Sieve Methods in Group Theory

Alex Lubotzky
Hebrew University
Jerusalem, Israel

joint with: Chen Meiri

Primes

1 ② ③ ~~4~~ ⑤ ~~6~~ ⑦ ~~8~~ ~~9~~ ~~10~~ ⑪ ~~12~~ $\cdots$

Let $\mathbf{P}(x) = \{p \leq x | p \textbf{ prime}\}, \pi(x) = \#\mathbf{P}(x)$

To get all primes up to $\mathcal{N}$ and greater than $\sqrt{\mathcal{N}}$ - erase those which are divided by primes less $\leq \sqrt{\mathcal{N}}$.

Ex:

$$\pi(\mathcal{N}) - \pi(\sqrt{\mathcal{N}}) = \sum_{A \subseteq \mathbf{P}(\sqrt{\mathcal{N}})} (-1)^{|A|} \left[\frac{N}{\pi_{p \in A} p} \right]$$

Sieve methods are sophisticated inclusion-exclusion inequalities.

Dirichlet: **primes on arithmetic progression**

$\exists\infty$ many primes on $a + d\mathbb{Z}$ if $(a, d) = 1$.

Think of it as $\mathbb{Z}$ acts on $\mathbb{Z}$ by

$$n : z \mapsto z + nd$$

if $(a, d) = 1$ the orbit of a meets ∞ many primes.

Open problem(s): $\mathbb{Z}$ acts on $\mathbb{Z}^m$

n: $(a_1, \ldots, a_m) \to (a_1, \ldots, a_m) + n(d_1, \ldots, d_m)$ are there ∞ many vectors on the orbit whose coordinates are all primes?

e.g. $n : (1, 3) \to (1, 3) + n(1, 1)$
Twin prime conjecture!

But true for $\mathbb{Z}^r, r \geq 2$ acting on $\mathbb{Z}^m$ (Green-Tau-Zigler).

but **Brun's sieve:** there exist ∞ many almost primes, i.e. $\exists$ a constant c s.t. the orbit has ∞ many vectors $(v_1, \ldots, v_m)$ where coordinates are product of at most c primes.

Affine Sieve Method

(Sarnak, Bourgain-Gamburd, Helfgott, Breuillard-Tao-Green, Pyber-Szabo, Salehi-Golsefidy–Varju)

Let $\Gamma \leq \mathrm{GL}_\mathrm{m}(\mathbb{Z})$ be a finitely generated infinite subgroup.
Assume $G = \bar{\Gamma}^Z$ = Zariski closure of Γ is such that G^0 has no central torus (e.g. G semi-simple), $v \in \mathbb{Z}^m$. Then Gv has ∞ many almost primes.

Key point: (Salehi-Golsefidy–Varju)

$$\Gamma \leq \mathrm{GL_n}(\mathbb{Z}), \quad \Gamma = \langle \mathrm{S} \rangle, |\mathrm{S}| < \infty, \mathrm{G}^0 = (\bar{\Gamma})^0 \text{ perfect}$$

$$q \in \mathbb{N}, \quad \pi_q : \mathrm{GL_n}(\mathbb{Z}) \to \mathrm{GL_n}(\mathbb{Z}/\mathrm{q}\mathbb{Z})$$

Then the Cayley graphs

$$Cay(\pi_q(\Gamma); \pi_q(S))$$

form a family of *expanders* when q runs over square-free integers (and conj: for all q).

Property (τ)

Expanders

X k-regular graph on n vertices.

A_X = adjacency matrix of X

an $n \times n$ matrix, e.v.'s

$$\lambda_0 = k \geq \lambda_1 \geq \cdots \geq \lambda_{n-1}.$$

Def: A family of k regular graphs (k fixed, $n \to \infty$) is a family of expanders if $\exists \varepsilon > 0$ s.t. $\lambda_1 \leq k - \varepsilon$ for all of them.

Main point: In a family of expanders X_i the random walk on X_i converges to the uniform distribution exponentially fast and uniformly on i.

