Super-strong Approximation I

Emmanuel Breuillard

Université Paris-Sud, Orsay, France

IPAM, February 9th, 2015

Strong Approximation

$\mathbf{G}$ = connected, simply connected, semisimple algebraic group defined over $\mathbb{Q}$.

Γ = a finitely generated Zariski-dense subgroup of $\mathbf{G}(\mathbb{Q})$.

Theorem (Nori, Matthews-Vaserstein-Weisfeiler)

For all sufficiently large prime numbers p, the reduction Γ_p of Γ is equal to $\mathbf{G}_p(\mathbb{F}_p)$.

Strong Approximation

Theorem (Nori, Matthews-Vaserstein-Weisfeiler)

For all sufficiently large prime numbers p, the reduction Γ_p of Γ is equal to $\mathbf{G}_p(\mathbb{F}_p)$.

Several proofs (Nori, Matthews-Vaserstein-Weisfeiler, Weisfeiler, Hrushovski-Pilay, Larsen-Pink...)

Nori for q prime, then Larsen-Pink, gave a description of all subgroups of $GL_d(\mathbb{F}_q)$, showing that they are essentially algebraic groups over $\mathbb{F}_q$.

Nori's theorem

Recall that C. Jordan proved that finite subgroups of $GL_d(\mathbb{C})$ have an abelian subgroup of index $O_d(1)$.

Let $\mathbf{G}_p \leqslant \mathrm{GL}_d$ be a semisimple simply connected d-dimensional algebraic group defined over $\mathbb{F}_p$.

Nori argues that:

Theorem (Nori)

There is $M = M(d)$ such that for every prime $p > M$ and every subgroup $H \leqslant \mathbf{G}_p(\mathbb{F}_p)$, either H is contained in a proper algebraic subgroup of $\mathbf{G}_p$ of complexity at most M or $H = \mathbf{G}_p(\mathbb{F}_p)$.

complexity = degree of the underlying algebraic variety

Nori's theorem

Theorem (Nori)

There is $M = M(d)$ such that for every prime $p > M$ and every subgroup $H \leqslant \mathbf{G}_p(\mathbb{F}_p)$, either H is contained in a proper algebraic subgroup of $\mathbf{G}_p$ of complexity at most M or $H = \mathbf{G}_p(\mathbb{F}_p)$.

Proof sketch:

Nori's theorem

Theorem (Nori)

There is $M = M(d)$ such that for every prime $p > M$ and every subgroup $H \leqslant \mathbf{G}_p(\mathbb{F}_p)$, either H is contained in a proper algebraic subgroup of $\mathbf{G}_p$ of complexity at most M or $H = \mathbf{G}_p(\mathbb{F}_p)$.

Proof sketch:

• By Jordan's theorem H contains a unipotent element, say $h_1 = \exp(\xi_1)$,
• Acting by the adjoint representation, we obtain $h_2 = \exp(\xi_2), ..., h_d = \exp(\xi_d)$ in H such that $\xi_1, ..., \xi_d$ span $Lie(\mathbf{G}_p)$.

Nori's theorem

Theorem (Nori)

There is $M = M(d)$ such that for every prime $p > M$ and every subgroup $H \leqslant \mathbf{G}_p(\mathbb{F}_p)$, either H is contained in a proper algebraic subgroup of $\mathbf{G}_p$ of complexity at most M or $H = \mathbf{G}_p(\mathbb{F}_p)$.

Proof sketch:

• The map $\Phi : \mathbb{F}_p^d \to \mathbf{G}_p(\mathbb{F}_p)$, $(t_1, \dots, t_d) \mapsto h_1^{t_1} \cdot \dots \cdot h_d^{t_d}$ is a bounded degree polynomial map whose image has dimension $d = \dim \mathbf{G}$, so by counting its image must have $\leqslant c(d)p^d$ elements.

• Hence $|H| > c(d)p^d$, but $|\mathbf{G}_p(\mathbb{F}_p)| < Cp^d$, so H has bounded index in $\mathbf{G}_p(\mathbb{F}_p)$, hence (since $\mathbf{G}_p$ is simply connected) is all of $\mathbf{G}_p(\mathbb{F}_p)$.

