Property (τ) and its applications

Alex Lubotzky
Hebrew University
Jerusalem

(i) expanders

(ii) diameters of finite simple groups.

(iii) computational group theory (the product replacement alg.).

(iv) Thurston's conj ($b_1(M) > 0$, hyp. mfd.).

(v) The virtual Haken ($n=3$)

<u>Def.</u> (Kazhdan 1967) A finitely generated group $\Gamma = \langle S \rangle$ has Property (T) if $\exists\ \varepsilon > 0$ s.t. for every non-trivial irreducible unitary rep. (H, ρ) (H = Hilbert space, $\rho : \Gamma \to U(H)$) and $\forall\ 0 \neq v \in H$, $\exists\ s \in S$ s.t.

$$\| \rho(s) v - v \| \geq \varepsilon \| v \|$$

i.e., <u>no</u> "almost" invariant vectors.

ε = Kazhdan constant of (Γ, S)

<u>Thm</u> $SL_n(\mathbb{Z})$, $n \geq 3$ has (T)

Application (Margulis 1975)

Assume $\Gamma = \langle S \rangle$ has T.

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

The Cayley graphs $Cay(\Gamma/N; S)$ form a family of EXPANDERS.

– Cayley graph of G w.r.t. S : $X = Cay(G;S)$

$$V(X) = G$$

$$Edges(X) : (a,b) \text{ if } \exists\, s \in S,\ b = sa.$$

– expanders A (finite) graph X is ε-expander if $\forall\, A \subset V(X)$ with $|A| \leq \frac{1}{2} |V(X)|$,

$$|\partial A| \geq \varepsilon |A|$$

when $\partial A = \{\cancel{y \in V(X) \mid dist(y,A) = 1}\}$

edges going <u>out</u> of A

Proof $\quad X = \mathcal{Cay}(\Gamma/N ; S)\ , \quad A \subseteq X.$

Γ acts on $L^2(\Gamma/N)$.

Let $\quad \chi_A$ = the characteristic function of A

so: $\exists\, s \in S$,

$$\| \rho(s)\chi_A - \chi_A \| \geq \varepsilon \|\chi_A\|$$
$$\|$$
$$\|\chi_{sA} - \chi_A\|$$

so $\quad \partial(A)$ is "large"......

Remark "change" χ_A to be in $L^2_0(\Gamma/N)$

History . Expanders in computer science (communication networks)

. random methods versus explicit constructions

Def: Let $\mathcal{L}$ be a family of finite-index normal subgroups of Γ, $\mathcal{L} = \{N_i\}_{i \in I}$

Γ has Property (τ) w.r.t. $\mathcal{L}$

if $\forall$ irr., non-trivial, unitary rep (H, ρ) of Γ, with $\operatorname{Ker} \rho \supseteq N_i$ for some i, H has no almost invariant vectors.

(i.e., $\exists \varepsilon > 0$ indep., s.t. $\forall (H, \rho)$ with $\operatorname{Ker} \rho \supset N_i$, $\forall\, 0 \neq v \in H$, $\exists\, s \in S$ s.t. $\|\rho(s)v - v\| \geq \varepsilon \|v\|$.

Say Γ has (τ) if $\mathcal{L}$ = all fin. index normal

Cor: If Γ has (τ) w.r.t. $\mathcal{L} = \{N_i\}$ then $\operatorname{Cay}(\Gamma/N_i; S)$ form a family of expanders

Equiv forms of (τ)

(Brooks, Buser, Cheeger, Alon, Milman, Dodziuk) + ...

G = simple Lie gp

Γ = a lattice in G ($\mu(G/\Gamma) < \infty$), $\Gamma = \langle S \rangle$.

K = max compact subgp of G

$X = G/K$ – the symmetric space

$\mathcal{L} = \{N_i\}$ – a family of fin. index subgps of Γ.

T.F.A.E. :

(1) Γ has (τ) w.r.t. $\mathcal{L}$

(2) $\exists \varepsilon$, $Cay(\Gamma/N_i ; S)$ are ε- expanders

(3) $\exists \varepsilon$, $\lambda_1(N_i \backslash X) \geq \varepsilon \quad \forall i$

(4) $\exists \varepsilon > 0$, $h(N_i \backslash X) \geq \varepsilon \quad \forall i$.

