Lecture 4

Recall: (Γ_n) expander

$\Updownarrow$

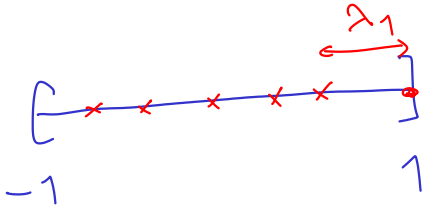
(i) $|\Gamma_n| \longrightarrow +\infty$

(ii) $\exists k, \forall n, \forall x \in V_n, \ val(x) \leq k$

$\frac{|E(w)|}{|w|}$

$\min_{1 \leq |w| \leq \frac{|V|}{2}}$

$\begin{cases} \text{(iii)} \quad \exists c>0, \ \forall n, \ h(\Gamma_n) \geq c \\ \Updownarrow \\ \text{(iii)}' \quad \exists c>0, \ \forall n, \ \lambda_1(\Gamma_n) \geq c \end{cases}$



$$M_n f(x) = \frac{1}{val(x)} \sum_{x,y} a(x,y) f(y)$$

Prop. [lecture 2, Prop. 2.24]

G finite group

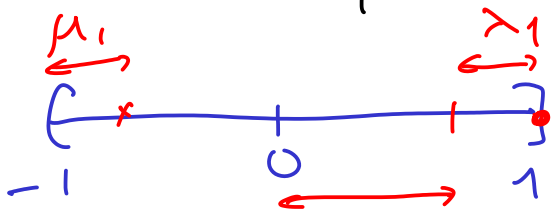
$1 \in S = S^{-1} \subset G$ symmetric generating set

$\Gamma = \mathcal{C}(G, S)$

For $g \in G$, $n \geq 1$,

$$\left| \frac{1}{|S|^n} \left| \{(s_1, \dots, s_n) \in S^n \mid s_1 \cdots s_n = g\} \right| - \frac{1}{|G|} \right| \leq \rho^n$$

where ρ = spectral radius of M_Γ on $\underline{1}^\perp$.



$\rho = \max(1-\lambda_1, 1-\mu_1)$

(to be corrected in statement in lecture 3!)

Proof -

[Notation: $\frac{1}{|S|^n} |\{(s_1, \dots, s_n) \in S^n \mid (\text{something})\}|$

$= \mathbb{P}((\text{something}))$,

$\frac{1}{|S|^n} \sum_{(s_1, \dots, s_n) \in S^n} f(s_1, \dots, s_n) = \mathbb{E}(f(s_1, \dots, s_n))$]

We want to understand

$p_n = \mathbb{P}(s_1 \cdots s_n = g)$

$\|$

$\mathbb{E}(\varphi(s_1 \cdots s_n))$

where φ = characteristic function of $g \in G$.

We expect $p_n \simeq \frac{1}{|G|}$, and the

reason this is natural is that

$$\frac{1}{|G|} = \frac{1}{|G|} \sum_{x \in G} \varphi(x)$$

is the average of φ over G.

So if we write

$$\varphi = \frac{1}{|G|} + \varphi_0$$

then $\mathbb{E}(\varphi(s_1 \cdots s_n)) = \frac{1}{|G|}$

$$+ \underbrace{\mathbb{E}(\varphi_0(s_1 \cdots s_n))}_{q_n}$$

Goal: show that $q_n \to 0$ (as fast as possible)

Formula: for any $f: G \to \mathbb{C}$, we have

$$\mathbb{E}(f(s_1 \cdots s_n)) =$$

$$\frac{1}{|S|^{n-1}} \sum_{(s_1,\dots,s_{n-1}) \in S^{n-1}} (M_r f)(s_1 \cdots s_{n-1})$$

$$= \mathbb{E}_{n-1}\left(M_r f(s_1 \cdots s_{n-1}) \right)$$

So

$$q_n = \mathbb{E}_{(n)}\left(\varphi_0(s_1 \cdots s_n) \right)$$

$$= \mathbb{E}_{(n-1)}\left(M_r \varphi_0(s_1 \cdots s_{n-1}) \right)$$

$$\vdots$$

$$= \mathbb{E}_{(0)}\left(M_r^n \varphi_0(1) \right)$$

$L \in G$

$$= \left(M_r^n \varphi_0 \right)(1)$$

We can bound this

$$\left| \left(M_r^n \varphi_0 \right)(1) \right| \le \| M_r^n \varphi_0 \|_\infty$$

