NOTES ON THE STRUCTURE OF APPROXIMATE GROUPS - WINTER SCHOOL LES DIABLERETS 2013

EMMANUEL BREUILLARD

1. Additive combinatorics on groups

1.1. **Introduction.** A key idea of Geometric Group Theory as initiated by Gromov and others some thirty or forty years ago is to study infinite groups, in particular finitely generated ones, as geometric objects via the study of their Cayley graphs. Typically we look at a group Γ generated by a finite symmetric set S and define the associated Cayley graph and word metric:

$$d_S(g,h) = \inf\{n \geqslant 0, g^{-1}h \in S^n\},$$

where $S^n := S \cdot \ldots \cdot S$ is the product set of n copies of S. In particular the ball of radius n around the identity $B_S(e,n)$ is nothing else but S^n. Usually people are interested in properties that are independent of the choice of S, and look at very large values of n. So S is of bounded size and n is large.

Additive combinatorics on groups on the other hand is concerned with products sets $A^n := A \cdot \ldots \cdot A$, where n is of bounded size, but A is a very large finite subset of an ambient group G. Traditionally, combinatorialists and number theorists have been interested in studying large finite subsets say of $\mathbb{Z}$ which do not grow much under addition. This is an old and well-developed subject of mathematics (much older than geometric group theory) with applications to many number theoretical questions (such as unique factorization in rings of algebraic integers, arithmetic progressions such as in the work of Green-Tao, Goldbach's problem, Warring's problem, etc).

Only very recently did people start to look at similar questions on non-abelian groups, only to find out that many of the tools developed in the commutative context could also be applied in a non-commutative setting. At a recent conference in Jerusalem one of the founders of modern additive combinatorics, Grigory Freiman, compared this surprise to that of Molière's Monsieur Jourdain who had been speaking prose all his life without knowing it.

1.2. **Examples of results from combinatorics.** Let us give two example of results from additive combinatorics:

Theorem 1.3 (Sum-product theorem (Bourgain-Katz-Tao))**.** *Suppose $A \subset \mathbb{F}_p$ is a subset of the field $\mathbb{F}_p$ with p elements (p prime). Then either $|A+A| > |A|^{1.01}$ or $|AA| > |A|^{1.01}$ or $|A| > p^{0.9}$*

In other words a subset of a prime field must grow either by addition or by multiplication unless it is almost all of the field. This can be viewed as a quantitative version of the fact the there are no non-trivial subring in $\mathbb{F}_p$. Of course one can form lots of subsets A that do not grow much under addition, or under multiplication: take a finite arithmetic progression, or geometric progression; then $|AA| \leqslant 2|A|$, but $|A|$ can be of arbitrary cardinality inside $\mathbb{F}_p$.

Date: March 2013.

Theorem 1.4 (Freiman-Ruzsa-Chang theorem)**.** *Let $A \subset \mathbb{Z}$ be a finite subset such that $|A + A| \leqslant K|A|$. Then A is $C(K)$-commensurable to a d-dimensional arithmetic progression P with $d = O(\log K)$.*

Here we used:

Definition 1.5 (K-commensurability)**.** *Two finite subsets A and B of an ambient group G are called K-commensurable if*

$$|A \cap B| \geqslant \frac{1}{K} \max\{|A|, |B|\}.$$

and

Definition 1.6 (Multidimensional arithmetic progression)**.** *A d-dimensional arithmetic progression in an ambient group G is a finite subset of the form $P := \pi(B)$, where $\pi : \mathbb{Z}^d \to G$ is a group homomorphism and $B := \prod_{i=1}^d [-L_i, L_i]$ is a "box" with side-lengths $L_i \in \mathbb{N}$.*

It is easy to see that P as above satisfies $|PP| \leqslant 2^d|P|$ because $B + B$ is contained in at most 2^d translates of B.

The proof of the Freiman-Ruzsa-Chang theorem is based on harmonic analysis on $\mathbb{Z}/p\mathbb{Z}$ for some suitably chosen prime p. The constant $C(K)$ given by this theorem is typically of order $e^{O(K^{O(1)})}$. Tom Sanders recently gave much better, almost polynomial, bounds. Conjecturally ("Polynomial Freiman-Ruzsa conjecture") one can take $C(K)$ to be of order $O(K^{O(1)})$.

In this theorem and its applications, the quality of the bounds (i.e. their dependence on K) are important.