(5) The Haar measure μ is the only fin. additive Γ- inv. measure on $\Gamma_{\hat{\mathcal{L}}}$.

– $\lambda_1(N_i \backslash X)$ = bottom of the spectrum ≡ "smallest" e.v. of Δ.

– $h(\ )$ = the isoperimetric constant ≡ Cheeger const.

~~(6) The Haar measure is the only fin additive~~

~~Γ-inv measure on Γ~~

Examples

1) $(T) \Longrightarrow (\tau)$

Thm (Kazhdan) G simple Lie group of $\mathbb{R}$-rank ≥ 2, $\Gamma \leq G$ a lattice (= discrete subgroup of finite covolume). Then Γ has (T).

e.g. $SL_n(\mathbb{Z})$, $n \geq 3$.

2) If $\Gamma \twoheadrightarrow \mathbb{Z}$ then Γ does not have (T) or (τ).

$\therefore$ $SL_2(\mathbb{Z})$ does not have (T) or (τ)

$$\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to S^1 = U_1(\mathbb{C})$$
$$1 \longmapsto e^{2\pi i/n}$$

but:

3) Theorem (Selberg 1965)

$G = SL_2(\mathbb{R})$, $\Gamma = SL_2(\mathbb{Z})$

$K = SO(2)$, $X = G/K = \mathbb{H}$ = upper half plane

$N_i = \mathrm{Ker}\left(SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/i\mathbb{Z})\right)$

then: $\lambda_1 \left(N_i \backslash X \right) \geq \frac{3}{16}$

Conj $\lambda_1 \geq \frac{1}{4}$ ($\Leftrightarrow$ no comp. series rep's in $L^2_0(N_i \backslash G)$)

- Luo - Rudnick - Sarnak $\lambda_1 \geq 0.21$
- Kim - Shahidi $\lambda_1 \geq 0.22\ldots$

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

Cor 1:

$$\mathrm{Cay}\left(SL_2(p); \left\{\begin{pmatrix}1&1\\0&1\end{pmatrix}, \begin{pmatrix}1&0\\1&1\end{pmatrix}\right\}\right)$$ are expanders

Cor: diameter $\leq C \cdot \log p$

open problem An algorithm.

– Partial result: M. Larsen

a chalange: $\begin{pmatrix}1 & \frac{p-1}{2}\\ 0 & 1\end{pmatrix} = \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}^{\frac{p-1}{2}}$

go to (5)

Theorem (Babai-Kantor-Lubotzky)

$\forall$ finite simple (non-abelian) gp G,

$\exists\, S \subseteq G$, with $|S| \leq 7$ s.t.

$$\mathrm{diameter}(\mathrm{Cay}(G;S)) = O(\log|G|)$$

Cor. 2 p odd

Cay$\left(SL_2(p) ; \begin{pmatrix}1&2\\0&1\end{pmatrix}, \begin{pmatrix}1&0\\2&1\end{pmatrix}\right)$ are expanders

open problem
~~Cor.~~ 3 Cay$\left(SL_2(p) ; \begin{pmatrix}1&3\\0&1\end{pmatrix}, \begin{pmatrix}1&0\\3&1\end{pmatrix}\right)$ are expanders ?

Open problem Are $SL_2(p)$ expanders for every choice of gen.'s ?

open problem Are $S_n = \mathrm{Sym}(n)$ expanders w.r.t. to some choice of gen.'s ? (of bounded size).

open problem For fixed p & $n \to \infty$, Are $SL_n(p)$ expanders w.r.t. some choice ?

(Ramanujan complexes ....).

Property (τ) and Computational Group Theory

see Lubotzky - Pak, JAMS 2001

Let G be a finite group given by d generators $g_1, \dots, g_d$

Problem Find (pseudo) random element of G

Naive aproach: Take a long random word in the generators

The Product Replacement Algorithm (PRA)

$k \geq d$

$$\Omega^k(G) = \{(h_1, \dots, h_k) \in G^k\}$$

$$\underline{h} \xrightarrow[1 \leq i \neq j \leq k]{\text{random}} (h_1, \dots, h_{i-1}, h_j^{\pm 1} h_i h_j^{\pm 1}, h_{i+1}, \dots, h_k)$$

one of 4 random

Start with $(g_1, \dots, g_d, e, \dots, e)$ and at time t pick random h_i from $\underline{h}(t)$.

