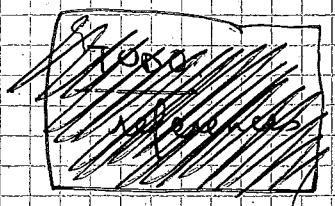
Lecture 2

Expansion of Cayley graphs of finite linear groups



1 - History / statements

We saw in the first lecture some statements of the type

"if $\mathcal{C}(G_i, S)$ is expanding

then M_i has such and such (interesting) property"

where $M_i \to M$ is a Galois covering with $\mathrm{Gal}(M_i/M) = G_i$

(and S generates $\pi_1(M)$).

We consider now special cases of this situation:

Let faithful representation $\rho : \pi_1(M) \to GL_n(\mathbb{C})$ be a finite-dim representation of M; let Γ be the image of ρ. We assume that

$$\Gamma \subset SL_n(\mathcal{O})$$

where $\mathcal{O} \subset K$ is the ring of integers in some number field [e.g. $\Gamma \subset SL_n(\mathbb{Z})$]

We can then construct a family of congruence quotients of Γ by

$$\Gamma_q = \ker\left(\Gamma \longrightarrow SL_n\left(\mathcal{O}_K/q\right)\right)$$

where $0 \neq q \subset \mathcal{O}$ runs over the ideals of $\mathcal{O}$.

These are finite index subgroups with

$$\Gamma/\Gamma_q \hookrightarrow SL_n\left(\mathcal{O}/q\right)$$

which is a finite linear group.

In particular we get

$$\pi_1(M) \twoheadrightarrow \Gamma \longrightarrow \Gamma/\Gamma_q$$

and finite Galois coverings corresponding $\Gamma_q \longrightarrow M$.

Γ/Γ_q

Q. In which circumstances is a family

$$\left(G\left(\Gamma/\Gamma_q\,;\,S\right)\right)_{q \in \mathcal{N}}$$

expanding ? ($\mathcal{N}$: some infinite set of ideals)

Note that this is a question about groups, and not manifolds.

Ex. (1) M a hyperbolic compact 3-manifold

There exists an embedding

$$\pi_1(M) \hookrightarrow SL_2\left(\mathcal{O}_{\mathbb{Q}(\sqrt{-d})}\left[1/N\right]\right)$$

where $\begin{cases} N \geq 1 \\ \mathcal{O} \subset \mathbb{Q}(\sqrt{-d}) \end{cases}$ for some squarefree integer d

In general, the image Γ of $\pi_1(M)$ is not of finite index in $SL_2(\mathcal{O}[\frac{1}{N}])$.

(2) Take $\Gamma = SL_m(\mathbb{Z})$, $m \geq 2$, $S \subset \Gamma$ gen and $\Gamma_q = \ker(\Gamma \to SL_m(\mathbb{Z}/q\mathbb{Z}))$

Then $\Gamma/\Gamma_q \cong SL_m(\mathbb{Z}/q\mathbb{Z})$ for all $q \geq 1$

so we are looking at

$$\mathcal{C}(SL_m(\mathbb{Z}/q\mathbb{Z}); \pi_q(S))$$

This is a case of arithmetic groups.

(3) Take $a \in \mathbb{Z} - \{0\}$ $\Gamma = \langle \underbrace{\begin{pmatrix} 1 & \pm a \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ \pm a & 1 \end{pmatrix}}_{S_a} \rangle < SL_2(\mathbb{Z})$

Then Γ has (in)finite index if $\begin{cases} 1 \leq |a| \leq 2 \\ |a| \geq 3 \end{cases}$

and

$$\Gamma/\Gamma_q = SL_2(\mathbb{Z}/q\mathbb{Z}) \text{ if } (a,q) = 1$$

Again $\mathcal{C}(SL_2(\mathbb{Z}/q\mathbb{Z}); \pi_q(S_a))$

Note here that the groups do not change, but the generating sets do. (essentially)

Q. (When) Are these families expanding?

Until a few years ago, rather little was known, but already this was recognized as very important.

1970's

Th 1 (Margulis, Kazhdan) If G is a discrete group which has Property (T) and $S \subset G$ finite generates G, then the family of all finite quotients of G is expanding family:

$$\mathcal{C}(G/H;\ \pi_H(S))_{H \lhd G,\ \text{f.i.}}$$

expands.

