Expander Graphs in Pure and Applied Mathematics

Alex Lubotzky
Einstein Institute of Mathematics, Hebrew University
Jerusalem 91904, ISRAEL

- Alexander Lubotzky, Discrete groups, expanding graphs and invariant measures. Reprint of the 1994 edition. Modern Birkhäuser Classics. Birkhäuser Verlag, Basel, 2010. iii+192
- Shlomo Hoory, Nathan Linial and Avi Wigderson, Expander graphs and their applications. Bull. Amer. Math. Soc. (N.S.) 43 (2006), no. 4, 439–561
- http://www.ams.org/meetings/national/jmm/2011_colloquium_lecture_notes_lubotzky_expanders.pdf

Def: **Expander Graphs**

For $0 < \varepsilon \in \mathbb{R}$,

$$X = (\underset{\text{vertices}}{V}, \underset{\text{edges}}{E}) \quad \text{a graph is } \varepsilon - \text{expander}$$

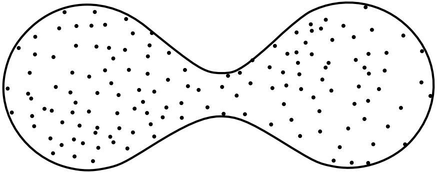
if

$$\forall Y \subseteq V, \text{ with } |Y| \leq \frac{|V|}{2}$$

$$|\partial Y| \geq \varepsilon |Y|$$

where $\partial Y = \text{boundry of } Y = \{x \in V | \text{dist}(x, Y) = 1\}$

not expander.



expander $\Rightarrow$ "fat and round"
expander $\Rightarrow$ logarithmic diameter

History

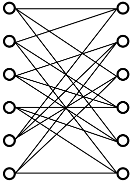
Barzdin & Kolmogorov (1967) (networks of nerve cells in the brain!)

Pinsker (1973) - communication networks

We want "families of expanders" (n, k, ε)-expanders, $n = |V| \to \infty$
k-regular, k-fixed (as small as possible)
ε-fixed (as large as possible)

Fact. Fixed $k \geq 3$, $\exists \varepsilon > 0$ s.t. "most" random k-regular graphs are ε-expanders.

(Pick $\pi_1, \ldots, \pi_k \in Sym(n)$ at random).



Many applications in CS:

Communication networks

pseudorandomness/Monte-Carlo algorithms

derandomization

error-correcting codes

$\vdots$

Over 4,000,000 sites with "expanders"

but many of them for dentists

Still over 400,000 are about expander graphs ... e.g.

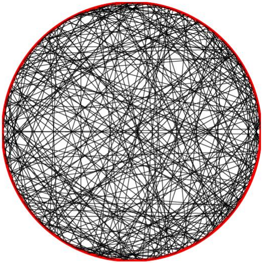


Figure: Inverse graph, level = 617

$$V = \{0, 1, \ldots, p-1\} \cup \{\infty\}$$

$$x \to x \pm 1 \quad \& \quad x \to -\frac{1}{x}$$

For applications one wants explicit construction

Kazhdan property (T) from representation theory

Def. (1967)
Let Γ be a finitely generated group, $\Gamma = \langle S \rangle \quad S = S^{-1}$.
Γ has (T) if $\exists \varepsilon > 0$ s.t.

$$\forall (\mathcal{H}, \rho) \quad \underset{\rho:\Gamma \to U(\mathcal{H}) = \text{unitary operators}}{\mathcal{H} - \text{Hilbert space}}$$

irreducible (**no** closed invariant subspace) and non-trivial $(\mathcal{H}, \rho) \neq (\mathbb{C}, \rho_0)$.

$$\forall\, 0 \neq v \in \mathcal{H}, \quad \exists\, s \in S \text{ s.t.}$$
$$\|\rho(s)v - v\| \geq \varepsilon \|v\|$$

i.e., no almost-invariant vectors

Explicit construction (Margulis 1973)

Assume $\Gamma = \langle S \rangle$ has (T),

$$\mathcal{L} = \{N \triangleleft \Gamma | [\Gamma : N] < \infty\}.$$

$$\text{Then } \{Cay(\Gamma/N; S) | N \in \mathcal{L}\}$$

is a family of expanders.

Remainder. $G = \langle S \rangle$ group, Cayley graph $Cay(G; S)$:

$$V = |G| \quad \text{and} \quad g_1 \sim g_2 \text{ if } \exists s \in S \text{ with } sg_1 = g_2.$$

"Proof"

$$X = Cay(\Gamma/N; S),\ Y \subseteq V(X) = \Gamma/N, |Y| \leq \frac{|V|}{2}$$

need to prove $|\partial Y| \geq \varepsilon' |Y|$
Γ acts on Γ/N by left translations and hence on $L^2(\Gamma/N)$. Take

$$\mathbf{1}_Y = \text{char. function of } Y = \begin{cases} 1 & y \in Y \\ 0 & y \notin Y \end{cases}$$

So some $s \in S$ moves $\mathbf{1}_Y$ by ε,

$$\rho(s)(\mathbf{1}_Y) = \mathbf{1}_{sY}$$

so $\mathbf{1}_{sY}$ is "far" from $\mathbf{1}_Y$, i.e. many vertices in sY are not in Y;
but $sY \setminus Y \subset \partial Y$ and we are done. $\square$

An important observation

We use (T) only for the rep's $L^2(\Gamma/N)$, in particular, finite dimensional!