Here is another interesting result about subsets of the free group. Razborov proved that if F is a free group and $A \subset F$ a finite subset, then $|AAA| \geqslant |A|^2/(\log |A|)^c$ for some positive c independent of A and F, unless A lies in a cyclic subgroup. S. R. Safin improved this:

Theorem 1.7 (Safin's theorem)**.** *Let F a free group, then for every $n \geqslant 3$ and every finite subset A in F*

$$|A^n| \geqslant \frac{|A|^{[\frac{n+1}{2}]}}{(62)^n}$$

unless A generates a cyclic group.

I don't know if $\frac{1}{2}$ is sharp in the above exponent for large n and $|A|$.

1.8. **The Freiman inverse problem.** The general problem ("Freiman inverse problem" as advertised in particular by T. Tao several years ago) is to describe the structure of large subsets A of an arbitrary ambient group G that satisfy $|AA| \leqslant K|A|$ for some fixed constant K.

The value $|AA|/|A|$ is usually called the *doubling constant* of A, equivalently we say that A has *doubling at most K*.

For example we easily have:

Proposition 1.9. *Let G be an arbitrary group. Suppose $|AA| = |A|$. Then there is a finite subgroup H of G and $A = aH = Ha$ for every $a \in A$.*

Proof. Pick $a \in A$ and set $H := Aa^{-1}$. The set H contains the identity, so $A \subset AH$. But $|AH| = |AHa| = |AA| = |A|$, hence $A = AH$. Iterating $A = AH^n$ for every $n \geqslant 1$ and it follows that the semigroup $\cup_n H^n$ is finite and contained in $a^{-1}A$. But a finite semigroup inside a group is a finite group. So the subgroup generated by H satisfies $\langle H \rangle \subset a^{-1}A$. In particular

$|\langle H\rangle| \leqslant |A| = |H|$. Hence $\langle H\rangle = H$. It follows that $A = Ha$ and that $H = AA^{-1}$. Finally $|H| = |A| = |AA| = |HaHa| = |HaH| = |a^{-1}HaH|$. But $a^{-1}HaH/H \simeq a^{-1}Ha/(a^{-1}Ha \cap H)$. Hence $a^{-1}Ha = H$ and we are done. □

Slightly trickier is the following:

Proposition 1.10. *Let G be an arbitrary group. Suppose $|AA| \leqslant 1.1|A|$. Then there is a finite subgroup H of G and $a \in A$ such that $aHa^{-1} = H$, $|H| \leqslant 1.2|A|$ and $A \subset aH$.*

Proof. We will prove that $H := AA^{-1}$ is stable under multiplication using the following observation: if $||1_A - 1_{gA}||_1 < 2|A|$, then $g \in H$. First we show that $H = A^{-1}A$ and that $|H| \leqslant 1.2|A|$.

Note that $\forall x, y \in G$, $||1_{xA} - 1_{yA}||_1 = |xA\Delta yA| = 2(|A| - |xA \cap yA|)$. But if $x, y \in A$, then $|xA \cup yA| = 2|A| - |xA \cap yA| \leqslant |A^2| \leqslant 1.1|A|$. Hence $\forall x, y \in A$, $|xA \cap yA| \geqslant 0.9|A|$ and

$$||1_A - 1_{x^{-1}yA}||_1 \leqslant 0.2|A|. \tag{1.10.1}$$

Since $|xA \cap yA| > 0$ we conclude that $xa = yb$ for some $a, b \in A$, i.e. $x^{-1}y \in AA^{-1}$. Hence $A^{-1}A = H = AA^{-1}$. In fact $xa = yb$ for at least $0.9|A|$ pairs (a, b) in $A \times A$. Therefore $|H| = |A^{-1}A| \leqslant |A|^2/0.9|A| \leqslant 1.2|A|$.