Nori's theorem

Theorem (Nori)

There is $M = M(d)$ such that for every prime $p > M$ and every subgroup $H \leqslant \mathbf{G}_p(\mathbb{F}_p)$, either H is contained in a proper algebraic subgroup of $\mathbf{G}_p$ of complexity at most M or $H = \mathbf{G}_p(\mathbb{F}_p)$.

Proof sketch:

• Using this theorem, one deduce the strong approximation theorem: Since Γ is assumed Zariski-dense, Γ_p will be "sufficiently Zariski-dense in $\mathbf{G}_p$", hence all of $\mathbf{G}_p(\mathbb{F}_p)$.

• This also gives a "quantitative" version of strong approximation: if $\Gamma = \langle S \rangle$, $S \subset \mathbf{G}(\mathbb{Q})$, then the largest bad prime p is at most $H(S)^{O_d(1)}$, where $H(S) =$ height of S.

Super-strong approximation

$\mathbf{G}$ = connected, simply connected, semisimple algebraic group defined over $\mathbb{Q}$.

Γ = a finitely generated Zariski-dense subgroup of $\mathbf{G}(\mathbb{Q})$.

S a finite symmetric generating subset of Γ.

Theorem (Super-strong approximation)

Then there is $\varepsilon = \varepsilon(S) > 0$ s.t. for all large enough prime numbers p, the reduction Γ_p of Γ is equal to $\mathbf{G}_p(\mathbb{F}_p)$ and the associated Cayley graph $\mathrm{Cay}(\mathbf{G}_p(\mathbb{F}_p), S_p)$ is an ε-expander.

Super-strong approximation

$\mathbf{G}$ = connected, simply connected, semisimple algebraic group defined over $\mathbb{Q}$.

Γ = a finitely generated Zariski-dense subgroup of $\mathbf{G}(\mathbb{Q})$.

S a finite symmetric generating subset of Γ.

Theorem (Super-strong approximation)

Then there is $\varepsilon = \varepsilon(S) > 0$ s.t. for all large enough prime numbers p, the reduction Γ_p of Γ is equal to $\mathbf{G}_p(\mathbb{F}_p)$ and the associated Cayley graph $\mathrm{Cay}(\mathbf{G}_p(\mathbb{F}_p), S_p)$ is an ε-expander.

... long history ... Sarnak-Xue, Gamburd, Bourgain-Gamburd, Helfgott, B-Green-Tao, Pyber-Szabo, Varjú, Salehi-Golsefidy-Varjú.

Super-strong approximation

Theorem (Super-strong approximation)

Then there is $\varepsilon = \varepsilon(S) > 0$ *s.t. for all large enough prime numbers* p*, the reduction* Γ_p *of* Γ *is equal to* $\mathbf{G}_p(\mathbb{F}_p)$ *and the associated Cayley graph* $\mathrm{Cay}(\mathbf{G}_p(\mathbb{F}_p), S_p)$ *is an* ε*-expander.*

What is an ε-expander ?

Super-strong approximation

Theorem (Super-strong approximation)

Then there is $\varepsilon = \varepsilon(S) > 0$ *s.t. for all large enough prime numbers* p*, the reduction* Γ_p *of* Γ *is equal to* $\mathbf{G}_p(\mathbb{F}_p)$ *and the associated Cayley graph* $\mathrm{Cay}(\mathbf{G}_p(\mathbb{F}_p), S_p)$ *is an* ε*-expander.*

What is an ε-expander ?

Definition (Expander)

A k-regular graph $\mathcal{G}$ is said to be an ε-expander if

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

Expanders

Definition (Expander)

A k-regular graph $\mathcal{G}$ is said to be an ε-expander if

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

Expanders

Definition (Expander)

A k-regular graph $\mathcal{G}$ is said to be an ε-expander if

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

Here $\lambda_1(\mathcal{G})$ is the first non-zero eigenvalue of the combinatorial Laplacian on $\mathcal{G}$, namely the operator on $\ell^2(\mathcal{G})$ defined by:

$$\Delta f(x) = kf(x) - \sum_{y \sim x} f(y),$$

where the sum is over the neighboring vertices y of the vertex $x \in \mathcal{G}$.