Def: $\Gamma = \langle S \rangle$ finitely generated groups. $\mathcal{L} = \{N_i\}$ family of finite index normal subgroups of Γ.

Γ has (τ) w.r.t. $\mathcal{L}$

if $\exists \varepsilon > 0$ s.t. $\forall (\mathcal{H}, \rho)$ non-trivial irr. rep.

with Ker $\rho \supset N_i$ for some i, $\forall\, 0 \neq v \in \mathcal{H}$

$\exists s \in S$ s.t. $\|\rho(s)v - v\| > \varepsilon \|v\|$.

Cor

(τ) *w.r.t.* $\mathcal{L} \Rightarrow Cay(\Gamma/N_i; S)$ expanders!

This is **iff** !!!

Thm (Kazhdan)

$SL_n(\mathbb{Z})$ has (T) for $n \geq 3$
($n \times n$ integral matrices, $\det = 1$)

$SL_2(\mathbb{Z})$ does not have (T) nor (τ) (has a free subgroup F of finite index and $F \twoheadrightarrow \mathbb{Z}$)
but:

Thm (Selberg)

$SL_2(\mathbb{Z})$ has (τ) w.r.t. congruence subgroups

$$\{\Gamma(m) = Ker(SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/m\mathbb{Z}))\}$$

Selberg's Thm is known as: $\lambda_1(\Gamma(m) \setminus \mathbb{H}) \geq \frac{3}{16}$.
$\mathbb{H}$ - upper half plane.

Eigenvalues & random walks

X finite k-regular graph, $X = (V, E)$

$$|V| = n.$$

$A = A_X$ - adjancency matrix, $A_{ij} = \#$ edges between i and j.

A symmetric matrix with eigenvalues

$$k = \lambda_0 \geq \lambda_1 \geq \cdots \geq \lambda_{n-1} \geq -k$$
$$\cdot\, \lambda_0 > \lambda_1 \quad \text{iff } X \text{ is connected}$$
$$\cdot\, \lambda_{n-1} = -k \quad \text{iff } X \text{ is bi-partite.}$$

Thm

X is ε-expander iff

$$\lambda_1 \leq k - \varepsilon'$$

The non-trivial eigenvalues $\lambda \neq \pm k$ control **the rate of convergence** of the random walk on X to the uniform distribution; so: Expanders "$\Leftrightarrow$" exponentially fast convergence to uniform distribution.

Thm (Alon-Boppana)

For k fixed, $\lambda_1(X_{n,k}) = 2\sqrt{k-1} + o(1)$ when $n \to \infty$

Ramanujan graph $\lambda(X) \leq 2\sqrt{k-1}$ (optimal)

$\forall k = p^\alpha + 1,\ p$ *prime*

$\exists\ \infty$ many k-regular Ramanujan graphs.

Open problem for other k's, e.g. k=7.

Expanders & Riemannian manifolds

M n-dim connected closed Riemannian manifold
$\Delta = -div(grad) = laplacian = Laplace - Beltrami\ operator.$
$e.\nu.\ 0 = \lambda_0 < \lambda_1 \leq \lambda_1 \leq \ldots \leq \lambda_i \leq \ldots$

Fact

$$\lambda_1(M) = inf\left\{ \frac{\int_M \|df\|^2}{\int_M |f|^2} \middle| f \in C^\infty(M), \int f = 0 \right\}$$

Def. The Cheeger constant $h(M)$

$h(M) = \inf_Y \frac{Area(\partial Y)}{Volume(Y)}$
Y - Open in M with $Vol(Y) \leq \frac{1}{2} Vol(M)$

Cheeger Inequality (1970)

$$\lambda_1(M) \geq \frac{1}{4} h^2(M)$$

Buser proved a converse: bounding $h(M)$ by $\lambda_1(M)$.

In summary

Thm
$\Gamma = \langle S \rangle$ *finitely generated group,* $\mathcal{L} = \{N_i\}$ *finite index normal subgroups.*

TFAE:

Representation (i) Γ has (τ) w.r.t. $\mathcal{L}$ i.e. $\exists \varepsilon_1$ s.t. $\forall (\mathcal{H}, \rho) \cdots$

Combinatorics (ii) $\exists \varepsilon_2 > 0$ s.t. $Cay(\Gamma / N_i; S)$ are ε_2-expanders

Random walks (iii) $\exists \varepsilon_3 > 0$ s.t.

$$\lambda_1(Cay(\Gamma / N_i; S)) \leq k - \varepsilon_3 \text{ where } k = |S|$$

Measure theoretic (iv) The Haar measure on $\hat{\Gamma}_{\mathcal{L}} = \varprojlim \Gamma/N_i$ is the only Γ-invariant mean on $L^\infty(\hat{\Gamma}_{\mathcal{L}})$

If $\Gamma = \Pi_1(M)$, M-closed Riemannian manifold and $\{M_i\}$ the corresponding covers:

Geometric (v) $\exists \varepsilon_5 > 0, \quad h(M_i) \geq \varepsilon_5$

Analytic (vi) $\exists \varepsilon_6 > 0, \quad \lambda_1(M_i) \geq \varepsilon_6$

Back to Selberg & Kazhdan

Selberg Thm $\lambda_1(\Gamma(M) \setminus \mathbb{H}) \geq \frac{3}{16}$

Cor
$Cay(SL_2(\mathbb{F}_p); \{ \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \})$ are expanders.
(Proof uses Weil's Riemann hypothesis for curves and Riemann surfaces).

