Subgroup Growth of Lattices in Semisimple Groups

Subgroup growth

Let Γ be a finitely generated group

$$a_n(\Gamma) = \#\{H \leq \Gamma \mid [\Gamma : H] = n\}$$

$$s_n(\Gamma) = \#\{ \qquad\qquad \leq n\}$$

Prop: $a_n(\Gamma) = \dfrac{t_n(\Gamma)}{(n-1)!}$ where

$$t_n(\Gamma) = \#\{\text{transitive homo } \Gamma \to S_n\}$$

Ex: $\Gamma = F_d$ = free group on $d \geq 2$ gen's.

$$a_n(\Gamma) \approx \frac{(n!)^d}{(n-1)!} = n(n!)^{d-1}$$

Cor: $\lim_{n\to\infty} \dfrac{\log s_n(F_d)}{\log(n!)} = -(1-d) = -\chi(F_d)$

Theorem (Liebeck-Shalev, Muller-Puchta)

Let $H = PSL_2(\mathbb{R})$ and Γ a lattice in H. Then

$$\lim_{n\to\infty} \frac{\log s_n(\Gamma)}{\log n!} = -\chi(\Gamma)$$

method of pf: counting $\mathrm{Hom}(\Gamma, S_n)$ is counting # of sol's of equations in S_n.

For a Fuchsian gp the equations are of types $[x,y]$, x^l and convolutions.

Express # by characters of S_n.

main work: estimate of character values.

Theorem (Lubotzky – Nikolov)

Let H be a simple Lie group of $\mathbb{R}$-rank ≥ 2 (e.g. $H = PSL_d(\mathbb{R})$, $d \geq 3$) and Γ a non-uniform lattice in H. Assume $H \not\cong D_4(\mathbb{C})$. Then

$$\lim_{n\to\infty} \frac{\log s_n(\Gamma)}{(\log n)^2/\log\log n} = \gamma(H)$$

where $\gamma(H)$ is a number easily calculated from the root system of H.

So: 1) limit exists.

2) independent of Γ only on H. (compare to the Furstenberg-Mostow-Margulis philo: lattices in the same Lie gp are "similar" – e.g. super-rigidity, word metric versus Riem. metric)

3) Conj The same hold for all H and all Γ.

Theorem H as before, $X = H/K$ a sym space, M a finite volume non-compact manifold covered by X. Let $b_n(M) = \#\leq n$-sheeted covers of M. Then:

$$\lim \frac{\log b_n(M)}{(\log n)^2/\log\log n} = \mathrm{vol}(H)$$

In spite of the geometric formulation the proof involves a lot of number theory since:

1) Margulis Theorem: Every lattice in H is arithmetic

2) Serre Conjecture: Every such lattice has the congruence subgroup property

Serre's conj is proved for "most" cases.

Counting congruence subgroups

Let k be a number field, i.e. $[k:\mathbb{Q}] < \infty$, $\mathcal{O}$ = ring of integers in k, G a s.s. k-group, $\Gamma = G(\mathcal{O})$

e.g. $\Gamma = SL_d(\mathbb{Z})$

For $0 \neq I \lhd \mathcal{O}$, $\Gamma(I) = \ker(G(\mathcal{O}) \to G(\mathcal{O}/I))$.

Def: A congruence subgroup is a (finite index) subgroup containing $\Gamma(I)$ for some I.

The Congruence Subgroup Problem:

Is every finite index subgroup a congruence subgroup?

Let

$$c_n(\Gamma) = \#\{\underline{\text{congruence}} \text{ subgps of } \Gamma \text{ of index} \le n\}$$

Theorem (Lubotzky, Invent. 95) $\exists\, 0 < a, b < \infty$

s.t. $$n^{a \log n/\log\log n} \le c_n(\Gamma) \le n^{b \log n/\log\log n}$$

Remarks 1) The fact that $c_n(\Gamma)$ is not polynomial played crutial role in:

Theorem. (Lubotzky - Mann - Segal 93) Let Γ be a finitely generated residually finite gp. Then Γ has polynomial subgroup growth (i.e., $s_n(\Gamma) \le n^{O(1)}$) iff Γ is virtually solvable of finite rank

Remark 2 we get:

$$\log C_n(\Gamma) = O\left(\frac{(\log n)^2}{\log\log n}\right)$$

Thm If C.S.P. fails then

$$\log S_n(\Gamma) = \Omega\left((\log n)^2\right)$$

Cor (i) If C.S.P. fails "most" subgroups are non-congruence.

