Lecture 3

Examples of expanders

Recall: (Γ_n) expander

$\Updownarrow$

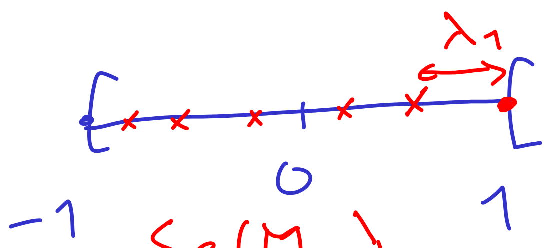
(i) $|\Gamma_n| \longrightarrow +\infty$.

(ii) $\exists k, \forall n, \forall x \in \Gamma_n, \ \mathrm{val}(x) \leq k$.

$$h(\Gamma_n) = \min_{1 \leq |W| \leq \frac{|V|}{2}} \frac{|\mathcal{E}(W)|}{|W|}$$

$$\left\{ \begin{array}{l} \text{(iii) } \exists c > 0, \forall n, \ h(\Gamma_n) \geq c. \\ \Updownarrow \\ \text{(iii)' } \exists c > 0, \forall n, \ \lambda_1(\Gamma_n) \geq c. \end{array} \right.$$

$$M_\Gamma f(x) = \frac{1}{\mathrm{val}(x)} \sum_{x,y} \underbrace{a(x,y)}_{\text{nb. of edges } x \leftrightarrow y} f(y)$$



$Sp(M_\Gamma)$

One property of expanders (useful for number theory):

<u>Prop.</u> G finite group

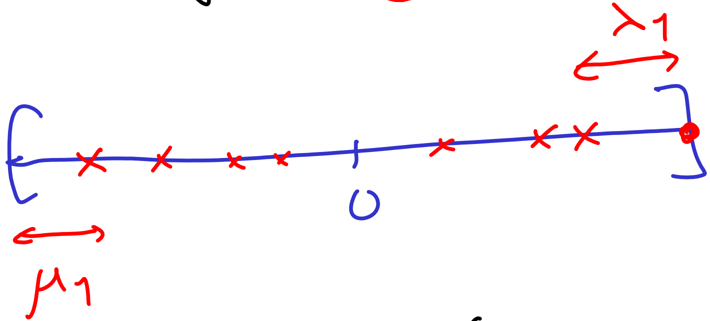
$S = S^{-1}$ generating set, $1 \in S$ not bipartite

For $g \in G$, $n \geq 1$,

$$\left| \frac{1}{|S|^n} \left|\left\{ (s_1, \dots, s_n) \in S^n \,\middle|\, s_1 \cdots s_n = g \right\}\right| - \frac{1}{|G|} \right| \leq \rho^n$$

$\mathcal{G}(G, S)$

where ρ = spectral radius of M_Γ on $1^\perp$



$$\rho = \min(\lambda_1, \mu_1)$$

(cf. also "expander mixing lemma")

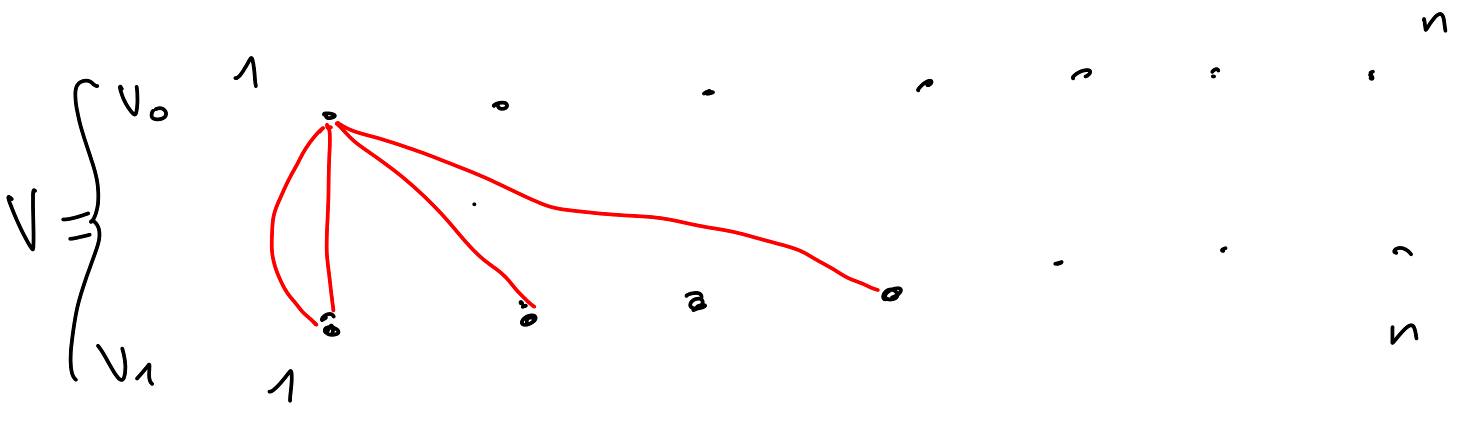
Back to expanders

It turns out that many interesting families of graphs are expanders.

