Groups and Graphs
Lecture II: expanders

Vietri, 6-10 giugno 2016

Search for (finite) graphs that are bot *sparse* and *highly connected*

Search for (finite) graphs that are bot *sparse* and *highly connected*

sparse, means that it has "not many edges"; this is obtained by imposing a bound on the degree of the vertices and letting the number of them grow to infinity.

Search for (finite) graphs that are bot *sparse* and *highly connected*

sparse, means that it has "not many edges"; this is obtained by imposing a bound on the degree of the vertices and letting the number of them grow to infinity.

highly connected is to be intended in the sense of "expanding (spreading) rapidly"

Let $\Gamma = (V, E)$ be a graph. For $\emptyset \neq F \subseteq V$ define the boundary of F

$$\partial(F) = \{e \in E \mid |e \cap F| = 1\}.$$

Let $\Gamma = (V, E)$ be a graph. For $\emptyset \neq F \subseteq V$ define the boundary of F

$$\partial(F) = \{e \in E \mid |e \cap F| = 1\}.$$

The expanding (or *isoperimetrical* or *Cheeger*) constant

$$h(\Gamma) = \inf\left\{ \frac{|\partial F|}{\min\{|F|, |V \setminus F|\}} \middle| F \subseteq V,\ 0 < |F| < \infty \right\}$$

If Γ is finite

$$h(\Gamma) = \min\left\{ \frac{|\partial F|}{|F|} \middle| F \subseteq V,\ 0 < |F| < |V|/2 \right\}$$

For $n \geq 3$

- K_n the *complete graph* on n vertices, then

$$h(K_n) = n - \left[\frac{n}{2}\right]$$

- C_n the *n-cycle*, then

$$h(C_n) = \frac{2}{[n/2]}$$

- Q_n the *n-hypercube*, then

$$h(Q_n) = 1$$

(to be proved later)

(Bassalygo and Pinsker, 1972)

For $k \geq 3$ an infinite family of finite graphs $\Gamma_n = (V_n, E_n)$, $1 \leq n \in \mathbb{N}$, is called a family of k-expanders if

- Γ_n is k-regular for every $n \geq 1$;
- $\lim_{n\to\infty} |V_n| = \infty$;
- there exists $\epsilon > 0$ such that $h(\Gamma_n) \geq \epsilon$ for every $n \geq 1$.

(Bassalygo and Pinsker, 1972)

For $k \geq 3$ an infinite family of finite graphs $\Gamma_n = (V_n, E_n)$, $1 \leq n \in \mathbb{N}$, is called a family of k-expanders if

- Γ_n is k-regular for every $n \geq 1$;
- $\lim_{n\to\infty} |V_n| = \infty$;
- there exists $\epsilon > 0$ such that $h(\Gamma_n) \geq \epsilon$ for every $n \geq 1$.

These have applications in several areas:

- statistical mechanics,
- combinatorics and probabilty,
- theoretical computer science,
- derandomization,
- coding theory,
- many others...

Existence of families of expanders for every $k \geq 3$ is not too difficult to establish

Theorem (Pisker, 1973)

There exists $\delta > 0$ such that for every $n \geq 2$, and every $k \geq 3$ there exists a k-regular graph Γ on n vertices with $h(\Gamma) \geq \delta$.

Existence of families of expanders for every $k \geq 3$ is not too difficult to establish

Theorem (Pisker, 1973)

There exists $\delta > 0$ such that for every $n \geq 2$, and every $k \geq 3$ there exists a k-regular graph Γ on n vertices with $h(\Gamma) \geq \delta$.

Proof is by a counting argument. With similar *probabilistic methods* it is indeed possible to prove that

Theorem

There exists $\delta > 0$ such that the probability that for a k-regular graph X ($k \geq 3$) one has $h(X) \geq \delta$ tends to 1 as $|V(X)| \to \infty$.

Existence of families of expanders for every $k \geq 3$ is not too difficult to establish

Theorem (Pisker, 1973)

There exists $\delta > 0$ such that for every $n \geq 2$, and every $k \geq 3$ there exists a k-regular graph Γ on n vertices with $h(\Gamma) \geq \delta$.

Proof is by a counting argument. With similar *probabilistic methods* it is indeed possible to prove that

Theorem

There exists $\delta > 0$ such that the probability that for a k-regular graph X $(k \geq 3)$ one has $h(X) \geq \delta$ tends to 1 as $|V(X)| \to \infty$.

Explicit construction is quite a different story

G. Margulis (1973). For $m \geq 3$, the set of vertices

$$V_m = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

Set $e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, and consider the transformations of V_m given by

$$S = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \qquad T = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}.$$

Edges are defined by setting that, for every $v \in V_m$, v is adjacent to vertices $Sv,\ Tv,\ Sv + e_1,\ Tv + e_2$ and to the other four vertices defined by the four inverse transformations. In this way an 8-regular graph M_m is obtained, of order m^2, for which it may be proved (Gabber and Galil) that

$$h(M_m) \geq \frac{8 - 5\sqrt{2}}{2} > \frac{4}{9}.$$

(M_m is not properly a simple graph, as it has loops and multiple edges, but these are in number which is linear in m).