To see that $HH \subset H$ we write:

$$||1_A - 1_{z^{-1}wx^{-1}yA}||_1 \leqslant ||1_A - 1_{z^{-1}wA}||_1 + ||1_{z^{-1}wA} - 1_{z^{-1}wx^{-1}yA}||_1,$$

we get from (1.10.1)

$$||1_A - 1_{z^{-1}wx^{-1}yAA}||_1 \leqslant 0.4|A|$$

for every $x, y, z, w \in A$. Hence $HH \subset H$. Hence H is a subgroup and $A \subset Ha$ for all $a \in A$, so $H = A^{-1}A \subset a^{-1}Ha$ and a normalizes H. □

Remark 1.11. *The above proof (due to G. Freiman) can be pushed with little effort to yield that if $|AA| < \frac{3}{2}|A|$, then $H = AA^{-1} = A^{-1}A$ is a finite subgroup of size $< \frac{3}{2}|A|$ which is normalized by A. Clearly $3/2$ is sharp, take $A = \{0, 1\} \in \mathbb{Z}$.*

Remark 1.12. *One can ask: for which values of $K \geqslant 1$ is it true that the condition $|AA| \leqslant K|A|$ implies that A is contained in boundedly many (in terms of K) cosets of a finite subgroup ? The answer is for all $K < 2$. This is due to Yayha Hamidoune. Clearly it is sharp because the arithmetic progressions $A := \{0, 1, \ldots, N\} \subset \mathbb{Z}$ have $|A + A| \leqslant 2|A|$.*

The next question one can ask is: for which values of K is it true that the condition $|AA| \leqslant K|A|$ implies that A is contained in an extension HL, where H is a finite subgroup normalized by L a d-dimensional arithmetic progression ? Clearly such a set has doubling at most 2^d.

But there are sets of doubling say 2^4 which are not of this form: take a ball of large radius in the discrete Heisenberg group

$$H_3(\mathbb{Z}) := \Big\{ \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}, x, y, z \in \mathbb{Z} \Big\}$$

Here 4 is the asymptotic dimension of the Heisenberg group, namely $|S^n| \simeq n^4$ up to multiplicative constants, for any given finite generating set S of $H_3(\mathbb{Z})$.

In 2008 Elon Lindenstrauss proposed a general conjectural statement, which we recently proved in joint work with Ben Green and Terry Tao.

Theorem 1.13 (BGT 2011, weak version). *Let G be a group, $K \geqslant 1$ a parameter and A a finite subset with $|AA| \leqslant K|A|$. Then there is a coset of a virtually nilpotent subgroup of G which intersects A in a subset of size $\geqslant |A|/C(K)$.*

Here one consequence of this:

Theorem 1.14 (Gromov's polynomial growth theorem). *Let $\Gamma := \langle S \rangle$ be a finitely generated group with polynomial growth (i.e. $|S^n| = O(n^D)$ for some $D > 0$). Then Γ is virtually nilpotent.*

Proof. [Proof that Theorem 1.13 implies Theorem 1.14] Since $|S^n| = O(n^D)$, there must be arbitrarily large n's for which $|S^{4n}| \leqslant 5^D|S^n|$. Indeed, suppose not, then $|S^{4n}| > 5^D|S^n|$ for all n large enough, $n \geqslant n_0$ say, and hence $5^{Dk}|S^{n_0}| < |S^{4^k n_0}| = O(4^{Dk} n_0^D)$ a contradiction for large n.

Pick such an n. By Theorem 1.13 applied to $A := S^n$ and $K = 5^D$, there is a virtually nilpotent subgroup H_n such that S^n has a large intersection with a coset of H_n. In particular $|S^{2n} \cap H_n| \geqslant |S^n|/C(D) \geqslant |S^{4n}|/(5^D C(D))$. Theorem 1.14 follows by applying the following lemma with $k = 2n$.

Lemma 1.15. *In a group $\Gamma = \langle S \rangle$ if $|S^k \cap H| > |S^{2k}|/C$ for some subgroup H, some $C > 0$ and some $k \geqslant C$, then $[\Gamma : H] \leqslant C$.*

Proof. Look at the Schreier graph of Γ/H. It is connected, so either $S^kH = \Gamma$ or $|S^kH/H| > k$. Write $S^k = \cup_{i=1}^N S^k \cap g_iH$. Clearly $\cup_{i=1}^N (S^k \cap g_iH)(S^k \cap H) \subset S^{2k}$. Hence $N|(S^k \cap H)| \leqslant |S^{2k}| < C|S^k \cap H|$. And hence $N = |S^kH/H| < C \leqslant k$. Hence $S^kH = \Gamma$, and $[\Gamma : H] = N < C$.
□ □

Remark 1.16. *In fact the above proves slightly more than Gromov's theorem. It shows that given $C, D > 0$ there is $n_0 = n_0(C, D)$ such that if $|S^n| \leqslant Cn^D$ for some $n \geqslant n_0$, then Γ is virtually nilpotent. Note that this is stronger than the strengthened version obtained by Gromov himself at the end of his paper: he showed (just by logic) that his theorem implies that there is $n_0 = n_0(C, D)$ such that if $|S^n| \leqslant Cn^D$ holds for all $n \geqslant n_0$, then Γ is virtually nilpotent. So the added value here is that we need only one scale where we have the doubling property.*

Tomorrow we will devote the lecture to the above theorem and its applications.

