PCMI LECTURE NOTES ON PROPERTY (T), EXPANDER GRAPHS AND APPROXIMATE GROUPS (PRELIMINARY VERSION)

EMMANUEL BREUILLARD

1. Lecture 1, Spectral gaps for infinite groups and non-amenability

The final aim of these lectures will be to prove spectral gaps for finite groups and to turn certain Cayley graphs into expander graphs. However in order to do so it is useful to have some understanding of the analogous spectral notions of amenability and Kazhdan property (T) which are important for infinite groups. In fact one important aspect of asymptotic group theory (the part of group theory concerned with studying the geometric and group theoretic properties of large finite groups) is the ability to pass from the world of infinite groups to the that of finite groups and vice-versa and to manage to transfer results from one world to the other.

We begin by reviewing the definition of amenability for a (countable) group and several of its equivalent definitions.

I. Amenability, Folner criterion.

In this lecture Γ will always denote a countable group.

Definition 1.1. *We say that Γ is* amenable *if there exists a sequence of finite subsets $F_n \subset \Gamma$ such that for every $\gamma \in \Gamma$,*

$$\frac{|\gamma F_n \Delta F_n|}{|F_n|} \to 0$$

as n tends to infinity.

The F_n's are called *Folner sets.* They do not need to generate Γ (in fact Γ is not assumed finitely generated). From this definition it follows easily however that Γ is the union of all $F_n F_n^{-1}$ and the $|F_n|$ tends to infinity unless Γ is finite.

The following properties can be easily deduced from this definition (exercise):

- Γ is amenable if and only if every finitely generated subgroup of Γ is amenable,
- $\mathbb{Z}^d$ is amenable
- if Γ has subexponential growth, then there is a sequence of word metric balls of radius tending to infinity which is a Folner sequence.

Date: July 14th 2012.

We will see at the end of this section that amenability is preserved under group extensions, and thus that every solvable group is amenable.

II. Isoperimetric inequality, edge expansion

If Γ is finitely generated, say by a finite symmetric (i.e. $s \in S \Rightarrow s^{-1} \in S$) set S, then we can consider its Cayley graph $\mathcal{G}(G, S)$, which is defined to be the graph whose vertices are the elements of Γ and edges are defined by putting an edge[1] between x and y if there is $s \in S$ such that $x = ys$.

Given a finite set F of elements in Γ, we let $\partial_S F$ be the set of group elements x which are not in F but belong FS. This corresponds to the boundary of F in the Cayley graphs (i.e. points outside F but at distance at most 1 from F).

The following is straightforward (exercise):

Proposition 1.2. *The group Γ is non-amenable if and only if its Cayley graph satisfies a linear isoperimetric inequality. This means that there is $\varepsilon > 0$ such that for every finite subset F of Γ*

$$|\partial_S F| \geqslant \varepsilon |F|.$$

Exercise: Show that amenability is preserved under quasi-isometry.
Exercise: Show that the non-abelian free groups F_k are non-amenable.

It follows from the last exercise that if a countable group contains a free subgroup, it is non-amenable. The converse is not true. In fact there are finitely generated torsion groups (i.e. every element is of finite order) which are non-amenable. Adian and Novikov showed that the Burnside groups $B(n, k) := \langle a_1, \ldots, a_k | \gamma^n = 1 \ \forall \gamma \rangle$ are non-amenable for n large enough.

III. Invariant means

Amenable groups were introduced by John von Neumann in the 1930's. His definition was in terms of invariant means (amenable = admits a mean).

Definition 1.3. *An* invariant mean *on a countable group Γ is a finitely additive probability measure m defined on the set of all subsets of Γ, which is invariant under the group action by left translations, i.e. $m(\gamma A) = m(A)$ for all $\gamma \in \Gamma$ and $A \subset \Gamma$.*

It is easily checked that an invariant mean is the same thing as a continuous linear functional $m : \ell^\infty(\Gamma) \to \mathbb{R}$ such that

- $f \geqslant 0 \Rightarrow m(f) \geqslant 0$,
- $\forall \gamma \in \Gamma$, $\gamma_* m = m$,
- $m(\mathbf{1}) = 1$.

Folner showed the following:

[1]We allow multiple edges between two distinct points, but no loop at a given vertex.

Proposition 1.4. *(Folner criterion) A group Γ is amenable (in the sense of I. above) if and only if admits an invariant mean.*

The proof of the existence of the invariant mean from the Folner sequence follows by taking a weak-$\star$ limit in $\ell^\infty(\Gamma)$ of the "approximately invariant" probability measures $\frac{1}{|F_n|}\mathbf{1}_{F_n}$. For the converse, one needs to approximate m in the weak topology by functions in ℓ^1, then take appropriate level sets of these functions. For the details, we refer the reader to the appendix of the book Bekka-delaHarpe-Valette [1]. We will also give an alternative argument for the converse in the exercises using Tarski's theorem on paradoxical decompositions.

IV. Random walks on groups, the spectral radius and Kesten's criterion.

In his 1959 Cornell thesis [2], Kesten studied random walks on Cayley graphs of finitely generated groups and he established yet another characterization of amenability in terms the rate of decay of the probability of return and in terms of the spectrum of the Markov operator associated to the random walk.

Before we state Kesten's theorem, let us first give some background on random walks on groups. This will be useful later on in Lectures 3 and 4 when we discuss the Bourgain-Gamburd method.

Suppose Γ is finitely generated and μ is a finitely supported symmetric (i.e. $\forall \gamma \in \Gamma, \mu(\gamma) = \mu(\gamma)$) probability measure on Γ whose support generates Γ.

We can associate to μ an operator P_μ on $\ell^2(\Gamma)$, *the Markov operator*, by setting for $f \in \ell^2(\Gamma)$

$$P_\mu f(x) = \sum_{\gamma\in\Gamma} f(\gamma^{-1}x)\mu(\gamma).$$

Clearly P_μ is self-adjoint (because μ is assumed symmetric) and moreover

$$P_\mu \circ P_\nu = P_{\mu*\nu},$$

for any two probability measures μ and ν on Γ, where $\mu * \nu$ denotes the convolution of the two measures, that is the new probability measure defined by

$$\mu * \nu(x) := \sum_{\gamma\in\Gamma} \mu(x\gamma^{-1})\nu(\gamma).$$

The convolution is the image of the product $\mu \otimes \nu$ under the product map $\Gamma \times \Gamma \to \Gamma$, $(x, y) \mapsto xy$ and is the probability distribution of the product random variable XY, if X is a random variable taking values in Γ with distribution μ and Y is a random variable with distribution ν.

The probability measure μ induced a *random walk* on Γ, i.e. a stochastic process $(S_n)_{n\geqslant 1}$ defined as

$$S_n = X_1 \cdot \ldots \cdot X_n,$$

where the X_i's are independent random variables with the same probability distribution μ on Γ. The process $(S_n)_n$ is a Markov chain and $p_{x\to y} := \mu(x^{-1}y)$ are the transition probabilities.

When μ is the probability measure

$$\mu = \mu_S := \frac{1}{|S|}\sum_{s\in S}\delta_s,$$

where δ_s is the Dirac mass at $s \in S$ and S is a finite symmetric generating set for Γ, we say that μ and its associated process (S_n) is the *simple random walk* on (Γ, S). It corresponds to the nearest neighbor random walk on the Cayley graph $\mathcal{G}(\Gamma, S)$, where we jump at each stage from one vertex to a neighorhing vertex with equal probability.

Kesten was the first to understand that studying the probability that the random walk returns to the identity after time n could be useful to classify infinite groups. This quantity is

$$Proba(S_n = 1) = \mu^n(1),$$

where we have denoted the n-th convolution product of μ with itself by $\mu^n := \mu * \ldots * \mu$.

We will denote the identity element in Γ sometimes by 1 sometimes by e.

Proposition 1.5. *Here are some basic properties of μ^n.*

- *$\mu^{2n}(1)$ is non-decreasing,*
- *$\mu^{2n}(x) \leqslant \mu^{2n}(1)$ for all $x \in \Gamma$.*

Note that $\mu^{2n+1}(1)$ can be zero sometimes (e.g. the simple random walk on the free group), but $\mu^{2n}(1)$ is always positive.

The Markov operator P_μ is clearly a contraction in ℓ^2 (and in fact in all ℓ^p, $p \geqslant 1$), namely $||P_\mu|| \leqslant 1$. A basic tool in the theory of random walks on groups is the *spectral theorem* for self-adjoint operators applied to P_μ. This will yield Kesten's theorem and more.

Proof of Proposition 1.5. Observe that $P_{\mu^n} = P_\mu^n$ and that $\mu^n(x) = P_\mu^n\delta_e(x) = \langle P_\mu^n\delta_e, \delta_x\rangle$ (in $\ell^2(\Gamma)$ scalar product). Denoting P_μ by P for simplicity it follows that

$$\mu^{2(n+1)}(1) = \langle P^n\delta_e, P^{n+2}\delta_e\rangle \leqslant ||P^n\delta_e|| \cdot ||P^2P^n\delta_e|| \leqslant ||P^n\delta_e||^2 = \mu^{2n}(1).$$

and that

$$\mu^{2n}(x) = \langle P^{2n}\delta_2, \delta_x\rangle \leqslant ||P^n\delta_e|| \cdot ||P^n\delta_x|| = \mu^{2n}(1),$$

where the last equality follows from the fact that $P^n\delta_x(y) = P^n\delta_e(yx^{-1})$. $\square$

Proposition-Definition 1.6. *(Spectral radius of the random walk) The* spectral radius *$\rho(\mu)$ of the Markov operator P_μ action on $\ell^2(\Gamma)$ is called the spectral radius of the random walk.*

Note that since P_μ is self-adjoint, its spectral radius coincides with its operator norm $||P_\mu||$, and with $\max\{|t|, t \in spec(P_\mu)\}$.

Let us apply the spectral theorem for self adjoint operators to P_μ. This gives a resolution of identity $E(dt)$ (measure taking values into self-adjoint projections), and a probability measure $\eta(dt) : \langle E(dt)\delta_e, \delta_e\rangle$ on the interval $[-1,1]$ such that for all $n \geqslant 1$,

$$\langle P^n \delta_e, \delta_e\rangle = \int_{[-1,1]} t^n \eta(dt). \tag{1.6.1}$$

Definition 1.7. *(Spectral measure) The* spectral measure *of the random walk is the measure η associated to the Markov operator P_μ by the spectral theorem as above.*

Exercise: Show that $\langle E(dt)\delta_x, \delta_x\rangle = \eta(dt)$ for all $x \in \Gamma$ and that the other spectral measures $\langle E(dt)f, g\rangle$, with $f, g \in \ell^2(\Gamma)$ are all absolutely continuous w.r.t η.

We can now state:

Theorem 1.8. *(Kesten) Let Γ be a finitely generated group and μ a symmetric probability measure with finite support generating Γ.*

- *$\forall n \geqslant 1$, $\mu^{2n}(1) \leqslant \rho(\mu)^{2n}$ and $\lim_{n\to+\infty}(\mu^{2n}(1))^{\frac{1}{2n}} = \rho(\mu)$,*
- *(Kesten's criterion) $\rho(\mu) = 1$ if and only if Γ is amenable.*

Proof of the first item. The existence of the limit and the upper bound follows from the subadditive lemma (i.e. if a sequence $a_n \in \mathbb{R}$ satisfies $a_{n+m} \leqslant a_n + a_m$, for all $n, m \in \mathbb{N}$, then $\frac{a_n}{n}$ converges to $\inf_{n\geqslant 1} \frac{a_n}{n}$). Indeed $\mu^{2(n+m)}(1) \geqslant \mu^{2n}(1)\mu^{2m}(1)$ (the chance to come back at 1 at time $2n + 2m$ is at least the chance to come back at time $2n$ and to come back again at time $2n + 2m$). Take logs.

In order to identify the limit as the spectral radius, we apply the spectral theorem to P_μ, and $\mu^{2n}(1)^{\frac{1}{2n}}$ coincides with $\langle P^{2n}\delta_e, \delta_e\rangle^{\frac{1}{2n}}$, which by (1.6.1) takes the form

$$\Big(\int_{[-1,1]} t^{2n}\eta(dt)\Big)^{\frac{1}{2n}}.$$

However when $n \to +\infty$, this tends to $\max\{|t|, t \in spec(P_\mu)\} = \rho(\mu)$. □

Below we sketch a proof of Kesten's criterion via an analytic characterization of amenability in terms of Sobolev inequalities.

Proposition 1.9. *Let Γ be a group generated by a finite symmetric set S and let μ a symmetric probability measure whose support generates Γ. The following are equivalent:*

1. *Γ is non-amenable,*
2. *there is $C = C(S) > 0$ such that $||f||_2 \leqslant C||\nabla f||_2$ for every $f \in \ell^2(\Gamma)$,*
3. *there is $\varepsilon = \varepsilon(S) > 0$ such that $\max_{s\in S} ||s \cdot f - f||_2 \geqslant \varepsilon||f||_2$ for all $f \in \ell^2(\Gamma)$,*
4. *$\rho(\mu) < 1$.*

Here ∇f is the function on the set of edges of the Cayley graph of Γ associated with S given by

$$\nabla f(e) = |f(e^+) - f(e^-)|,$$

where e^+ and e^- are the extremities of the edge e.

Proof. Note that condition (3) does not depend on the generating set (only the constant ε may change). For the equivalence between (3) and (4) observe further that a finite collection of unit vectors in a Hilbert space average to a vector of norm strictly less than 1 if and only if the angle between at least two of them is bounded away from zero (and the bounds depend only on the number of vectors).