Expanders

Definition (Expander)

A k-regular graph $\mathcal{G}$ is said to be an ε-expander if

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

Expanders are sparse well connected graphs. They satisfy a linear isoperimetric inequality

$$|\partial A| > c_\varepsilon |A|$$

for every subset A of at most $|\mathcal{G}|/2$ vertices.
In particular their diameter is very small:

$$diam(\mathcal{G}) \ll C_\varepsilon \log |\mathcal{G}|.$$

Expanders

Definition (Expander)

A k-regular graph $\mathcal{G}$ is said to be an ε-expander if

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

Although a random k-regular graph is an ε-expander, constructing one is not easy.

Margulis (1972) gave the first construction by observing that if Γ is a finitely generated group with Kazhdan's property (T), then the Cayley graphs of its finite quotients (w.r.t. a fixed generating set in Γ) must be ε-expanders for some uniform $\varepsilon > 0$.

Expanders

Definition (Expander)

A k-regular graph $\mathcal{G}$ is said to be an ε-expander if

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

For example if $d \geqslant 3$, the Cayley graphs of $\mathrm{SL}_d(\mathbb{Z}/n\mathbb{Z})$ w.r.t a fixed generating subset of $\mathrm{SL}_d(\mathbb{Z})$ are ε-expanders for some ε independent of n.

This is still true for $d = 2$, but relies on Selberg's 3/16-theorem, instead of property (T).

Super-strong approximation

Let us go back to:

Theorem (Super-strong approximation)

If $\mathbf{G}$ *is a simply connected semisimple* $\mathbb{Q}$*-group and* $\Gamma \leqslant \mathbf{G}(\mathbb{Q})$ *is Zariski-dense, then there is* $\varepsilon = \varepsilon(S) > 0$ *s.t. for all large enough prime numbers* p*, the reduction* Γ_p *of* Γ *is equal to* $\mathbf{G}_p(\mathbb{F}_p)$ *and the associated Cayley graph* $\mathrm{Cay}(\mathbf{G}_p(\mathbb{F}_p), S_p)$ *is an* ε*-expander.*

Super-strong approximation

Let us go back to:

Theorem (Super-strong approximation)

If $\mathbf{G}$ is a simply connected semisimple $\mathbb{Q}$-group and $\Gamma \leqslant \mathbf{G}(\mathbb{Q})$ is Zariski-dense, then there is $\varepsilon = \varepsilon(S) > 0$ s.t. for all large enough prime numbers p, the reduction Γ_p of Γ is equal to $\mathbf{G}_p(\mathbb{F}_p)$ and the associated Cayley graph $\mathrm{Cay}(\mathbf{G}_p(\mathbb{F}_p), S_p)$ is an ε-expander.

The key point here is that Γ is an arbitrary Zariski-dense subgroup (possibly of infinite index in $\mathbf{G}(\mathbb{Z})$, without property (T)).

Super-strong approximation

Let us go back to:

Theorem (Super-strong approximation)

If $\mathbf{G}$ is a simply connected semisimple $\mathbb{Q}$-group and $\Gamma \leqslant \mathbf{G}(\mathbb{Q})$ is Zariski-dense, then there is $\varepsilon = \varepsilon(S) > 0$ s.t. for all large enough prime numbers p, the reduction Γ_p of Γ is equal to $\mathbf{G}_p(\mathbb{F}_p)$ and the associated Cayley graph $\mathrm{Cay}(\mathbf{G}_p(\mathbb{F}_p), S_p)$ is an ε-expander.

The key point here is that Γ is an arbitrary Zariski-dense subgroup (possibly of infinite index in $\mathbf{G}(\mathbb{Z})$, without property (T)).

Gamburd's thesis, Lubotzky's 1,2,3-problem

Gamburd's thesis, Lubotzky's 1,2,3-problem

Inspired by earlier work of Sarnak-Xue, Gamburd proved in his 1999 thesis that the super-strong approximation theorem holds for Zariski-dense subgroups of $SL_2(\mathbb{Z})$ with sufficiently large limit set, i.e. s.t. that the limit set in $\mathbb{P}^1(\mathbb{R})$ has Hausdorff dimension at least $5/6$.