It soon appeared that Cayley graphs could provide a promising setting where to look for expanders families.

remark. If $\Gamma = \Gamma[G, S]$ is a Cayley graph, and $F \subset G$, then the cardinality of the boundary of F in Γ is just

$$|FS - S|.$$

Thus, the isoperimetrical bound may be expressed purely in group-theoretical language by requiring that there exists $\epsilon > 0$ such that

$$|FS_0| \geq (1 + \epsilon)|F|,$$

where $S_0 = S \cup \{1_G\}$, for all $F \subseteq G$ with $|F| \leq |G|/2$.

The following Theorem is the final achievement of a research whose many steps where contributed by several authors: A. Lubotzky, M. Kassabov, N. Nikolov, P. Sarnak, E. Breuillard, B. Green, T. Tao (just a few)

Theorem

There exist $k \in \mathbb{N}$ and $\epsilon > 0$ such that, for every non-abelian finite simple group G, a symmetric set S of k generators may be selected for which the Cayley graph $\Gamma[G, S]$ is an ϵ expander.

The following Theorem is the final achievement of a research whose many steps where contributed by several authors: A. Lubotzky, M. Kassabov, N. Nikolov, P. Sarnak, E. Breuillard, B. Green, T. Tao (just a few)

Theorem

There exist $k \in \mathbb{N}$ and $\epsilon > 0$ such that, for every non-abelian finite simple group G, a symmetric set S of k generators may be selected for which the Cayley graph $\Gamma[G, S]$ is an ϵ expander.

Such general k and ϵ are not explicitly computed: it is believed that a careful analysis of the various exstimates would yield $k \sim 1000$ and $\epsilon = 10^{-10}$, although for certain families of simple groups much better values have been proved.

Let $\Gamma = (V, E)$ be a finte graph. The adjacency matrix $A(\Gamma)$ is the matrix indexed on V defined by the adjacency relation:

$$A_{xy} = \begin{cases} 1 & \text{if } \{x, y\} \in E \\ 0 & \text{otherwise} \end{cases}$$

Let $\Gamma = (V, E)$ be a finte graph. The adjacency matrix $A(\Gamma)$ is the matrix indexed on V defined by the adjacency relation:

$$A_{xy} = \begin{cases} 1 & \text{if } \{x, y\} \in E \\ 0 & \text{otherwise} \end{cases}$$

$A(\Gamma)$ is real symmetric, its eigenvalues all real. If $n = |V|$ denote by

$$\mu_0, \mu_1, \dots, \mu_{n-1}$$

the spectrum of $A(\Gamma)$, i.e. the list of eigenvalues counted with multiplicity and such that $\mu_0 \geq \mu_1 \geq \cdots \geq \mu_{n-1}$

Since all diagonal elements of $A(\Gamma)$ are 0, we have

$$\sum_{i=0}^{n-1} \mu_i = Tr(A(\Gamma)) = 0.$$

The linear operator $A = A(\Gamma)$ on the $\mathbb{C}$-space $\mathcal{C}(\Gamma) = \{f \mid f : V \to \mathbb{C}\}$

$$(Af)(x) = \sum_{y \in V} A_{xy} f(y) = \sum_{x \sim y \in V} f(y) \qquad (f \in \mathcal{C},\ x \in V)$$

The linear operator $A = A(\Gamma)$ on the $\mathbb{C}$-space $\mathcal{C}(\Gamma) = \{f \mid f : V \to \mathbb{C}\}$

$$(Af)(x) = \sum_{y \in V} A_{xy} f(y) = \sum_{x \sim y \in V} f(y) \qquad (f \in \mathcal{C},\ x \in V)$$

If $\Gamma = (V, E)$ is k-regular, and $f \in \mathcal{C}$ is a constant, then for each $x \in V$

$$(Af)(x) = \sum_{y \in V} A_{xy} f = d_\Gamma(x) f = kf$$

The linear operator $A = A(\Gamma)$ on the $\mathbb{C}$-space $\mathcal{C}(\Gamma) = \{f \mid f : V \to \mathbb{C}\}$

$$(Af)(x) = \sum_{y \in V} A_{xy} f(y) = \sum_{x \sim y \in V} f(y) \qquad (f \in \mathcal{C},\ x \in V)$$

If $\Gamma = (V, E)$ is k-regular, and $f \in \mathcal{C}$ is a constant, then for each $x \in V$

$$(Af)(x) = \sum_{y \in V} A_{xy} f = d_\Gamma(x) f = kf$$

Lemma

Let Γ be k-regular, then

1. $\mu_0 = k$,
2. $|\mu_i| \leq k$ *for all* $i = 0, \ldots, n-1$;
3. *if* Γ *is connected* $\mu_0 > \mu_1$.
4. Γ *is bipartite if and only if* $\mu_{n-1} = -k$.

$\mu_0 - \mu_1 = k - \mu_1$ is called the *principal spectral gap* of Γ.