The equivalence between (2) and (3) is clear because $||\nabla f||_2$ is comparable (up to multiplicative constants depending on the size of S only) to $\max_{s \in S} ||s \cdot f - f||_2$.

Condition (2) easily implies (1), because the linear isoperimetric inequality $|\partial_S F| \geqslant \varepsilon |F|$ is immediately derived from (2) by taking $f = \mathbf{1}_F$ the indicator function of F.

The only less obvious implication is (1) $\Rightarrow$ (2) as we need to go from sets to arbitrary functions. The idea to do this is to express f as a sum of indicator functions of sublevel sets. Namely, for $t \geqslant 0$, let $A_t = \{\gamma \in \Gamma; f(\gamma) > t\}$. Then for $x \in \Gamma$

$$f(x) = \int_0^{+\infty} \mathbf{1}_{t<f(x)} dt = \int_0^{+\infty} \mathbf{1}_{A_t}(x) dt$$

and, say if $f(e^+) > f(e^-)$ for an edge e of $\mathcal{G}(\Gamma, S)$

$$|f(e^+) - f(e^-)| = \int_0^{+\infty} \mathbf{1}_{f(e^-)<t<f(e^+)} dt = \int_0^{+\infty} \mathbf{1}_{\partial A_t}(e) dt$$

where ∂A (for any subset $A \subset \Gamma$) is the set of edges connecting a point in A to a point outside A.

Summing over all vertices x and all edges e we obtain the *co-area formulae*:

$$\int_0^{+\infty} |A_t| dt = ||f||_1$$

and

$$\int_0^{+\infty} |\partial_e A_t| dt = ||\nabla f||_1$$

If Γ is non-amenable, it satisfies the linear isoperimetric inequality and therefore there is $\varepsilon > 0$ such that $|\partial A| \geqslant \varepsilon |A|$ for every finite subset A of Γ. Applying this to A_t and using the co-area formulae, we conclude:

$$||\nabla f||_1 \geqslant \varepsilon ||f||_1$$

for every ℓ^1 function on Γ. To get the ℓ^2 estimate, simply note that $||f||_2^2 = ||f^2||_1$ and

$$||\nabla f^2||_1 \leqslant 2 ||\nabla f||_2 ||f||_2$$

for every $f \in \ell^2$ as one can see by applying the Cauchy-Schwartz inequality (combined with $|x^2 - y^2| = |x - y||x + y|$ and $|x + y|^2 \leqslant 2(x^2 + y^2)$). $\square$

Exercise: if $1 \to \Gamma_1 \to \Gamma_2 \to \Gamma_3 \to 1$ is an exact sequence, then Γ_2 is amenable if and only if Γ_1 and Γ_3 are amenable [hint: one can use property (3) as a working definition for amenability].

V. Linear groups and the Tits alternative

... to be continued ...

References

[1] B. Bekka, P. de la Harpe and A. Valette, *Kazhdan's property* (T) New Mathematical Monographs, 11. Cambridge University Press, Cambridge, 2008. xiv+472 pp.

[2] H. Kesten, *Symmetric random walks on groups,* Trans. Amer. Math. Soc., **92** (1959), 336–354.

Laboratoire de Mathématiques, Bâtiment 425, Université Paris Sud 11, 91405 Orsay, FRANCE

E-mail address: emmanuel.breuillard@math.u-psud.fr

LECTURE 2: THE TITS ALTERNATIVE AND KAZHDAN'S PROPERTY (T) (PRELIMINARY VERSION)

EMMANUEL BREUILLARD

I. The Tits alternative.

A very interesting large class of groups is provided by the *linear groups*, namely the subgroups of $\mathrm{GL}_d(K)$, for some (commutative) field K. There are few general tools to study arbitrary finitely generated groups (often one has to resort to combinatorics and analysis as we did in Lecture 1 above for example). However for linear groups the situation is very different and a wide range of techniques (including algebraic number theory and algebraic geometry) become available.

Jacques Tits determined in 1972 which linear groups are amenable by showing his famous alternative:

Theorem 0.1. *(Tits alternative [18]) Let Γ be a finitely generated linear group (overs some field K). Then*
- *either Γ is virtually solvable (i.e. has a solvable finite index subgroup),*
- *or Γ contains a non-abelian free subgroup F_2.*

Remark. Virtually solvable subgroups of $\mathrm{GL}_d(K)$ have a subgroup of finite index which can be triangularized over the algebraic closure (Lie-Kolchin theorem).

In particular (since free subgroups are non-amenable and subgroups of amenable groups are amenable),

Corollary 0.2. *A finitely generated linear group is amenable if and only if it is virtually solvable.*

The proof of the Tits alternative uses a technique called "ping-pong" used to find generators of a non-abelian free subgroup in a given group. The basic idea is to exhibit a certain geometric action of the group Γ on a space X and two elements $a, b \in \Gamma$, the "ping-pong players" whose action on X has the following particular behavior:

Lemma 0.3. *(Ping-pong lemma) Suppose Γ acts on a set X and there are two elements $a, b \in \Gamma$ and 4 disjoint (non-empty) subsets A^+, A^-, B^+, and B^- of X such that*
- *a maps B^+, B^- and A^+ into A^+,*
- *a^{-1} maps B^+, B^- and A^- into A^-,*
- *b maps A^+, A^- and B^+ into B^+, and*
- *b^{-1} maps A^+, A^- and B^- into B^-.*

Then a and b are free generators of a free subgroup $\langle a, b\rangle \simeq F_2$ in Γ.

Date: July 14th 2012.

Proof. The subset A^+ is called the attracting set for a and A^- the repelling set, and similarly for the other letters. Pick a reduced word w in a and b and their inverses. Say it starts with a. Pick a point p not in A^+ and not in the repelling set of the last letter of w (note that there is still room to choose such a p) Then the above ping-pong rules show that $w \cdot p$ belongs to A^+ hence is not equal to p. In particular w acts non trivially on X and hence is non trivial in Γ. $\square$

Remark. There are also other variant of the ping-pong lemma (e.g. it is enough that there are disjoint non-empty subsets A and B such that any (positive or negative) power of a sends B inside A and any power of b sends A inside B (e.g. take $A := A^+ \cup A^-$ and $B := B^+ \cup B^-$ above). But the above is the most commonly used in practice.

On Tits' proof. Tits' proof uses algebraic number theory and representation theory of linear algebraic groups to construct a local field ($\mathbb{R}$, $\mathbb{C}$ or a finite extension of $\mathbb{Q}_p$ or $\mathbb{F}_p((t))$) K and an irreducible linear representation of Γ in $GL_m(K)$ whose image is unbounded. If Γ is not virtually solvable, one can take $m \geqslant 2$. Then he shows that one can change the representation (passing to an exterior power) and exhibit an element γ of Γ which is semisimple and has the property that both γ and γ^{-1} have a unique eigenvalue (counting multiplicity) of maximal modulus (such elements are called proximal elements). Then one considers the action of Γ on the projective space of the representation $X := \mathbb{P}(K^m)$ and observes that the powers γ^n, $n \in \mathbb{Z}$, have a contracting behavior on X: for example the positive powers γ^n, $n \geqslant 1$ push any compact set not containing the eigenline of maximal modulus of γ^{-1} inside a small neighborhood around the eigenline of maximal modulus of γ. Using irreducibility of the action, one then find a conjugate $c\gamma c^{-1}$ of γ such that $a := \gamma^n$ and $b = c\gamma^n c^{-1}$ exhibit the desired "ping-pong" behavior for all large enough n and thus generate a free subgroup. For details, see the original article [18] or e.g. [3].

It turns out that one can give a shorter proof of the corollary, which by-passes the proof of the existence of a free subgroup. This was observed by Shalom [16] and the argument, which unlike the proof of the Tits alternative does not require the theory of algebraic groups, is as follows.

Sketch of a direct proof of Corollary 0.2. Let us first assume that Γ is an unbounded subgroup of $\mathrm{GL}_n(k)$, for some local field k, which acts strongly irreducibly (i.e. it does not preserve any finite union of proper linear subspaces). If Γ is amenable, then it must preserve a probability measure on $\mathbb{P}(k^n)$. However recall:

Lemma 0.4. *(Furstenberg's Lemma) Suppose μ is a probability measure on the projective space $\mathbb{P}(k^n)$. Then the stabilizer of μ in $\mathrm{PGL}_n(k)$ is compact unless μ is degenerate in the sense that it is supported on a finite number of proper (projective) linear subspaces.*

For the proof of this lemma, see Zimmer's book [20] or try to prove it yourself. Clearly the stabilizer of a degenerate measure preserves a finite union of proper subspaces. This contradicts our assumption.

To complete the proof, it remains to see that if Γ is not virtually solvable, then we can always reduce to the case above. This follows from two claims.

Claim 1. A linear group is not virtually solvable if and only if it has a finite index subgroup which has a linear representation in a vector space of dimension at least 2 which is absolutely strongly irreducible (i.e. it preserves no finite union of proper vector subspaces defined over any field extension).

Claim 2. If a finitely generated subgroup Γ of $\mathrm{GL}_d(K)$ acts absolutely strongly irreducibly on K^d, $d \geqslant 2$, and K is a finitely generated field, then K embeds in a local field k in such a way that Γ is unbounded in $\mathrm{GL}_d(k)$. □

Exercise. Prove Claim 1.

The proof of Claim 2 requires some basic algebra and number theory as proceeds as follows.

Exercise. Prove that if a subgroup of $\mathrm{GL}_d(\overline{K})$ acts irreducibly ($\overline{K}$=algebraic closure) and all of its elements have only 1 in their spectrum (i.e. are unipotents), then $d = 1$ (hint: use Burnside's theorem that the only subalgebra of $M_n(\overline{K})$ acting absolutely irreducibly is all of $M_n(\overline{K})$.)
Exercise. Show that a finitely generated field K contains only finitely many roots of unity and that if $x \in K$ is not a root of unity, they there is a local field k with absolute value $|\cdot|$ such that K embeds in k and $|x| \neq 1$ (hint: this is based on Kronecker's theorem that if a polynomial in $\mathbb{Z}[X]$ has all its roots within the unit disc, then all its roots are roots of unity; see [18, Lemma 4.1] for a full proof).
Exercise. Use the last two exercises to prove Claim 2.

II. Kazhdan's property (T)

Let us go back to general (countable) groups and introduce another spectral property of groups, namely Kazhdan's property (T). Our goal here is to give a very brief introduction. Many excellent references exist on property (T) starting with the 1989 Asterisque monograph by de la Harpe and Valette [**?**], the recent book by Bekka-de la Harpe-Valette for the classical theory; see also Shalom 2006 ICM talk for more recent developments.

Let π be a unitary representation of Γ on a Hilbert space $\mathcal{H}_\pi$. We say that π admits (a sequence of) *almost invariant vectors* if there is a sequence of unit vectors $v_n \in \mathcal{H}_\pi$ ($||v_n|| = 1$) such that $||\pi(\gamma)v_n - v_n||$ converges to 0 as n tends to $+\infty$ for every $\gamma \in \Gamma$.

Definition 0.5. *(Kazhdan's property (T)) A group Γ is said to have* Kazhdan's property (T) *if every unitary representation π admitting a sequence of almost invariant vectors admits a non-zero Γ-invariant vector.*

Groups with property (T) are sometimes also called *Kazhdan groups.*

A few simple remarks are in order following this definition:

- The definition resembles that of non-amenability, except that we are now considering all unitary representations of Γ and not just the left regular reprensentation $\ell^2(\Gamma)$ (given by $\lambda(\gamma)f(x) := f(\gamma^{-1}x)$). Indeed by Proposition **??**(3) above shows that a group is amenable if and only if the regular representation on $\ell^2(\Gamma)$ admits a sequence of almost invariant vectors.
- Property (T) is inherited by quotient groups of Γ (obvious from the definition).
- Finite groups have property (T) (simply average an almost invariant unit vector over the group).
- If Γ has property (T) and is amenable, then Γ is finite (indeed $\ell^2(\Gamma)$ has a non-zero invariant vector iff the constant function 1 is in $\ell^2(\Gamma)$ and this is iff Γ is finite).

A first important consequence[1] of property (T) is the following:

Proposition 0.6. *Every countable group with property (T) is finitely generated.*

Proof. Let S_n be an increasing family of finite subsets of Γ such that $\Gamma = \bigcup_n S_n$. Let $\Gamma_n := \langle S_n \rangle$ be the subgroup generated by S_n. We wish to show that $\Gamma_n = \Gamma$ for all large enough n. Consider the left action of Γ on the coset space Γ/Γ_n and the unitary representation π_n it induces on ℓ^2 functions on that coset space, $\ell^2(\Gamma/\Gamma_n)$. Let $\pi = \oplus_n \pi_n$ be the Hilbert direct sum of the $\ell^2(\Gamma/\Gamma_n)$ with the natural action of Γ on each factor. We claim that this unitary representation of Γ admits a sequence of almost invariant vectors. Indeed let v_n be the Dirac mass at $[\Gamma_n]$ in the coset space Γ/Γ_n. We view v_n as a (unit) vector in π. Clearly for every given $\gamma \in \Gamma$, if n is large enough γ belongs to Γ_n and hence preserves v_n. Hence $||\pi(\gamma)v_n - v_n||$ is equal to 0 for all large enough n and the $(v_n)_n$ form a family of almost invariant vectors. By Property (T), there is a non-zero invariant vector $\xi := \sum_n \xi_n$. The Γ-invariance of ξ is equivalent to the Γ-invariance of all $\xi_n \in \ell^2(\Gamma/\Gamma_n)$ simultaneously. However observe that if $\xi_n \neq 0$, then Γ/Γ_n must be finite (otherwise a non-zero constant function cannot be in ℓ^2). Since there must be some n such that $\xi_n \neq 0$, we conclude that some Γ_n has finite index in Γ. But Γ_n itself is finitely generated. It follows that Γ is finitely generated. □

So let Γ have property (T), and let S be a finite generating set for Γ. Then from the very definition we observe that there must be some $\varepsilon = \varepsilon(S) > 0$ such that for every unitary representation π of Γ without non-zero Γ-invariant vectors, one has:

$$\max_{s \in S} ||\pi(s)v - v|| \geqslant \varepsilon ||v||,$$

for every vector $v \in \mathcal{H}_\pi$.