The expansion property enables to apply Brun's method in this non-commutative setting!

In the classical case (number theory) we know the "error term" of taking $[1, 2, \dots, \mathcal{N}]$ mod q when $q \leq \sqrt{\mathcal{N}}$. Here we need to know that the ball of radius n in Γ w.r.t. S (with $\mathcal{N} \approx C^n$ points) is mapped approx uniformly to $\pi_q(\Gamma)$ for $q \sim \mathcal{N}^\delta$.

Up to now, Γ is acting on $\mathbb{Z}^n$.
Let now Γ act on itself!

The Group Sieve

How to measure sets in countable group?

Ex: $G = SL_n(\mathbb{C})$, For almost every $\gamma \in G$, $C_G(g)$ is abelian.
Pf: Almost every $\gamma \in G$ is diagonalizable with distinct eigenvalues. $\square$

What about a similar property for $\Gamma = SL_n(\mathbb{Z})$?
How to measure a subset Y of Γ?

Basic setting:

Let $\Gamma = \langle S \rangle$ a finitely generated group $|S| < \infty$, $S = S^{-1}$, $1 \in S$.
A random walk on Γ (or better on $Cay(\Gamma; s)$) is $(w_k)_{k\in\mathbb{N}}$, with $w_0 = e$ and $w_{k+1} = w_k \cdot s$ with $s \in S$ chosen randomly.

For a subset $Y \subseteq \Gamma$ put:

$$p_k(\Gamma, S, Y) = Prob(w_k \in Y) =$$

"probability the walk visits Y in the k-th step"

The Basic Theorem:

Let $\{\mathcal{N}_i\}_i \in \mathbb{N}$ be a sequence of finite index normal subgroups of $\Gamma, \Gamma_i = \Gamma/\mathcal{N}_i$. Assume $\exists d \in \mathbb{N}, \varepsilon > 0$ and $\beta < 1$ s.t.

(1) $\forall i \neq j \in \mathbb{N}, Cay(\Gamma/\mathcal{N}_i \cap \mathcal{N}_j; S)$ are ε-expanders.

(2) $|Y_i|/|\Gamma_i| \leq \beta$ where $Y_i = Y\mathcal{N}_i/\mathcal{N}_i$

(3) $|\Gamma_i| \leq i^d$

(4) $\Gamma/\mathcal{N}_i \cap \mathcal{N}_j \stackrel{\sim}{\to} \Gamma/\mathcal{N}_i \times \Gamma/\mathcal{N}_j$

Then $\exists \tau > 0$ s.t. $p_k(G, S, Y) \leq e^{-\tau k}$ for every $k \in \mathbb{N}$ (i.e. Y is exponentially small).

A typical example:

$\Gamma = \mathrm{SL_m}(\mathbb{Z})$ (or a Zariski dense subgroup).

$\mathcal{N}_p = Ker(\mathrm{SL_m}(\mathbb{Z}) \to \mathrm{SL_m}(\mathbb{Z}/\mathrm{p}\mathbb{Z}))$
p-prime.

$Y \subseteq \Gamma$ an interesting subset.

Easy cases: Y a subvariety; $\mathrm{SL_{n-1}}(\mathbb{Z})$, the unipotent elements, non semisimple elements

cor: each of these sets is exponentially small.

Compare to: Almost every element of $\mathrm{SL_m}(\mathbb{C})$ is semisimple.

Compare to works of Borovick, Kapovich, Myasnikov, Schupp, Shpilrain ...

also: Arzhantseva-Ol'shanskii and of course Gromov, $\cdots$ random groups;

also: Bassino-Martino-Nicaud-Ventura-Weil.

Our main application: *Powers in linear groups*

Background:

Malcev (60's):

Γ fin. gen. nilpotent group, $m \in \mathbb{N}$, then the **set** $\Gamma^m = \{x^m | x \in \Gamma\}$ contains a finite index subgroup of Γ (like in $\mathbb{Z}^r$).

