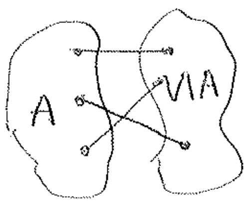
Expander graphs & product replacement algorithm.

$\mathcal{G} = (V, E)$ – finite graph; V = vertices, E = edges.

For $A \subset V$, $\partial A = \{v \in V \setminus A : \exists \text{edge from } v \text{ to } A\}$.

Def. Isoperimetric constant $h(\mathcal{G})$:

$$h(\mathcal{G}) = \min_{A \subsetneq V} \frac{|\partial A|}{\min\{|A|, |V \setminus A|\}}$$

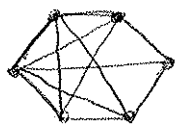


examples. 1)

$\mathcal{G}$ is cycle graph with n vertices:

$$h(\mathcal{G}) = \frac{2}{[\frac{n}{2}]}.$$

2)



$\mathcal{G}$ is complete graph with n vertices:

$$h(\mathcal{G}) = 1.$$

Remark. For $A \subset V$, $|A| \leq \frac{1}{2}|V|$, we have

$$|A \cup \partial A| \geq (1 + h(\mathcal{G}))\,|A|.$$

Def: Fix $k \in \mathbb{N}$, $\varepsilon > 0$.

A family of finite graphs $\mathcal{G}_n = (V_n, E_n)$ is (k, ε)-expander family if

- $|V_n| \longrightarrow \infty$
- Every vertex has $\leq k$ neighbours
- $h(\mathcal{G}_n) \geq \varepsilon$.

Γ – a group, $S \subset \Gamma$ – finite generating set, $S = S^{-1}$

V – a finite set on which Γ acts transitively.

$E = \{(v, sv) : v \in V, s \in S\}$, $\mathcal{G} = (V, E)$.

$$\mathcal{H} = \ell_0^2(V) = \{f : V \to \mathbb{C} : \sum_{v \in V} f(v) = 0\} \text{ – Hilbert space.}$$

$$\langle f_1, f_2 \rangle = \sum_{v \in V} f_1(v) \overline{f_2(v)}.$$

$\rho : \Gamma \to \mathcal{U}(\mathcal{H})$ – unitary representation.

$$\rho(\gamma) f(v) = f(\gamma^{-1} v), \quad \gamma \in \Gamma, v \in V.$$

<u>Lemma.</u> $h(\mathcal{G}) \geq \inf \{ \frac{1}{4} \max_{s \in S} \|\rho(s) f - f\|^2 : f \in \mathcal{H}, \|f\| = 1\}$.

$\ulcorner$ Let $V = A \sqcup B$ be a partition of V, $|A| = a$, $|B| = b$.

$$F(v) = \begin{cases} b, & v \in A, \\ -a, & v \in B. \end{cases}$$

Then $\sum_v F(v) = 0$ and $\|F\|^2 = ab^2 + ba^2 = |V| ab$.

Let $f = \frac{1}{\sqrt{|V| ab}} \cdot F$.

For $s \in S$,
$$F(s^{-1} v) - F(v) = \begin{cases} b + a, & s^{-1} v \in A, v \in B, \\ -a - b, & s^{-1} v \in B, v \in A \\ 0, & \text{otherwise} \end{cases}$$

$$\|\rho(s) F - F\|^2 = (a+b)^2 \, |(sA \cap B) \cup (sB \cap A)| \leq (a+b)^2 \cdot 2 |\partial A|.$$

$$\|\rho(s) f - f\|^2 \leq \frac{2(a+b)^2 |\partial A|}{|V| \cdot ab} = 2 \cdot \left(\frac{1}{a} + \frac{1}{b}\right) \cdot |\partial A|$$

$$\leq 4 \cdot \frac{|\partial A|}{\min\{a, b\}}.$$

Hence, $\frac{|\partial A|}{\min\{|A|, |B|\}} \geq \frac{1}{4} \max_{s \in S} \|\rho(s) f - f\|^2$,

which implies the claim. $\lrcorner$

Construction of expander graphs.