And conversely it is clear that if there is a finite subset S in Γ with the above property, then every unitary representation of Γ with almost invariant vectors has an invariant vector. Hence this is equivalent to Property (T).

[1]This was in fact the reason for its introduction by Kazhdan in 1967 (at age 21). He used it to prove that non-uniform lattices in (higher rank) semisimple Lie groups are finitely generated. Nowadays new proofs exist of this fact, which are purely geometric and give good bounds on the size of the generating sets, see Gelander's lecture notes from the PCMI summer school.

Definition 0.7. *(Kazhdan constant) The (optimal) number $\varepsilon(S) > 0$ above is called a Kazhdan constant for the finite set S.*

Another important property of Kazhdan groups is that they have finite abelianization:

Proposition 0.8. *Suppose Γ is a countable group with property (T). Then $\Gamma/[\Gamma,\Gamma]$ is finite.*

Proof. Indeed, $\Gamma/[\Gamma,\Gamma]$ is abelian hence amenable. It also has property (T), being a quotient of a group with property (T). Hence it is finite (see itemized remark above). $\square$

This implies in particular that the non-abelian free groups do not have property (T) although they are non-amenable. In fact Property (T) is a rather strong spectral property a group might have. I tend to think of it as a rather rare and special property a group might have (although in some models of random groups, almost every group has property (T)).

Exercise. Show that if Γ has a finite index subgroup with property (T), then it has property (T). And conversely, if Γ has property (T), then every finite index subgroup also has property (T).

In fact establishing Property (T) for any particular group is never a simple task. In his seminal paper in which he introduced Property (T) Kazhdan proved that Property (T) for simple Lie groups of rank[2] at least 2. Then he deduced (as in the above exercise) that Property (T) is inherited by all discrete subgroups of finite co-volume in the Lie group G (i.e. lattices).

Theorem 0.9. *(Kazhdan 1967) A lattice in a simple real Lie group of real rank at least 2 has property (T).*

There are several proofs of Kazhdan's result for Lie groups (see e.g. Zimmer's book [20] and Bekka-delaHarpe-Valette [2] for two slightly different proofs). They rely of proving a "relative property (T)" for the pair $(\mathrm{SL}_2(\mathbb{R}) \ltimes \mathbb{R}^2, \mathbb{R}^2)$. This relative property (T) means that every unitary representation of the larger group with almost invariant vectors admits a non-zero vector which is invariant under the smaller group. One proof of this relative property makes use of Furstenberg's lemma above (Lemma 0.4). The proof extends to simple groups defined over a local field with rank at least 2 (over this local field).

Using a more precise understanding of the irreducible unitary representations of simple real Lie groups of rank one Kostant was able to prove that the rank one groups $Sp(n,1)$ and F_4^{-20} have property (T). However the other rank one groups $SU(n,1)$ and $SO(n,1)$ (including $SL_2(\mathbb{R})$) do not have property (T).

[2] In fact he proved it for rank at least 3 by reducing the proof to $\mathrm{SL}_3(\mathbb{R})$ since every simple real Lie group of rank at least 3 contains a copy of $\mathrm{SL}_3(\mathbb{R})$, but it was quickly realized by others (treating the case of $Sp_4(\mathbb{R})$) that the argument extends to groups of rank 2 as well.

The discrete group $\mathrm{SL}_n(\mathbb{Z})$ is a lattice in $\mathrm{SL}_n(\mathbb{R})$ and hence has property (T) by Kazhdan's theorem. Nowadays (following Burger and Shalom) they are more direct proofs that $\mathrm{SL}_n(\mathbb{Z})$ has property (T) (see the exercise sheet for Shalom's proof using bounded generation). Other examples of groups with property (T) include

Recently property (T) was established for $\mathrm{SL}_n(R)$, $n \geqslant 3$, where R is an arbitrary finitely generate commutative ring with unit, and even for $EL_n(R)$ for certain non-commutative rings R. For example:

Theorem 0.10. *(Ershov and Jaikin-Zapirain [?]) Let R be a (non-commutative) finitely generated ring with unit and $EL_n(R)$ be the subgroup of $n \times n$ matrices generated by the elementary matrix subgroups $Id_n + RE_{ij}$. If $n \geqslant 3$, then $EL_n(R)$ has property (T).*

In particular, if $\mathbb{Z}\langle x_1, \ldots, x_k\rangle$ denotes the free associative algebra on k generators, $EL_n(\mathbb{Z}\langle x_1, \ldots, x_k\rangle)$ has property (T) for all $k \geqslant 0$ and $n \geqslant 3$. As an other special case, the so-called *universal lattices* $EL_n(\mathbb{Z}[x_1, ..., x_k]) = \mathrm{SL}_n(\mathbb{Z}[x_1, ..., x_k])$, where $\mathbb{Z}[x_1, ..., x_k]$ is the ring of polynomials on k (commutative) indeterminates has property (T) when $n \geqslant 3$. This remarkable result extends earlier works of Kassabov, Nikolov and Shalom on various special cases. The Kazhdan constant in this case behave asymptotically as $\frac{1}{\sqrt{n+k}}$ for large n and k.

An important tool in some of these proofs (e.g. see Shalom ICM talk [17]) is the following characterization of property (T) in terms of affine actions of Hilbert spaces.

Theorem 0.11. *(Delorme-Guichardet) A group Γ has property (T) if and only if every action of Γ by affine isometries on a Hilbert space must have a global fixed point.*

See [?] or [2] for a proof. Kazhdan groups enjoy many other fixed point properties (e.g. Serre showed that they cannot act on trees without a global fixed point) and related rigidity properties (see e.g. the lectures by Dave Morris in this summer school).

Although the above class of examples of groups with property (T) all come from the world of linear groups, Kazhdan groups also arise geometrically, for example as hyperbolic groups through Gromov's random groups. For example the following holds:

Theorem 0.12. *In the density model of random groups, if the density is $< \frac{1}{2}$, then the random group is infinite and hyperbolic with overwhelming probability. If the density is $> \frac{1}{3}$, then the random group has property (T) with overwhelming probability.*

It is unknown whether $\frac{1}{3}$ is the right threshold for property (T). Below $\frac{1}{12}$ random groups have small cancellation $C'(1/6)$ and Ollivier and Wise proved that below $\frac{1}{6}$ they act freely and co-compactly on a $CAT(0)$ cube complex and are Haagerup, hence they do not have property (T).

For a proof of the above see Zuk [?], Ollivier [?], Gromov [?] and Ghys' Bourbaki talk [?]. In fact Zuk proved a similar result for a slightly different model of random groups (the so-called triangular model) and Ollivier sketches a reduction of the above to Zuk's theorem in [?]. The proof of this result is based on a geometric criterion for property (T) (due to Zuk, Ballmann-Zwiatkowski, originating in the work of Garland).

Let Γ be a group generated by a finite symmetric set S (with $e \notin S$). Let $L(S)$ be the finite graph whose vertices are the elements of S and an edge is drawn between two vertices s_1 and s_2 iff $s_1^{-1}s_2$ belongs to S. Suppose that $L(S)$ is connected (this is automatic if S is replaced say by $S \cup S^2 \setminus \{e\}$).

Theorem 0.13. *(local criterion for property (T)) Let Γ be a group generated by a finite symmetric set S (with $e \notin S$) such that the first non-zero eigenvalue of the Laplacian on the finite graph $L(S)$ is $> \frac{1}{2}$. Then Γ has property (T).*

For a short proof, see Gromov's random walks in random groups paper [?] and the end of Ghys' Bourbaki talk [?].

For certain groups of geometric origin, such as $Out(F_n)$ and the mapping class groups, determining whether they have property (T) are not can be very hard. For example it is not known whether $Out(F_n)$ has property (T) for $n \geqslant 4$ (even open for $Aut(F_n)$, not true for $n = 2, 3$ though). For the mapping class group, check the work of Andersen.

III. Uniformity issues in the Tits alternative, non-amenability and Kazhdan's property (T)

A well-known question of Gromov from [12] is whether the various invariants associated with an infinite group (such as the rate of exponential growth, the isoperimetric constant of a non-amenable group, the Kazhdan constant of a Kazhdan group, etc) can be made uniform over the generating set.

For example we say:

Definition 0.14. *Consider the family of all finite symmetric generating sets S of a given finitely generated group. Γ. We say that Γ*

- *has uniform exponential growth if $\exists \varepsilon > 0$ such that $\lim \frac{1}{n} \log |S^n| \geqslant \varepsilon$, for all S,*
- *is uniformly non-amenable if $\exists \varepsilon > 0$ such that $|\partial_S A| \geqslant \varepsilon |A|$ for S,*
- *has uniform property (T) if $\exists \varepsilon > 0$ such that $\max_S ||\pi(s)v - v|| \geqslant \varepsilon ||v||$ for all S and all unitary representations of Γ with no non-zero invariant vector.*
- *satisfies the uniform Tits alternative if $\exists N \in \mathbb{N} > 0$ such that S^N contains generators of a non-abelian free subgroup F_2.*

Note that there are some logical implications between these properties. For example if Γ satisfies the uniform Tits alternative, or if Γ (is infinite and) has uniform property (T), then Γ is uniformly non-amenable (exercise). Similarly if Γ is uniformly non-amenable, then Γ has uniform exponential growth.

Uniform exponential growth holds for linear groups of exponential growth (Eskin-Mozes-Oh [8]), for solvable groups of exponential growth (Osin), but fails for general groups as Wilson gave an example of a non-amenable group (even containing F_2) whose exponential growth is not uniform [19].

The uniform Tits alternative is known to hold for non-elementary hyperbolic groups (Koubi) and for non-virtually solvable linear group is known by work of Breuillard-Gelander [4]. In this case the uniformity is even stronger as one has:

Theorem 0.15. *(B. [6]) Given $d \in \mathbb{N}$, there is $N = N(d) \in \mathbb{N}$ such that for any field K and any finite symmetric set $S \subset \mathrm{GL}_d(K)$ one has S^N contains two generators of a non-abelian free subgroup F_2 unless $\langle S \rangle$ is virtually solvable.*

The uniformity in the field here requires some non-trivial number theory (see [5]). Of course this result implies that the rate of exponential growth is also bounded below by a positive constant depending only on the size of the matrix and not on the field. So the uniform exponential growth is also uniform in the field. However this is known to hold only for non-virtually solvable groups. It is an open question as to whether or not it also holds uniformly over all virtually solvable subgroups of $\mathrm{GL}_d(K)$ of exponential growth. In fact even the case of solvable subgroups of $\mathrm{GL}_2(\mathbb{C})$ is open. One can show however that if this is indeed the case, then this would imply the Lehmer conjecture from number theory [7], and that the analogous uniform Tits alternative for free semi-groups does not hold.

The above uniform Tits alternative has applications outside the world of infinite linear groups. It turns out that the uniformity in the field allows one to transfer information from the infinite world to the finite world (we'll see more of that in the remainder of this course). For example the following can be derived from Theorem 0.15

Corollary 0.16. *There is $N = N(d) \in \mathbb{N}$ and $\varepsilon = \varepsilon(d) > 0$ such that if S is a generating subset of $\mathrm{SL}_d(\mathbb{F}_p)$ (p arbitrary prime number), then S^N contains two elements a, b which generate $\mathrm{SL}_d(\mathbb{F}_p)$ and have no relation of length $\leqslant (\log p)^\varepsilon$. In other words the Cayley graph $\mathcal{G}(\mathrm{SL}_d(\mathbb{F}_p), \{a^{\pm 1}, b^{\pm 1}\})$ has girth at least $(\log p)^\varepsilon$.*

It is an open question whether one can take $\varepsilon = 1$ in the above result.

Uniform property (T) is even more mysterious. Examples where constructed by Osin and Sonkin [14]. Lattices in semisimple Lie groups with property (T) do not have uniform property (T) in general (examples were constructed by Gelander and Zuk). But it is an open problem to determine whether $\mathrm{SL}_n(\mathbb{Z})$ has uniform property (T) for $n \geqslant 3$.

1. Lecture 3: Property (τ) and expanders

To be continued...

References

[1] L. Bartholdi and A. Erschler, *Groups of given intermediate word growth*, preprint 2011 arXiv1110.3650.
[2] B. Bekka, P. de la Harpe and A. Valette, *Kazhdan's property* (T) New Mathematical Monographs, 11. Cambridge University Press, Cambridge, 2008. xiv+472 pp.

[3] E. Breuillard and T. Gelander, *On dense free subgroups of Lie groups*, J. Algebra 261 (2003), no. 2, 448–467.

[4] E. Breuillard and T. Gelander, *Uniform independence for linear groups*, Invent. Math. **173** (2008), no. 2, 225–263.

[5] E. Breuillard, *A Height Gap Theorem for finite subsets of* $\mathrm{GL}_d(\overline{\mathbb{Q}})$ *and non amenable subgroups*, preprint 2010.