3.1 _ Random graphs

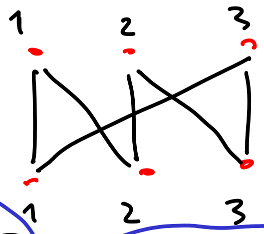
Pinsker (1973)
Barzdin - Kolmogorov (1967)
} random construction

Take: $n \geq 1$, $d \geq 3$



Connect each $i \in V_0$ to d random $j \in V_1$ (with permutations); we get

$(n!)^d$ finite graphs $\Gamma_{(\sigma_i)}$ (bipartite) (d-regular)



$n = 3$

$d = 2$

$\sigma_1 = \mathrm{Id}$

$\sigma_2 = (1\,2\,3)$

<u>Prop.</u> $\exists\, c > 0$, s.t.

$$\lim_{n \to \infty} \frac{1}{(n!)^d} \left| \left\{ (\sigma_i)_{1 \le i \le d} \;\middle|\; h\left(\Gamma_{(\sigma_i)}\right) \ge c \right\} \right| = 1$$

$$\sigma_i : V_0 \xrightarrow{\sim} V_1, \quad 1 \le i \le d$$

In particular for n large enough, there is at least one $\Gamma_{(\sigma_i)}$ with $h(\Gamma_{(\sigma_i)}) \ge c$.

$\longrightarrow$ get (many) expanders.

<u>But</u>: (1) can one exhibit "deterministic" expanders?

(2) in some applications, one is given some explicit graphs, and one needs to know that <u>these</u> are expanders!

3.2. Cayley graphs as expanders

<u>Typically</u>: start with an infinite group G [ex. $G = SL_m(\mathbb{Z})$] $m \geq 2$

and a sequence of normal subgroups

$$G_n \triangleleft G$$

of <u>finite index</u>

(ex. $G_n = \ker\left(SL_m(\mathbb{Z}) \longrightarrow \overbrace{SL_m(\mathbb{Z}/n\mathbb{Z})}^{\text{finite}}\right)$)

"congruence subgroups" $\quad g \longmapsto g \bmod n$

Let $S = S^{-1} \subset G$ be a finite set

Then consider

$$\boxed{\Gamma_n = \mathcal{C}(G/G_n, S \bmod G_n)}$$

If S generates G then these are connected finite graphs.

[<u>Ex.</u> $S = \{ \mathrm{Id} \pm E_{ij} \mid 1 \leq i \neq j \leq m \}$

<u>$m=3$</u>: $\mathrm{Id} + E_{1,3} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -1 & 1 \end{pmatrix}$]

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad = \mathrm{Id} - E_{3,2}$

These types of families occur naturally (in geometry, number theory, ...)

<u>Q.</u> Are such $(\mathcal{G}(G/G_n, S))_{n \geq 1}$ expanders?

<u>Theorems</u>:

(1) [Margulis, 1973]

If G has <u>Property (T)</u> of

Kazhdan then $\left(\mathcal{C}(G/G_n, S)\right)_{n \geq 1}$ (any fixed generating set)

is an expander [provided $\boxed{\lim_{n\to\infty} [G : G_n] = +\infty}$]

(e.g. (Kazhdan) $G = SL_m(\mathbb{Z})$, for $m \geq 3$)

[e.g. $\mathcal{C}\left(SL_3(\mathbb{Z}/_{n}\mathbb{Z}), \{Id \pm E_{i,j}\}\right)$

is an expander, because

$$SL_3(\mathbb{Z}) \xrightarrow{\pi_n} SL_3(\mathbb{Z}/_{n}\mathbb{Z})$$

is surjective for all n, so

$$SL_3(\mathbb{Z})/\ker(\pi_n) \simeq SL_3(\mathbb{Z}/_{n}\mathbb{Z})\Big)$$
]

(2) [Brooks; Burger; Selberg]
$\simeq 1985$

$\mathcal{C}(SL_2(\mathbb{Z}/_{n}\mathbb{Z}), S)$ is an expander.

└ any fixed generating set

(3) (Q. (Lubotzky): G = subgroup generated by

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

in $SL_2(\mathbb{Z})$ and

$$G_n = \ker\left(G \longrightarrow SL_2(\mathbb{Z}/n\mathbb{Z})\right) ?)$$

Difficulty: $[SL_2(\mathbb{Z}) : G] = +\infty$

but $G/G_n = SL_2(\mathbb{Z}/n\mathbb{Z})$ (if n coprime to 3)

[Bourgain-Gamburd, 2005; based on an important intermediate result of Helfgott]

For $G \subset SL_2(\mathbb{Z})$ Zariski-dense in $SL_2(\mathbb{C})$ [eg G above]

$$\left(\mathcal{C}\left(G/_{\ker \pi_p},\ S\right)\right)_{p \text{ prime}}$$

is an expander (for all fixed generating set $S \subset G$).

(4) [Bourgain - Varjú (2010)]

Let $G \subset SL_m(\mathbb{Z})$ Zariski-dense, $S = S^{-1} \subset G$ fixed generating set; then $\exists\ N \geq 1$
$m \geq 2$

$$\left(\mathcal{C}\left(G/_{\ker \pi_n},\ S\right)\right)_{n \geq 1}$$

$SL_m(\mathbb{Z}/n\mathbb{Z})$ $\quad (n, N) = 1$

is an expander.

[eg. Lubotzky example, $N = 3$]

[<u>Fact:</u> $G \subset SL_m(\mathbb{Z})$ is Zariski-dense $\iff$ for all p large enough, the map

$$G \longrightarrow SL_m(\mathbb{Z}/p\mathbb{Z})$$

is <u>surjective</u>.]

<u>Q.</u> $(SL_2(\mathbb{F}_p))_{p \text{ prime}}$

$k \geq 3$

<u>Q?</u> is $(\mathcal{C}(SL_2(\mathbb{F}_p), S_p))_p$ expander, where S_p is an arbitrary generating set mod p?

[Breuillard - Gamburd: for subsets of primes]