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 $f \in \ell^2_0(\Gamma/\Gamma_p)$ 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 $\max\{||a^{\pm1}||, ||b^{\pm1}||\}^n$, hence $w(a, b)$ is not killed modulo p if p is larger that $\max\{||a^{\pm1}||, ||b^{\pm1}||\}^n$, 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