(ii) C.S.P. is a purely group theoretic problem. What about non-arithmetic lattices?

neg answer for all known non-arith lattices in $SO(n,1)$.

Almost nothing known for $SU(n,1)$, except of one lattice of Ron Livne.

Denote:

$$\alpha_+(\Gamma) = \limsup_n \frac{\log c_n(\Gamma)}{(\log n)^2/\log\log n}$$

$$\alpha_-(\Gamma) = \liminf_n \quad \ldots\ldots$$

Theorem (Goldfeld - Lubotzky - Pyber)

$$\alpha_+(SL_2(\mathbb{Z})) = \alpha_-(SL_2(\mathbb{Z})) = \frac{3-2\sqrt{2}}{4}$$

Theorem (G-L-P) Assuming G.R.H. (generalized Riemann hyp.) then for every number field k and $\Gamma = SL_2(\mathcal{O})$

$$\alpha_+(\Gamma) = \alpha_-(\Gamma) = \frac{3-2\sqrt{2}}{4}$$

Moreover, this is true unconditionally if $Gal(k/\mathbb{Q})$ is abelian.

The "message" of the pf for SL_2 is:

The main contribution to $C_n(\Gamma)$ comes from preimage of the subgroups of $SL_2(\mathbb{Z}/m\mathbb{Z}) = \prod_{p|m} SL_2(\mathbb{Z}/p\mathbb{Z})$

which lie between

$$U(m) = \prod_{p|m} \left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \mid * \in \mathbb{F}_p \right\} = \text{unipotent radical of Borel}$$

and $$B(m) = \prod_{p|m} \left\{ \begin{pmatrix} a & * \\ 0 & a^{-1} \end{pmatrix} \mid a \in \mathbb{F}_p^*, * \in \mathbb{F}_p \right\} = \text{Borel}$$

Here m = product of carefully chosen diff primes.

See below for more. Extends this to general groups:

Conjecture (G-L-P) Let k be any number field, G simple k-alg (Chevalley) group, $\Gamma = G(\mathcal{O})$, $r = \mathrm{rank}(G)$, $d = \dim(G)$, $K = |\Phi^+| = \#$ of pos. roots (in the absol. root sys. of G) and $R = R(G) = \frac{K}{r} = \frac{d-r}{2r}$

Then: $$\alpha_+(\Gamma) = \alpha_-(\Gamma) = \frac{\left(\sqrt{R(R+1)} - R\right)^2}{4R^2}$$

Call this number $\gamma(G)$. ↵

Theorem (G-L-P) Assuming GRH

$\alpha_-(\Gamma) \geq \gamma(G)$ and unconditional if $\mathrm{Gal}(k/\mathbb{Q})$ is abelian.

Theorem (L-N) $\alpha_+(\Gamma) \leq \gamma(G)$ always.

Back to the theorem on subgroup growth of lattices in semisimple gp H of $rk(H) \geq 2$.

By Galois cohomology if $H \neq D_4(\mathbb{C})$ all non-uniform arithmetic lattices of H are defined over field $E/\mathbb{Q}$ with $E \subseteq k$ and $Gal(k/\mathbb{Q})$ has a abelian subgp of index ≤ 4. This also suffices.

Also Serre's conj is proved for all non-uniform lattices.

For all of them the root system is the same - so

$$\lim_n \frac{\log s_n(\Gamma)}{(\log n)^2/\log\log n} = \gamma(H)$$

follows.

Proof of upper bound:

Let $\Gamma = G(\mathbb{Z})$. By standard subgp growth methods - the problem is reduced to counting $H \leq \prod_{p|m} G(\mathbb{F}_p)$.