Cor
$\begin{pmatrix} 1 & \frac{p-1}{2} \\ 0 & 1 \end{pmatrix}$ $\left(= \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)^{\frac{p-1}{2}} \right)$ can be written as a word of length $O(\log p)$ using $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$.

Open problem How? Algorithm? (Partial; Larsen). (New proof by Bourgain-Gamburd (Helfgott) but also without algorithm).

Thm
For a fixed n, $Cay(SL_n(\mathbb{F}_p); \{A, B\})$ are expanders (A, B generators for $SL_n(\mathbb{Z})$).

Can they all be made into a family of expanders together - all n all p? and even all $q = p^e$?

Conj (Babai-Kantor-Lubotzky (1989))

All non abelian finite simple groups are expanders in a uniform way (same k, same ε).

This was indeed proved as an accumulation of several works and several methods

Kassabov - Lubotzky - Nikolov (2006): Groups of Lie type except Suzuki.

Kassabov (2006): $Aln(n)$ and $Sym(n)$.

Breuillard - Green - Tao (2010): Suzuki Groups.

Other generators

What happened if we slightly change the set of generators?

Ex 1 $Cay(SL_2(\mathbb{F}_p); \{\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right)\}$ are expanders (Selberg)

Ex 2 $Cay(SL_2(\mathbb{F}_p); \{\left(\begin{smallmatrix}1&2\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1&0\\2&1\end{smallmatrix}\right)\}$ are expanders (Pf: $\left\langle \left(\begin{smallmatrix}1&2\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1&0\\2&1\end{smallmatrix}\right) \right\rangle$ is of finite index in $SL_2(\mathbb{Z})$ and use Selberg.)

What about Ex 3 $Cay(SL_2; \{\left(\begin{smallmatrix}1&3\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1&0\\3&1\end{smallmatrix}\right)\})$?
$\left\langle \left(\begin{smallmatrix}1&3\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1&0\\3&1\end{smallmatrix}\right) \right\rangle$ is of infinite index in $SL_2(\mathbb{Z})$ (but Zariski dense?)
"Lubotzky 1-2-3 problem".

Answer:

Yes! (Bourgain-Gamburd/Helfgott)
with Far reaching generalizations; Breuillard-Green-Tao, Pyber-Szabo, Salehi-Golsefidy-Varju.

These generalizations have dramatic number theoretic applications. This will be the topic of lecture II.

Thm

$\exists \infty$ *many primes*

Proof.

Put a topology on $\mathbb{Z}$ by declaring the arithmetic progressions $Y_{a,d} = \{a + dn / n \in \mathbb{Z}\}$ to be a basis for the topology ($d \neq 0$)
For every $p \in \mathbb{Z},\ p\mathbb{Z} = Y_{o,p}$ is open and closed.
$\mathbb{Z} \setminus \bigcup_{p \text{ prime}} p\mathbb{Z} = \{\pm 1\}$ is **not** open so $\exists\infty$-many primes. $\square$

Homework: Let $\hat{\mathbb{Z}}$ = completion of $\mathbb{Z}$ w.r.t. this topology. Then

1. $\hat{\mathbb{Z}} = \prod_p \hat{\mathbb{Z}}_p$ ($\hat{\mathbb{Z}}_p$ – p-adic integers).
2. The invertible elements of $\hat{\mathbb{Z}}$ is equal to $\overline{\mathcal{P}} \setminus \mathcal{P}$ (where $\mathcal{P} = \{p \in \mathbb{Z} | p \text{ prime}\}$
3. (2) is **exactly** Dirichlet primes on arithmetic progressions.

Expander Graphs in Number Theory

Alex Lubotzky
Einstein Institute of Mathematics, Hebrew University
Jerusalem 91904, ISRAEL

- Alexander Lubotzky, Discrete groups, expanding graphs and invariant measures. Reprint of the 1994 edition. Modern Birkhäuser Classics. Birkhäuser Verlag, Basel, 2010. iii+192
- Shlomo Hoory, Nathan Linial and Avi Wigderson, Expander graphs and their applications. Bull. Amer. Math. Soc. (N.S.) 43 (2006), no. 4, 439–561
- http://www.ams.org/meetings/national/jmm/2011_colloquium_lecture_notes_lubotzky_expanders.pdf

Thm (Dirichlet)

$b, q \in \mathbb{Z}$ with $(b,q) = 1$, $\exists\ \infty$ many primes in $b + q\mathbb{Z}$

or: $x \in \mathbb{Z}$, $\nu(x) = \#$ *prime factors of* x, *then for every* $b,\ q \in \mathbb{Z},\ \ \exists\, \infty\, x's$ *in* $b + q\mathbb{Z}$ *with* $\nu(x) \leq 1 + \nu\left((b,q)\right)$.

