}{p}$

(b) (M? - R? - Tao) λ averages to 0 on most short intervals.

$$\sum_{\substack{N<n\le 2N\\ p}} \frac{\lambda(n)\lambda(n+p)}{p} = O(NL)$$

Meaning: Consider the graph Γ : vertices $N<n\le 2N$ and $n \frown n+p \iff p\mid n$ $p\in P$

Γ' some vertices and $n \frown n+p \iff p\in P$ weight $1/p$

$A = Ad_\Gamma - Ad_{\Gamma'}$ a matrix in $0, 1-\frac{1}{p}$ and $-\frac{1}{p}$

$$\mathbb{E}\left(\sum_{\substack{p\in P\\ p\mid n}} 1\right) = \sum_{p\in P}\text{Prob}(p\mid n) = \sum_{p\in P}\frac{1}{p} = L + O\left(\frac{|P|}{N}\right)$$

In fact all eigenvalue are $O(\sqrt{L})$ if we restrict $A|_X \subset \{N<n\le 2N\}$ s.t. $|\{N<n\le 2N\}\cap X| < \varepsilon$

The big conjecture is the following:

(Weak) Chowla conjecture: $\sum_{n\le X}\frac{\lambda(n+a_1)\cdots\lambda(n+a_k)}{n} = o(\log X)$ $\xrightarrow{\text{Tao}}$ weak Sarnak conjecture

Towards that end, we would like to show

$$\sum_{\substack{N<n\le 2N\\ p\in P}} \frac{f(n+a_1\cdot p)\cdots f(n+a_k\cdot p)}{p} - \sum_{\substack{N<n\le 2N\\ p\in P}} \frac{f(n+a_1p)\cdots f(n+a_kp)}{p} \text{ is } o(LN)$$

for $f: N\le 2N\to\mathbb{C}$ bdded

This would be true if a certain hypergraph has a wonderful ppty is Friedman-Widgerson.

V is a set. E is a set of 'edges' $(v_1,\cdots,v_k)$ we see Γ is regular of deg d if

$\forall v_1,\cdots,v_{k-1}\in V$, $\exists$ exactly d elmts of V s.t. $(v_1,\cdots,v_{k-1},v)\in E$

Given W the space of functions $V\to\mathbb{C}$. then Γ define multi-linear operator.

$$T: (f_1\cdots f_k) \longmapsto \sum_{(v_1\cdots v_k)\in E} f_1(v_1)\cdots f_k(v_k)$$

You can write T a tensor $T = \sum_{(v_1 \cdots v_k) \in E} e_{v_1} \otimes \cdots \otimes e_{v_k}$ where $e_1, \ldots, e_n$ the standard basis of $f: V \to \mathbb{C}$

Define $\vec{1}: V \to \mathbb{C}$ as $\vec{1} = e_1 + \cdots + e_n$. For Γ regular of deg d.

$$G := T - \frac{d}{n} \underbrace{\vec{1} \otimes \cdots \otimes \vec{1}}_{k\text{-times}}$$ the adjacency matrix.

First eigenvalue $\lambda_1(\mu) = \|\mu\|_{L^2 \times \cdots \times L^2 \to \mathbb{C}} := \sup_{\|f_i\|_2 = 1} |T(f_1, \ldots, f_k)|$

Second eigenval: $\lambda_2 = \lambda_1(G)$ kills off the top guy

Thm: The first eigenval of a d-regular k-uniform hypergraph is $dn^{\frac{k-2}{2}}$ (corresp to $\vec{1}, \vec{1}, \vec{1}$)

Lemma For T symm, $\exists w \in W$ s.t. $T(w, \ldots, w) = |T|$ with $|w| = 1$

Thm Every 3-uniform d-regular hypergraph has second eigenval $\geq \sqrt{d(1-d)/n}$

Thm: For n, $d \geq C' \log n$, a random 3-uniform hypergraph on n vertices with dn^2 edges chosen randomly has second eigenval $\leq C(\log n)^{3/2}\sqrt{d}$ with Prob $= 1$