1) $V_n = \mathbb{Z}/n \times \mathbb{Z}/n$. The group $\Gamma = SL_2(\mathbb{Z}) \ltimes \mathbb{Z}^2$ acts on V_n transitively, $S = \left\{ \begin{pmatrix} 1 & \pm 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ \mp 1 & 1 \end{pmatrix}, \begin{pmatrix} \pm 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ \pm 1 \end{pmatrix} \right\}$.

We have shown that $\exists \varepsilon > 0$: for every unitary representation $\rho : \Gamma \to \mathcal{U}(\mathcal{H})$ with no $\mathbb{Z}^2$-inv. vectors: $\forall f \in \mathcal{H}$:

$$\max_{s \in S} \| \rho(s) f - f \| \geq \varepsilon .$$

Apply this to the representations $\rho_n : \Gamma \to \mathcal{U}(\ell_0^2(V_n))$.

Then by Lemma, $h(\mathcal{G}_n) \geq \frac{1}{4} \varepsilon^2$.

2) $d \geq 3$. $V_n = \Gamma / \Gamma(n)$ where $\Gamma = SL_d(\mathbb{Z})$ and $\Gamma(n)$ is the congruence subgroup of level n.
$S \subset \Gamma$ any symmetric generating set for Γ.
$\mathcal{G}_n$ = corresponding graph on V_n.
Then since Γ has Kazhdan property, $\{\mathcal{G}_n\}$ is an expander family.

Is $\left\{ SL_2(\mathbb{Z}) / SL_2(\mathbb{Z})(n) \right\}$ an expander family?

$\Gamma = SL_2(\mathbb{Z})$, $\Gamma(n) < \Gamma$ – congruence subgroup.
$S \subset \Gamma$ – symmetric generating set.
$\mathcal{G}_n$ = corresponding graphs on $\Gamma / \Gamma(n)$.

$M_n = \Gamma(n) \backslash \mathbb{H}^2$ – hyperbolic surface.

$0 = \lambda_0(M_n) < \lambda_1(M_n) \leq \lambda_2(M_n) \leq \dots$ – eigenvalues of Laplace operator on M_n.

<u>Prop.</u> $\exists c > 0$: $h(\mathcal{G}_n) \geq c$ for all n $\iff$ $\exists c' > 0$: $\lambda_1(M_n) \geq c'$ for all n.

Thm (Selberg '65) $\lambda_1(M_n) \geq \frac{3}{16}$ for all n.

Hence, $\{\mathcal{G}_n\}$ is an expander family

Conj. (Selberg '65) $\lambda_1(M_n) \geq \frac{1}{4}$ for all n.

Random walks on graphs.

Fix a finite graph $\mathcal{G} = (V, E)$.
Assume that each vertex has k neighbours and $\mathcal{G}$ is connected.

A random walk on $\mathcal{G}$ is a sequence of random variables ξ_n with values in V such that if $\xi_n = v$, then $\xi_{n+1} = $ (a neighbour of v) with probability $\frac{1}{k}$.

Let $M = (m_{vw})$ be the matrix indexed by $V \times V$:

$$m_{vw} = \begin{cases} \frac{1}{k}, & \text{if } (v,w) \in E \\ 0, & \text{otherwise} \end{cases}$$

Then $\mathrm{Prob}(\xi_{n+1} = v) = \sum_{w \in V} m_{vw} \cdot P(\xi_n = w)$.