Twin Prime Conjecture

$\exists\ \infty$ *many* p *with* $p+2$ *also a prime,*

or: $\exists \infty$ *many* $x \in \mathbb{Z}$ *with* $\nu\left(x(x+2)\right) \leq\ 2.$

a stronger version TPC on arithmetic progressions.

A far reaching generalization (Schinzel):

- $\{0\} \neq \Lambda \leq \mathbb{Z}$ a subgroup, i.e. $\Lambda = q\mathbb{Z}$, $q \neq 0$ and $b \in \mathbb{Z}$
- θ = orbit of b under Λ $= b + q\mathbb{Z}$
- $f(x) \in \mathbb{Q}[x]$ a poly, integral on θ

Say: (θ, f) primitive if $\forall\ 2 \leq k \in \mathbb{Z}$,

$$\exists x \in \theta \ \text{ s.}t. \ \ (f(x), k) = 1.$$

Conjecture

If $f(x) \in \mathbb{Q}[x]$ is a product of t irreducible factors & (θ, f) primitive then $\exists \infty \ \ x \in \theta$ with $\nu(f(x)) \leq t$

Higher dimensional generalization

Conjecture (Hardy-Littlewood)

- $\Lambda \leq \mathbb{Z}^n$
- $\forall j,$ *the j-th coordinate is non-constant on* Λ
- $b \in \mathbb{Z}^n, \quad \theta = b + \Lambda$
- $f(\mathbf{x}) = x_1 \cdot \ldots \cdot x_n, \quad (\theta, f)$*-primitive.*

Then $\exists\ \infty$ many $x \in \theta$ with $\nu(f(x)) \leq n$
Moreover, this set is Zariski dense.

Note: H-L conj $\Rightarrow$ TPC:
take $b = (1,3) \in \mathbb{Z}^2$ and $\Lambda = \mathbb{Z}(1,1)$.

A famous special case:

Thm (Green-Tao (2008))

$\forall k \in \mathbb{N}$, *the set of primes contains an arithmetic progression of length* k.

Indeed: Look at $\mathbb{Z}^k$ and

$$\Lambda = \mathbb{Z} \cdot (1,1,\dots,1) + \mathbb{Z} \cdot (0,1,2,3,\dots,k-1)$$

Then the orbit of $(1,1,1,\dots,1)$ is the set

$$\{(m, m+n, m+2n, \dots, m+(k-1)n \mid m,n \in \mathbb{Z}\}.$$

H-L Conj says it has ∞ many vectors with prime coordinates.

H-L conj suggests a similar result for the orbit $\Lambda.b$ where $\Lambda \leq GL_n(\mathbb{Z})$. But never been asked maybe because of examples like this:

Ex: Let $\Lambda = \left\langle \left(\begin{smallmatrix} 7 & 6 \\ 8 & 7 \end{smallmatrix}\right) \right\rangle$ & $b = \binom{1}{1}$.

The orbit $\Lambda.b$ is in $= \left\{ \binom{x}{y} \in \mathbb{Z}^2 | 4x^2 - 3y^2 = 1 \right\}$
so: $3y^2 = 4x^2 - 1 = (2x-1)(2x+1)$
so y never a prime.

But there are extensions of H-L conj (and even results) and they came from expanders!

Sieve

For $x \in \mathbb{R}$, let

$$\mathbb{P}(x) = \{p \leq x | p \text{ prime}\}$$
$$P(x) = \prod_{p \in \mathbb{P}(x)} p$$
$$\pi(x) = |\mathbb{P}(x)|.$$

Prime Number Theorem

$$\pi(x) \sim \frac{x}{\log x}$$

R.H. is about the error term

An explicit formula for $\pi(x)$:

$$\pi(x) - \pi(\sqrt{x}) = -1 + \sum_{S \subseteq \mathbb{P}(\sqrt{x})} (-1)^{|S|} \left\lfloor \frac{x}{\prod_{p \in S} p} \right\rfloor$$

Proof: Inclusion exclusion.

But useless! Too many terms

Brun's Sieve

Let $f(x) = x(x+2)$
Let

$$S(f,z) := \sum_{\substack{n \le x \\ (f(n), P(z))=1}} 1 =$$

$$= \#\{n \le x |\ \text{all prime divisors of } f(n) \ \text{ are } \ > z\}$$

(so if z is "large", say x^δ then n has few prime divisors).