For **further reference** let us observe what is encoded in a power of the adjacency matrix $A = A(\Gamma)$ of a graph $\Gamma(V, E)$

For **further reference** let us observe what is encoded in a power of the adjacency matrix $A = A(\Gamma)$ of a graph $\Gamma(V, E)$

It is not difficult to prove, by induction, that for every $m \geq 1$, and any $x, y \in V$

A^m_{xy} *is the number of different walks of length* m *in* Γ *from* x *to* y*.*

For instance,

$$A^2_{xx} = deg_\Gamma(x), \qquad A^3_{xx} = 0$$

Also, clearly, if $\mu_0, \ldots, \mu_{n-1}$ are the eigenvalues of A, then the eigenvalues of A^m are their powers: $\mu_0^m, \ldots, \mu_{n-1}^m$. So, if Γ is k-regular, then

$$\mu_0^2 + \cdots + \mu_{n-1}^2 = tr(A^2) = nk.$$

Theorem (Alon, Milman and Dodziuk)

Let Γ be a connected, k-regular graph on n vertices. Then

$$\frac{k-\mu_1}{2} \leq h(\Gamma) \leq \sqrt{2k(k-\mu_1)}.$$

Theorem (Alon, Milman and Dodziuk)

Let Γ be a connected, k-regular graph on n vertices. Then

$$\frac{k-\mu_1}{2} \leq h(\Gamma) \leq \sqrt{2k(k-\mu_1)}.$$

Thus, for $k \geq 3$

an infinite family of finite connected k-regular graphs $\Gamma_n = (V_n, E_n)$, $1 \leq n \in \mathbb{N}$, with $|V_n| \to \infty$, is a family of k-expanders if and only there exists $\epsilon > 0$ such that

$$k - \mu_1 \geq \epsilon$$

for every $n \geq 1$.

example: the n-cube

The adjacency matrix of Q_2 (a square) is $A(Q_2) = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$,

and its eigenvalues are $2, 0, 0, -2$.
In general, show that

$$A(Q_{n+1}) = \begin{pmatrix} A(Q_n) & I_n \\ I_n & A(Q_n) \end{pmatrix}$$

A simple inductive argument shows that the eigenvalues of Q_n are $n - 2t$, for $t = 0, \ldots, n$, each with multeplicity $\binom{n}{t}$.
In particular, $\mu_1(Q_n) = n - 2$, whence, by the Theorem,

$$h(Q_n) \geq \frac{n - (n-2)}{2} = 1.$$

On the other hand, if $F = \{(0, a_2, \ldots, a_n) \mid a_1 \in \{0, 1\}\} \subseteq V(Q_n) = \{0, 1\}^n$, then

$$|\partial F| = 2^{n-1} = |F|$$

So $h(Q_n) = 1$.

$\Gamma = (V, E)$ a (connected k-regular) graph, $A = A(\Gamma)$. We show that $h(\Gamma) \geq \frac{k-\mu_1}{2}$

$\Gamma = (V, E)$ a (connected k-regular) graph, $A = A(\Gamma)$. We show that $h(\Gamma) \geq \frac{k-\mu_1}{2}$

A is a hermitian operator on $\mathcal{C}(\Gamma)$; i.e. $< Af, g >=< f, Ag >$ where, for $f, g \in \mathcal{C}(\Gamma)$,

$$< f, g >= \sum_{x \in V} f(x)\overline{g(x)}$$

$\Gamma = (V, E)$ a (connected k-regular) graph, $A = A(\Gamma)$. We show that $h(\Gamma) \geq \frac{k-\mu_1}{2}$

A is a hermitian operator on $\mathcal{C}(\Gamma)$; i.e. $< Af, g > = < f, Ag >$ where, for $f, g \in \mathcal{C}(\Gamma)$,

$$< f, g > = \sum_{x \in V} f(x)\overline{g(x)}$$

$\mathcal{Z}$: set eigenvectors relative to $\mu_0 = k$ is the set of constant functions. Thus $\mathcal{C}(\Gamma) = \mathcal{Z} \oplus \mathcal{Z}^{\perp}$ where

$$f \in \mathcal{Z}^{\perp} \Leftrightarrow \sum_{x \in V} f(x) = 0.$$

Have the Rayleigh bounds

$$\frac{< Af, f >}{< f, f >} \in [\mu_{n-1}, \mu_1] \quad \forall f \in \mathcal{Z}^{\perp}$$

An *orientation* of $\Gamma = (V, E)$ is just a total ordering on V.

Given an orientation, have each $E \ni e = \{e_-, e_+\}$ with $e_- < e_+$.

Let $|E| = m$ and the m-dimensional $\mathbb{C}$-space

$$\mathcal{L}(\Gamma) = \{u \mid u : E \to \mathbb{C}\}$$

The *incidence matrix* M indexed on $V \times E$: $M_{xe} = \begin{cases} 1 & \text{if } x = e_+ \\ -1 & \text{if } x = e_- \\ 0 & \text{if } x \notin e \end{cases}$

defines an operator $\delta : \mathcal{L}(\Gamma) \to \mathcal{C}(\Gamma)$

$$(\delta u)(x) = \sum_{x=e_+} u(e) - \sum_{x=e_-} u(e) \qquad (u \in \mathcal{L}(\Gamma),\ x \in V)$$

Its dual operator $\delta^* : \mathcal{C}(\Gamma) \to \mathcal{L}(\Gamma)$ is given by

$$(\delta^* f)(e) = f(e_+) - f(e_-) \qquad (f \in \mathcal{C}(\Gamma),\ e \in E)$$

and $\quad < \delta^* f, u >_{\mathcal{C}} = < f, \delta u >_{\mathcal{L}} \quad (f \in \mathcal{C}(\Gamma),\ u \in \mathcal{L}(\Gamma))$

Simple computation shows that (independently of the chosen orientation) the Laplace operator $\delta\delta^* : \mathcal{C}(\Gamma) \to \mathcal{C}(\Gamma)$ has matrix

$$L = kI_n - A.$$

It is real symmetric, has the same eigenvectors as A and its eigenvalues are

$$k - \mu_{n-1} \geq \cdots \geq k - \mu_1 \geq k - k = 0.$$

$\ker(L) = \mathcal{Z}$ (constant functions). Thus, if $f \in \mathcal{Z}^\perp$ then

$$\frac{< \delta^* f, \delta^* f >}{< f, f >} = \frac{< \delta\delta^* f, f >}{< f, f >} = \frac{< Lf, f >}{< f, f >} \in [k - \mu_1, k - \mu_{n-1}]$$

Let $F \subseteq V$, with $1 \leq |F| \leq |V|/2$.