In particular, this applies to $G = SL_m(\mathbb{Z})$, $m \geq 3$.

So for Ex. 2, if $m \geq 3$, we have expanders.

Th 2 - (Selberg; ...; Clozel) + Burger-Sarnak + Burger/Brooks

If $G \subset SL_m(\mathbb{C})$ is arithmetic then the family of all congruence quotients of G is expanding.

This uses automorphic methods, and hence is by no means elementary. This applies to Ex. 1 in the finite index case ($\Gamma < SL_2(\mathbb{C})$ with $\ldots$) and so $\left\{\begin{array}{l} \text{Ex. 2 for } m=2 \\ \text{Ex. 3 for } 2 \leq |a| \leq 2 \text{ only} \end{array}\right.$

So there are still many open cases. Note in particular the great importance of the generating set (in appearance), which seem strange!

Things are now much better understood!

Th (Salehi-Golsefidy, Vaj'i 2011)

Let $\Gamma \subset SL_m(\mathbb{Z})$ be given, $S = S^{-1}$ a finite generating set of Γ.

① Assume that the Zariski closure $G = \overline{\Gamma}$ satisfies $G^\circ = [G^\circ, G^\circ]$

There exists $q_0 \geq 1$ s.t.

$$\left(\mathcal{C}(\Gamma/\Gamma_q ; \pi_q(S)) \right)_{q \text{ coprime to } q_0}$$

is an expanding family.

② Conversely if

$$\left(\mathcal{C}(\Gamma/\Gamma_q ; \pi_q(S)) \right)_{q \text{ prime large enough}}$$

is expanding, then

$$G^\circ = [G^\circ, G^\circ].$$

~~History~~

Ex: (1) If $G = SL_m$, then $G = G^\circ = [G, G]$

In this case, can take all q [Bourgain-Vaj'i]

(2) If $G = GL_1$, this does not work

(3) If working over $K/\mathbb{Q}$, apply to $\Gamma \subset (\mathrm{Res}_{K/\mathbb{Q}} G)(\mathbb{Z})$ (there are surprises! cf $S - G \cong V$)

5bis

$\exists C$, $\forall p$,

$$\begin{pmatrix} 1 & \frac{p-1}{2} \\ 0 & 1 \end{pmatrix} \in SL_2(\Gamma_p)$$

Cor.

can be written

$$S_1 \cdots S_m$$

with $S_i^{\pm 1} \in \left\{ \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix} \right\}$

$m \leq C \log p$

Q Find (S_i) effectively !

(4) The method is effective, but horribly weak: for as far as expansion etc goes (6)

$$\Gamma = \left\langle \begin{pmatrix} 1 & \pm 3 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ \pm 3 & 1 \end{pmatrix} \right\rangle$$

it gives

$$\geq 1 - (\Gamma : \Gamma_p) \geq 2^{-2^{36}}$$

for $p \geq 2^{2^{46}}$

History:

2004 Helfgott: "growth" for $SL_2(\mathbb{F}_p)$

Gill, Helfgott, Helfgott: G SL_m SP_{2g} (partial)

2006: Bourgain, Gamburd: $SL_2(\mathbb{F}_p)$

Bourgain, Gamburd, Sarnak: $SL_2(\mathbb{Z}/q\mathbb{Z})$ sqf.

2010: Pyber–Szabó: "growth in general"

Breuillard–Green–Tao:

2009: Varjú: $G = SL_m$, q squarefree

3. Some key ingredients

What is it that makes this work? To give some insight we assume $G = SL_m$, $q = p$ prime. Then Γ dense $\Rightarrow \forall p$ prime large $\Gamma/\Gamma_p = SL_m(\mathbb{F}_p)$.

(I) We always work with "the same" generating set S for all q, and do not change it, although one might wonder

whether this is necessary or not.

This is because of the following argument that goes back to Margulis:

(1) we may replace S by any $T' = T \subset S^{\ell}$, for $\ell \geq 1$ (fixed)

(2) by the Tits alternative, one can find such $\ell (= \ell(\Gamma)$, in fact, independent) (Breuillard-Gelander)

s.t. $\Gamma_1 = \langle T \rangle \subset \Gamma = \langle S \rangle$ is a free group with the same Zariski closure SL_m

Since $\mathcal{C}(\Gamma/\Gamma_q, S)$ have "more" edges, it is enough to work with T.