Recall $$\mu(n) = \begin{cases} 1 & n=1 \\ (-1)^r & n = p_1 \cdot \ldots \cdot p_r \text{ distinct} \\ 0 & \text{otherwise} \end{cases}$$

then $$\sum_{d|n} \mu(d) = \begin{cases} 1 & n=1 \\ 0 & n>1 \end{cases}$$

Then:

$$
\begin{aligned}
S(f,z) &= \sum_{\substack{n\le x\\ (f(n),P(z))=1}} 1\\
&= \sum_{n\le x} \sum_{d|(f(n),P(z))} \mu(d) =\\
&= \sum_{d|P(z)} \Big(\sum_{\substack{n\le x\\ f(n)\equiv 0(d)}} 1 \Big)
\end{aligned}
$$

Let $\beta(d) = \#\{m \mod d | \ f(m) \equiv 0(d)\}$
Running over all n's up to x, we cover approximately $\frac{x}{d}$ times the residues mod d, and approx $\frac{x}{d}\beta(d)$ of them give zeroes for f mod d.

So:

$$S(f,z) = \sum_{d|P(z)} \mu(d)(\frac{\beta(d)}{d}x + r(d))$$

$r(d)$ = error term.
$\frac{\beta(d)}{d}$ = multiplicative function of d.
Brun developed a method to analyze such sums and deduced $S(f,z) \geq C\frac{x}{\log(x)^2}$

Thm

$\exists\infty$ *many* n, *with* $v(n(n+2)) \leq 18$

World record toward TPC:
$\nu(n(n+2)) \leq 3$ (Chen).

His "combinatorial sieve" proved an "almost version" of H-L conj:

$b + \Lambda$ has ∞ many vectors of "almost" primes ($\#$ prime factors is bounded by $r = r(n)$).

Key observation for us: (Sarnak 2005) Brun's method works for $\Lambda.b$, $\Lambda \leq GL_n(\mathbb{Z})$ provided Λ has (τ) w.r.t. congruence subgroups $\Lambda(q) = Ker(\Lambda \to GL_n(\mathbb{Z}/q\mathbb{Z}))$ for q square-free!

The orbit $\Lambda.b$ is "counted/graded" by the balls of radius at most ℓ w.r.t. a fixed set of generators Σ of Λ.

$B(\ell) = \{\gamma \in \Lambda | \text{ length}_\Sigma(\gamma) \leq \ell\}$ acts on $b \in \mathbb{Z}^n$ and reduced mod $q \in \mathbb{Z}$.
Because of (τ), $B(\ell).b(\mod q)$ distributes almost uniformly over the vectors $\Lambda.b(\mod q)$

This is exactly the expander property!! So what we really need is "τ for $\Lambda \leq GL_n(\mathbb{Z})$ w.r.t. congruence subgroups $\Lambda(q), q$ square-free."

Let's take a little break from number theory to see what we have about
"τ w.r.t. congruence subgroups for subgroups Λ of $GL_n(\mathbb{Z})$".

Kazhdan property (T), Selberg Theorem, Ramanujan Conjecture, Jacquet-Langlands correspondence gave it for "most" arithmetic groups. General conj was formulated by Lubotzky-Weiss.
Solved (at least in char 0) by Burger-Sarnak and finally Clozel (2003).

All this for arithmetic groups $\Gamma = G(\mathbb{Z})$.

What about $\Lambda \leq G(\mathbb{Z})$ Zariski dense but of infinite index?
Zariski dense $\Rightarrow \Lambda$ is mapped onto $G(\mathbb{Z}/m\mathbb{Z})$ for most m's.
(Strong approximation for linear groups).
So: If $\Lambda = \langle S \rangle$ then $Cay(G(\mathbb{Z}/m\mathbb{Z}); S)$ is connected.
Are these expanders?

First challenge:

$$\Lambda = \left\langle \left(\begin{smallmatrix} 1 & 3 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 3 & 1 \end{smallmatrix}\right) \right\rangle; \text{ the } 1-2-3 \text{ problem.}$$

Partial results by Gamburd & Shalom (90's)

1st Breakthrough

Helfgott (2005 - 2008) If $A \subseteq G = SL_2(\mathbb{F}_p)$ ($\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$) a generating subset then,either

$$A \cdot A \cdot A = G \ \textbf{ or } \ |A \cdot A \cdot A| \geq |A|^{1+\varepsilon}$$

for some fixed $\varepsilon > 0$ (independent of p).

(Helfgott result was slightly weaker, this is a polished form "**the product property**")

This implies poly-log diameter for all generating set (Babai Conjecture)

Method "translating" via trace "sum-product results" from $\mathbb{F}_p$ to "product result" in $SL_2(\mathbb{F}_p)$

Thm (Bourgain-Katz-Tao)

If $A \subseteq \mathbb{F}_p$ *with* $p^{\delta} \leq |A| \leq p^{1-\delta}$, *then* $|A+A| + |A \cdot A| \geq c|A|^{1+\varepsilon}$ *where* c *and* ε *depend only on* δ.

2nd Breakthrough

Bourgain-Gamburd (2006 – 2010)

$$\forall 0 < \delta \in \mathbb{R}, \;\; \exists \varepsilon = \varepsilon(\delta) \in \mathbb{R} \;\text{ s.t. }\; \forall p, \forall S \subseteq SL_2(\mathbb{F}_p)$$

generating set:

if girth $(Cay(SL_2(\mathbb{F}_p); S)) \geq \delta \log p$ then $Cay(SL_2(\mathbb{F}_p); S)$ is an ε-expander.