[6] E. Breuillard, *A strong Tits alternative*, preprint, arXiv:0804.1395.

[7] E. Breuillard, *On uniform exponential growth for solvable groups*, Pure Appl. Math. Q. 3 (2007), no. 4, part 1, 949967

[8] A. Eskin, S. Mozes and H. Oh, *On uniform exponential growth for linear groups* Invent. Math. **160** (2005), no. 1, 1–30.

[9] R. Grigorchuk, *On the gap conjecture concerning group growth*, preprint 2011, arXiv1202.6044

[10] T. Ceccherini-Silberstein, R. Grigorchuk and P. de la Harpe, *Amenability and paradoxical decompositions for pseudogroups and discrete metric spaces* in Proc. Steklov Inst. Math. 1999, no. 1 (224), 57–97

[11] M. Gromov, *Groups of polynomial growth and expanding maps*, Inst. Hautes tudes Sci. Publ. Math. No. 53 (1981), 53–73.

[12] M. Gromov, *Asymptotic invariants of infinite groups*, Geometric group theory, Vol. 2 (Sussex, 1991), 1295, London Math. Soc. Lecture Note Ser., 182, Cambridge Univ. Press, Cambridge, 1993

[13] H. Kesten, *Symmetric random walks on groups,* Trans. Amer. Math. Soc., **92** (1959), 336–354.

[14] D. Osin and D. Sonkin, *Uniform Kazdhan groups.*

[15] Ch. Pittet and L. Saloff-Coste, *Survey on random walks on groups and isoperimetric profile*, available on L. Saloff-Coste web-page.

[16] Y. Shalom, *The growth of linear groups*, J. Algebra 199 (1998), no. 1, 169174.

[17] Y. Shalom, *The algebraization of Kazhdan's property (T)*, International Congress of Mathematicians. Vol. II, 12831310, Eur. Math. Soc., Zrich, 2006.

[18] J. Tits, *Free subgroups in linear groups*, Journal of Algebra, **20** (1972), 250-270.

[19] J. Wilson, *Further groups that do not have uniformly exponential growth*, J. Algebra 279 (2004), no. 1, 292301.

[20] R. Zimmer, *Ergodic theory and semisimple groups*, Monographs in Mathematics, 81. Birkhuser Verlag, Basel, 1984. x+209 pp.

Laboratoire de Mathématiques, Bâtiment 425, Université Paris Sud 11, 91405 Orsay, FRANCE

E-mail address: `emmanuel.breuillard@math.u-psud.fr`

LECTURE 3: PROPERTY (τ) AND EXPANDERS (PRELIMINARY VERSION)

EMMANUEL BREUILLARD

There are many excellent existing texts for the material in this lecture, starting with Lubotzky's monograph [11] and recent AMS survey paper [10]. For expander graphs and their use in theoretical computer science, check the survey by Hoory, Linial and Wigderson [6]. We give here a brief introduction.

I. Expander graphs

We start with a definition.

Definition 0.1. *(Expander graph) A finite connected k-regular graph $\mathcal{G}$ is said to be an ε-expander if for every subset A of vertices in $\mathcal{G}$, with $|A| \leqslant \frac{1}{2}|\mathcal{G}|$, one has the following isoperimetric inequality:*

$$|\partial A| \geqslant \varepsilon |A|,$$

where ∂A denotes the set of edges of $\mathcal{G}$ which connect a point in A to a point in its complement A^c.

The optimal ε as above is sometimes called the *discrete Cheeger constant* of the graph:

$$h(\mathcal{G}) = \inf_{A \subset \mathcal{G}, |A| \leqslant \frac{1}{2}|\mathcal{G}|} \frac{|\partial A|}{|A|},$$

Just as in Lecture 1, when we discussed the various equivalent definitions of amenability, it is not a surprise that this definition turns out to have a spectral interpretation.

Given a k-regular graph $\mathcal{G}$, one can consider the Markov operator (also called averaging operator, or sometimes Hecke operator in reference to the Hecke graph of an integer lattice) on functions on vertices on $\mathcal{G}$ defined as follows:

$$Pf(x) = \frac{1}{k} \sum_{x \sim y} f(y),$$

where we wrote $x \sim y$ to say that y is a neighbor of x in the graph.

This operator is easily seen to be self-adjoint on $\ell^2(\mathcal{G})$, which is a finite dimensional Euclidean space. Moreover it is a contraction, namely $||Pf||_2 \leqslant ||f||_2$ and hence its spectrum is real and contained in $[-1, 1]$. We can write the eigenvalues of P in decreasing

Date: July 14th 2012.

order as $\mu_0 = 1 \geqslant \mu_1 \geqslant \ldots \geqslant \mu_{|\mathcal{G}|}$. The top eigenvalue μ_0 must be 1, because the constant function $\mathbf{1}$ is clearly an eigenfunction of P, with eigenvalue 1. On the other hand, since $\mathcal{G}$ is connected $\mathbf{1}$ is the only eigenfunction (up to scalars) with eigenvalue 1. This is immediate by the maximum principle (if $Pf = f$ and f achieve its maximum at x, then f must take the same value $f(x)$ at each neighbor of x, and this value spreads to the entire graph). Hence the second eigenvalue μ_1 is strictly less than 1.

Instead of P, we may equally well consider $\Delta := Id - P$, which is then a non-negative self-adjoint operator. This operator is called the *combinatorial Laplacian* in analogy with the Laplace-Beltrami operator on Riemannian manifolds.

$$\Delta f(x) := f(x) - \frac{1}{k} \sum_{x \sim y} f(y).$$

Its eigenvalues are traditionally denoted by $\lambda_0 = 0 < \lambda_1 \leqslant \ldots \leqslant \lambda_{|\mathcal{G}|}$ and :

$$\lambda_i(\mathcal{G}) = 1 - \mu_i(\mathcal{G}).$$

As promised, here is the connection between the spectral gap an the edge expansion.

Proposition 0.2. *(Discrete Cheeger-Buser inequality) Given a connected k-regular graph, we have:*

$$\frac{1}{2}\lambda_1(\mathcal{G}) \leqslant \frac{1}{k} h(\mathcal{G}) \leqslant \sqrt{2\lambda_1(\mathcal{G})}$$

The proof of this proposition follows a similar line of argument as the proof we gave in Lecture 1 of the Kesten criterion relating the Folner condition and the spectral radius of the averaging operator. See Lubotzky's book [11] for detailed derivation.

We note in passing that, since P is self-adjoint, the following holds:

$$||P||_{\ell_0^2} = \max_{i \neq 0} |\mu_i|$$

where ℓ_0^2 is the space of functions on $\mathcal{G}$ with zero average, and

$$\mu_1 = \sup\{\frac{\langle Pf, f\rangle}{||f||_2^2}; \sum_{x \in \mathcal{G}} f(x) = 0\}$$

and hence

$$\lambda_1 = \inf\{\frac{\langle \Delta f, f\rangle}{||f||_2^2}; \sum_{x \in \mathcal{G}} f(x) = 0\} = \frac{1}{k} \inf\{\frac{||\nabla f||_2^2}{||f||_2^2}; \sum_{x \in \mathcal{G}} f(x) = 0\}.$$

Expander graphs have many very interesting applications in theoretical computer science (e.g. in the construction of good error correcting codes, see [6]). There typically one wants to have a graph of (small) bounded degree (i.e. k is bounded) but whose number of vertices is very large. For this it is convenient to use the following definition:

Definition 0.3. *(family of expanders) Let $k \geqslant 3$. A family $(\mathcal{G}_n)_n$ of k-regular graphs is said to be a family of expanders if the number of vertices $|\mathcal{G}_n|$ tends to $+\infty$ and if there is $\varepsilon > 0$ independent of n such that for all n*

$$\lambda_1(\mathcal{G}_n) \geqslant \varepsilon.$$

Although almost every random k-regular graph is an expander (Pinsker 1972), the first explicit construction of an infinite family of expander graphs was given using Kazhdan's property (T) and is due to Margulis [13] (see below Proposition 0.5).

Clearly an ε-expander graph of size N has diameter at most $O(\frac{1}{\varepsilon}\log|\mathcal{G}|)$. But more is true. A very important feature of expander graphs is the fact that the simple random walk on such a graph equidistributes as fast as could be towards the uniform probability distribution. This is made precise by the following proposition:

Proposition 0.4. *(Random walk characterization of expanders) Suppose $\mathcal{G}$ is a k-regular graph such that $|\mu_i(\mathcal{G})| \leqslant 1-\varepsilon$ for all $i \neq 0$, then there is $C = C(\varepsilon, k) > 0$ such that if $n \geqslant C\log|\mathcal{G}|$ then*

$$\max_{x,y} |\langle P^n\delta_x, \delta_y\rangle - \frac{1}{|\mathcal{G}|}| \leqslant \frac{1}{|\mathcal{G}|^{10}}.$$

Conversely for every $C > 0$ there is $\varepsilon = \varepsilon(C,k) > 0$ such that if the k-regular graph $\mathcal{G}$ satisfies

$$\max_{x} |\langle P^{2n}\delta_x, \delta_x\rangle - \frac{1}{|\mathcal{G}|}| \leqslant \frac{1}{|\mathcal{G}|^{10}},$$

for some $n \leqslant C\log|\mathcal{G}|$, then $\mathcal{G}$ satisfies $|\mu_i(\mathcal{G})| \leqslant 1-\varepsilon$ for all $i \neq 0$ (and in particular is an expander).

Here $\langle P^n\delta_x, \delta_y\rangle$ can be interpreted in probabilistic terms as the transition probability from x to y at time n, namely the probability that a simple (=equiprobable nearest neighbor) random walk starting at x visits y at time n.

The condition here that $||P|| = \max_{i\neq 0}|\mu_i(\mathcal{G})| \leqslant 1-\varepsilon$ is only slightly stronger than being an expander. The only difference is that we require the smallest eigenvalue $\mu_{\mathcal{G}}$ to be bounded away from -1 as well. In practice this is often satisfied and one can always get this by changing $\mathcal{G}$ into the induced k^2-regular graph obtained by connecting together vertices at distance 2 in $\mathcal{G}$ (which has the effect of changing P into P^2, hence squaring the eigenvalues).

The exponent 10 in the remainder term is nothing special and can be replaced by any exponent > 1.

Proof. The function $f_x := \delta_x - \frac{1}{|\mathcal{G}|}\mathbf{1}$ has zero mean on $\mathcal{G}$, hence

$$|\langle P^n\delta_x, \delta_y\rangle - \frac{1}{|\mathcal{G}|}| = |\langle P^n f_x, \delta_y\rangle| \leqslant ||P||^n ||f_x|| ||\delta_y|| \leqslant \sqrt{2}(1-\varepsilon)^n.$$

Now this is at most $1/|\mathcal{G}|$ as some as $n \geqslant C_\varepsilon \log|\mathcal{G}|$ for some $C_\varepsilon > 0$.

Conversely observe that $trace(P^{2n}) = \sum_{x\in\mathcal{G}} \langle P^{2n}\delta_x, \delta_x\rangle$, and hence summing the estimates for $\langle P^{2n}\delta_x, \delta_x\rangle$, we obtain

$$|trace(P^{2n}) - 1| \leqslant \frac{1}{|\mathcal{G}|^9},$$

But on the other hand $trace(P^{2n}) = 1 + \mu_1^{2n} + \ldots + \mu_{|\mathcal{G}|}^{2n}$, hence

$$\max_{i\neq 0} |\mu_i|^{2n} \leqslant \mu_1^{2n} + \ldots + \mu_{|\mathcal{G}|}^{2n} \leqslant \frac{1}{|\mathcal{G}|^9},$$

thus recalling that $|\mathcal{G}|^{1/\log|\mathcal{G}|} = e$, we obtain the desired upper bound on $\max_{i\neq 0}|\mu_i|$. □

This fast equidistribution property is usually considered as a feature of expander graphs, a consequence of the spectral gap. We will see in the last lecture, when explaining the Bourgain-Gamburd method, that the proposition can also be used in the reverse direction and be used to establish the spectral gap.

For more about random walks on finite graphs and groups and the speed of equidistribution (the cut-off phenomenon, etc) see the survey by Saloff-Coste [14].

II. Property (τ)

Margulis [13] was the first to construct an explicit family of k-regular expander graphs. For this he used property (T) through the following observation:

Proposition 0.5. *((T) implies (τ)) Suppose Γ is a group with Kazhdan's property (T) and S is a symmetric set of generators of Γ of size $k = |S|$. Let $\Gamma_n \leqslant \Gamma$ be a family of finite index subgroup such that the index $[\Gamma : \Gamma_n]$ tends to $+\infty$ with n. Then the family of Schreier graphs $\mathcal{S}(\Gamma/\Gamma_n, S)$ forms a family of k-regular expanders.*

Recall that the Schreier graph of a coset space Γ/Γ_0 associated to a finite symmetric generating set S of Γ is the graph whose vertices are the left cosets of Γ_0 in Γ and one connects $g\Gamma_0$ to $h\Gamma_0$ if there is $s \in S$ such that $g\Gamma_0 = sh\Gamma_0$.