Outstanding performances!

but why??

Diaconis - Saloff-Coste (Invent. 98) ....

L. - Pak:

Identify $\Omega_k(G) = \mathrm{Epi}(F_k, G)$

Nielsen moves $R_{ij}^{\pm}(x_\ell) = \begin{cases} x_i x_j^{\pm 1} & \ell = i \\ x_\ell & \ell \neq i \end{cases}$

$L_{ij}^{\pm}$ ....

generate $\mathrm{Aut}^+(F_k)$. $\alpha \in \mathrm{Aut}$, $\varphi \in \mathrm{Epi}$

$\mathrm{Aut}^+(F_k)$ acts on $\mathrm{Epi}(F_k, G)$ so

$\Omega_k(G)$ quotients of $X(\mathrm{Aut}^+(F_k); \{R_{ij}, L_{ij}\})$

Cor: If $\mathrm{Aut}(F_k)$ has (T) or (τ)

then $\Omega_k(G)$ are expanders

in which case PRA converges

extremely fast!

mixing time $\underline{O(\log(G))}$

open problem Does $Aut(F_k)$ has (τ)?

related problem Does M_g has (τ)?

Still $Aut(\mathbb{Z}^k) = GL_k(\mathbb{Z})$ has (τ)

so PRA fast on abelian gps.

- also on nilpotent groups

(linear versus subexp).

Remark what is really needed is:

"non-abelian Selberg theorem".

Define Congruence subgroups of $Aut(F)$

$$K(C) = Ker\left(Aut(F) \to Aut(F/C)\right)$$

C char. fin. index in F

Q1: Congruence subgroup problem?

Q2: Selberg theorem?

when F = free abelian gp, reduces to the classical problems.

Thurston's conjecture

$M = M^n$ n-dim hyperbolic manifold.
Then $\exists$ a finite sheeted cover
$M' \twoheadrightarrow M$, with $\beta_1(M') > 0$
$(\beta_1(M') = \dim H_1(M'; \mathbb{R}))$

Equivalent form:

$\Gamma \leq SO(n,1)$ a lattice.
Then $\exists$ finite index subgroup Γ'
with $\Gamma' \twoheadrightarrow \mathbb{Z}$ (i.e., $|\Gamma'/_{[\Gamma', \Gamma']}| = \infty$)

Remark Thurston's conj. $\Rightarrow$ Serre Conj:
Congruence subgroup property
fails for arithmetic lattices
in $SO(n,1)$

<u>Def</u> The Selberg property

Γ an arithmetic lattice in G (= s.s. Lie gp). Γ has the Selberg Property if Γ has (τ) w.r.t. <u>congruence</u> subgroups

<u>Many results</u>:
Selberg, Jacquet-Langlands, Gelbart, Li, P.S.; Gruenewald-Mennicke ....
(with various explicit constants). closed.

<u>Cor</u>: $SL_2(\mathbb{Z}[\frac{1}{p}])$ has (τ) but not (T).

The Burger - Sarnak method (Invent. 91)

arithmetic lattices $\Gamma_1 \leq \Gamma_2$

$\quad\quad\quad\quad\quad\quad\quad\quad\;\; \wedge\!\!\!/\!/ \quad\quad\;\; \wedge\!\!\!/\!/$

simple Lie gps $G_1 \leq G_2$

and $\Gamma_2 \cap G_1 = \Gamma_1$

(a) If Γ_1 has Selberg so is Γ_2.

(b) If Γ_1 has (τ) so is Γ_2.

(c) applied to Thurston's conj

(A. Lubotzky, Ann. of Math. 1996)

The Sandwich Lemma

$$\begin{array}{lccccc} \text{arith lat.} & \Gamma_1 & < & \Gamma_2 & < & \Gamma_3 \\ & \wedge & & \wedge & & \wedge \\ \text{simple Lie gps} & G_1 & < & G_2 & < & G_3 \end{array}$$

and $G_i \cap \Gamma_{i+1} = \Gamma_i$

(a) If Γ_1 has Selberg and Γ_3 does not have c then Γ_2 does not have the congruence subgroup property.