The theorem applies for
(a) random generators
(c) every set of gen's of $SL_2(\mathbb{F}_p)$ coming from $\Lambda \leq SL_2(\mathbb{Z})$
In particular solved the 1-2-3 problem!

This motivated Bourgain-Gamburd-Sarnak to

a. formulate "affine sieve" method for "almost prime" vectors on orbits $\Lambda.b$ when $\Lambda \leq GL_n(\mathbb{Z})$ provided Λ has τ w.r.t. congruence subgroups $\mod q$, q-square free

b. proved "τ mod such q's" if $\bar{\Lambda}^{\text{Zariski}} \simeq SL_2$.

Even the special case (b) had some beautiful applications.

But the series of breakthroughs has not slowed down ...

Thm (Breuillard-Green-Tao/Pyber-Szabo (2010))

The "product theorem" of Helfgott holds $\forall$ finite simple group of Lie type of bounded Lie rank, i.e.,

$$\forall r \in \mathbb{N}, \ \exists\, \varepsilon = \varepsilon(r)$$
$$\forall\ G = G_r(\mathbb{F}_q)\ (e.g.\ SL_r(\mathbb{F}_q)) \ \ if\ A \subseteq G$$

generating set then either

$$A \cdot A \cdot A = G \ \ or \ \ |A \cdot A \cdot A| > |A|^{1+\varepsilon}$$

Thm (Salehi-Golsefidy - Varju (2011))

$\Lambda \leq GL_n(\mathbb{Z})$ *If* $G^0 = \bar{\Lambda}^0$*-the connected component of the Zariski closure of* Λ *- is perfect (e.g. semisimple), then*

$$\Lambda \text{ has } (\tau) \text{ w.r.t. } \Lambda(q) = Ker(\Lambda \to GL_n(\mathbb{Z}/q\mathbb{Z}))$$

for q *square-free*

Also: Bourgain-Varju; in some cases w.r.t. all q.

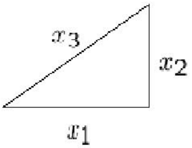
Thm (Salehi-Golsefidy - Sarnak (The Affine Sieve))

$\Lambda \leq GL_n(\mathbb{Z})$, $G^0 = \bar{\Lambda}^0$, *if the reductive part of* G^0 *is semisimple,* $b \in \mathbb{Z}^n$ *and* $f(\mathbf{x}) \in \mathbb{Q}[\mathbf{x}]$ *is integral on* $\theta = \Lambda.b$

Then $f(x)$ *has infinitely many almost prime values on* $\Lambda.b$.

Applications

(I) For integral right angle triangles $x_3^2 = x_1^2 + x_2^2$

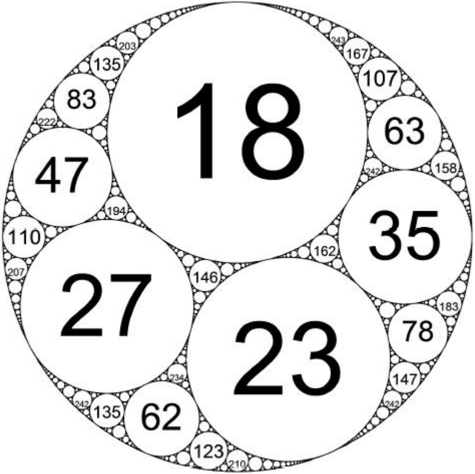


$6 | \frac{x_1 x_2}{2}$ = the area (ex!)
The solutions are on the orbit of $\Lambda.b$ with

$$\Lambda = O_F(\mathbb{Z}), \; F = x_1^2 + x_2^2 - x_3^2, \; b = \begin{pmatrix} 3 \\ 4 \\ 5 \end{pmatrix}$$

$\therefore \; \exists \; \infty$ triangles with areas almost prime.
Green-Tao 6 primes !

Integral Apollonian packing



see http://www.youtube.com/watch?v=DK5Z709J2eo

Apollonius Given three mutually tangents circles C_1, C_2, C_3, $\exists$ exactly two C_4, C_4' tangents to all three.

Descartes

The curvatures ($\frac{1}{\text{radii}}$) of C_4 and C_4' are solutions of

$$F(a_1, a_2, a_3, a_4) = 2(a_1^2 + a_2^2 + a_3^2 + a_4^2) - (a_1 + a_2 + a_3 + a_4)^2$$

$$\therefore a_4' = 2a_1 + 2a_2 + 2a_3 - a_4$$

So, start with 4 circles (e.g. (18, 27, 23, 146)) and apply:

$$S_1 = \begin{pmatrix} -1 & 2 & 2 & 2 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \qquad S_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 2 & -1 & 2 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

$$S_3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 2 & 2 & -1 & 2 \\ 0 & 0 & 0 & 1 \end{pmatrix} \text{ and } S_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 2 & 2 & 2 & -1 \end{pmatrix},$$

$$\Lambda = \langle S_1, S_2, S_3, S_4 \rangle$$

The affine sieve gives results like: ∞ many almost prime circles.