Proof. The group Γ acts on the finite dimensional Euclidean space $\ell_0^2(\Gamma/\Gamma_n)$ of ℓ^2 functions with zero average on the finite set Γ/Γ_n. Denote the resulting unitary representation of Γ by π_n. Property (T) for Γ gives us the existence of a Kazhdan constant $\varepsilon = \varepsilon(S) > 0$ such that $\max_{s\in S}||\pi(s)v - v|| \geqslant \varepsilon||v||$ for every unitary representation π of Γ without invariant vectors. In particular, this applies to the π_n since they have no non-zero Γ-invariant vector. This implies that the graphs $\mathcal{G}_n := \mathcal{S}(\Gamma/\Gamma_n, S)$ are ε-expanders, because if $A \subset \mathcal{G}_n$ has size at most half of the graph, then $v := 1_A - \frac{|A|}{|\mathcal{G}|}\mathbf{1}$ is a vector in $\ell_0^2(\Gamma/\Gamma_n)$ and $||\pi_n(s)v - v||^2 = ||\pi_n(s)1_A - 1_A||^2 = |sA\Delta A|$, while $||v||^2 = 2|A|(1 - \frac{|A|}{|\mathcal{G}_n|}) \geqslant |A|$. In particular $|\partial A| \geqslant \varepsilon^2|A|$. □

So we see that Cayley graphs (or more generally Schreier graphs) of finite quotients of finitely generated groups can be yield families of expanders. This is the case for the family of Cayley graphs of $\mathrm{SL}_3(\mathbb{Z}/m\mathbb{Z})$ associated to the reduction mod m of a fixed generating set S in $\mathrm{SL}_3(\mathbb{Z})$. To characterize this property, Lubotzky introduced the following terminology:

Definition 0.6. *(Property (τ)) A finitely generated group Γ with finite symmetric generating set S is said to have* property (τ) *with respect to a family of finite index normal subgroups $(\Gamma_n)_n$ if the family of Cayley graphs $\mathcal{G}(\Gamma/\Gamma_n, S_n)$, where $S_n = S\Gamma_n/\Gamma_n$ is the projection of S to Γ/Γ_n, is a family of expanders. If the family $(\Gamma_n)_n$ runs over all finite index normal subgroups of Γ, then we say that Γ has* property (τ).

Proposition 0.5 above shows that every group with property (T) has property (τ). The converse is not true and property (τ) is in general a weaker property which holds more often. For example Lubotzky and Zimmer showed that an irreducible lattice in a semisimple real Lie group has property (τ) as soon as one of the simple factors of the ambient semisimple Lie group is of real rank at least 2 (and hence has property (T) by Kazhdan's theorem).

Property (τ) is stable under quotients and under passing to and from a finite index subgroup. In particular groups with property (τ) have finite abelianization, just as Kazhdan's groups.

Arithmetic lattices in semisimple algebraic groups defined over $\mathbb{Q}$ admit property (τ) with respect to the family of all congruence subgroups. Namely:

Theorem 0.7. *(Selberg, Burger-Sarnak, Clozel) Let $\mathcal{G} \subset \mathrm{GL}_d$ is a semisimple algebraic $\mathbb{Q}$-group, $\Gamma = \mathcal{G}(\mathbb{Z}) = \mathcal{G}(\mathbb{Q}) \cap \mathrm{GL}_d(\mathbb{Z})$ and $\Gamma_m = \Gamma \cap \ker(\mathrm{GL}_d(\mathbb{Z}) \to \mathrm{GL}_d(\mathbb{Z}/m\mathbb{Z}))$, then Γ has property (τ) with respect to the Γ_m's.*

This property is also called the *Selberg property* because in the case of $\mathcal{G} = \mathrm{SL}_2$ it follows (see below) from the celebrated theorem of Selberg, which asserts that the non-zero eigenvalues of the Laplace-Beltrami laplacian on the hyperbolic surfaces of finite co-volume $\mathbb{H}^2/\ker(\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z}))$ are bounded below by a positive constant independent of m (in fact $\frac{3}{16}$). The general case was established by Burger-Sarnak and Clozel.

This connects property (τ) for lattices with another interesting feature of some lattices, namely the *congruence subgroup property.* This property of an arithmetic lattice asks that every finite index subgroup contains a congruence subgroup (i.e. a subgroup of the form $\mathcal{G}(\mathbb{Z}) \cap \ker(\mathrm{GL}_d(\mathbb{Z}) \to \mathrm{GL}_d(\mathbb{Z}/m\mathbb{Z}))$. It is easy to see that if $\mathcal{G}(\mathbb{Z})$ has both the Selberg property and the congruence subgroup property, then it has property (τ) (with respect to all of its finite index subgroups). See the exercise sheet.

An interesting open problem in this direction is to determine whether or not lattices in $SO(n,1)$ can have property (τ) or not. Lubotzky and Sarnak conjecture that they do not, and this would also follow from Thurston's conjecture that such lattices have a subgroup of finite index with infinite abelianization.

The link between Selberg's $\frac{3}{16}$ theorem and property (τ) is provided by the following general fact, which relates the combinatorial spectral gap of a Cayley (or Schreier) graph of finite quotients of the fundamental group of a manifold with the spectral gap for the analytic Laplace-Beltrami operator on the Riemannian manifold.

Recall that given a connected Riemannian manifold M the Laplace-Beltrami operator is a non-negative self-adjoint operator for L^2 functions with respect to the Riemannian volume measure and that if M is compact, its spectrum is discrete $\lambda_0(M) = 1 < \lambda_1(M) \leqslant \ldots$ (e.g. see [1]).

The fundamental group $\Gamma = \pi_1(M)$ acts freely and co-compactly on the universal cover $\widetilde{M}$ by isometries (for the lifted Riemannian metric on $\widetilde{M}$). Given a base point $x_0 \in \widetilde{M}$, the set

$$\mathcal{F}_M = \{x \in \widetilde{M}; d(x, x_0) < d(x, \gamma \cdot x_0) \ \forall \gamma \in \Gamma \setminus \{1\}\}$$

is a (Dirichlet) fundamental domain for the action of Γ on $\widetilde{M}$. Moreover the group Γ is generated by the finite symmetric set $S := \{\gamma \in \Gamma; \gamma\overline{\mathcal{F}_M} \cap \overline{\mathcal{F}_M} \neq \varnothing\}$. We can now state:

Theorem 0.8. *(Brooks [3], Burger [4]) Let M be a compact Riemannian manifold with fundamental group $\Gamma = \pi_1(M)$. Let S be the finite symmetric generating set of Γ obtained from a Dirichlet fundamental domain $\mathcal{F}_M$ as above. Then there are constants $c_1, c_2 > 0$ depending on M only such that for every finite cover M_0 of M*

$$c_1\lambda_1(M_0) \leqslant \lambda_1(\mathcal{G}(\Gamma/\Gamma_0, S)) \leqslant c_2\lambda_1(M_0),$$

where Γ_0 is the fundamental group of M_0 and $\mathcal{G}(\Gamma/\Gamma_0, S))$ the Schreier graph of the finite coset space Γ/Γ_0 associated to the generating set S.

We deduce immediately:

Corollary 0.9. *Suppose $(M_n)_n$ is a sequence of finite covers of M. Then there is a uniform lower bound on $\lambda_1(M_n)$ if and only if $\Gamma := \pi_1(M)$ has property (τ) with respect to the sequence of finite index subgroups $\Gamma_n := \pi_1(M_n)$.*

The proof consists in observing that the Schreier graph can be drawn on the manifold M_0 as a dual graph to the decomposition of M_0 into translates of the fundamental domain $\mathcal{F}_M$. The inequality on the left hand side is easier as one can use the interpretation in terms of Cheeger constants and given a set A of vertices with $|\partial A| \leqslant \varepsilon|A|$ one can look at the corresponding union of fundamental domains in M_0 and see that its boundary has small surface area compared to its volume. The other direction is a bit more involved and requires comparing the Rayleigh quotients $\frac{||\nabla f||}{||f||}$ of a function on M_0 with the combinatorial Rayleigh quotients of the function on the vertices of the graph obtained by averaging f over each fundamental domain. The result also extends to non-compact hyperbolic manifolds of finite co-covolume (see [2, Section 2] and [5, Appendix]).

For more on property (τ) we refer the reader to the book by Lubotzky and Zuk [12].

References

[1] M. Berger, P. Gauduchon, E. Mazet, *Le spectre d'une variete Riemannienne*, Lecture Notes in Mathematics, Vol. 194 Springer-Verlag, Berlin-New York 1971 vii+251 pp.

[2] J. Bourgain, A. Gamburd, P. Sarnak, *Generalization of Selberg's* 3/16 *theorem and affine sieve*, Acta Math. 207 (2011), no. 2, 255290.

[3] R. Brooks, *The first eigenvalue in a tower of coverings*, Bull. Amer. Math. Soc. (N.S.) 13 (1985), no. 2, 137140.

[4] M. Burger,*Spectre du laplacien, graphes et topologie de Fell* Comment. Math. Helv. 63 (1988), no. 2, 226252.

[5] J. Ellenberg, Ch. Hall and E. Kowalski, *Expander graphs, gonality and variation of Galois representations*, arXiv:1008.3675

[6] S. Hoory, N. Linial and A. Wigderson, *Expander graphs and their applications,* Bull. Amer. Math. Soc. (N.S.) **43** (2006), no. 4, 439–561.

[7] M. Kassabov, *Symmetric Groups and Expander Graphs*, Invent. Math. **170** (2007), no. 2, 327-354.

[8] M. Kassabov, A. Lubotzky, N. Nikolov, *Finite simple groups as expanders*, Proc. Natl. Acad. Sci. USA **103** (2006), no. 16, 6116–6119

[9] H. Kesten, *Symmetric random walks on groups,* Trans. Amer. Math. Soc., **92** (1959), 336–354.

[10] A. Lubotzky, *Expander graphs in pure and applied mathematics*, (notes for the colloquium lectures, AMS annual meating 2010).

[11] A. Lubotzky, *Finite simple groups of Lie type as expanders,* `arxiv:math/0904.3411`.

[12] A. Lubotzky, A Zuk, *Property* (τ), draft of book.

[13] G. Margulis, *Explicit constructions of expanders*, Problemy Peredacl Informacii **9** (1973), 71–80.

[14] L. Saloff-Coste, *Random walks on finite groups*, Probability on discrete structures, 263–346, Encyclopaedia Math. Sci., 110, Springer, Berlin, 2004. Harry Kesten, Editor

Laboratoire de Mathématiques, Bâtiment 425, Université Paris Sud 11, 91405 Orsay, FRANCE

E-mail address: `emmanuel.breuillard@math.u-psud.fr`

LECTURE 4: APPROXIMATE GROUPS AND THE BOURGAIN-GAMBURD METHOD (PRELIMINARY VERSION)

EMMANUEL BREUILLARD

I. The Bourgain-Gamburd method

Up until the Bourgain-Gamburd 2005 breakthrough the only known ways to turn $\mathrm{SL}_d(\mathbb{F}_p)$ into an expander graph (i.e. to find a generating set of small size whose associated Cayley graph has a good spectral gap) was either through property (T) (as in the Margulis construction) when $d \geqslant 3$ or through the Selberg property (and the dictionary between combinatorial expansion of the Cayley graphs and the spectral gap for the Laplace-Beltrami Laplacian on towers of covers of hyperbolic manifolds) when $d = 2$.

This poor state of affairs was particularly well-illustrated by the embarrassingly open question of Lubotzky, the *Lubotzky* $1-2-3$ *problem*, which asked whether the subgroups $\Gamma_i := \langle S_i \rangle \leqslant \mathrm{SL}_2(\mathbb{Z})$ for $i = 1, 2$ and 3 given by

$$S_i = \{ \begin{pmatrix} 1 & \pm i \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ \pm i & 1 \end{pmatrix} \}$$

have property (τ) with respect to the family of congruence subgroups $\Gamma_i \cap \ker(\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}))$ as p varies among the primes. The answer for $i = 1$ and 2 follows as before from Selberg's $\frac{3}{16}$ theorem, because both Γ_1 and Γ_2 are subgroups of finite index in $\mathrm{SL}(2, \mathbb{Z})$ (even $\Gamma_1 = \mathrm{SL}_2(\mathbb{Z})$). However Γ_3 has infinite index in $\mathrm{SL}_2(\mathbb{Z})$ and therefore none of these methods applies.

Bourgain and Gamburd changed the perspective by coming up with a more head-on attack of the problem showing fast equidistribution of the simple random walk directly (which as we saw yields a spectral gap) by more analytic and combinatorial means. One of these combinatorial ingredients was the notion of an approximate group (see below) which was subsequently studied for its own sake and lead in return to many more applications about property (τ) and expanders as we are about to describe.

Let us now state the Bourgain-Gamburd theorem:

Theorem 0.1. *(Bourgain-Gamburd* [1]*) Given $k \geqslant 1$ and $\tau > 0$ there is $\varepsilon = \varepsilon(k, \tau) > 0$ such that every Cayley graph $\mathcal{C}(\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}), S)$ of $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ with symmetric generating set S of size $2k$ and girth at least $\tau \log p$ is an ε-expander.*

Date: July 19th 2012.

We recall that the *girth* of a graph is the length of the shortest loop in the graph. Conjecturally all Cayley graphs of $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ are ε-expanders for a uniform ε, and this was later established for almost all primes in Breuillard-Gamburd [4] using the Uniform Tits alternative. But the Bourgain-Gamburd theorem is the first instance of a result on expanders where a purely geometric property, such as large girth, is shown to imply a spectral gap.

