Talk 1 of Mini Course 3 by Emmanuel Kowalski

"Sieve in discrete groups"

References:

① CUP 2008

② Bourbaki report. Exp 10.28.

§ 1: What is sieve?

Local global principle:

Notation: Γ discrete group

$\Gamma \xrightarrow{\rho} GL_n(\mathbb{Z})$. homomorphism.

Examples: (1) $\Gamma = \mathbb{Z}$.

(2) $\Gamma \subset SL_n(\mathbb{Z})$, Γ: Zariski-dense in SL_n.

($\Gamma = SL_n(\mathbb{Z})$).

(3) Γ = mapping class-group of a closed surface of genus g.

$\Gamma \twoheadrightarrow Sp_{2g}(\mathbb{Z})$.

Local information:-

$\Gamma \xrightarrow{\rho} GL_n(\mathbb{Z}) \xrightarrow{\rho_p} GL_n(\mathbb{Z}/p\mathbb{Z})$

gives $\Gamma \longrightarrow \Gamma_p = \mathrm{Im}(\rho_p \circ \rho)$ for some finite group Γ_p.

Example ① $\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}$

② (strong approximation) for $p \geq p_0(\Gamma)$, we have $\Gamma_p = SL_n(\mathbb{Z}/p\mathbb{Z})$.

③ $\Gamma_p = Sp_{2g}(\mathbb{F}_p)$ for all p.

- we need some independence of the ρ_p modulo distinct primes.
- we require that for $p_1, \ldots, p_r$ distinct $\Gamma \longrightarrow \prod_{i=1}^{r} \Gamma_{p_i}$, is still onto.
- (If not, one must reformulate the problem).

Example. ① Chinese Remainder theorem.

② OK if all p_i's are $\geq p_0(\Gamma)$.

③ OK.

We want to say something about $X \subset \Gamma$ of the type $X = \{ \gamma \in \Gamma : \gamma \bmod p \notin \Omega_p \subset \Gamma_p \}$ for all $p \in P$ (subset of primes)

for some $\Omega_p \subset \Gamma_p$.

• Example: ① $\Omega_p = \{0, -2\} \subset \mathbb{Z}/p\mathbb{Z}$

$$X \cap \{1, \dots, N\} = \{ n \le N : p \nmid n, p \nmid n+2 \text{ for all } p \le Q \}.$$

for $P = \{ p \le Q \}$.

• If $Q \simeq \sqrt{N}$, then $X \cap \{1, \dots, N\} = \{ p \le N, p > Q, p+2 \text{ prime} \}$.

② [Affine Sieve] (Bourgain-Gamburd-Sarnak)

Let $f : SL_n(\mathbb{Z}) \longrightarrow \mathbb{Z}$ polynomial non-constant.

(e.g. $f(g) = \prod_{1 \le i,j \le n} a_{ij}$).

Let $\Omega_p \subset \Gamma_p$ be $\{ g \in \Gamma_p : f(g) = 0 \pmod p \}$.

$$P = \{ p \ge p_0, p \le Q \}.$$

$X = \{ \gamma \in \Gamma : f(g) \text{ has no prime factor} < Q$
except $p \le p_0 \}$.

$X \cap \{ \gamma \in \Gamma : |f(\gamma)| \le N \}$.

· If $Q = N^\beta$ for some $\beta > 0$, then $\gamma \in X$ has $\le \frac{1}{\beta}$ prime factors or $f(\gamma) = 0$.

(3) see Thursday.

§2. Implementing:

The size of X can be measured in different ways.

Method 1:- Fix a norm $\|\cdot\|$ on $GL_n(\mathbb{R})$ and try to estimate $|X \cap \{\gamma \in \Gamma : \|\gamma\| \le T\}|$ as $T \to \infty$.

(Here one uses typically spectral or ergodic counting methods). (related to talks of (renewal) Hee Oh, A. Kontorovich)

Method 2:- Fix $S = S^{-1}$, finite symmetric generating set and let ℓ_S be the word-length

Estimate. $|X \cap \{\gamma \in \Gamma : l_S(\gamma) \le N\}|$ as $N \to \infty$?

Problem: often $\{\gamma \in \Gamma \mid l_S(\gamma) \le N\}$ not known.

• (Exception: Γ free, see Bourgain-Gamburd-Sarnak).