Fix an orientation such that $x < y$ for all $x \in F$, $y \in V - F$, and consider $f \in \mathcal{C}(\Gamma)$ defined by

$$f(x) = \begin{cases} |V| - |F| & \text{if } x \in F \\ -|F| & \text{if } x \in V - F \end{cases}$$

Then $f \in \mathcal{Z}^{\perp}$, hence

$$\frac{< Lf, f >}{< f, f >} \geq k - \mu_1$$

We have

$$< f, f > = \sum_{x \in V} f(x)^2 = |F||V|(|V| - |F|),$$

$$< Lf, f > = < \delta^* f, \delta^* f >_{\mathcal{L}} = \sum_{e \in E} (f(e_+) - f(e_-))^2 = \sum_{e \in \partial F} |V|^2 = |\partial F||V|^2$$

Hence

$$k - \mu_1 \leq \frac{|\partial F||V|^2}{2|F||V|(|V| - |F|)} = \frac{|\partial F||V|}{|F|(|V| - |F|)}$$

so

$$\frac{|\partial F|}{|F|} \geq \frac{(|V| - |F|)}{|V|}(k - \mu_1) \geq \frac{k - \mu_1}{2}$$

End of proof.

So $k - \mu_1$ controls $h(\Gamma)$. But, how small can μ_1 be?

Hence

$$k - \mu_1 \le \frac{|\partial F||V|^2}{2|F||V|(|V| - |F|)} = \frac{|\partial F||V|}{|F|(|V| - |F|)}$$

so

$$\frac{|\partial F|}{|F|} \ge \frac{(|V| - |F|)}{|V|}(k - \mu_1) \ge \frac{k - \mu_1}{2}$$

End of proof.

So $k - \mu_1$ controls $h(\Gamma)$. But, how small can μ_1 be?

Theorem (Serre | Alon and Boppana)

Let $k \ge 2$ and $\Gamma_n = (V_n, E_n)$ $(n \in \mathbb{N})$ a sequence of k-regular connected graphs, with $\lim_{n\to\infty} |V_n| = \infty$. Then

$$\liminf_{n\to\infty} \mu_1(\Gamma_n) \ge 2\sqrt{k-1}.$$

A connected k-regular graph (for $k \geq 3$) is called a Ramanujan graph if every eigenvalue $\mu \neq \pm k$ of its adjacency matrix satisfies

$$|\mu| \leq 2\sqrt{k-1}.$$

A connected k-regular graph (for $k \geq 3$) is called a Ramanujan graph if every eigenvalue $\mu \neq \pm k$ of its adjacency matrix satisfies

$$|\mu| \leq 2\sqrt{k-1}.$$

Example: Paley graphs

$\mathbb{F} = GF(q)$, $q = p^m \equiv 1 \pmod 4$, $Q = \{a^2 \mid 0 \neq a \in \mathbb{F}\}$.

The Paley graph P_q is the Cayley graph $\Gamma[\mathbb{F}, Q]$ ($\mathbb{F}$ the additive group).

- P_q is regular with degree $k = \frac{q-1}{2}$,
- $\mu_1(P_Q) = \frac{-1+\sqrt{q}}{2} \leq \sqrt{2(q-3)} = 2\sqrt{k-1}$

hence P_q is a Ramanujan graph

Theorem (J. Friedman)

Fir fixed $k \geq 3$ and $\epsilon > 0$ the probability that, for a k-regular graph Γ on n vertices,

$$\mu_1(\Gamma) \leq 2\sqrt{k-1} + \epsilon$$

tends to 1 as $n \to \infty$.

Theorem (J. Friedman)

Fir fixed $k \geq 3$ and $\epsilon > 0$ the probability that, for a k-regular graph Γ on n vertices,

$$\mu_1(\Gamma) \leq 2\sqrt{k-1} + \epsilon$$

tends to 1 as $n \to \infty$.

An infinite family of finite graphs $\Gamma_n = (V_n, E_n)$, $1 \leq n \in \mathbb{N}$, is called a family of Ramanujan expanders if

- there exists $k \geq 3$ such that Γ_n is k-regular for every $n \geq 1$;
- $\lim_{n\to\infty} |V_n| = \infty$;
- $\mu_1(\Gamma_n) \leq 2\sqrt{k-1}$ for every $n \geq 1$.

Theorem (J. Friedman)

Fir fixed $k \geq 3$ and $\epsilon > 0$ the probability that, for a k-regular graph Γ on n vertices,

$$\mu_1(\Gamma) \leq 2\sqrt{k-1} + \epsilon$$

tends to 1 as $n \to \infty$.

An infinite family of finite graphs $\Gamma_n = (V_n, E_n)$, $1 \leq n \in \mathbb{N}$, is called a family of Ramanujan expanders if

- there exists $k \geq 3$ such that Γ_n is k-regular for every $n \geq 1$;
- $\lim_{n\to\infty} |V_n| = \infty$;
- $\mu_1(\Gamma_n) \leq 2\sqrt{k-1}$ for every $n \geq 1$.