Hence, if $p_n = (\mathrm{Prob}(\xi_n = v))_{v \in V}$ represents the distribution of ξ_n, then

$$p_n = M p_{n-1} = M^n p_0.$$

Note that M is a symmetric matrix, and

$$\sum_v m_{vw} = \sum_w m_{vw} = 1.$$

Hence, by Perron-Frobenius Thm,

$$\mathrm{Spec}(M) = \{ \lambda_0 = 1 > \lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_{|V|-1} \geq -1 \}.$$

We also consider a <u>lazy random walk on $\mathcal{G}$</u>.

a sequence of random variables η_n defined recursively as: if $\eta_n = v$, then $\eta_{n+1} = \begin{cases} v, \text{ with prob.} = \frac{1}{2}, \\ (\text{a neighbour of } v), \text{ with prob.} = \frac{1}{2k}. \end{cases}$

This random walk corresponds to the matrix

$$N = \frac{1}{2}(id + M),$$

with eigenvalues $\mu_i = \frac{1}{2}(1 + \lambda_i)$.

<u>Prop.</u> For every initial distribution,

$$\left| P(\eta_n = v) - \frac{1}{|V|} \right| \leq \mu_1^n \cdot |V|.$$

$p_n = N^n p_0$. Let $p_0 = p_0^{(0)} + \ldots + p_0^{(|V|-1)}$ be the decomposition with respect to eigenspaces of N.

$\mu_0 = 1$, with eigenvector $(1, \ldots 1) = v_0$, so

$$p_0^{(0)} = \frac{\langle p_0, v_0 \rangle \cdot v_0}{\|v_0\|^2} = \left(\frac{1}{|V|}, \cdots \frac{1}{|V|}\right) = p_\infty.$$

$$\| N^n p_0 - p_\infty \| \leq \sum_{i \geq 1} \mu_i^n \cdot \|p_0^{(i)}\| \leq \mu_1^n \cdot |V|.$$

Prop. For every finite graph $\mathcal{G}$,

$$\frac{h(\mathcal{G})^2}{2k^2} \leq 1-\lambda_1 \leq 2 \cdot \frac{h(\mathcal{G})}{k}.$$

Generating random elements in groups.

Let G be a finite group.

$$\Omega_k(G) = \{(g_1, \dots g_k) : g_i \in G, \ \langle g_1, \dots g_k \rangle = G\}.$$

Product replacement algorithm: is a lazy random walk defined as follows: $\eta_0 = (g_1, \dots g_k) \in \Omega_k$, and η_{n+1} is defined recursively by

$$\eta_{n+1} = \begin{cases} \eta_n, & \text{with probability } \frac{1}{2}, \\ R_{i,j}^{\pm} \eta_n \text{ or } L_{i,j}^{\pm} \eta_n, & \text{with equal probabilities,} \end{cases}$$

where

$$R_{ij}^{\pm} : (g_1, \dots g_k) \longmapsto (g_1, \dots g_i g_j^{\pm 1}, \dots g_k),$$

$$L_{ij}^{\pm} : (g_1, \dots g_k) \longmapsto (g_1, \dots g_j^{\pm 1} g_i, \dots g_k).$$

Let F_k be a free group with k generators. $\pi : F_k \to G$. The transformations $R_{i,j}^{\pm 1}$, $L_{ij}^{\pm 1}$ define automorphisms of F_k. In fact, the subgroup $Aut^+(F_k)$ generated by $\{R_{ij}^{\pm}, L_{ij}^{\pm}\}$ has index 2 in $Aut(F_k)$.

Open problem: Does $Aut(F_k)$, $k > 3$, have property (T)?

The product replacement algorithm defines a structure of the graph on $\Omega_k(G)$. Let Ω be one of the connected components of the graph.

Thm. (Lubotzky - Pak)
Assume that $Aut(F_k)$ has property (T).
Then for the product replacement algorithm on Ω: $\exists \lambda_k \in (0,1)$:

$$\boxed{\left| \operatorname{Prob}(\eta_n = \omega) - \frac{1}{|\Omega|} \right| \leq \lambda_k^n \cdot |\Omega|.}$$

Thm (Lubotzky - Pak)
Assume that G is abelean, and $k \geq 3$
Then the above estimate holds unconditionally.

Proof. The action $Aut(F_k)$ on Ω factors through the action of $SL_k^{\pm}(\mathbb{Z})$ on $\mathbb{Z}^k$. Since $SL_k^{\pm}(\mathbb{Z})$ has property (T), the claim follows. $\square$