Gamburd's thesis, Lubotzky's 1,2,3-problem

A related simple yet inspiring question of Lubotzky, the Lubotzky $1,2,3$-problem was the following: Let Γ_n be the subgroup of $\mathrm{SL}_2(\mathbb{Z})$ generated by

$$\begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix}, \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$$

Γ_1 and Γ_2 have finite index in $\mathrm{SL}_2(\mathbb{Z})$, so by Selberg's theorem Γ_n mod p is a family of expanders as p grows. But what about Γ_3 ? it has infinite index...

This was solved by Bourgain-Gamburd and their proof paved the way for the general case.

Lubotzky's super-alternative

Another incarnation of super-strong approximation is the following:

Theorem (Lubotzky super-alternative)

Let k be a field of characteristic zero, and $\Gamma \leqslant GL_d(k)$ a finitely generated linear group. Then there is a subgroup Γ_0 of bounded index in Γ such that

- *either the subgroup Γ_0 is solvable,*
- *or for all large enough p, Γ_0 maps onto $\mathbf{G}_p(\mathbb{F}_p)$ (where $\mathbf{G}$ is some connected, simply connected, semisimple algebraic $\mathbb{Q}$-group),in such a way that its Cayley graph is an ε-expander, for some $\varepsilon > 0$ independent of p, and a fixed generating set of Γ_0.*

Super-strong approximation

Conjecture (folklore)

There is $\varepsilon > 0$ *such that all Cayley graphs of* $\mathbf{G}(\mathbb{Z}/n\mathbb{Z})$ *are* ε*-expanders, uniformly in* n *and in the generating set.*

Super-strong approximation

Conjecture (folklore)

There is $\varepsilon > 0$ *such that all Cayley graphs of* $\mathbf{G}(\mathbb{Z}/n\mathbb{Z})$ *are* ε*-expanders, uniformly in n and in the generating set.*

partial progress:

• uniformity in n for n square-free by Salehi-Golsefidy-Varjú, and by Bourgain-Varjú for $\mathbf{G} = \mathrm{SL}_d$.

• uniformity in the generating set for $\mathbf{G} = \mathrm{SL}_2$ and n in a density one subset of the primes (B+Gamburd).

• uniformity in n for n prime and "most" generating sets (B+Green+Guralnick+Tao).

Finite simple groups

Conjecture (also folklore)

Given d*, there is* $\varepsilon > 0$ *such that all Cayley graphs of all finite simple groups of rank at most* d *are* ε*-expanders.*

We know:

Theorem (B.-Green-Guralnick-Tao)

Given $d > 0$ *there is* $c, \varepsilon > 0$ *such that every finite simple group* G *of rank at most* d *admits a good generating pair, i.e. one whose associated Cayley graph is an* ε*-expander. In fact the proportion of bad pairs is at most* $|G|^{-c}$*.*

Finite simple groups

Conjecture (also folklore)

Given d, there is $\varepsilon > 0$ such that all Cayley graphs of all finite simple groups of rank at most d are ε-expanders.

We know:

Theorem (B.-Green-Guralnick-Tao)

Given $d > 0$ there is $c, \varepsilon > 0$ such that every finite simple group G of rank at most d admits a good generating pair, i.e. one whose associated Cayley graph is an ε-expander. In fact the proportion of bad pairs is at most $|G|^{-c}$.

• Kassabov showed that there is a symmetric generating set of bounded size making the alternating group A_n an ε-expander, but with "usual" generators A_n is not an expander.

Finite simple groups

Conjecture (also folklore)

Given d, there is $\varepsilon > 0$ such that all Cayley graphs of all finite simple groups of rank at most d are ε-expanders.

We know:

Theorem (B.-Green-Guralnick-Tao)

Given $d > 0$ there is $c, \varepsilon > 0$ such that every finite simple group G of rank at most d admits a good generating pair, i.e. one whose associated Cayley graph is an ε-expander. In fact the proportion of bad pairs is at most $|G|^{-c}$.