Theorem (Margulis/Lubotzky, Phillips and Sarnak/Morgenstern)

For every prime p and $m \geq 1$, there exist infinite $(p^m + 1)$-regular Ramanujan graphs.

Representations.

Representations.

Let G be a finite group, $S = S^{-1}$ a set of generators of G with $1 \notin S$, and $\Gamma = \Gamma[G, S]$ the associated Cayley graph.

• Write $A = A(\Gamma)$ and $\mathcal{C} = \mathcal{C}(\Gamma) = \{f \mid f : V \to \mathbb{C}\}$.

• Then, multiplication defines the *regular representation* $r : G \to GL(\mathcal{C})$, in the usual way:

$$(r(g)f)(x) = f(xg^{-1})$$

for all $g, x \in G$, $f \in \mathcal{C}$.

• Let A_r be the matrix associated to $\sum_{s \in S} r(s)$. Then, for every $f \in \mathcal{C}$ and $x \in G$

$$Af(x) = \sum_{y \sim x} f(y) = \sum_{s \in S} f(xs) = \sum_{s \in S} (r(s^{-1})f)(x) = A_r f(x)$$

Representations.

Let G be a finite group, $S = S^{-1}$ a set of generators of G with $1 \notin S$, and $\Gamma = \Gamma[G, S]$ the associated Cayley graph.

• Write $A = A(\Gamma)$ and $\mathcal{C} = \mathcal{C}(\Gamma) = \{f \mid f : V \to \mathbb{C}\}$.

• Then, multiplication defines the *regular representation* $r : G \to GL(\mathcal{C})$, in the usual way:

$$(r(g)f)(x) = f(xg^{-1})$$

for all $g, x \in G$, $f \in \mathcal{C}$.

• Let A_r be the matrix associated to $\sum_{s \in S} r(s)$. Then, for every $f \in \mathcal{C}$ and $x \in G$

$$Af(x) = \sum_{y \sim x} f(y) = \sum_{s \in S} f(xs) = \sum_{s \in S} (r(s^{-1})f)(x) = A_r f(x)$$

• *The operator A_r coincides with that defined by the adjacency matrix A of Γ.*

The regular representation r is the orthogonal sum of all the *irreducible* complex representations of G (each with multiplicity equal to its dimension). For such an irreducible representation ρ, write

$$A_\rho = \sum_{s \in S} \rho(s).$$

Then $A = A_r$ is the orthogonal sum of all the A_ρ (with right multiplicities). In particular

The regular representation r is the orthogonal sum of all the *irreducible* complex representations of G (each with multiplicity equal to its dimension). For such an irreducible representation ρ, write

$$A_\rho = \sum_{s \in S} \rho(s).$$

Then $A = A_r$ is the orthogonal sum of all the A_ρ (with right multiplicities). In particular

• *The set of eigenvalues of A is the union of the set of eigenvalues of A_ρ, while ρ runs on the set of irreducible complex representations of G.*

The regular representation r is the orthogonal sum of all the *irreducible* complex representations of G (each with multiplicity equal to its dimension). For such an irreducible representation ρ, write

$$A_\rho = \sum_{s \in S} \rho(s).$$

Then $A = A_r$ is the orthogonal sum of all the A_ρ (with right multiplicities). In particular

- *The set of eigenvalues of A is the union of the set of eigenvalues of A_ρ, while ρ runs on the set of irreducible complex representations of G.*

Observing that the eigenvalue $\mu_0 = k$ corresponds to the trivial representation 1_G, we have

The regular representation r is the orthogonal sum of all the *irreducible* complex representations of G (each with multiplicity equal to its dimension). For such an irreducible representation ρ, write

$$A_\rho = \sum_{s \in S} \rho(s).$$

Then $A = A_r$ is the orthogonal sum of all the A_ρ (with right multiplicities). In particular

• *The set of eigenvalues of A is the union of the set of eigenvalues of A_ρ, while ρ runs on the set of irreducible complex representations of G.*

Observing that the eigenvalue $\mu_0 = k$ corresponds to the trivial representation 1_G, we have

• *The fisrt non-trivial eigenvalue μ_1 of A is the maximum of the eigenvalues of A_ρ, while ρ runs on the set of irreducible non-trivial complex representations of G.*

- A a finite abelian group, $S = \{s_1, \ldots, s_k\} = S^{-1}$ a set of generators of A.

- The irreducible $\mathbb{C}$-representations of A are the elements of the *dual*

$$\hat{A} = \{\rho \mid \rho : A \to S^1 \ \mathit{homom.}\}$$

where $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$.

- If $\rho \in \hat{A}$, then A_ρ is the multiplication in $\mathbb{C}$ by $\sum_{s \in S} \rho(s)$. Hence

$$\mu = \max \Big\{ \sum_{s \in S} \rho(s) \mid 1 \neq \rho \in \hat{A} \Big\}.$$

- Let $r = \left[\frac{2k}{k-1} \right] + 1$, consider the partition of the circle S^1 in r-sections of width $2\pi/r$, determined by the r-th roots of unity, and write $\zeta = e^{2\pi i/r}$. This partition induces a partition of the set of k-uples $(S^1)^k$ (in r^k blocks).