Many questions: ∞-many primes? How many?
∞-many "twin primes" (="kissing primes")? etc.
See notes for references.

Expander Graphs in Geometry

Alex Lubotzky
Einstein Institute of Mathematics, Hebrew University
Jerusalem 91904, ISRAEL

- Alexander Lubotzky, Discrete groups, expanding graphs and invariant measures. Reprint of the 1994 edition. Modern Birkhäuser Classics. Birkhäuser Verlag, Basel, 2010. iii+192
- Shlomo Hoory, Nathan Linial and Avi Wigderson, Expander graphs and their applications. Bull. Amer. Math. Soc. (N.S.) 43 (2006), no. 4, 439–561
- http://www.ams.org/meetings/national/jmm/2011_colloquium_lecture_notes_lubotzky_expanders.pdf

M = orientable n-dimensional closed hyperbolic manifold
(closed $\equiv$ compact without boundary,
hyperbolic $\equiv$ constant curvature -1).

Equivalently:

$$V = \mathbb{R}^{n+1}$$
$$f(x_1, \dots, x_n, x_{n+1}) = x_1^2 + \cdots + x_n^2 - x_{n+1}^2$$
$$G = SO(f) = \{A \in SL_{n+1}(\mathbb{R}) | f(A\overline{x}) = f(\overline{x})\} = SO(n, 1)$$

K = maximal compact subgroup $= SO(n)$
$\mathbb{H}^n = G/K = n$ - dim Hyperbolic space
$M = \Gamma \setminus G/K = \Gamma \setminus \mathbb{H}^n$
$\Gamma = \pi_1(M)$, Γ- torsion free cocompact lattice in G

geometry of $M \leftrightsquigarrow$ group theory of Γ

Conj (Thurston-Waldhausen)

M has a finite cover M_0 with $\beta_1(M_0) = \dim H_1(M_0, \mathbb{R}) > 0$.

Eq: Γ has a finite index subgroup Γ_0 with $\Gamma_0 \twoheadrightarrow \mathbb{Z}$.

Conj (Lubotzky-Sarnak)

*Γ does **not** have (τ), i.e. if $\Gamma = \langle S \rangle$*
*$\{Cay(\Gamma/N; S) | N \triangleleft \Gamma, [\Gamma : N] < \infty\}$ is **not** a family of expanders.*

Remark: Γ does not have (T).

Conj (Serre)

*For Γ arithmetic, Γ does **not** have the congruence subgroup property (CSP).*

(T-W) $\Rightarrow$ (L-S) $\Rightarrow$ (Se)

Why?
(T-W) $\Rightarrow$ (L-S)
since infinite abelian quotient implies no (τ).

(L-S)$\Rightarrow$ (Se) as we said: arithmetic groups have (τ) w.r.t. congruence subgroups (Selberg, ... , Clozel).

The most important case is $n = 3$, here we also have:

Conj (Virtual Haken)

$M = M^3$ has a finite cover which is Haken.

eq: Γ has finite index Γ_0 such that either $\Gamma_0 \twoheadrightarrow \mathbb{Z}$ or $\Gamma_0 = A \underset{C}{*} B (C \lneqq A, B)$.

Haken $\equiv$ contains an incompressable surface i.e. a properly embedded orientable surface $S(\neq S^2)$ with $\pi_1(S) \hookrightarrow \pi_1(M)$.

Most important open conj left for 3-manifolds (after Perelman).

First use of expanders in geometry (Lubotzky (1997))

Thm

Thurston-Waldhausen conj is true for arithmetic lattices in $SO(n,1)$, $\neq 3,7$.

Main pt: (The Sandwich Lemma)

$$G_1 \leq G_2 \leq G_3 - \text{simple Lie gps}$$
$$\Gamma_1 \leq \Gamma_2 \leq \Gamma_3 - \text{arithmetic lattices}$$
$$\Gamma_2 = G_2 \cap \Gamma_3, \Gamma_1 = G_1 \cap \Gamma_2$$

Then: (a) If Γ_1 has the Selberg property (i.e. τ w.r.t. congruence subgroups) and Γ_3 does not have (τ) then Γ_2 does **not** have the C.S.P.
(b) If Γ_1 has Selberg and Γ_3 has congruence $\Gamma_0 \twoheadrightarrow \mathbb{Z}$, then Γ_2 also has $\Gamma_0' \twoheadrightarrow \mathbb{Z}$.

After that Put $\Gamma \leq SO(n,1)$ as Γ_2 in such a Sandwich (use Galois cohomology, Selberg, J-L, Kazhdan-Borel-Wallach)

A second use (Lackenby 2005)

$n = 3$
An attack on the virtual Haken conjecture using (τ)

Heegaard splitting $M = M^3$ then $M = H_1 \cup H_2$ where H_1 and H_2 are two handle bodies glued along their boundaries $\partial H_1 \simeq \partial H_2$ - genus g surface.

Every M has such decomposition!
$g(M) =$ Heegaard genus of $M =$ the minimal g.