• Kassabov-Lubotzky-Nikolov nevertheless showed that there are uniform ε, k an a choice of a generating set of size k for each finite simple group, s.t. the Cayley graph is an ε-expander.

Finite simple groups

Also here is a general lower bound on λ_1.

Theorem (B-Green-Tao)

For every $\varepsilon > 0$, every finite simple group G and every Cayley graph $\mathcal{G}$ of G satisfies:

$$\lambda_1(\mathcal{G}) \geqslant \frac{1}{|G|^{\varepsilon}},$$

except for possibly finitely many exceptions.

Remarks:

Finite simple groups

Also here is a general lower bound on λ_1.

Theorem (B-Green-Tao)

For every $\varepsilon > 0$, every finite simple group G and every Cayley graph $\mathcal{G}$ of G satisfies:

$$\lambda_1(\mathcal{G}) \geqslant \frac{1}{|G|^{\varepsilon}},$$

except for possibly finitely many exceptions.

Remarks:

• The proof of the above Theorem does not use the classification of finite simple groups.
• in fact the proof shows that any finite group admitting a Cayley graph with $\lambda_1 < 1/|G|^{\varepsilon}$ must have a large quotient with a cyclic subgroup of bounded index (hence cannot be simple).

Finite simple groups

Also here is a general lower bound on λ_1.

Theorem (B-Green-Tao)

For every $\varepsilon > 0$, every finite simple group G and every Cayley graph $\mathcal{G}$ of G satisfies:

$$\lambda_1(\mathcal{G}) \geqslant \frac{1}{|G|^\varepsilon},$$

except for possibly finitely many exceptions.

Remarks:

- A conjecture of Babai asserts that

$$diam(\mathcal{G}) \ll (\log|G|)^{O(1)}$$

for all finite simple G. The above Theorem thus gives $diam(\mathcal{G}) \ll |G|^{o(1)}$ unconditionally.

Finite simple groups

Also here is a general lower bound on λ_1.

Theorem (B-Green-Tao)

For every $\varepsilon > 0$, every finite simple group G and every Cayley graph $\mathcal{G}$ of G satisfies:

$$\lambda_1(\mathcal{G}) \geqslant \frac{1}{|G|^{\varepsilon}},$$

except for possibly finitely many exceptions.

Remarks:

- Babai's conjecture implies a similar bound for λ_1, i.e. $> 1/(\log |G|)^{O(1)}$.

Finite simple groups

Also here is a general lower bound on λ_1.

Theorem (B-Green-Tao)

For every $\varepsilon > 0$, every finite simple group G and every Cayley graph $\mathcal{G}$ of G satisfies:

$$\lambda_1(\mathcal{G}) \geqslant \frac{1}{|G|^\varepsilon},$$

except for possibly finitely many exceptions.

Remarks:

• Babai's conjecture was verified for $\mathrm{SL}_2(\mathbb{F}_p)$ by Helfgott, then by B-Green-Tao and Pyber-Szabo for $\mathbf{G}(\mathbb{F}_q)$ with $\mathbf{G}$ of bounded rank (using approximate groups and additive combinatorics), and also for the (non simple) groups $\mathbf{G}(\mathbb{Z}/p^n\mathbb{Z})$ by Dinai and Bradford (using the Solovay-Kitaev algorithm).

Applications

Why do we care about spectral gaps ?

Knowing that a Cayley graph is an expander tells you that random walks on it equidistribute as fast as possible, in $O(\log |\mathcal{G}|)$ steps.

Applications

Why do we care about spectral gaps ?

Knowing that a Cayley graph is an expander tells you that random walks on it equidistribute as fast as possible, in $O(\log |\mathcal{G}|)$ steps.

So this gives information about "generic" elements of the original Zariski-dense subgroup Γ and allows to perform various forms of counting at the group level (e.g. the affine sieve of Bourgain-Gamburd-Sarnak... see Alireza's talk).

Applications

Why do we care about spectral gaps ?

Knowing that a Cayley graph is an expander tells you that random walks on it equidistribute as fast as possible, in $O(\log |\mathcal{G}|)$ steps.