- Suppose there exist $\alpha, \beta \in \hat{A}$, $\alpha \neq \beta$, such that the k-uples $(\alpha(s_1), \ldots, \alpha(s_k))$ and $(\beta(s_1), \ldots, \beta(s_k))$ belong to the same block of the partition on $(S^1)^k$.

- Then, for each $i = 1, \ldots, k$, $\alpha^{-1}\beta(s_i)$ belongs to the arc (ζ^{-1}, ζ) of S^1. Hence

$$\sum_{i=1}^{k} \alpha^{-1}\beta(s_i) \geq k \cdot \cos \frac{\pi i}{r}.$$

- Since $1 \neq \alpha^{-1}\beta$, deduce $\mu \geq k \cdot \cos \frac{\pi i}{r} \geq k\left(1 - \frac{2}{r}\right)$, and the contradiction

$$r \leq 2k/(k-\mu)$$

- So, for all $\alpha, \beta \in \hat{A}$, if $\alpha \neq \beta$ then $(\alpha(s_1), \ldots, \alpha(s_k))$ and $(\beta(s_1), \ldots, \beta(s_k))$ belong to different blocks of the partition on $(S^1)^k$. Therefore

$$|A| = |\hat{A}| \leq r^k.$$

Lemma

Let Γ be a Cayley graph of degree $k \geq 2$ for the finite abelian group A. Then for every eigenvalue $\mu \neq k$ of $A(\Gamma)$

$$|A| \leq \left(\frac{2k}{k-\mu} + 1\right)^k.$$

Theorem (Lubotzky and Weiss)

Let $k \geq 3$. If the inifinite family of Cayley graphs $(\Gamma[G_n, S_n])_{n\in\mathbb{N}}$, with $|S_n| \leq k$, is a family of expanders, then there exists a constant $c > 0$ such that, for every $n \in \mathbb{N}$ and every subgroup M of G_n

$$|M/M'| \leq c^{|G_n:M|}.$$

An almost immediate consequence is

Theorem (L. W.)

Let $1 \leq d \in \mathbb{N}$. There do not exist infinite families of expanders $\Gamma[G_n, S_n]$ where all groups G_n are soluble of derived length at most d.

A group H is *residually finite* if the intersection of all normal subgroups of H of finite index is trivial, or, equivalently, if the intersection of the kernels of the finite homomorphic images of H is trivial
(e.g. the groups $GL(n, \mathbb{Z})$ are residually finite).

Let H be a finitely generated, residually finite group, and for every $n \in \mathbb{N}$ let $\pi_n : H \to G_n$ be a surjective homomorphism onto a finite group G_n, with $|G_{i+1}| > |G_i|$. Fix a finite set of generators $S = S^{-1}$ of H; then $\pi_n(S)$ is a set of generators of G_n and is closed by inversion. By setting $S_n = \pi_n(S) - \{1\}$, one obtains a family of Cayley graphs $\Gamma[G_n, S_n]$ whose degree does not exceed $|S|$.

Many of the first construction of families of expanders were obtained by showing that certain properties of the 'mother' group H (although usually difficult to establish) ensure that the family $\Gamma[G_n, S_n]$ is a family of expanders.

We give a definition which work for discrete groups.

Let H be a finitely generated group and $S = S^{-1}$ a finite set of generators. H satisfies the Kazhdan (T)-property if there exists a constant $\kappa = \kappa(H, S) > 0$ such that for every *unitary* representation (V, ρ) of H and every $v \in V$

$$\max_{s \in S} ||\rho(s)v - v|| \geq \kappa ||v||$$

Property (T) does not depend on S (although the constant κ does).

If G is finite, Kazhdan property is trivial. For G finite and $S = S^{-1}$ a set of generators, let $\kappa(G, S)$ the K. constant, and A the adjacency matrix of $\Gamma[G, S]$

The regular representation r of G on $\mathcal{C}(\Gamma)$ is unitary: for all $g \in G$ and $u \in \mathcal{C}(\Gamma)$,

$$< r(g)u, r(g)u >= \sum_{x \in G} |u(xg)|^2 = \sum_{x \in G} |u(x)|^2 =< u, u > .$$

The restriction to the subspace $\mathcal{Z}^{\perp} = \{u \in \mathcal{C}(\Gamma) \mid \sum_{x \in G} u(x) = 0\}$ (which is r-invariant) is also unitary.
Now, by applying the operator $A_r = A$, a simple computation yields

$$\frac{||r(s)u - u||^2}{||u||^2} = 2 = 2\frac{< r(s)u, u >}{||u||^2}$$

for every $s \in S$ and $u \in \mathcal{C}(\Gamma)$. If $|S| = k$ we have (remember $A_r = \sum_{s \in S} r(s)$),

$$\frac{< Au, u >}{||u||} = \frac{< A_r u, u >}{||u||} = k - \frac{1}{2} \sum_{s \in S} \frac{||r(s)u - u||^2}{||u||^2}.$$

If $\mu = \mu_1$ is the first eigenvalue $\neq k$ of A, we know that

$$\mu = \max_{u \in \mathcal{Z}^\perp} \frac{< Au, u >}{||u||^2}$$

Then

$$k - \mu = \frac{1}{2} \inf_{0 \neq u \in \mathcal{Z}^\perp} \sum_{s \in S} \frac{||r(s)u - u||^2}{||u||^2} \geq \frac{1}{2} \Big(\inf_{0 \neq u \in \mathcal{Z}^\perp} \max_{s \in S} \frac{||r(s)u - u||^2}{||u||^2} \Big)$$

and finally, substituting the Kazhdan constant,

$$k - \mu \geq \frac{1}{2} \kappa(G, S)^2.$$

Theorem

Let H be a finitely generated group, $\mathcal{N}$ a family of normal subrgoups of finite index of H, and, for every $N \in \mathcal{N}$, let π_N be the projection $H \to H/N$. If H satisfies property (T), then for every finite set of generators $S = S^{-1}$ of H, the family of Cayley graphs $\Gamma[H/N, \pi_N(S)]$ is a family of expanders.

