Approximate groups and their applications: part 3

E. Breuillard

Université Paris-Sud, Orsay

St. Andrews, August 3-10, 2013

Expander graphs

Let $\mathcal{G}$ be a k-regular connected finite graph with N vertices. The Laplacian on $\mathcal{G}$ is a non-negative symmetric operator on the space of functions on the set of vertices of $\mathcal{G}$ defined by

$$\Delta f(x) := f(x) - \frac{1}{k} \sum_{y \sim x} f(y)$$

Here $y \sim x$ means that y is a neighbor of the vertex x (i.e. they are connected by an edge).

Expander graphs

Let $\mathcal{G}$ be a k-regular connected finite graph with N vertices. The Laplacian on $\mathcal{G}$ is a non-negative symmetric operator on the space of functions on the set of vertices of $\mathcal{G}$ defined by

$$\Delta f(x) := f(x) - \frac{1}{k} \sum_{y \sim x} f(y)$$

Here $y \sim x$ means that y is a neighbor of the vertex x (i.e. they are connected by an edge).

Definition (Spectrum)

The spectrum of $\mathcal{G}$ is the set of eigenvalues of Δ. We order them as

$$0 = \lambda_0 < \lambda_1 \leqslant \lambda_2 \leqslant \ldots \leqslant \lambda_N \leqslant 2$$

Expander graphs

Definition

The graph $\mathcal{G}$ is said to be a ε-expander if

$$\lambda_1(\mathcal{G}) > \varepsilon$$

Expander graphs

Definition

The graph $\mathcal{G}$ is said to be a ε-expander if

$$\lambda_1(\mathcal{G}) > \varepsilon$$

There is also an equivalent definition in terms of isoperimetry. Let $h(\mathcal{G})$ be the largest constant $h > 0$ such that for every subset A of vertices of $\mathcal{G}$ of size $< \frac{N}{2}$,

$$|\partial A| > h|A|$$

where ∂A is the boundary of A ($=$ edges connecting a point in A to a point outside A).

Expander graphs

Definition

The graph $\mathcal{G}$ is said to be a ε-expander if

$$\lambda_1(\mathcal{G}) > \varepsilon$$

There is also an equivalent definition in terms of isoperimetry. Let $h(\mathcal{G})$ be the largest constant $h > 0$ such that for every subset A of vertices of $\mathcal{G}$ of size $< \frac{N}{2}$,

$$|\partial A| > h|A|$$

where ∂A is the boundary of A ($=$ edges connecting a point in A to a point outside A).

Lemma (Cheeger-Buser)

One has

$$\frac{1}{2}\lambda_1 \leqslant \frac{1}{k}h(\mathcal{G}) \leqslant \sqrt{2\lambda_1}$$

Expander Cayley graphs

A sequence of k-regular graphs with $N_i := |\mathcal{G}_i|$ going to ∞ is called a *family of expanders* if there is a uniform $\varepsilon > 0$ such that $\lambda_1(\mathcal{G}_i) > \varepsilon$ for all i.

Expander Cayley graphs

A sequence of k-regular graphs with $N_i := |\mathcal{G}_i|$ going to ∞ is called a *family of expanders* if there is a uniform $\varepsilon > 0$ such that $\lambda_1(\mathcal{G}_i) > \varepsilon$ for all i.

Margulis (1972) gave the first construction of a family expanders: using representation theory and Kazhdan's property (T), he showed that the family of Cayley graphs of $\mathrm{SL}_3(\mathbb{Z}/n\mathbb{Z})$ with respect to a fixed generating set of $\mathrm{SL}_3(\mathbb{Z})$ is a family of expanders.

Expander Cayley graphs

A sequence of k-regular graphs with $N_i := |\mathcal{G}_i|$ going to ∞ is called a *family of expanders* if there is a uniform $\varepsilon > 0$ such that $\lambda_1(\mathcal{G}_i) > \varepsilon$ for all i.

Margulis (1972) gave the first construction of a family expanders: using representation theory and Kazhdan's property (T), he showed that the family of Cayley graphs of $\mathrm{SL}_3(\mathbb{Z}/n\mathbb{Z})$ with respect to a fixed generating set of $\mathrm{SL}_3(\mathbb{Z})$ is a family of expanders.