Let $R(G) = \frac{\kappa}{2} = \frac{|\Phi^+|}{\text{rank}}$

The main new ingredient:

For $H \leq G(\mathbb{F}_p)$ denote:

$$\ell(H) = \frac{\log [G(\mathbb{F}_p) : H]}{\log |H^\Delta|}$$

where H^Δ = max. abelian quotient of H of order coprime to p.

Thm [LN] Given G then:

$$\liminf_{p \to \infty} \min \{ \ell(H) \mid H \leq G(\mathbb{F}_p) \} \geq R(G)$$

The real meaning: The essential min is for the Borel subgp B for which $[G(\mathbb{F}_p) : B] \sim p^{|\Phi^+|}$ and $|B^\Delta| = (p-1)^{\text{rank}}$

The problem is reduced to an external problem on abelian gps

Thm [GLP] Let d and R be fixed pos. Suppose $A = \mathbb{Z}/x_1\mathbb{Z} \times \cdots \times \mathbb{Z}/x_t\mathbb{Z}$ s.t.

(i) no x_i repeats more than d times.

(ii) $r|A|^R \le n$ for some pos. r and n.

Then as $n \to \infty$, we have:

$$\Delta_r(A) \le n^{(\gamma(R)+o(1))\log n/\log\log n}$$

where $\gamma(R) = \dfrac{\left(\sqrt{R(R+1)} - R\right)^2}{4R^2}$

A baby version:

Let $$M(n) = \max \left\{ \prod_{p,p' \in \mathcal{P}} \text{g.c.d.}\,(p-1, p'-1) \right|$$

$\mathcal{P}$ = set of diff primes with $\prod_{p \in \mathcal{P}} p \le n$

Thm

$$\lim_{n \to \infty} \frac{\log M(n)}{(\log n)^2 / \log\log n} = \frac{1}{4}$$

Pf of upper bound a special case of the above.

Pf of lower bound needs Bombieri-Vinogradov R.H. on the average.

Pf of lower bound Take $G = SL_2$.

Counting congruence subgps $\rightsquigarrow$

Counting subgroups of $G(\hat{\mathbb{Z}}) = SL_2(\hat{\mathbb{Z}}) = \prod_p SL_2(\mathbb{Z}_p)$

Let $x \in \mathbb{R}$ very large:

$P = \{ p \le x \mid p \text{ prime} \}$

$\ell = \pi(x) = |P| \sim \frac{x}{\log x}$

$m = \prod_{p \in P} p \sim e^x$

$2 \mid p-1 \quad \forall p$, so: $B(p) = \left\{ \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \right\} \to C_{p-1} \to C_2$

So $B(m) = \prod_{p \mid m} B(p) \twoheadrightarrow C_2^{\ell}$ = vector space of dim ℓ over $\mathbb{F}_2$.

subspaces of C_2^{ℓ} is $\sim 2^{\ell^2/4}$

$\therefore \exists\ 2^{\ell^2/4}$ subgps of $G(m)$ of index at most m^2

$\log n / (\log\log n)^2$

A better counting using R.H.

$x \in \mathbb{R}$ large, q prime $\sim x^{1/2-\varepsilon}$

$\mathcal{P} = \{p \le x \mid p \text{ prime } \& \; p \equiv 1 \pmod q\}$

$\ell = \pi(x; q, 1) = |\mathcal{P}| \sim \dfrac{x}{(q-1)\log x} \sim \dfrac{x^{1/2}}{\log x}$

$m = \prod_{p \in \mathcal{P}} p \sim e^{x/q-1} \sim e^{x^{1/2}}$

$q \mid p-1 \quad \forall p \in \mathcal{P}$ so $B(\mathcal{P}) \twoheadrightarrow C_q$

So $B(m) = \prod_{p \mid m} B(\mathcal{P}) \longrightarrow\!\!\!\!\rightarrow C_q^{\ell}$ = ℓ-dim v. space over $\mathbb{F}_q$

subspaces of index q^r in C_q^{ℓ}

is $\sim q^{r(\ell-r)}$.

Optimization on r gives:

$C_n(\Gamma) \gtrsim n^{\gamma(\Gamma)\log n/\log\log n}$ as needed.

Without R.H.? By "R.H. on the average"