So this gives information about "generic" elements of the original Zariski-dense subgroup Γ and allows to perform various forms of counting at the group level (e.g. the affine sieve of Bourgain-Gamburd-Sarnak... see Alireza's talk).

This line of thought was pioneered by Rivin, Kowalski, Sarnak, Lubotzky and others.

Counting in Zariski-dense subgroups

Let $\Gamma = \langle S \rangle \leqslant \mathbf{G}$ be a Zariski-dense subgroup of the semisimple algebraic group $\mathbf{G}$.

Let $\mu = \mu_S$ be the uniform measure on the symmetric generating set S.

Theorem (Subvarieties are exponentially small)

Suppose $\mathcal{V} \leqslant \mathbf{G}$ is a proper algebraic subvariety. Then

$$\mu^n(\mathcal{V}) \leqslant c_0(\mathcal{V}) \cdot e^{-cn},$$

where $c_0(\mathcal{V}) > 0$ is a constant depending only on the complexity (i.e. degree) of $\mathcal{V}$, and $c > 0$ depends only on μ.

Generic pairs are free and dense

Recall the Tits alternative: is $\Gamma \leqslant \mathbf{G}$ is Zariski-dense, it contains a Zariski-dense free subgroup.

Theorem (Aoun)

If $\mathcal{Z}$ is the set of pairs (a, b) in Γ that do not generate a free Zariski-dense subgroup, then

$$\mu^n \otimes \mu^n(\mathcal{Z}) \leqslant e^{-cn}$$

cf. related work of Fuchs-Rivin.

The group sieve method

The super-strong approximation theorem gives a method to establish that certain subsets $\mathcal{Z}$ of the Zariski-dense subgroup $\Gamma \leqslant \mathbf{G}(\mathbb{Q})$ are very small (i.e. with exponential decay of the hitting probability). For example Lubotzky and Meiri give the following criterion:

Lemma (Lubotzky-Meiri sieve)

Let $\mathcal{Z} \subset \Gamma$ be a subset. Assume that there is $\alpha < 1$ such that for all large primes p,

$$|\mathcal{Z} \bmod p| < \alpha |\mathbf{G}_p(\mathbb{F}_p)|$$

Then $\mathcal{Z}$ is exponentially small, i.e.

$$\mu^n(\mathcal{Z}) < e^{-cn}.$$

(μ is the uniform probability measure on a generating set of Γ.)

Further examples

Say that the subset $\mathcal{Z} \leqslant \Gamma$ is *exponentially small* if $\exists c > 0$ s.t.

$$\mu^n(\mathcal{Z}) \leqslant e^{-cn}$$

Theorem (Lubotzky-Meiri)

The set $\mathcal{Z}$ of proper powers in Γ is exponentially small.

Further examples

Say that the subset $\mathcal{Z} \leqslant \Gamma$ is *exponentially small* if $\exists c > 0$ s.t.

$$\mu^n(\mathcal{Z}) \leqslant e^{-cn}$$

Theorem (Lubotzky-Meiri)

The set $\mathcal{Z}$ of proper powers in Γ is exponentially small.

Theorem (Lubotzky-Rosenzweig)

Every element in Γ outside of an exponentially small set, is semisimple and Galois generic.

This builds on work of Prasad-Rapinchuk showing *existence* of Galois generic elements in Zariski-dense subgroups, and related work of Jouve-Zywina-Kowalski.

Some references:

• E. Breuillard, *Approximate groups and super-strong approximation*, a survey, Groups St.Andrews conf. proc (2014).

• A. Salehi-Golsefidy and P. P. Varjú. *Expansion in perfect groups*, Geom. Funct. Anal., 22(6):1832–1891, (2012).

• E. Breuillard, B. Green, and T. Tao. *Approximate subgroups of linear groups*, Geom. Funct. Anal., 21(4):774–819, (2011).

• L. Pyber and E. Szabó, *Growth in finite simple groups of lie type of bounded rank.* , arXiv:1005.1858.

• J. Bourgain and A. Gamburd. *Uniform expansion bounds for Cayley graphs of* $SL_2(\mathbb{F}_p)$, Ann. of Math. (2), 167(2):625–642, (2008).