The Bourgain-Gamburd result answers positively the Lubotzky $1-2-3$ problem:

Corollary 0.2. *Every non-virtually solvable subgroup* Γ *in* $\mathrm{SL}_2(\mathbb{Z})$ *has property* (τ) *with respect to the congruence subgroups* $\Gamma_p := \Gamma \cap \ker(\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}))$ *as* p *varies among the primes.*

Proof. Let S be a symmetric generating set for Γ. By the Tits alternative (or using the fact that $\mathrm{SL}_2(\mathbb{Z})$ is virtually free), there is $N = N(\Gamma) > 0$ such that S^N contains two generators of a free group a, b. Now in order to prove the spectral gap for the action of S on $\ell^2(\Gamma/\Gamma_p)$ it is enough to prove a spectral gap for the action of a and b. Indeed suppose there is $f \in \ell_0^2(\Gamma/\Gamma_p)$ such that $\max_{s\in S} ||s \cdot f - f|| \leqslant \varepsilon ||f||$. Then writing a and b as words in S of length at most N, we conclude that $||a \cdot f - f|| \leqslant N\varepsilon||f||$ and $||b \cdot f - f|| \leqslant N\varepsilon||f||$. Since N depends only on Γ and not on p we have reduced the problem to proving spectral gap for $\langle a, b\rangle$ and we can thus assume that $\Gamma = \langle a, b\rangle$ is a 2-generated free subgroup of $\mathrm{SL}_2(\mathbb{Z})$.

Then it is easy to verify that the logarithmic girth condition holds for this new Γ. Indeed the size of the matrices $w(a, b)$, where w is a word of length n do not exceed $\max\{||a^{\pm 1}||, ||b^{\pm 1}||\}^n$, hence $w(a, b)$ is not killed modulo p if p is larger that $\max\{||a^{\pm 1}||, ||b^{\pm 1}||\}^n$, that is if n is smaller that $\tau \log p$ for some $\tau = \tau(a, b) > 0$. We can then apply the theorem and we are done. □

Before we go further, let us recall the following:

Theorem 0.3. *(Strong Approximation Theorem, Nori* [9]*, Weisfeiler* [15]*) Let* Γ *be a Zariski-dense subgroup of* $\mathrm{SL}_d(\mathbb{Z})$*. Then its projection modulo* p *via the map* $\mathrm{SL}_d(\mathbb{Z}) \to \mathrm{SL}_d(\mathbb{Z}/p\mathbb{Z})$ *is surjective for all but finitely many primes* p*.*

This is a deep result (see also alternate proofs by Hrushovski-Pillay via model theory and by Larsen-Pink), which in the special case of $\mathrm{SL}_2(\mathbb{Z})$ is in fact just an exercise (once one observes that the only large subgroups of $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ are dihedral, diagonal, or upper triangular). It will be important for us, because it says that $\Gamma/\Gamma_p = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ as soon as p is large enough, and we will use several key features of $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ in the proof of Theorem 0.1.

We are now ready for a sketch of the Bourgain-Gamburd theorem.

Let $\nu = \frac{1}{|S|}\sum_{s\in S} \delta_s$ be the symmetric probability measure supported on the generating set S. Our first task will be to make explicit the connection between the decay of the probability of return to the identity and the spectral gap, pretty much as we did in Lecture 3. We may write:

$$\nu^{2n}(e) = \langle P_\nu^{2n}\delta_e, \delta_e\rangle = \frac{1}{|G_p|}\sum_{x\in G_p}\langle P_\nu^{2n}\delta_x, \delta_x\rangle$$

where we have used the fact that the Cayley graph is homogeneous (i.e. vertex transitive) and hence the probability of return to the e starting from the e is the same as the one of returning to x starting from x, whatever $x \in G_p$ may be, so $\langle P_\nu^{2n}\delta_e, \delta_e\rangle = \langle P_\nu^{2n}\delta_x, \delta_x\rangle$.

A key ingredient here is that we will make use of an important property of finite simple groups of Lie type (such as $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$) which is that they have no non-trivial finite dimensional complex representation of small dimension. This is due to Frobenius for $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ and to Landazuri and Seitz for arbitrary finite simple groups of Lie type. For $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ this says that the dimension of a non-trivial irreducible (complex) representation is always at least $\frac{p-1}{2}$.

A consequence of this fact is the following *high multiplicity trick*: the eigenvalues of P_ν on $\ell_0^2(\Gamma/\Gamma_p)$ all appear with multiplicity at least $\frac{p-1}{2}$. Indeed, first by the above strong approximation theorem $\Gamma/\Gamma_p = G_p := \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ and the regular representation $\ell^2(\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}))$ can be decomposed into irreducible (complex) linear representations, each of which appears with a multiplicity equal to its dimension[1]. The operator P_ν preserves each one of these invariant subspaces, and hence its non-trivial eigenvalues appear with a multiplicity at least equal to $\frac{p-1}{2}$. Since $\frac{p-1}{2} \simeq |G_p|^{\frac{1}{3}}$, we get

$$\nu^{2n}(e) = \frac{1}{|G_p|}(\mu_0^{2n} + \mu_1^{2n} + \ldots + \mu_{|G_p|-1}^{2n}) \gg \mu_1^{2n}\frac{|G_p|^{\frac{1}{3}}}{|G_p|}$$

where the μ_i's are the eigenvalues of P_ν, $\mu_0 = 1$ and $G_p = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, and $\gg$ means larger than up to a positive multiplicative constant.

Hence

$$\mu_1^{2n} \ll \nu(e)^{2n}|G|^{\frac{2}{3}}$$

So if we knew that

$$\nu^{2n}(e) \ll \frac{1}{|G_p|^{1-\beta}}$$

for some small $\beta < \frac{1}{3}$ and for n of size say at most $C\log|G_p|$ for some constant $C > 0$, we would deduce the following spectral gap:

$$\mu_1 \leqslant e^{-\frac{1/3-\beta}{C}} < 1$$

(recall that $|G_p|^{\frac{1}{\log|G_p|}}$ equals e and is independent of $|G_p|$;-))

[1]This is a standard fact from the representation theory of finite groups, see e.g. Serre [11].

Therefore, thanks to this high multiplicity trick, proving a spectral gap boils down to establishing rapid decay of the probability of return to the identity in a weaker sense than what we had in Lecture 3, namely it is enough to establish that

$$\nu^{2n}(e) \ll \frac{1}{|G_p|^{1-\beta}} \tag{0.3.1}$$

for some $n \leqslant C \log |G_p|$ and some $\beta > 0$, where C and β are constants independent of p.

Now we have not used the girth assumption yet (in fact we will use it one more time towards the end of the argument). This tells us that the Cayley graph looks like a tree (a $2k$-regular homogeneous tree) on any ball of radius $< \tau \log p$ (note that the Cayley graph is vertex transitive, so it looks the same when viewed from any point). In particular the random walk behaves exactly like a random walk on a free group on k-generators at least for times $n < \tau \log p$. However, we saw in Lecture 1, that

$$\nu^{2n}(e) \leqslant \rho(\nu)^{2n}$$

for every n, where $\rho(\nu)$ is the spectral radius of the random walk. For the simple random walk on a free group F_k, the spectral radius is $\rho = e^{-C_k} := \frac{\sqrt{2k-1}}{k} < 1$ (as was computed by Kesten, see [8]). Hence for $n \simeq \tau \log p \simeq \frac{\tau}{3} \log |G_p|$ we have:

$$\nu^{2n}(e) \ll \frac{1}{|G_p|^{\alpha}} \tag{0.3.2}$$

where $\alpha = \alpha(\tau) = C_k \tau / 3 > 0$.

However $\alpha(\tau)$ will typically be small, and our task is now to bridge the gap between (0.3.2), which holds at time $n \simeq \tau \log p$ and (0.3.1), which we want to hold before $C \log p$ for some constant C independent of p.

Hence we need $\nu^{2n}(e)$ to keep decaying at a certain controlled rate for the time period $\tau \log p \leqslant n \leqslant C \log p$. This decay will be slower than the exponential rate taking place at the beginning thanks to the girth condition, but still significant. And this is where approximate groups come into the game.

II. Approximate groups

Approximate groups were introduced around 2005 by T. Tao, who was motivated both by their appearance in the Bourgain-Gamburd theorem and because they form a natural generalization to the non-commutative setting of the objects studied in additive combinatorics such as finite sets of integers with small doubling.

Definition 0.4. *Let G be a group and $K \geqslant 1$ a parameter. A finite subset $A \subset G$ is called a K-approximate subgroup of G if the following holds:*

- $A^{-1} = A$, $1 \in A$
- *there is $X \subset G$ with $X = X^{-1}$, $|X| \leqslant K$, such that $AA \subset XA$.*

Here K should be thought as being much smaller than $|A|$. In practice it will be important to keep track of the dependence in K. If $K = 1$, then A is the same thing as a finite subgroup. Another typical example of an approximate group is an interval $[-N, N] \in \mathbb{Z}$, or any homomorphic image of it. More generally any homomorphic image of a word ball in the free nilpotent group of rank r and step s is a $C(r, s)$-approximate group (a nilprogression). A natural question regarding approximate groups is to classify them and Tao coined this the "non-commutative inverse Freiman problem" (in honor of G. Freiman who classified approximate subgroups of $\mathbb{Z}$ back in the 60's, see [13]). Recently Breuillard-Green-Tao proved such a classification theorem [6] for arbitrary approximate groups showing that they are essentially built as extensions of a finite subgroup by a nilprogression.

For linear groups and groups of Lie type such as $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ a much stronger classification theorem can be derived:

Theorem 0.5. *(Pyber-Szabo* [10]*, Breuillard-Green-Tao* [5]*) Suppose* $\mathbf{G}$ *is a simple algebraic group of dimension* d *defined over a finite field* $\mathbb{F}_q$ *(such as* $\mathrm{SL}_n(\mathbb{F}_q)$*). Let* A *be a* K*-approximate subgroup of* $\mathbf{G}(F_q)$*. Then*

- *either* A *is contained in a proper subgroup of* $\mathbf{G}(\mathbb{F}_q)$*,*
- *or* $|A| \leqslant K^C$*,*
- *or* $|A| \geqslant |\mathbf{G}(\mathbb{F}_q)|/K^C$*.*

where $C = C(d) > 0$ *is a constant independent of* q*.*

This result can be interpreted by saying that there are no non-trivial approximate subgroups of simple algebraic groups (disregarding the case when A is contained in a proper subgroup).

Theorem 0.5 was first proved by H. Helfgott for $\mathrm{SL}_2(\mathbb{F}_p)$, p prime, by combinatorial means (using the Bourgain-Katz-Tao *sum-product theorem* [2]). The general case was later established independently by Pyber-Szabo and Breuillard-Green-Tao using tools from algebraic geometry and the structure theory of simple algebraic groups.

Let us now go back to the proof of the Bourgain-Gamburd theorem. The connection with approximate groups appears in the following lemma:

Lemma 0.6. *(ℓ^2-flattening lemma) Suppose* μ *is a probability measure on a group* G *and* $K \geqslant 1$ *is such that*

$$||\mu * \mu||_2 \geqslant \frac{1}{K}||\mu||_2.$$

Then there is a K^C*-approximate subgroup* A *of* G *such that*

- $\mu(A) \gg \frac{1}{K^C}$
- $|A| \ll K^C ||\mu||_2^{-2}$,

where C *and the implied constants are absolute constants.*

For the proof of this lemma, see the original paper of Bourgain-Gamburd [1] or [14, Lemma 15]. It is based on a remarkable graph theoretic lemma, the Balog-Szemeredi-Gowers lemma, which allows one to show the existence of an approximate group whenever we have a set which only statistically looks close to an approximate group. Namely if $A \subset G$ is such that the probability that ab belongs to A for a random choice (with uniform distribution) of a and b in A is larger than say $\frac{1}{K}$, then A has large intersection with some K^C-approximate group of comparable size.

The above lemma combined with Theorem 0.5 implies the desired controlled decay of $\nu^{2n}(e)$ in the range $\tau \log p \leqslant n \leqslant C \log p$, namely (recall that $\nu^{2n}(e) = ||\nu^n||_2^2$):

Corollary 0.7. *There is a constant $\varepsilon > 0$ such that*

$$||\nu^n * \nu^n||_2 \leqslant ||\nu^n||_2^{1+\varepsilon}$$

for all $n \geqslant \tau \log p$ and as long as $||\nu^n||_2^2 \geqslant \frac{1}{|G_p|^{1-\frac{1}{10}}}$ say.

Indeed, if the lower bound failed to hold at some stage, then by the ℓ^2-flattening lemma, there would then exist an p^ε-approximate subgroup A of G_p of size $< |G_p|^{1-\frac{1}{10}}$ such that $\nu^n(A) \geqslant \frac{1}{p^{C\varepsilon}}$. By the classification theorem, Theorem 0.5, A must be a contained in a proper subgroup of $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. But those all have a solvable subgroup of bounded index. In fact proper subgroups of $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ are completely known (see e.g. [1, Theorem 4.1.1] and the references therein) and besides a handful of bounded subgroups, they are contained either in the normalizer of the diagonal subgroup, or in a Borel subgroup (upper triangular matrices). Hence there is 2-step solvable subgroup A of G_p such that $\nu^n(A) \geqslant \frac{1}{p^{C\varepsilon}}$ for some n between $\tau \log p$ and $C \log p$. But $\nu^n(A)$ is essentially non-increasing, that is $\nu^n(A) = \sum_x \nu^m(x^{-1})\nu^{n-m}(xA) \leqslant \max \nu^{n-m}(xA)$ and so $\nu^{2(n-m)}(A) \geqslant \nu^{n-m}(xA)^2 \geqslant (\nu^n(A))^2 \geqslant \frac{1}{p^{2C\varepsilon}}$ for all m. In particular there is $n_0 = n - m < \frac{\tau}{10} \log p$ for which $\nu^{n_0}(A) \geqslant \frac{1}{p^{C\varepsilon}}$. However at time n_0, we are before the girth bound and the random walk is still in the tree. But in a free group the only 2-step solvable subgroups are cyclic subgroups, so subsets of elements whose second commutator vanish must in fact commute and occupy a very tiny part of the free group ball of radius n_0. This contradicts the lower bound $\frac{1}{p^{C\varepsilon}}$. See the original paper for the details.