(b) If Γ_1 has Selberg and Γ_3 has cong. Γ_3^* with $\Gamma_3^* \twoheadrightarrow \mathbb{Z}$, Then Γ_2 has congruence subgp Γ_2^* with $\Gamma_2^* \twoheadrightarrow \mathbb{Z}$.

<u>Theorem</u> Let $\Gamma \leq SO(n,1)$ arithmetic lattice (If $n=7$, assume Γ not of type ${}^{3,6}D_4$. If $n=3$ and Γ comes from units of a quaternion alg over L, $[L:\mathbb{Q}]<\infty$ and L has a unique complex emb, then assume L has a subfield of index 2)

Then $\exists$ a congruence subgp Γ^* of Γ with $\Gamma^* \twoheadrightarrow \mathbb{Z}$.

<u>Pf:</u> By Galois cohomology:

$$\begin{array}{ccccc} \Gamma_1 & \leq & \Gamma & \leq & \Gamma_3 \\ \wedge\!\!\wedge & & \wedge & & \wedge\!\!\wedge \\ SO\binom{2}{3},1) & \leq & SO(n,1) & \leq & SU(n,1) \end{array}$$

Γ_1 has Selberg by Selberg, J.-L., J.-Gelbart & Sarnak

Γ_3 is of simple type and has $\Gamma_3^* \twoheadrightarrow \mathbb{Z}$ by Kazhdan, Shimura, Borel-Wallach. //

(τ) & virtual Haken conj

(Marc Lackenby)

<u>Conj</u> $M = M^3$ closed hyperbolic mfd.

$\Gamma = \pi_1(M)$ has a finite index subgp Γ'

with (*) Γ' is either a non-trivial free product with amalgam or HNN-ext. (HNN $\Leftrightarrow$ $\Gamma' \twoheadrightarrow \mathbb{Z}$).

Let as before $\mathcal{L} = \{N_i\}$ normal in Γ.

<u>Thm.</u> (Lackenby) Let Γ be a <u>fin. presented</u> gp. Then Γ has (at least) one of the following:

1) Γ has (τ) w.r.t. $\mathcal{L}$.

2) For infinitely many i's, N_i has (*)

3) $$\inf_i \frac{d(N_i) - 1}{[\Gamma : N_i]} = 0$$

"Pf" Assume no (1) & no (3) - we prove (2).

Let $X_i = Cay(\Gamma/N_i ; S)$, $D_i \subseteq X_i$ a subset with $|D_i| \leq \frac{|X_i|}{2}$ and $\frac{|\partial D_i|}{|D_i|} = h(X_i)$. Lemma $|D_i| \geq \frac{|X_i|}{4}$ ☒.