Lubotzky and others (in particular Lubotzky-Phillips-Sarnak) have refined and pushed Margulis method to other groups (e.g. arithmetic subgroups of SL_2). They also asked the following question:

Question: Which finite groups can be turned into expanders ? Namely given an infinite family of finite groups, can one find a generating set of bounded size with respect to which the associated Cayley graphs form a family of expanders ?

Results of Kassabov–Lubotzky-Nikolov

Solvable groups are not expanders:

Theorem (Lubotzky-Weiss)

Given $k, \ell > 0$, if G_i is any family of k-generated finite solvable groups with derived length $\leqslant \ell$, then $\lambda_1(G_i)$ tends to 0 as $|G_i|$ tends to $+\infty$.

Results of Kassabov–Lubotzky-Nikolov

Solvable groups are not expanders:

Theorem (Lubotzky-Weiss)

Given $k, \ell > 0$, if G_i is any family of k-generated finite solvable groups with derived length $\leqslant \ell$, then $\lambda_1(G_i)$ tends to 0 as $|G_i|$ tends to $+\infty$.

But it is expected that simple groups are:

Theorem (Kassabov-Lubotzky-Nikolov)

There is $k > 0$ and $\varepsilon > 0$ such that every* finite simple group has a generating set of size k w.r.t which the associated Cayley graph is an ε-expander.

every* : with the exception of the family of Suzuki groups; now this family can be included in the theorem (work of B-Green-Tao).

Random walk characterisation of expanders

Yet another way to understand the expander property is in terms of fast equidistribution of random walks.

Random walk characterisation of expanders

Yet another way to understand the expander property is in terms of fast equidistribution of random walks.

Suppose $\mathcal{G}$ is a Cayley graph of a finite group G with (symmetric) generating set S of size k. Let

$$\mu := \frac{1}{k} \sum_{s \in S} \delta_s$$

be the uniform probability measure on S (δ_s is the Dirac mass at s).

Yet another way to understand the expander property is in terms of fast equidistribution of random walks.
Suppose $\mathcal{G}$ is a Cayley graph of a finite group G with (symmetric) generating set S of size k. Let

$$\mu := \frac{1}{k} \sum_{s \in S} \delta_s$$

be the uniform probability measure on S (δ_s is the Dirac mass at s).
The convolution of two measures μ, ν on a group G is the image of the product measure $\mu \otimes \nu$ under the product map $G \times G \to G$, $(x, y) \mapsto xy$.

$$\mu * \nu(x) := \sum_{y \in G} \mu(xy)\nu(y^{-1})$$

Then the n-th convolution power

$$\mu^{*n} := \mu * \ldots * \mu$$

represents the probability distribution of the nearest neighbor random walk on the Cayley graph $\mathcal{G}$.
Note that as $n \to +\infty$, the random walk becomes equidistributed in G, i.e. $\mu^{*n}(x) \to \frac{1}{|G|}$ for every $x \in G$.
We fix the size k of the generating set.

Then the n-th convolution power

$$\mu^{*n} := \mu * \ldots * \mu$$

represents the probability distribution of the nearest neighbor random walk on the Cayley graph $\mathcal{G}$.
Note that as $n \to +\infty$, the random walk becomes equidistributed in G, i.e. $\mu^{*n}(x) \to \frac{1}{|G|}$ for every $x \in G$.
We fix the size k of the generating set.

Lemma (Rapid mixing definition of expanders)

The Cayley graph $\mathcal{G}$ is an ε-expander if and only if the random walk becomes well equidistribution already in less than $C_\varepsilon \log |G|$ steps, namely:

$$\sup_{x \in G} |\mu^{*n}(x) - \frac{1}{|G|}| \leqslant \frac{1}{|G|^{10}}$$

for all $n \geqslant C_\varepsilon \log |G|$. ($C_\varepsilon \simeq \varepsilon^{-1}$).

The Bourgain-Gamburd method

In 2005, Bourgain and Gamburd came up with a new (more analytic) method for proving that certain Cayley graphs are expanders.