Thm (Lackenby)

$M = M^3$

$$\underset{\text{Cheeger Constant}}{\underset{\|}{h(M)}} \leq \frac{8\pi(g(M)-1)}{Vol(M)}.$$

So a first connection between expansion and $g(M)$.

Idea of Proof One can arrange Heegaard decomposition with approx. equal sizes (by volume). Area ∂H is given by Gauss-Bonnet.

Easy to see: $M_0 \twoheadrightarrow M$ finite cover

$$g(M_0) \leq [M_0 : M]g(M)$$

Define: for $\Gamma = \pi_1(M)$
$\mathcal{L} = \{N_i\}$ finite index normal subgroups of Γ, M_i-the covers

$$\text{Heegaard genus gradient} = \chi_{\mathcal{L}}(M) = \inf_i \frac{g(M_i)}{[M_i : M]}.$$

Ex: If M fibres over a circle (i.e., $\Gamma \twoheadrightarrow \mathbb{Z}$ with fin. gen. kernel) then $\chi_{\mathcal{L}}(M) = 0$

Conj (Heegaard gradient conj)

If $\chi_{\mathcal{L}}(M) = 0$ then $\exists$ finite sheeted cover which fibres over a circle.

Thm (Lackenby)

$M = M^3, \mathcal{L} = \{N_i\}$ finite index normal subgroups of $\Gamma = \pi_1(M)$, with corresponding covers $\{M_i\}$. If:

(1) $\chi_{\mathcal{L}}(M) > 0$, *and*

(2) Γ *does* **not** *have* (τ) *w.r.t.* $\mathcal{L}$.

Then M is virtually Haken.

Cor

Lubotzky-Sarnak conj (no (τ) for Γ) and Heegaard gradient conj ($\chi_{\mathcal{L}}(M) = 0 \Rightarrow$ fibres over S^1) imply the virtual Haken conj.

Several unconditional results

- Lackenby
- Lackenby-Long-Reid
- Long-Lubotzky-Reid

Sieve Method in Group Theory

We used the sieve method to sieve over the orbit of $\Lambda \leq GL_n(\mathbb{Z})$ acting on $\mathbb{Z}^n$.
But we can also use it for the action of Λ on itself!
It provides a way "to measure" subsets Z of Λ (a countable set)

w_k= the random k-step on $Cay(\Lambda; S)$.
Say Z of Λ is "exponentially small" if $Prob(w_k \in Z) < Ce^{-\delta k}$ for some constants $C, \delta > 0$.

Group Sieve Method

Thm

- $\Gamma = \langle S \rangle$ *finitely generated group.*
- $\mathcal{L} = \{N_i\}_{i \in I}$, $I \subseteq \mathbb{N}$, *finite index normal subgroups.*
- $Z \subseteq \Gamma$ *a subset.*

Assume: $\exists\, d \in \mathbb{N}^+$, $0 < \beta \in \mathbb{R}$ s.t.

(1) Γ has (τ) w.r.t. $\{N_i \cap N_j\}$

(2) $|\Gamma/N_i| \leq i^d$

(3) $\Gamma/(N_i \cap N_j) \simeq \Gamma/N_i \times \Gamma/N_j$

(4) $\left|ZN_i/N_i\right| \leq (1-\beta)|\Gamma/N_i|$

Then Z is exponentially small

Applications

I. Linear Groups

Thm (Lubotzky-Meiri (2010))

- $\Gamma \leq GL_n(\mathbb{C})$ *not virtually-solvable.*
- $2 \leq m \in \mathbb{N},\ Z(m) = \{g^m | g \in \Gamma\}$
- $Z = \bigcup_{2 \leq m \in \mathbb{N}} Z(m) =$ *proper powers*

Then Z is exponentially small in Γ.

History: -Malcev

- Hrushovski-Kropholler-Lubotzky-Shalev

II. The mapping class group

Fix $g \geq 1$, $MCG(g)$ = the mapping class group of a closed surface S of genus g = homeomorphisms modulo isotopic to the identity $\cong Aut(\pi_1(S))/Inn(\pi_1(S)) = Out(\pi_1(S))$.

This is a finitely generated group.

Thm (Rivin (2008))

The set of non pseudo-Anosov elements in the mapping class group $MCG(g)$ of a genus g surface is exponentially small.

History -Thurston
-Maher, Rivin
-Kowalski, Lubotzky-Meiri

Random 3-manifolds

The Dunfield-Thurston model:
Every $\varphi \in MCG(g)$ gives rise to a 3-mainfold M obtained by gluing 2 handle bodies H_1 and H_2 along $\partial H_1 \overset{\varphi}{\simeq} \partial H_2$.

Every 3-mfd is obtained like that!

Remember

$MCG(g)$ is a finitely generated group!

Fix a set of generators S. A random walk on $Cay(MCG(g); S)$ gives "random 3-mfd's" (with $g(M) \leq g$).

How does random 3-mfd behave?

Some results by Dunfield & Thurston.
Some by Kowalski.
A great potential for Sieve methods. Use $MCG(g) \to Sp(2g, \mathbb{Z})$.
(Work of Grunewald-Lubotzky gives many additional representations with arithmetic quotients which have property (τ) so one can apply sieve).