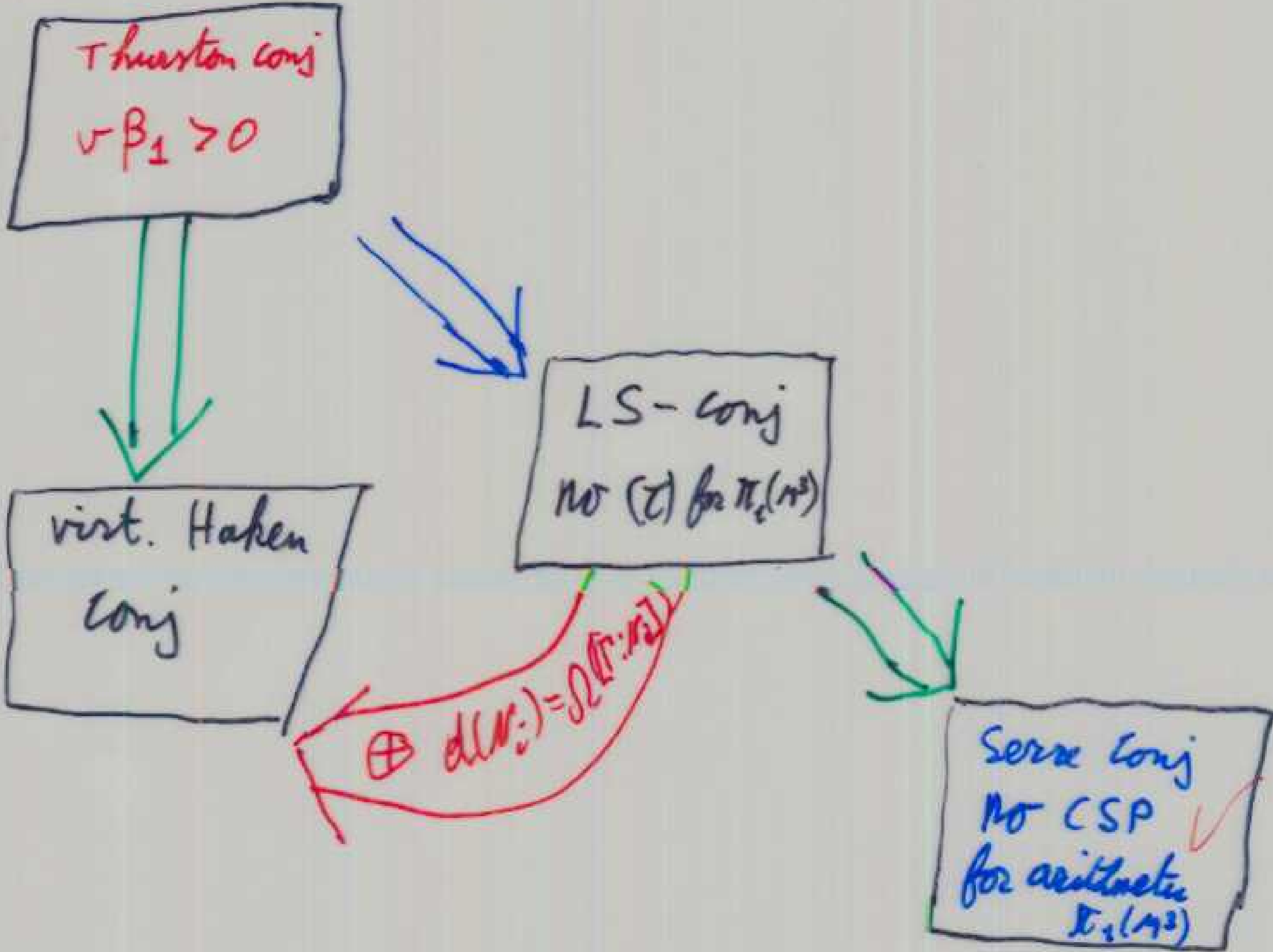
think of X_i as a 2-dim complex s.t. $\pi_1(X_i) = N_i$ (a standard procedure: start with K - 2-dim complex with one vertex .... & $\pi_1(K) = \Gamma$).

Let A_i = closure of union of all 2-cells intersecting D_i

B_i = ... D_i^c

$C_i = A_i \cap B_i$

$X_i = A_i \cup B_i$, and van Kampen gives the decomposition .... ☒



<u>LS (Lubotzky - Sarnak) conj</u> $\Gamma = \pi_1(M^3)$, M^3 a 3-dim hyperbolic mfd, does not have (τ).

Pro-p aprach to LS-conj (+ $\frac{d(N_i)}{[\Gamma:N_i]} > \varepsilon > 0$)

Pf of Serre conj $\Gamma = \pi_1(M^3)$ has the same number of gen's & rel's

$\therefore$ $\Gamma_{\hat{p}}$ - a Golod Shafarevich gp

$\therefore$ not p-adic analytic

$\therefore$ Γ does not have CSP. $\boxtimes$

Theorem (Zelmanov) G a G-S pro-p group contains a free pro-p gp.

$\therefore$ Every finite p-gp is a quotient of some finite index subgp of G (Lemma of $\Gamma' \leq \Gamma = \pi_1(M^3)$).
($\therefore$ non-trivial result for hyp mfd)

Q6. Assume Γ a discrete res.-p G-S gp. Does Γ have an infinite amenable G-S quotient?
If yes then $\Rightarrow$ LS conj.

One may also try:

$\Gamma = \pi_1(M^3)$ is hyp. gp of G-S.

replace inductively by quotients Γ_i

which are hyp of G-S and

$\rho(\Gamma_i) \xrightarrow[i\to\infty]{} 1$

($\rho(\Gamma_i)$ = the normalized norm of the random walk).

If so then $\Rightarrow$ LS conj

Regarding $\frac{d(N_i)}{[\Gamma : N_i]}$: pro-p helps

but so far weak results

$d(N_i) \geq c\,(\log [\Gamma : N_i])^2$.