(T is fixed)

(3) Because Γ_1 is free, there exists $\delta > 0$ s.t. for all $p > p_0$, the reduction maps

$$\Gamma_1 \longrightarrow SL_m(\mathbb{F}_p)$$

are injective when restricted to the ball of radius $\delta \log p$ in the Cayley graph.

$\exists\, q_0$, $(q, q_0) = 1$

$\Gamma \twoheadrightarrow SL_m(\mathbb{F}_q)$

so $\Gamma_q = \Gamma_1 / \Gamma_{1,q}$

In particular, these balls "grow" fast at the beginning.

(II) Ultimately, expansion (for p prime) is obtained by a counting argument for loops that goes back to Sarnak–Xue (with earlier occurrence in a paper of Huxley) whose crucial group-theoretic ingredient goes back to Frobenius for SL_2:

Th. Let $m \geq 2$, $p \geq 3$ prime.

The smallest dimension of a $\neq 1$ irreducible complex representation of $SL_m(\mathbb{F}_p)$ is

$$\geq \frac{p-1}{2}.$$

How can this be used?

Let $N_{2k} = |\{$loops from 1 of length $2k$ in the Cayley graph$\}|$

There is a spectral expansion:

$$N_{2k} = |S|^{2k} \times \frac{1}{|V|} \sum_{\varphi} (1-\lambda_\varphi)^{2k}$$

where φ runs over an orthonormal basis of $L^2(V)$, with $1 \in \{\varphi\}$, and $\Delta\varphi = \lambda_\varphi \varphi$.

Note that we can drop any terms by positivity (since $2k$ is even).

Now observe that $SL_2(\mathbb{F}_p) = \Gamma/\Gamma_p$ acts linearly on $\ker(\Delta - \lambda \mathrm{Id})$ for any λ by the regular rep.

For $\lambda \neq 0$, this action is not trivial (since there are no invariant vectors in $L^2(\Gamma)$ except 1!) hence

$$\dim \ker(\Delta - \lambda_1 \mathrm{Id}) \geq \frac{p+1}{2}$$

So we get roughly

$$N_{2k} \geq |S|^{2k} \times \left(\frac{1}{|\Gamma/\Gamma_q|} + \frac{p-1}{2} \frac{1}{|\Gamma/\Gamma_q|} (1-\lambda_1 \right.$$

Now if we could establish that

$$N_{2k} \leq C_\varepsilon |S|^{2k} \times \frac{1}{|\Gamma/\Gamma_q|} p^{\varepsilon}$$

for sufficiently small $\varepsilon > 0$

some $k = \alpha \log p$, $\alpha > 0$

then we would derive

$$C_\varepsilon p^{\varepsilon} \geq 1 + \frac{p-1}{2} (1-\lambda_1)^{2k}$$

$$\geq \frac{p-1}{2} p^{\alpha \log(1-\lambda_1)}$$

which, if p is large enough, implies something like

$$\varepsilon \geq 1 + \alpha \log(1-\lambda_1)$$

If $0 < \varepsilon < 1$ then

$$\underbrace{\alpha \log(1-\lambda_1)}_{<0} \geq \underbrace{\varepsilon - 1}_{<0}$$

certainly gives a spectral gap.

So the problem is:

- given $\varepsilon > 0$ small enough
- find α (arbitrarily large, but indep of p)
- such that

$$N_{2h} \leq C(\varepsilon) |S|^{2h} \frac{p^{\varepsilon}}{|\Gamma/\Gamma_p|} \qquad (*)$$

Note: asymptotically

$$\lim_{h \to \infty} \frac{N_{2h}}{|S|^{2h}} = \frac{1}{|\Gamma/\Gamma_p|}$$

by equidistribution / (connectedness, non-bipartiteness)

so we want something { close to equidistribution after a time comparable to the optimal equid time

but the large dimension of $\mathcal{E}$ eigenspaces gives us a crucial amount of "wiggle-room" to make this not too hopeless.

III How to get $(*)$?

This is where Bourgain-Gamburd made the connection with Helfgott's & Growth Theorem.