Hrushovski-Kropholler-Lubotzky-Shalev (1995) If Γ is either a solvable or linear fin. gen. group s.t. Γ^m contains a finite index subgroup of Γ, then Γ is virtually nilpotent.

Remark:

$\exists$ solvable Γ (not virt. nilp.) with Γ^m contains a **coset** of finite index subgroup, but for non-solv linear Γ^m is never "of finite index".

Thm (Lubotzky-Meiri): Let Γ be a fin. generated subgroup of $\mathrm{GL_d}(\mathbb{C})$ that is not virtually solvable. Then

$$Y = \{g \in \Gamma | \exists m \geq 2, \ x \in \Gamma \text{ s.t. } g = x^m\}$$
$$= \bigcup_{m \geq 2} \Gamma^m$$

is exponentially small.

Note:

Much stronger than [HKLS]:

(i) There only "not of finite index", here a quantitative estimate – "exp small"

(ii) All m's together!

It is possible to prove (ii) only due to (i)!

Open problem: The set of commutators in Γ (even $\Gamma = \mathrm{SL}(3, \mathbb{Z})$).

Other applications:

Thm (Breuillard-de Cornulier-Lubotzky-Meiri)

Γ a fin. gen. group, $\Gamma = \langle S \rangle$.
$Cn(\Gamma) = \#$ conj classes of Γ represented by elements of length $\leq n$ w.r.t. S.

If Γ is non-virt-solvable linear group then $Cn(\Gamma)$ grows exponentially

(conj by Guba & Sapir).
True also with # characteristic polynomials.

Thm (Lubotzky-Rosenzweig)

Γ a finitely generated group $\leq \mathrm{GL_n}(\mathbb{F})$

$\mathbb{F}$ a finitely generated field, $char = 0$,
$G = \bar{\Gamma}$

G^0 without central torus

$\exists$ Π: $G/G^0 \to$ FINITE GROUPS

s.t. $P_r(Gal(\mathbb{F}(\gamma)/\mathbb{F}) \neq \Pi(\gamma G_0))$ is exponentially small

$\mathbb{F}(\gamma)$ = splitting field of the characteristic poly of γ.

This generalizes special cases by Rivin, Jouve, Kowalski, Zywina

(compare: Gallagher, Prasad-Rapinchuk, Gorodnik-Nevo)

Thm: (Rivin, Kowalski)

Γ = mapping class group = $MCG(g)$

Then the **non** pseudo-Anasov elements is an exp. small subset

Conj of Thurston (see also Maher).

Thm: (Lubotzky-Meiri)/(Malestein-Souto)

A similar result for the Torelli subgroup $Ker(MCG(g) \to Sp(2g, \mathbb{Z}))$

(asked by Kowalski)

Analogous results for $Aut(Fn)$

Thm: (Rivin, Kapovich)
The non iwip and the non hyperbolic elemnts of $Aut(F_n)$ are exp. small subsets.

Thm: (Lubotzky-Meiri)
A similar result for
$IA(F_n) = Ker(Aut(F_n) \to GL_n(\mathbb{Z}))$

The key ingredient for the last result:
Let $A = Aut(F_n)$, and $|G| < \infty$.
$\pi : F_n \twoheadrightarrow G, R = Ker(\pi)$.
$\Gamma(\pi) = \{\alpha \in A | \pi \circ \alpha = \pi\}$

Then $[A : \Gamma(\pi)] < \infty$ and $\Gamma(\pi)$ preserves R and induces $\bar{\pi} : \Gamma \to GL(\bar{R} = R/[R, R])$.
The image is in $C_G(\bar{R})$ and:

Thm(Grunewald-Lubotzky) under suitable conditions, $Im(\Gamma(\pi))$ is an arithmetic group (and so is $Im(IA(F) = Torelli)$).

This enables to apply the above machinery.

Potentials applications

Apply sieve method on MCG to get results on random 3-manifolds á la Dunfield & Thurston.