The Bourgain-Gamburd method

In 2005, Bourgain and Gamburd came up with a new (more analytic) method for proving that certain Cayley graphs are expanders.
Their idea is based on the above random walk characterisation of the expander property: we will prove fast equidistribution directly, then deduce the expander property (i.e. the lower bound on λ_1).

The Bourgain-Gamburd method

In 2005, Bourgain and Gamburd came up with a new (more analytic) method for proving that certain Cayley graphs are expanders.

Their idea is based on the above random walk characterisation of the expander property: we will prove fast equidistribution directly, then deduce the expander property (i.e. the lower bound on λ_1).

One (of several) key ingredients in their method are the approximate subgroups, or rather the absence of non-trivial approximate subgroups of G (which as we saw last time is a feature of bounded rank finite simple groups).

The Bourgain-Gamburd method

In 2005, Bourgain and Gamburd came up with a new (more analytic) method for proving that certain Cayley graphs are expanders.
Their idea is based on the above random walk characterisation of the expander property: we will prove fast equidistribution directly, then deduce the expander property (i.e. the lower bound on λ_1).
One (of several) key ingredients in their method are the approximate subgroups, or rather the absence of non-trivial approximate subgroups of G (which as we saw last time is a feature of bounded rank finite simple groups).

Theorem (Bourgain-Gamburd 2005)

Let $\mathcal{G}$ be a k-regular Cayley graph of $G := \mathrm{SL}_2(\mathbb{F}_p)$ (p prime). Assume that the girth of $\mathcal{G}$ is at least $\tau \log p$. Then $\exists \varepsilon(\tau) > 0$ s.t.

$$\lambda_1(\mathcal{G}) > \varepsilon.$$

Other expander results based on the Bourgain-Gamburd method

Their theorem has since been generalized in some (but not yet all) directions. Here are some recent results proved using the Bourgain-Gamburd method:

Theorem (B.-Green-Guralnick-Tao: Random pairs in $\mathbf{G}(q)$)

There is $\varepsilon = \varepsilon(r) > 0$ such that every finite simple group G of rank $\leqslant r$ has a pair of generators whose associated Cayley graph is an ε-expander.
In fact almost every pair works, i.e. the number of possible exceptions is at most $|G|^{2-\eta}$ for some $\eta = \eta(r) > 0$.

Remark: This includes the family of Suzuki groups $Suz(2^{2n+1})$, thus completing the missing bit in the theorem of Kassabov, Lubotzky and Nikolov.

Other expander results based on the Bourgain-Gamburd method

Theorem (B.-Gamburd: Uniformity in $SL_2(\mathbb{F}_p)$)

There is a set of primes $\mathcal{P}_0$ of density one among all primes such that every k-generated Cayley graph of $SL_2(\mathbb{F}_p)$, $p \in \mathcal{P}_0$, is an ε_k-expander for some $\varepsilon_k > 0$.

In fact one can conjecture the following strong uniformity:

Conjecture (Uniformity conjecture)

There is $\varepsilon = \varepsilon(k, r) > 0$ such that every k-generated Cayley graph of a finite simple group of rank at most r is an ε-expander.

Other expander results based on the Bourgain-Gamburd method

Theorem (B.-Gamburd: Uniformity in $SL_2(\mathbb{F}_p)$)

There is a set of primes $\mathcal{P}_0$ of density one among all primes such that every k-generated Cayley graph of $SL_2(\mathbb{F}_p)$, $p \in \mathcal{P}_0$, is an ε_k-expander for some $\varepsilon_k > 0$.

In fact one can conjecture the following strong uniformity:

Conjecture (Uniformity conjecture)

There is $\varepsilon = \varepsilon(k, r) > 0$ such that every k-generated Cayley graph of a finite simple group of rank at most r is an ε-expander.

Remark. Both the BGGT and the BG results above can be seen as evidence towards this conjecture. This would also imply the uniform logarithmic diameter conjecture mentioned last time.