Example. It may be proved that for every $n \geq 3$, the group $SL(n, \mathbb{Z})$ satisfies property (T). Hence, if for every $m \geq 2$, π_m is the reduction modulo m on $\mathbb{Z}$, then

for every finite set of generators S of $SL(n, \mathbb{Z})$ $(n \geq 3)$ with $S = S^{-1}$ and $1 \notin S$ (e.g. the set of all elementary matrices $I_n \pm E_{ij}$), the family of Cayley graphs

$$\Gamma[SL(n, \mathbb{Z}/m\mathbb{Z}), \pi_m(S)]$$

is a family of expanders.

Example 2. (Lubotzky) Let $d \geq 3$, p a prime. For every $n \geq 2$ consider the *congruence subgroup*

$$N_m = \Gamma(p^m) = \ker(SL(d, \mathbb{Z}) \to SL(d, \mathbb{Z}/p^m\mathbb{Z})).$$

N_1 has finite index in $SL(d, \mathbb{Z})$, hence it is finitely generated, and it may be proved (this is not difficult) that it inherits property (T) from $SL(d, \mathbb{Z})$.
Now, for every $m \geq 1$, $P_m = N_1/N_m$ is a finite p-group (its order is $p^{(m-1)(d^2-1)}$), hence P_m is soluble for every m.
Fix a finite set S of generators of N_1 (with usual properties). Then the family of Cayley graphs

$$\Gamma[P_m, SN_m/N_m]$$

is a family of expanders.

Notice. $SL(2,\mathbb{Z})$ does not satisfy porperty (T). However, for certain set of generators, similar conclusions may be proved by using the weaker property (τ) introduced by Lubotzky (that we are not going to define, but refers to the representation of a suitable class of finite images of a given residually finite group).

Verification of property (τ) may involve non-trivial number theoretical results. For instance, the proof that this is the case for $SL(2,\mathbb{Z})$ and the class of *congruence subgroups*, relies on a deep result of Selberg. Using, that, Lubotzky proved

Theorem (Lubotzky)

For every prime $p \geq 3$, let $S_p = \{\sigma_1, \sigma_1^{-1}, \tau_1, \tau_1^{-1}\}$, where

$$\tau_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \sigma_1 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Then the family of Cayley graphs $\Gamma[SL(2,p), S_p]$ is a family of expanders.

The same argument shows that, by taking $S'_p = \{\sigma_2, \sigma_2^{-1}, \tau_2, \tau_2^{-1}\}$, with

$$\tau_2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \qquad \sigma_2 = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}.$$

then the family of graphs $\Gamma[SL(2,p), S'_p]$ is a family of expanders.

The same argument shows that, by taking $S'_p = \{\sigma_2, \sigma_2^{-1}, \tau_2, \tau_2^{-1}\}$, with

$$\tau_2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \qquad \sigma_2 = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}.$$

then the family of graphs $\Gamma[SL(2,p), S'_p]$ is a family of expanders. However,

Lubotzky method does not say anything about, for instance, the family of Cayley graphs $\Gamma[SL(2,p), \{\sigma_3, \sigma_3^{-1}, \tau_3, \tau_3^{-1}\}]$ $(p > 3)$, with

$$\tau_3 = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} \qquad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix}.$$

The reason is that, in $SL(2,\mathbb{Z})$, both subgroups $\langle \tau_1, \sigma_1 \rangle$ and $\langle \tau_2, \sigma_2 \rangle$ have finite index, while the subgroup $\langle \tau_3, \sigma_3 \rangle$ has infinite index (this question was set by Lubotky himself; in the next lecture we will see how, by completely different methods, it has now an answer).

Recall: a k-regular, connected graph is called a Ramanujan graph if

$$\mu_1 \leq 2\sqrt{k-1}$$

where μ_1 is the largest eigenvalue $\neq k$ of the adjacency matrix.

Theorem (Lubotzky, Phillips and Sarnak)

For every prime p, there exist infinite $(p+1)$-regular Ramanujan graphs.

We survey the construction for $p \equiv 1 \pmod 4$.

We start by a Theorem of Jacobi, saying that there are $8(p+1)$ quadruples $(a_0, a_1, a_2, a_3) \in \mathbb{Z}^4$ such that

$$a_0^2 + a_1^2 + a_2^2 + a_3^2 = p.$$

and among them, there are exactly $p+1$ with $a_0 > 0$ and a_1, a_2, a_3 even.