$$\le |G|^{1/2} \| M_r^n \varphi_0 \|_{L^2}$$

(since $\|f\|_\infty \leq |G|^{1/2} \|f\|_2$

because

$$|f(x)|^2 \leq \sum_y |f(y)|^2 = |G| \|f\|_2^2 \Big)$$

$$\leq |G|^{1/2} \rho^n \|\varphi_0\|_{L^2}$$

(since $\varphi_0 \perp 1$, by def. of Γ).

Now since φ_0 is orthogonal projection of φ on $1^\perp$, we have

$$\|\varphi_0\|_{L^2} \leq \|\varphi\|_{L^2} = \sqrt{\frac{1}{|G|}}.$$

$$\left[\|\varphi\|_2^2 = \|\varphi_0\|_2^2 + \|\langle \varphi, 1 \rangle\|^2 \right]$$

$\longrightarrow$

$$\boxed{q_n \leq \rho^n}$$

□

Proof of formula:

$$\frac{1}{|S|^n} \sum_{(s_i) \in S^n} f(s_1 \dots s_n)$$

$$= \frac{1}{|S|^{n-1}} \sum_{(s_i) \in S^{n-1}} \underbrace{\frac{1}{|S|} \sum_{s_n \in S} f((s_1 \dots s_{n-1}) s_n)}_{g(s_1 \dots s_{n-1})}$$

where $g(x) = \frac{1}{|S|} \sum_{s \in S} f(xs)$

$$\left(\begin{array}{l} \text{by def. of} \\ \mathcal{C}(G,S) \end{array} \right) = (M_n f)(x)$$

□

A sketch of an application [§5.3]

Theorem (Lubotzki - Meiri, 2012?)

Let $1 \in S = S^{-1}$ be a finite generating set of $SL_3(\mathbb{Z})$ [or $SL_m(\mathbb{Z})$, $m \geq 2$].

There exists $c, c' > 0$ s.t.

$$\frac{1}{|S|^n} \left| \{ (s_1, \dots, s_n) \in S^n \mid \begin{array}{l} \exists\ h \in SL_3(\mathbb{Z}), \\ \exists\ m \geq 2, \\ h^m = s_1 \cdots s_n \end{array} \} \right|$$

$$\leq c\, e^{-c'n}, \text{ for } n \geq 1.$$

Proof combines:

(1) expander properties of quotients of $SL_3(\mathbb{Z})$ [recall Property (T)].

(2) sieve methods

(3) prime number theory (Siegel-Walfisz Th.)

(4) (geometric) group theory

Idea: first, fix m.

Observation: for any p, we have

$$\mathbb{P}(s_1 \cdots s_n = h^m) \leq \mathbb{P}(s_1 \cdots s_n \bmod p = h^m \bmod p) \quad (\text{for some } h)$$

and the RHS can be estimated using equidistribution: it is

$$\sum_{\text{all } x \in SL_3(\mathbb{F}_p) \text{ of the form } h^m} \mathbb{P}(s_1 \cdots s_n \bmod p = x)$$

$$= \frac{1}{|SL_3(\mathbb{F}_p)|} |\{h^m\}| + \underbrace{O\left(|SL_3(\mathbb{F}_p)| p^{n}\right)}_{= O\left(p^{g} p^{n}\right)}.$$

However, the best one can show about [redacted] is something like:

Lemma. If $p \equiv 1 \bmod m$ then

$$\frac{1}{|SL_3(\mathbb{F}_p)|} |\{h^m\}| \leq 1 - \frac{5}{72}$$

(only $\frac{p-1}{m}$ elements of $\mathbb{F}_p^\times$ are m-th powers)

Now continue with $p \equiv 1 \bmod m$.

The bound above is still only $1 - \frac{5}{72} + O(-)$

but at least this is uniform with respect to ρ because $\exists \rho < 1$ s.t. $S\rho \leq \rho$ for all ρ by expansion.