The proof is now complete as we have now a device, namely Corollary 0.7, to go from (0.3.2) to (0.3.1) by applying this upper bound iteratively a bounded number of times. We are done.

III. Super-strong approximation

The Bourgain-Gamburd method has been used and refined by many authors in the past few years. We briefly mention two recent results (among many others) which use these ideas to establish further examples of expander Cayley graphs and groups with property (τ).

The first states that random Cayley graphs of finite simple groups of Lie type of bounded rank are uniformly expanders. Or more formally:

Theorem 0.8. *(Random Cayley graphs, Breuillard-Green-Guralnick-Tao* [7]*) Given $k \geqslant 2$ and $d \geqslant 1$, there is $\varepsilon, \gamma > 0$, such that the probability that k elements chosen at random in $\mathbf{G}(\mathbb{F}_q)$ generate $\mathbf{G}(\mathbb{F}_q)$ and turn it into an ε-expander is at least $1 - O(\frac{1}{|\mathbf{G}(\mathbb{F}_q)|^\gamma})$. Here $\mathbf{G}$ is any simple algebraic group of dimension at most d over $\mathbb{F}_q$.*

The second deals with the property (τ) for *thin groups*, that is discrete Zariski-dense subgroups of semisimple Lie groups which are not lattices.

Theorem 0.9. *(Super-strong approximation, Bourgain-Varju* [3]*) If $\Gamma \leqslant \mathrm{SL}_d(\mathbb{Z})$ is a Zariski-dense subgroup, then it has property (τ) with respect to the family of congruence subgroups $\Gamma \cap \ker(\mathrm{SL}_d(\mathbb{Z}) \to \mathrm{SL}_d(\mathbb{Z}/n\mathbb{Z}))$, where n is an arbitrary integer.*

This theorem can be viewed as a vast generalization of Selberg's theorem, and indeed it gives a different proof (via the Brooks-Burger dictionary mentioned in Lecture 3) of the uniform spectral gap for the first eigenvalue of the Laplacian on the congruence covers of the modular surface $\mathbb{H}^2/\,\mathrm{SL}_2(\mathbb{Z})$ (although not such a good bound as $\frac{3}{16}$ of course). Despite its resemblance with Corollary 0.2, the proof of this theorem is much more involved, in particular the passage from n prime to arbitrary n requires much more work (see already Varju's thesis [14] for the special case of square free n).

References

[1] J. Bourgain, A. Gamburd, *Uniform expansion bounds for Cayley graphs of* $\mathrm{SL}_2(\mathbb{F}_p)$, Ann. of Math. **167** (2008), no. 2, 625–642.
[2] J. Bourgain. N. Katz, T. Tao, *A sum-product estimate for finite fields, and applications*, Geom. Func. Anal. **14** (2004), 27–57.
[3] J. Bourgain, P. Varju, *Expansion in* $\mathrm{SL}(d, q)$, preprint.
[4] E. Breuillard, A. Gamburd, *Strong uniform expansion in* $\mathrm{SL}(2, p)$, Geom. Funct. Anal. **20** (2010), no. 5, 1201-1209.
[5] E. Breuillard, B. Green and T. Tao, *Approximate subgroups of linear groups*, GAFA 2011.
[6] E. Breuillard, B. Green and T. Tao, *The structure of approximate groups*, preprint 2011.
[7] E. Breuillard, B. Green, R. Guralnick and T. Tao, *Expansion in finite simple groups of Lie type*, in preparation.
[8] H. Kesten, *Symmetric random walks on groups,* Trans. Amer. Math. Soc., **92** (1959), 336–354.
[9] M. V. Nori, *On subgroups of* $\mathrm{GL}_n(\mathbb{F}_p)$, Invent. math., 88 (1987), 257–275.
[10] L. Pyber, E. Szabó, *Growth in finite simple groups of Lie type*, preprint (2010) arXiv:1001.4556
[11] J.P. Serre, *Representation of finite groups*, Springer translation.
[12] T. Tao, *Product set estimates in noncommutative groups*, Combinatorica **28** (2008), 547–594.
[13] T. C. Tao and V. H. Vu, *Additive Combinatorics*, CUP 2006.
[14] P. Varjú, *Expansion in $SL_d(\mathcal{O}_K/I)$, I squarefree,* preprint.
[15] B. Weisfeiler, *Strong Approximation for Zariski-dense Subgroups of Semi-Simple Algebraic Groups*, Annals of Math., 2nd Ser., Vol. 120, No. 2. (Sep., 1984), pp. 271–315.

Laboratoire de Mathématiques, Bâtiment 425, Université Paris Sud 11, 91405 Orsay, FRANCE
E-mail address: emmanuel.breuillard@math.u-psud.fr

EXERCISES FOR THE PCMI SUMMER SCHOOL

EMMANUEL BREUILLARD

1. Amenability, paradoxical decompositions and Tarski numbers

In this exercise, we prove yet another characterization of amenability, which is due to Tarski [7, 4] and states that a group is non-amenable if and only if it is paradoxical.

Let Γ be a group acting on a set X. This Γ-action is said to be N-*paradoxical* if one can partition X into $n+m \leqslant N$ disjoint pieces

$$X = A_1 \cup \ldots \cup A_n \cup B_1 \cup \ldots \cup B_m$$

in such a way that there are elements $a_1, \ldots, a_n \in \Gamma$ and $b_1, \ldots, b_m \in \Gamma$ such that

$$X = \bigcup_{i=1}^{n} a_i A_i \text{ and } \bigcup_{j=1}^{m} b_j B_j$$

We say that Γ is paradoxical if it is N-paradoxical for some finite $N \in \mathbb{N}$ for the action of Γ on itself by left translations.

1) Prove that the non-abelian free group F_2 and in fact any group Γ containing the free group F_2 is 4-paradoxical.

2) Suppose that Γ is a 4-paradoxical group and $\Gamma = A_1 \cup A_2 \cup B_1 \cup B_2$ is a paradoxical decomposition as defined above. Show that Γ *plays ping-pong* on itself, where the ping-pong players are $a := a_1^{-1} a_2$ and $b := b_1^{-1} b_2$ .Deduce that Γ contains a non-abelian free subgroup F_2.

3) Define the *Tarski number* $\mathcal{T}(\Gamma)$ of a group Γ to be the smallest integer N if it exists such that Γ is N-paradoxical. By the above $\mathcal{T}(\Gamma) = 4$ if and only if Γ contains F_2. Show that if Γ is amenable, then $\mathcal{T}(\Gamma) = +\infty$.

4) Suppose that Γ is finitely generated with symmetric generating set S and is endowed with the corresponding word metric d (i.e. $d(x,y) := \inf\{n \in \mathbb{N}, x^{-1}y \in S^n\}$). Show that $\mathcal{T}(\Gamma)$ is finite if and only if there exists a surjective 2-to-1 mapping $\phi : \Gamma \to \Gamma$ with the property that $\sup_{\gamma \in \Gamma} d(\gamma, \phi(\gamma)) < +\infty$.

5) Given $k \in \mathbb{N}$, let $\mathcal{G}_k$ be the bi-partite graph obtained by taking two copies Γ_1 and Γ_2 of Γ as the left and right vertices respectively and by placing an edge between $\gamma \in \Gamma_1$

Date: July 14th 2012.

and $\gamma' \in \Gamma_2$ if and only if $d(\gamma, \gamma') \leqslant k$ in the word metric of Γ. Show that if there is some finite $k \in \mathbb{N}$ such that $\mathcal{G}_k$ admits a $(2,1)$ perfect matching[1], then Γ is paradoxical.

6) Prove the following version of *Hall's marriage lemma* for infinite bi-partite graphs. Let k be a positive integer (we will need the result for $k = 2$ only). Suppose $\mathcal{B}$ is a bi-partite graph whose set of left vertices is countable infinite as is the set of right vertices. Suppose that for every finite subset of left vertices L, the number of right vertices connected to some vertex in L has size at least $k|L|$, while for every finite subset R of right vertices, the number of left vertices connected to some vertex in R has size at least $|R|$. Show that $\mathcal{B}$ admits a $(k,1)$ perfect matching. [Hint: first treat the case $k = 1$, then reduce to this case.]

7) Using 6) that if Γ is a non-amenable finite generated group, then there is $k \geqslant 1$ such that $\mathcal{G}_k$ has a $(2,1)$ perfect matching.

8) Conclude the proof of Tarski's theorem for arbitrary (not necessarily finitely generated) groups.

2. Kazhdan's property (T) for $\mathrm{SL}_n(\mathbb{Z})$ via bounded generation

The goal of this exercise is to show how bounded generation can be useful to establish property (T) and to provide a proof (due to Shalom [6]) that $\mathrm{SL}_n(\mathbb{Z})$, $n \geqslant 3$, has property (T) along these lines.

I. Preliminaries for general G.

1) Show that property (T) for a finitely generated group G is equivalent to the following. Given a finite generating set S, there is $C > 0$ such that for any $\varepsilon > 0$ and any unitary representation $(\pi, \mathcal{H}_\pi)$ of G, if $v \in \mathcal{H}_\pi$ satisfies $||\pi(s)v - v|| \leqslant \varepsilon$ for all $s \in S$, then there is an G-invariant vector $w \in \mathcal{H}_\pi$ such that $||v - w|| \leqslant C\varepsilon$.

2) Let $\varepsilon \leqslant 1$. Suppose $(\pi, \mathcal{H}_\pi)$ is a unitary representation of G and v is a unit vector in $\mathcal{H}_\pi$ such that $\sup_{g \in G} ||\pi(g)v - v|| \leqslant \varepsilon$. Show that G admits a non-zero invariant vector w with $||v - w|| < \varepsilon$. (Hint: use the circumcenter).

3) Suppose G admits finitely (or compactly) generated subgroups $H_1, \ldots, H_n$ with property (T) such that $G = H_1 \ldots H_n$ in the sense that any element of G can be written as a product $h_1 \cdot \ldots \cdot h_n$ with $h_i \in H_i$ (i.e. G is *boundedly generated by the H_i's*). Show that G has property (T).

Deduce from this that in order to prove that $\mathrm{SL}_n(\mathbb{R})$ has property (T) it is enough to prove that $\mathrm{SL}_3(\mathbb{R})$ has property (T).

4) A pair (G, H) of groups, where H is a subgroup of G, is said to have *relative property* (T) if any unitary representation of G with almost invariant vectors admits an

[1]By definition this is a subset of edges of $\mathcal{G}_k$ such that the induced bi-partite graph has the property that every vertex on the left hand side is connected to exactly two vertices on the right hand side, while every vertex on the right hand side is connected to exactly one vertex on the left hand side.

H-invariant vector. Show that if G is boundedly generated by subgroups $H_1, \ldots, H_n$ and each H_i is normalized by a finitely (or compactly) generated subgroup $L_i \leqslant G$ such that (L_i, H_i) has relative property (T), then G has property (T).

II. Bounded generation for $\mathrm{SL}_n(\mathbb{Z})$.

1) Prove that $\mathrm{SL}_n(\mathbb{R})$, $n \geqslant 2$, is boundedly generated by its *elementary subgroups*, namely the subgroups H_{ij} of the form $Id_n + \mathbb{R}E_{ij}$, where E_{ij} is the elementary $n \times n$ matrix all of whose entries are 0 except the ij entry.

2) Using elementary operations on rows and columns, show that in order to prove that $\mathrm{SL}_n(\mathbb{Z})$, $n \geqslant 3$, is boundedly generated by its elementary subgroups $Id + \mathbb{Z}E_{ij}$, it is enough to do this for $n = 3$. (hint: reduce to the case when the first $n-1$ entries of the bottom row of a given matrix in $\mathrm{SL}_n(\mathbb{Z})$ are relatively prime).

We won't do the $n = 3$ case here. Anybody interested in advised to look at [1, Lemma 4.1.6] or the original article [3].

III. Relative property (T) for $\mathrm{SL}_2(\mathbb{Z}) \ltimes \mathbb{Z}^2$.

We want to prove that if $(\pi, \mathcal{H})$ is a unitary representation of $\mathrm{SL}_2(\mathbb{Z}) \ltimes \mathbb{Z}^2$ with almost invariant vectors, then there is a $\mathbb{Z}^2$ invariant vector. We follow an argument due to M. Burger [2].

The restriction $\pi_{|\mathbb{Z}^2}$ is a unitary representation of $\mathbb{Z}^2$. The dual of $\mathbb{Z}^2$ is the torus $T := \widehat{\mathbb{Z}^2} = (\mathbb{R}/\mathbb{Z})^2$. Recall that according to the spectral theorem, there exists a resolution of identity $E : T \to \mathcal{B}(\mathcal{H})$, which assigns to every Borel set $\Omega \subset T$ a self-adjoint projection $E(\Omega) : \mathcal{H} \to \mathcal{H}$, such that

a) $E(\varnothing) = 0$, $E(T) = Id$, $E(A \cap B) = E(A)E(B)$, and $E(A \cup B) = E(A) + E(B)$ if $A \cap B = \varnothing$.

b) for every $v, w \in \mathcal{H}$, $\Omega \mapsto (E(\Omega)v, w)$ is complex measure and for all $\xi \in \mathbb{Z}^2$

$$(\pi(\xi)v, w) = \int_T e^{2i\pi\xi\cdot\omega}(E(d\omega)v, w)$$

The idea of the proof is to study the probability measures $\mu_v(\Omega) := (E(\Omega)v, v)$ when v is an almost invariant vector and to show, using the action of $\mathrm{SL}_2(\mathbb{Z})$, that they must charge $\{0\}$, implying that $\pi_{|\mathbb{Z}^2}$ has invariant vectors. Now come the details.