1- Note that the argument of Margulis gives

$$\frac{N_{2h}}{|S|^{2h}} \leq C_1 \rho^{-\delta}$$

for $\begin{cases} \text{some } \delta > 0 \\ h = \alpha_1 \log \rho, \quad \alpha_1 > 0 \text{ (small)} \end{cases}$

2- Bourgain - Gamburd's crucial new ingredient is the "L^2 - flattening lemma":

Lemma - If $\exists \beta > 0$ s.t.

$$\frac{N_{2h}}{|S|^{2h}} \leq C \rho^{-\beta} \quad (*)$$

for $\begin{cases} \text{some } \beta > 0 \\ h = \alpha_1 \log \rho \end{cases}$

then

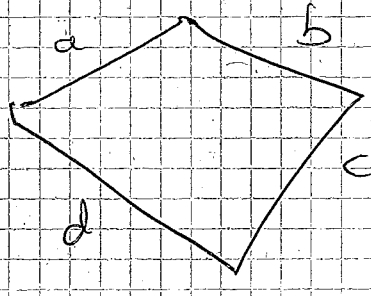
$$\frac{N_{4h}}{|S|^{4h}} \leq C \rho^{-\beta - \gamma}, \quad \max\left[\frac{1}{|\Gamma/\Gamma_\rho|} \right] \quad (*)$$

~~unless~~ ~~$\rho^{-\beta} \leq \frac{1}{|\Gamma/\Gamma_\rho|}$~~

~~Another record case we can do~~

The idea is as follows:

consider a loop of length $4h$



$abcd = 1$

and a, b, c, d are in

$A_h = \{$ words of length $h\}$

If N_{4k} is "very large", this means that $abcd = 1$ has "many" solutions in A_k.

What are sets with "lots" of sol? to this equation

These are ~~subgroups~~ ($|A_k|^3$ solutions)!

Here the ~~=~~ numerics is such that if (~~$\$$~~) fails then the ab of solution is comparable to $|A_k|^{3-\gamma}$.

Th. (Helfgott + ~~Tao~~; Bourgain; Nikolov-Pyber)

$\exists \; c > 0 \quad \left(c = \frac{1}{3024} \; K\right)$

$\forall p \geq 3$

$\forall \; A \subset SL_2(\mathbb{F}_p)$, ~~$\quad$~~ A generating $SL_2(\mathbb{F}_p)$

$1 \in A^{-1}$

either

$$A \cdot A \cdot A = SL_2(\mathbb{F}_p)$$

or

$$|A \cdot A \cdot A| \geq |A|^{1+c}$$

NB Nothing so strong holds for abelian groups! Here the second case basically gives the second alternative, and the first contradicts the negation of the first.

Why can Helfgott's Th. be true?

We can only give a very weak version of not-impossibility argument:

assume we want to ~~believe~~ not believe it; we try to find a counter example; one ~~clean~~ clean "not quite" counter example is $A = H \subsetneq SL_2(\mathbb{F}_p)$ but of course A does not generate.

What about $A = H \cup \{g_0\}$ for some $g_0 \notin H$?

Take
$$\begin{cases} H = \left\{ \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \mid t \in \mathbb{F}_p \right\} \\ g_0 \notin H, \quad g_0 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \ c \neq 0 \end{cases}$$

Fact: $A = H \cup \{g_0\}$ satisfies

$$|A \cdot A \cdot A \cdot A| \geq \frac{(p-1)^3}{2} - 1$$

Proof Let $H^\circ = H \setminus \{1\}$

Consider
$$\psi \begin{cases} H^\circ \times H^\circ \times H^\circ \longrightarrow SL_2(\mathbb{F}_p) \\ (g_1, g_2, g_3) \longmapsto g_1 g_0 g_2 g_0^{-1} g_3 \end{cases}$$

Compute: ψ is injective

So $$(p-1)^3 = |\psi(H^\circ \times H^\circ \times H^\circ)| \leq |\underbrace{A \cdot A \cdots A}_{5 \text{ times}}|$$

□

This argument is a prototype of a so-called Larsen–Pink (approx.) inequality, which are crucial in ~~[illegible]~~ proving growth theorems by showing that if A generates G (finite simple of Lie type) then

$$|V \cap A|$$

can not be very large if V is a subvariety (of small complexity).