Other expander results based on the Bourgain-Gamburd method

Theorem (super-strong-approximation)

Let $\mathbf{G}$ *be a semisimple algebraic group over* $\mathbb{Q}$*. Suppose* $\Gamma = \langle S \rangle$ *is a finitely generated Zariski-dense subgroup of* $\mathbf{G}(\mathbb{Q})$*. Then the reduction mod p map* $\mathbf{G}(\mathbb{Z}) \to \mathbf{G}(\mathbb{Z}/p\mathbb{Z})$ *is surjective in restriction to* Γ *if the prime p is large enough and the associated Cayley graphs form a family of expanders.*

Other expander results based on the Bourgain-Gamburd method

Theorem (super-strong-approximation)

Let $\mathbf{G}$ be a semisimple algebraic group over $\mathbb{Q}$. Suppose $\Gamma = \langle S \rangle$ is a finitely generated Zariski-dense subgroup of $\mathbf{G}(\mathbb{Q})$. Then the reduction mod p map $\mathbf{G}(\mathbb{Z}) \to \mathbf{G}(\mathbb{Z}/p\mathbb{Z})$ is surjective in restriction to Γ if the prime p is large enough and the associated Cayley graphs form a family of expanders.

One can also consider reduction modulo a square-free or even arbitrary integer n (instead of the prime p). One has:

Theorem (Bourgain-Varju)

Suppose $S \leqslant \mathrm{SL}_d(\mathbb{Z})$ is a finite symmetric set generating a Zariski-dense subgroup, then the Cayley graphs $\mathcal{G}_n$ of $\mathrm{SL}_d(\mathbb{Z}/n\mathbb{Z})$ with respect to S form a family of expanders as $n \in \mathbb{N}$ grows.

The Bourgain-Gamburd method

The lower bound on λ_1 in the Bourgain-Gamburd method is achieved by proving the fast equidistribution of the random walk. This is done in three stages:

1. Initial stage $(n \leqslant c_1 \log |G|)$. One needs to prove exponential non-concentration of μ^{*n} on proper subgroups H, i.e.:

$$\sup_{H \lneq G} \mu^{*n}(H) \leqslant \frac{1}{|G|^{\delta}}$$

2. Middle stage $(c_1 \log |G| \leqslant n \leqslant c_2 \log |G|)$. One needs to prove sub-exponential decay of μ^{*n}, i.e. the following ℓ^2-flattening

$$\mu^{*2n}(1) \leqslant (\mu^{*n}(1))^{1+\varepsilon}$$

(this step uses the classification of approximate groups)

3. Final stage $(n \geqslant c_2 \log |G|)$. From $\mu^{*n}(1) \leqslant \frac{1}{|G|^{1-\delta}}$, one uses "quasirandomness" (i.e. good lower bounds on the dimension of irreducible reps. of G) to get the spectral gap.

Let Γ be a finitely generated group. Say that $g \in \Gamma$ is a *proper power* if $\exists m \geqslant 2$ and $h \in \Gamma$ such that

$$g = h^m.$$

Let Γ be a finitely generated group. Say that $g \in \Gamma$ is a *proper power* if $\exists m \geqslant 2$ and $h \in \Gamma$ such that

$$g = h^m.$$

Let Γ^m denote the set of m-powers, and $\Gamma^{\geqslant 2} := \cup_{m \geqslant 2} \Gamma^m$ the set of proper powers.

Let Γ be a finitely generated group. Say that $g \in \Gamma$ is a *proper power* if $\exists m \geqslant 2$ and $h \in \Gamma$ such that

$$g = h^m.$$

Let Γ^m denote the set of m-powers, and $\Gamma^{\geqslant 2} := \cup_{m \geqslant 2} \Gamma^m$ the set of proper powers.

How large can the set of proper powers $\Gamma^{\geqslant 2}$ be ?

Let Γ be a finitely generated group. Say that $g \in \Gamma$ is a *proper power* if $\exists m \geqslant 2$ and $h \in \Gamma$ such that

$$g = h^m.$$

Let Γ^m denote the set of m-powers, and $\Gamma^{\geqslant 2} := \cup_{m \geqslant 2} \Gamma^m$ the set of proper powers.