This means: $\exists\ A > 1$ s.t.

The bound is

$$\leq 1 - \frac{5}{72} + \frac{1}{100}$$

for $p \leq A^n$, $p \equiv 1 \bmod m$.

Next idea: use sieve to combine information from many primes.

Prop. ("large sieve"; Linnik; Rényi-Turan; K.; L-M; Peled)

$\exists\ c_1 > 0$
$\exists\ A > 1$ s.t.

$$\mathbb{P}(s_1 \cdots s_n = h^m) \sim$$

$$\leq c_1 \frac{1}{H_m} = O\left(\frac{nm}{A^n}\right)$$

where $H_m = \sum_{\substack{p \leq A^n \\ p \equiv 1 \pmod m}} \frac{1}{p} \gg_m \frac{1}{\varphi(m)} \frac{A^n}{n}$

Prime Number Th. in arith. prog.

[cf. Exercise 3.3]

This gives a statement for fixed m.

How to handle all $m \geq 2$?

. Finitely many : OK ✓

. Polynomially many in terms of n is OK: say we look at all $m \leq 10n^4$

Then we need to bound from below

$$\sum_{\substack{p \le A^n \\ p \equiv 1 \bmod m}} 1$$

uniformly for $m \le 10n^4$; note

$$10n^4 = O\left((\log A^n)^4\right)$$

so this is within Siegel-Walfisz territory:

$$\sum_{\substack{p \le A^n \\ p \equiv 1 \bmod m}} 1 \gg \frac{1}{\varphi(m)} \frac{A^n}{\log A^n}$$

uniformly for $m \le (\log A^n)^C$ (for any C)

Last step: handle large m's

a priori by following [5.3.4]

Lemma: There exists $c_2 > 0$ s.t.: If $g = s_1 \cdots s_n$ in $SL_3(\mathbb{Z})$, $s_i \in S$, and $g = h^m$ for some $\begin{cases} m \geq 2 \\ h \in SL_3(\mathbb{Z}) \end{cases}$.

Either:

(1) all eigenvalues of h are (cubic) roots of unity ($\Rightarrow$ same for g)

(2) $m \leq c_2^n$ — done above ✓

Idea: if h has an eigenvalue not a root of unity, it has an eigenvalue λ, $|\lambda| > 1$, then $h^m = g$ has eigenvalue λ^m

which is very large, in particular

$$\|g\| \geq |\lambda|^m$$

which is incompatible with

$$g = s_1 \cdots s_n$$

if m is too large compared with n. (Comparison between the length n of g as a product of generators and $\|g\|$, an analytic distance).

Final step: handle separately the case where all eigenvalues of $g = s_1 \cdots s_n$ are cube roots of unity. This also uses expansion but is easier!

Q. Large sieve?

$\Omega_p \subset \mathbb{F}_p$

Arithmetic version:

$$\left| \{ n \le N \mid n \bmod p \notin \Omega_p \text{ for } p \le Q \} \right|$$

[ex. $\Omega_p = \{0\}$ $\longrightarrow$ n coprime to all $p \le Q$

Ω_p = non-squares

$\longrightarrow$ don't get any squares]

$$\le \frac{N + Q^2}{\sum_{p \le Q} \frac{|\Omega_p|}{p}} \le Q$$

[so we should typically take $Q^2 \le N$]

Discrete group version:

G group, $G \to \Gamma_p$ finite quotients

$1 \in S = S^{-1}$ gen. set (finite)

$\Omega_p \subset \Gamma_p$

$$\frac{1}{|S|^n} \left| \{ (s_1, \dots, s_n) \mid \forall p \le Q, \right.$$
$$\left. s_1 \cdots s_n \bmod p \notin \Omega_p \} \right|$$

$$\ll \frac{1}{\sum_{p \le Q} \frac{|\Omega_p|}{|\Gamma_p|}}$$

provided $Q \le \boxed{A^n}$ for some $A > 1$ determined by expansion properties (under certain assumptions on $G \to \Gamma_p$)

[cf Th. 5.3.1]

(cf. "The large sieve and its applications")