1) Verify that a) and b) imply that given $\omega \in T$, l'image $ImE(\{\omega\})$ is the joint eigenspace of $\mathbb{Z}^2$ with eigenvalue $e^{2i\pi\omega\cdot\xi}$ (i.e. $\forall \xi \in \mathbb{Z}^2$, $\pi(\xi)v = e^{2i\pi\omega\cdot\xi}v$ iff $v \in ImE(\{\omega\})$). In particular $E(\{0\})$ is the orthogonal projection to the invariant vectors.

2) Let $v \in \mathcal{H}$ be a unit vector and μ_v be the probability measure on T given by $\Omega \mapsto (E(\Omega)v, v)$. Show that $|\mu_v(B) - \mu_w(B)| \leqslant 2||v - w||$ for every Borel set $B \subset T$ and all $v, w \in \mathcal{H}$. Also check that $g_*\mu_v = \mu_{\pi(g)v}$, where $g \in \mathrm{SL}_2(\mathbb{Z})$ acts on T in the natural way and $g_*\mu(\Omega) := \mu(g^{-1}\Omega)$.

3) Given a sequence of almost invariant unit vectors $(v_k)_k$ for $\mathrm{SL}_2(\mathbb{Z}) \ltimes \mathbb{Z}^2$, show that μ_{v_k} converges weakly to the Dirac mass at $0 \in T$.

4) If π has no $\mathbb{Z}^2$ invariant vectors, show that $\mu_v(\{0\}) = 0$ for every v.

5) Let $a := Id + 2E_{12}$ and $b := Id + 2E_{21}$ be two elementary matrices in $\mathrm{SL}_2(\mathbb{Z})$. Show the following lemma (which is one way to show that $\mathrm{SL}_2(\mathbb{Z})$ has no invariant measure on the projective line $\mathbb{P}(\mathbb{R}^2)$ and hence is non-amenable). There is $\varepsilon_0 > 0$ such that for every probability measure μ on $\mathbb{R}^2 \setminus \{0\}$, there is a Borel subset $Y \subset \mathbb{R}^2 \setminus \{0\}$ such that $|\mu(gY) - \mu(Y)| \geqslant \varepsilon_0$ for some $g \in \{a^{\pm 1}, b^{\pm 1}\}$.

6) Conclude.

IV. Property (T) for $\mathrm{SL}_n(\mathbb{Z})$. Show finally that $\mathrm{SL}_n(\mathbb{Z})$ has property (T) using bounded generation of the elementary subgroups $Id_n + \mathbb{Z}E_{pq}$ and relative property (T) for the pair $(\mathrm{SL}_2(\mathbb{Z}) \ltimes \mathbb{Z}^2, \mathbb{Z}^2)$. (hint: set the H_i's to be the subgroups generated by two distinct elementary subgroups and find subgroups L_i in $\mathrm{SL}_n(\mathbb{Z})$ such that $H_i \simeq \mathbb{Z}^2$ is normal in $L_i \simeq \mathrm{SL}_2(\mathbb{Z}) \ltimes \mathbb{Z}^2$, then use I.4. to conclude.)

Does this work for $\mathrm{SL}_n(\mathbb{R})$?

3. Harmonic functions and property (T)

One of the amazing things about property (T) is that it can be used to prove theorems that at first sight seem far removed from any question involving spectral gaps or unitary representations. The most outstanding example of this is Margulis' famed proof of the Normal Subgroup Theorem (which states that a normal subgroup in a higher rank lattice is either finite or of finite index). Margulis' proof proceeds by showing that any quotient of the lattice by a non-central subgroup is both amenable and has property (T) hence is finite.

Another such example is the following fact, which is a key step in Kleiner's proof of Gromov's polynomial growth theorem ([5] and the references therein):

Theorem[2]: Any finitely generated infinite group admits a non-constant Lipschitz harmonic function.

Let Γ be a group generated by a finite symmetric set $S = \{s_1^{\pm 1}, \ldots, s_k^{\pm 1}\}$. A function on Γ is said to be harmonic if for all $x \in \Gamma$

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

We say it is Lipschitz if $|f(x) - f(y)| \leqslant C d(x, y)$ for some $C > 0$ and all $x, y \in \Gamma$, where $d(x, y)$ is the word metric induced by S on Γ.

[2] This result is almost a counter-example to the somewhat provocative assertion I once heard according to which there is no property that is both non-trivial and holds for all finitely generated groups.

The goal of this exercise will be to prove this theorem. The proof splits in two parts: first we treat the case when Γ is non-amenable. Then the case when Γ does not have property (T). A finitely generated group which does not fall into one of these two categories must be finite, hence the result.

0) First prove that on a finite group, every harmonic function is constant (hint: maximum principle).

I. The non-amenable case.
1) (Bogolyubov) Let μ be the symmetric and finitely supported measure $\mu := \frac{1}{|S|}\sum_{s\in S}\delta_s$ on Γ. Show that every action of Γ by homeomorphisms on a compact space X admits a stationnary measure, namely a Borel probability measure ν on X such that $\mu * \nu = \nu$ (i.e. $\frac{1}{|S|}\sum_{s\in S}\nu(sA) = \nu(A)$ for every Borel subset $A \subset X$).

2) (Building bounded harmonic functions) Let ν is a stationary measure for μ on a compact Γ-space X. Show that for every bounded continuous function f on X the function $\phi_f : \gamma \mapsto \int_X f(\gamma \cdot x)d\nu(x)$ is harmonic and bounded on Γ.

3) Use 1) and 2) to prove that if Γ is non-amenable, then Γ admits a non-constant bounded harmonic function.

II. Negating Property (T).
Recall that according to the Delorme-Guichardet theorem, Γ has property (T) if and only if every affine isometric action of Γ on a Hilbert space has a global fixed point (property (FH)). We will need the following stronger fact: if Γ does not have property (T), then there is an affine isometric action on some Hilbert space $\mathcal{H}$ such that the ℓ^2-displacement function

$$D_S(x) := \big(\sum_{s\in S} d(x, s\cdot x)^2\big)^{\frac{1}{2}}$$

is everywhere positive and attains its minimum at some point $x_0 \in \mathcal{H}$. Here $d(x,y)^2 = ||x-y||^2$ is the (square of the) distance in the Hilbert space $\mathcal{H}$ and $\gamma \cdot x$ denotes the affine action of Γ in $\mathcal{H}$.

The proof we give below of this strengthening of $(FH) \Rightarrow (T)$ uses *ultralimits*, which are an extremely useful tool in all sorts of contexts when one wants to make uniform a seemingly non-uniform statement.

We briefly recall the construction of an ultralimit of metric spaces. We refer the reader to Misha Kapovich notes from this year's Park City summer school for more details. A non-principal ultrafilter ω is a set of subsets of $\mathbb{N}$ such that a) $A \in \omega$ and $A \subset B \Rightarrow B \in \omega$, b) if $A, B \in \omega$, then $A \cap B \in \omega$, c) for every $A \subset \mathbb{N}$, either A or A^c belongs to ω, and d) no singleton belongs to ω (check that this is equivalent to the definition in terms of $\{0,1\}$-valued finitely additive measures given in Misha's notes). The existence of a non-principal ultrafilter is guaranteed by Zorn's lemma.

Given a sequence of pointed metric spaces (X_n, d_n, x_n) recall that their *ultralimit* along ω is defined as the set of equivalence classes of sequences $(y_n)_n$ such that $\forall n, y_n \in X_n$ and $\sup_n d_n(y_n, x_n) < +\infty$, where (y_n) and (y'_n) are equivalent if $\lim_\omega d_n(y_n, y'_n) = 0$.

Let now $\mathcal{H}$ be a Hilbert space endowed with an affine isometric action of Γ. Let d be the Euclidean distance on $\mathcal{H}$. Given a sequence of scalars $\lambda_n > 0$, and a sequence of base points $x_n \in \mathcal{H}_n$, we can form the ultralimit of the sequence of pointed metric spaces $(\mathcal{H}, \lambda_n d, x_n)$, say $(\mathcal{H}_\omega, d_\omega, x_\omega) = \lim_\omega(\mathcal{H}, \lambda_n d, x_n)$.

1) Show that $(\mathcal{H}_\omega, d_\omega, x_\omega)$ is again a Hilbert space endowed with an affine isometric action of Γ.

2) Let $\mathcal{H}$ be a Hilbert space endowed with an affine isometric action of Γ admitting no global fixed point. Show that for every $n \in \mathbb{N}$, there is $x_n \in \mathcal{H}$ such that for every y in the ball of radius $nD_S(x_n)$ one has

$$D_S(y) \geqslant (1 - \frac{1}{n})D_S(x_n).$$

3) Prove the aforementioned strengthening of $(FH) \Rightarrow (T)$ using an ultralimit of a renormalised sequence of pointed Hilbert spaces contradicting the uniformity.

4) Show that if x_0 realizes the minimum of $D_S(x)$ and $D_S(x_0) > 0$, then for every $v \in \mathcal{H}$ the map $\gamma \mapsto Re(\gamma \cdot x_0, v)$ (Re = real part) is harmonic and Lipschitz (hint: differentiate $D_S(x)^2$).

5) Conclude the proof of the theorem from the introduction. Can one make the harmonic function unbounded ?

References

[1] B. Bekka, P. de la Harpe and A. Valette, *Kazhdan's property* (T) New Mathematical Monographs, 11. Cambridge University Press, Cambridge, 2008. xiv+472 pp.
[2] M. Burger, *Kazhdan constants for* $\mathrm{SL}(3, \mathbb{Z})$, J. Reine Angew. Math. 413 (1991), 36-67.
[3] D. Carter and G. Keller, *Bounded elementary generation of* $SL_n(\mathcal{O})$. Amer. J. Math. 105 (1983), no. 3, 673-687.
[4] T. Ceccherini-Silberstein, R. Grigorchuk and P. de la Harpe, *Amenability and paradoxical decompositions for pseudogroups and discrete metric spaces* in Proc. Steklov Inst. Math. 1999, no. 1 (224), 57–97
[5] B. Kleiner, *A new proof of Gromov's theorem on groups of polynomial growth*, J. Amer. Math. Soc. 23 (2010), no. 3, 815-829.
[6] Y. Shalom, *Bounded generation and Kazhdan's property* (T), Inst. Hautes tudes Sci. Publ. Math. No. 90 (1999), 145-168.
[7] A. Tarski, *Cardinal algebras*, Oxford University Press, (1949).

E-mail address: emmanuel.breuillard@math.u-psud.fr

EXERCISE SHEET 2

EMMANUEL BREUILLARD

1. Some facts on expanders

1) (Schreier graphs as expanders) Suppose G is a finite group with symmetric generating set S and $\mathcal{C}(G,S)$ is its Cayley graph. Suppose G acts transitively on a set X and let $\mathcal{S}(X,S)$ be the Schreier graph of this action, namely the graph with vertex set X and edges given by $x \simeq y$ iff there is $s \in S$ s.t. $x = s \cdot y$.

Show that $\lambda_2(\mathcal{S}(X,S)) \leqslant \lambda_2(\mathcal{C}(G,S))$. In particular the quotient Schreier graphs obtained from a family of expanders Cayley graphs are expander graphs. (hint: show that every eigenvalue of the Schreier graph is an eigenvalue of the Cayley graph).

Deduce that if Γ is a finitely generated group which has property (τ) with respect to a family of finite index normal subgroups $(\Gamma_i)_i$ which is such that every finite index subgroup of Γ contains some Γ_i, then Γ has property (τ). In particular the Selberg property for an arithmetic lattice combined with the congruence subgroup property imply property (τ).

2. Some basics on approximate groups

3) (Ruzsa's triangle inequality) Given two finite sets A, B in an ambient group G, we set

$$d(A,B) := \log \frac{|AB^{-1}|}{|A||B|},$$

a quantity called the *Ruzsa distance* between the sets A and B.

1) Show the triangle inequality: given any three finite sets A, B, C in G.

$$d(A,C) \leqslant d(A,B) + d(B,C),$$

[hint: consider the map $(b,x) \mapsto (a_x^{-1}b, b^{-1}c_x)$, where $a_x^{-1}c_x$ is a representation of $x \in A^{-1}C$.]

2) Deduce that if A is a finite subset of G such that $|AAA| \leqslant K|A|$ for some real number $K \geqslant 0$, then for every integer $n \geqslant 3$ we have $|A^n| \leqslant K^{2n-5}|A|$.

4) (Sets of small doubling)

Date: July 19th 2012.

0) Let A be a finite subset of a group G such that $|AA| = |A|$. Show that $A = aH$, where H is a finite group and a normalizes H.

Now suppose we only know that

$$|AA| \leqslant K|A|,$$

for some $K \geqslant 1$.

1) Show that $|A^{-1}A| \leqslant K^2|A|$.

2) Show that if K is close enough to 1, then the only such sets A must be contained in a coset of a subgroup H of G of size at most $2|A|$ (hint: show that $A^{-1}A$ is a group).

3) Push the argument to prove that $|AA| < \frac{3}{2}|A|$ if and only if there is a subgroup H of G and a in the normalizer of H in G such that $A \subset aH$ and $|A| > \frac{2}{3}|H|$ (hint: show first that $A^{-1}A = AA^{-1}$).

References

E-mail address: `emmanuel.breuillard@math.u-psud.fr`