Method-3:- Fix S as above.

$$\frac{1}{|S|^N} \left| \{(s_1, \dots, s_N) \in S^N : s_1 \cdots s_N \in X\} \right|$$

as $N \to \infty$. $(= P(Y_N \in X)$, where $Y_N = s_1 \cdots s_N$ is a random walk on $\Gamma)$.

$(\because F_S \to \Gamma \to GL_n(\mathbb{Z}))$

• Link with expanders:

Fix p; one needs to understant —

$|\{\gamma \in \Gamma : \gamma \equiv \gamma_0 \pmod p\}|$ for $\gamma_0 \in \Gamma_p$, $T \to \infty$.

• If $1 \in S$, $\left| P(Y_N = \gamma_0 \pmod p) - \frac{1}{|\Gamma_p|} \right| \le \rho_{\Gamma,p}^N$

for $\rho_{\Gamma,p} < 1$, the spectral radius of the averaging operator.

$$\varphi : \Gamma_p \longrightarrow \mathbb{C}$$

$$(M\varphi)(x) = \frac{1}{|S|} \sum_{s \in S} \varphi(xs).$$

restricted to functions of mean 0.

$$\left(\sum_{x \in \Gamma_p} \varphi(x) = 0 \right).$$

Modulo $q = p_1 \cdots p_r$, square free.

$$\left| \mathbb{P}(Y_N = \gamma_i \pmod{p_i},\ 1 \le i \le r) - \frac{1}{\prod_{i=1}^{r} |\Gamma_{p_i}|} \right|$$

$$\le \rho_{\Gamma,q}^{N}$$

for some $\rho_{\Gamma,q} < 1$.

- Hence, we have good control of reductions modulo q square free.

If $(\mathcal{C}(\Gamma_q ; S \bmod q))_q$ - square free., is an expander; so that

$$\Gamma_q = \prod_{p \mid q} \Gamma_p.$$

$\exists \rho < 1,\ \rho_{\Gamma,q} \le \rho < 1, \forall q$

what should one expect.

$$\mathbb{P}(Y_N \in X) \approx \prod_{p \in P} \left(1 - \frac{|\Omega_p|}{|\Gamma_p|}\right) -$$

heuristically.

· Small sieves

we assume $\frac{|\Omega_p|}{|\Gamma_p|} = \frac{K}{p} + O\left(\frac{1}{p^2}\right)$.

(or something like this on average for some $K > 0$).

(typically $\Omega_p = Y(\mathbb{F}_p)$, where $Y \subset SL_n$ has codimension 1)

Theorem (B-G-S : affine sieve)

$\Gamma \subset SL_n(\mathbb{Z})$, Zariski-dense in SL_n.

(finitely generated) $f : SL_n(\mathbb{Z}) \longrightarrow \mathbb{Z}$ polynomial non-constant.

By Varju's theorem, the

$$\left(\mathcal{C}\left(SL_n(\mathbb{Z}/q\mathbb{Z}) \setminus \{r \bmod q : f(r) = 0 \pmod p\}\right)\right)_{q\text{-sqf}}$$ is an expander.

Brun's Sieve,

then there exists $\gamma > 1$, $\gamma = \gamma(P_0, \ell, K)$

s.t. $P(Y_N \in X) \geq c(\gamma) \frac{1}{N^K}$, for some

$c(\gamma) > 0$, if $P = \{p \leq \gamma^N\}$.

$$\prod_{p \leq \gamma^N} \left(1 - \frac{K}{p}\right) \sim \frac{1}{(\log \gamma^N)^K}$$

Corollary:- $\Omega_p = \{\gamma : f(\gamma) = 0\}$

$\exists \ \Omega = \Omega(\gamma, K)$.

s.t. $\{\gamma \in \Gamma : f(\gamma) = 0$ or has $\leq \gamma$ prime factors$\}$

is Zariski-dense in SL_n.

Remarks:- ① $\{n^2 : n \in \mathbb{Z}\} \subset \mathbb{Z}$ is Zariski-dense.

Is it conceivable that -

$\{\gamma \in \Gamma : f(\gamma)$ has $\leq \gamma$ prime factors$\}$.

$\subset \{\gamma \in \Gamma : a_{ij}(\gamma)$ is a square $\forall i, j\}$.

(2). What is γ ??

It depends - on K

- $\boxed{S}$ = spectral radius.

Theorem (Kowalski) $\Gamma = \left\langle \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} \right\rangle$

p prime $\neq 3$; $\rho_{\Gamma,p} \leq 1 - 2^{-32}$, for $p \geq 2^{2^{47}}$.