How large can the set of proper powers $\Gamma^{\geqslant 2}$ be ?

It depends on the group. For example:

- if Γ is finite, then $\Gamma^{\geqslant 2} = \Gamma$,
- if Γ is a f.g. infinite torsion p-group (e.g. a Golod-Shafarevich group), then $\Gamma = \Gamma^m$ if $\gcd(p, m) = 1$,
- Malcev showed that if Γ is nilpotent, then for every $m \geqslant 1$, Γ^m contains a finite index subgroup of Γ.

In 1996, Hrushovski-Kropholler-Lubotzky-Shalev proved that if Γ is linear and non virtually solvable, then for all finite $n \geqslant 2$, Γ is not a finite union of translates of $\cup_{2 \leqslant m \leqslant n} \Gamma^m$.

More applications: the Lubotzky-Meiri group sieve method

In 1996, Hrushovski-Kropholler-Lubotzky-Shalev proved that if Γ is linear and non virtually solvable, then for all finite $n \geqslant 2$, Γ is not a finite union of translates of $\cup_{2 \leqslant m \leqslant n} \Gamma^m$.
Thanks to the recent progress on approximate groups and expanders we now know:

Theorem (Lubotzky-Meiri 2012)

If Γ is linear and non virtually solvable, then Γ is not a finite union of translates of $\Gamma^{\geqslant 2}$. In fact $\Gamma^{\geqslant 2}$ is exponentially small, meaning that if μ is the uniform probability measure on a generating set of Γ, then

$$\mu^n(\Gamma^{\geqslant 2})$$

decays to 0 exponentially fast as $n \to +\infty$.

The group sieve method

For simplicity assume that $\Gamma \leqslant SL_d(\mathbb{Z})$ is Zariski-dense.

Lemma

Every proper algebraic subvariety $\mathcal{V}$ of SL_d is exponentially small, i.e. $\mu^n(\mathcal{V})$ decays exponentially fast.

The group sieve method

For simplicity assume that $\Gamma \leqslant SL_d(\mathbb{Z})$ is Zariski-dense.

Lemma

Every proper algebraic subvariety $\mathcal{V}$ of SL_d is exponentially small, i.e. $\mu^n(\mathcal{V})$ decays exponentially fast.

Proof: reduce mod p and use the super-strong-approximation theorem (i.e. that Γ mod p are expanders hence μ^n has fast equidistribution).

The group sieve method

For simplicity assume that $\Gamma \leqslant SL_d(\mathbb{Z})$ is Zariski-dense.

Lemma

Every proper algebraic subvariety $\mathcal{V}$ of SL_d is exponentially small, i.e. $\mu^n(\mathcal{V})$ decays exponentially fast.

Proof: reduce mod p and use the super-strong-approximation theorem (i.e. that Γ mod p are expanders hence μ^n has fast equidistribution).

Lemma (group sieve)

Let $\Gamma = \langle S \rangle$ as above and $\Gamma_p := \Gamma \cap \ker(\mathrm{SL}_d(\mathbb{Z}) \to \mathrm{SL}_d(\mathbb{Z}/p\mathbb{Z})$. Let $Z \subset \Gamma$ be such that there is $c > 0$ such that for some increasing sequence of primes p_j with $p_j \leqslant j^C$,

$$|Z\Gamma_{p_j}/\Gamma_{p_j}| < (1-c)|\Gamma/\Gamma_{p_j}|.$$

Then Z is exponentially small, i.e. $\mu^n(Z)$ decays exponentially fast.

The group sieve method

The proof of the group sieve lemma relies on the following elementary fact from probability theory:

Lemma (2nd moment method)

Let $A_1, \ldots, A_L$ be events such that for some $c > 0$

- $\mathbb{P}(A_j) < 1 - c$ *and*
- $\forall j, j'$, $|\mathbb{P}(A_j \cap A_{j'}) - \mathbb{P}(A_j)\mathbb{P}(A_{j'})| < \Delta$,

Then

$$\mathbb{P}(\cap_{j=1}^{L} A_j) \leqslant \frac{1}{c}\left(\frac{1}{L} + \Delta\right)$$