In the integral quaternion algebra

$$\mathbb{H}(\mathbb{Z}) = \{a_0 + a_1 i + a_2 j + a_3 k \mid a_0, a_1, a_2, a_3 \in \mathbb{Z}\}$$

let S_p be the set of all elements $u = a_0 + a_1 i + a_2 j + a_3 k$ such that

$$N(u) = a_0^2 + a_1^2 + a_2^2 + a_3^2 = p, \quad a_0 > 0 \text{ and } a_1, a_2, a_3 \text{ are even.}$$

Then, by the above remark $|S_p| = p + 1$.
Let Λ be the multiplicative monoid generated by $S_p \cup \{p, -p\}$ in $\mathbb{H}(\mathbb{Z})$; then if $u \in \Lambda$, then $N(u)$ is a power of p (since norm is multiplicative).
Let $\sim$ be the relation on Λ defined by $u \sim v$ if there exist $a, b \in \mathbb{N}$ such that $\pm p^a u = p^b v$. One shows that $\sim$ is a congruence on Λ; moreover the factor monoid $H = \Lambda/\sim$ is a group, and the projection $\rho : \Lambda \to H$ is injective on S_p (i.e. $|\rho(S_p)| = p + 1$). Then, consider the Cayley graph

$$Y = \Gamma[H, \rho(S_p)].$$

Fundamental fact: Y is an infinite $(p+1)$–regular tree (the Bruhat-Tis tree for $GL(2, p)$).

Let q be an odd prime, $\tau_q : \mathbb{H}(\mathbb{Z}) \to \mathbb{H}(\mathbb{Z}/q\mathbb{Z})$ the reduction modulo q. Then $\tau_q(\Lambda)$ is contained in the group $\mathbb{H}(\mathbb{Z}/q\mathbb{Z})^*$ of non-zero elements of $\mathbb{H}(\mathbb{Z}/q\mathbb{Z})$; also τ_q defines homomorphism

$$\Phi_q : H \to \mathbb{H}(\mathbb{Z}/q\mathbb{Z})/Z,$$

where $Z = (\mathbb{Z}/q\mathbb{Z})^*$ is the center of $\mathbb{H}(\mathbb{Z}/q\mathbb{Z})$, and, for q large enough, $|\Phi_q(\rho(S_p)| = p+1$. The Cayley graph

$$X_{p,q} = \Gamma[\Phi_q(H), \Phi_q(\rho(S_p))]$$

is a quotient graph of the tree Y, and it is a Ramanujian graph (this requires deep number theory)

Now, if $q \equiv 1 \pmod 4$, the quaternion algebra $\mathbb{H}(\mathbb{Z}/q\mathbb{Z})$ is isomorphic to the matrix algebra $M_2(\mathbb{Z}/q\mathbb{Z})$, via isomorphism ϕ given by

$$a_0 + a_1 i + a_2 j + a_3 k \mapsto \begin{pmatrix} a_0 + \ell a_1 & a_2 + \ell a_3 \\ -a_2 + \ell a_3 & a_0 - \ell a_1 \end{pmatrix} \tag{1}$$

where $\ell^2 = -1$ in $\mathbb{Z}/q\mathbb{Z}$. Thus $X_{p,q}$ is isomorphic to the Cayley graph

$$\Gamma[PSL(2, q), T_p)]$$

where T_p is the set of matrix in (1) (modulo scalars)

Property (T) is a very strong one: as an effect, the Cayley graph of the finite images of an (infinite) group satisfying property (T) form a family of expanders with respect to any 'homogeneous' choice of generators.

This is not the case for all simple groups; for example, alternating (or symmetric) groups. The groups $Alt(n)$ are not together realizable as quotients of a finitely generated group satisfying (T).
If, for every $n \geq 3$, we set $\tau_n = (1\ n)$, $\sigma_n = (1\ 2 \ldots n)$, and $S_n = \{\tau_n, \sigma_n, \sigma_n^{-1}\}$, then S_n is a set of generators for $Sym(n)$, but the isoperimetrical constant of the Cayley graphs $\Gamma[Sym(n), S_n]$ tends to zero, as $n \to \infty$. Nevertheless,

Theorem (Kassabov)

There exists $k \in \mathbb{N}$ and $\epsilon > 0$ such that, for every $n \geq 2$, there is a symmetric generating set S_n of size at most k of $Alt(n)$ such that the Cayley graph $\Gamma[Alt(n), S_n]$ is an ϵ-expander.

At the same time, Kassabov and Nikolov proved a Theorem

For $d \geq 3$ and $m \geq 1$, the group $SL(d, \mathbb{Z}[x_1, \ldots, x_m])$ satisfies property (τ).

that allowed to show, for example, that set of k generators for the groups $SL(d, q)$ ($d \geq 3$) exist, such that the corresponding Cayley graphs are ϵ-expanders, with k, $\epsilon > 0$ independent of d and q.

The same authors, together with Lubotzky, then proved that all finite simple groups, except Suzuki groups, form a family of expanders.

The final gap (Suzuki groups) was filled by Breuillard, Green and Tao, who applied new ideas that were being developed in connection to growth properties in finite (or algebraic) Lie groups.

At the same time, Kassabov and Nikolov proved a Theorem

For $d \geq 3$ and $m \geq 1$, the group $SL(d, \mathbb{Z}[x_1, \ldots, x_m])$ satisfies property (τ).

that allowed to show, for example, that set of k generators for the groups $SL(d, q)$ ($d \geq 3$) exist, such that the corresponding Cayley graphs are ϵ-expanders, with k, $\epsilon > 0$ independent of d and q.

The same authors, together with Lubotzky, then proved that all finite simple groups, except Suzuki groups, form a family of expanders.

The final gap (Suzuki groups) was filled by Breuillard, Green and Tao, who applied new ideas that were being developed in connection to growth properties in finite (or algebraic) Lie groups.

coming next: growths