1.17. **Additive combinatorics toolkit.** There are a few combinatorial tricks and tools that one uses all the time when one deals with sets of small doubling. The first one is the so-called Ruzsa inequality. Given two finite subsets A, B in a group G let

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

Clearly $d(A,B) = d(B,A)$ and $d(A,B) \geqslant 0$ because $|AB^{-1}| \geqslant |A|, |B|$. What is remarkable is the following:

Lemma 1.18. *Given three finite subsets A, B, C in G, the triangle inequality holds*

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

Hence $d(A,B)$ is called the *Ruzsa distance* between A and B. The proof is very easy:
Proof. Consider the map $AC^{-1} \times B \to AB^{-1} \times BC^{-1}$, which sends (x,b) to $(a_x b^{-1}, bc_x^{-1})$, where we made a choice of $a_x \in A$ and $c_x \in C$ for each $x \in AC^{-1}$. Then quite obviously this map is injective. Hence $|B||AC^{-1}| \leqslant |AB^{-1}||BC^{-1}|$, which is another way to phrase the triangle inequality $d(A,C) \leqslant d(A,B) + d(B,C)$. □

As a consequence:

$$\frac{|AA^{-1}|}{|A|} = e^{d(A,A)} \leqslant e^{d(A,A^{-1})+d(A^{-1},A)} = (\frac{|AA|}{|A|})^2.$$

Using the triangle inequality one can also prove:

Lemma 1.19 (Small tripling lemma). *If A is any finite subset in a group G, and $n \geqslant 3$, then*

$$\frac{|A^n|}{|A|} \leqslant (\frac{|A^3|}{|A|})^{n-2}$$

Another widely used argument is the following covering lemma:

Lemma 1.20 (Ruzsa covering lemma). *Suppose A, B are subsets in a group G such that $|AB| \leqslant K|A|$, then there is a subset $X \subset B$ of size $\leqslant K$ such that $B \subset A^{-1}AX$.*

Proof. Pick a maximal family of disjoint translates Ab_i, $b_1, \ldots, b_N \in B$. Clearly $N \leqslant K$. Then for every $b \in B$ Ab intersects some Ab_i non trivially and hence $b \in A^{-1}Ab_i$. Take $X = \{b_1, \ldots, b_N\}$. □

Dealing with conditions like $|AA| \leqslant K|A|$, or $|A^{-1}A| \leqslant K|A|$ can be cumbersome at times and it is easy to run into unessential technical difficulties that hide the real ones. This is why Terry Tao came up with another set of axioms for a subset A, closely related to the small doubling condition, which is much easier to handle. He coined the following definition:

Definition 1.21 (Approximate groups). *Let G be a group and $K \geqslant 1$ a parameter. A subset A of G is called an K-approximate subgroup if*

- *$A = A^{-1}$ and $1 \in A$,*
- *$AA \subset XA$ for some subset $X \subset G$ with $|X| \leqslant K$.*

Note: this makes sense for A infinite as well. But we will be mainly concerned with finite ones and by abuse of language A will always be assumed finite in the sequel.

Clearly a K-approximate subgroup has doubling at most K. The converse is not true of course, but we have the following partial converse:

Proposition 1.22 (Tao 2007). *Suppose A is a finite subset of an ambient group G such that $|AA| \leqslant K|A|$. Then there is an $O(K^{O(1)})$-approximate subgroup H of G such that $A \subset XH \cap HY$ for some subsets X, Y of size at most $O(K^{O(1)})$ and $|H| \leqslant O(K^{O(1)})|A|$.*

This proposition essentially reduces the study of sets of small doubling to that of approximate groups. In a similar flavor one shows that is $|A^3| \leqslant K|A|$, then $(A \cup A^{-1} \cup \{1\})^2$ is a $O(K^{O(1)})$-approximate subgroup. And that if $|AA| \leqslant K|A|$, then A has a subset of size $\geqslant |A|/O(K^{O(1)})$ which has tripling at most $O(K^{O(1)})$.

2. Hilbert's fifth problem and approximate groups

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