An introduction to approximate groups and their applications

E. Breuillard, (based on joint work with Ben Green and Terence Tao)

Université Paris-Sud, Orsay

Gdansk, May 24 2013

A finite subset $A \subset G$ of an ambient group G has doubling at most K if

$$|AA| \leqslant K|A|.$$

A finite subset $A \subset G$ of an ambient group G has doubling at most K if

$$|AA| \leqslant K|A|.$$

A central problem in additive combinatorics is to understand the structure of such sets.

A finite subset $A \subset G$ of an ambient group G has doubling at most K if

$$|AA| \leqslant K|A|.$$

A central problem in additive combinatorics is to understand the structure of such sets.

Examples:

- A is a finite subgroup $\to AA = A$. In this case $K = 1$.
- $A = \{a, a+b, a+2b, \ldots, a+Nb\}$ an arithmetic progression in $\mathbb{Z}$. In this case $K \leqslant 2$.
- A any subset with $|A| > |G|/2$ in a finite group G. In this case $AA = G$ and $K \leqslant 2$.

Lemma (K=1)

Let A be a finite subset in a group G. Suppose $|AA| = |A|$. Then:

- *$A = aH$ for some finite subgroup H of G and some (all) $a \in A$,*
- *H is normalized by every element of A.*

Lemma (K=1)

Let A be a finite subset in a group G. Suppose $|AA| = |A|$. Then:

- *$A = aH$ for some finite subgroup H of G and some (all) $a \in A$,*
- *H is normalized by every element of A.*

A proof:

- $\forall a, a' \in A$, $a'A = aA$. So $a^{-1}a'A = A$ and $A^{-1}AA = A$.

Lemma (K=1)

Let A be a finite subset in a group G. Suppose $|AA| = |A|$. Then:

- *$A = aH$ for some finite subgroup H of G and some (all) $a \in A$,*
- *H is normalized by every element of A.*

A proof:

- $\forall a, a' \in A$, $a'A = aA$. So $a^{-1}a'A = A$ and $A^{-1}AA = A$.
- Let $H := A^{-1}A$. Then $H = H^{-1}$, $e_G \in H$, and $HA = A$.

Lemma (K=1)

Let A be a finite subset in a group G. Suppose $|AA| = |A|$. Then:

- *$A = aH$ for some finite subgroup H of G and some (all) $a \in A$,*
- *H is normalized by every element of A.*

A proof:

- $\forall a, a' \in A$, $a'A = aA$. So $a^{-1}a'A = A$ and $A^{-1}AA = A$.
- Let $H := A^{-1}A$. Then $H = H^{-1}$, $e_G \in H$, and $HA = A$.
- So $H^n A = A$ for all $n \in \mathbb{N}$. And $\langle H \rangle := \cup_n H^n$ is a finite subgroup.

Lemma (K=1)

Let A be a finite subset in a group G. Suppose $|AA| = |A|$. Then:

- *$A = aH$ for some finite subgroup H of G and some (all) $a \in A$,*
- *H is normalized by every element of A.*

A proof:

- $\forall a, a' \in A$, $a'A = aA$. So $a^{-1}a'A = A$ and $A^{-1}AA = A$.
- Let $H := A^{-1}A$. Then $H = H^{-1}$, $e_G \in H$, and $HA = A$.
- So $H^n A = A$ for all $n \in \mathbb{N}$. And $\langle H \rangle := \cup_n H^n$ is a finite subgroup.
- Since $|A| \leqslant |H| \leqslant |H^n| \leqslant |A|$, it must be that $H = \langle H \rangle$ is a subgroup.

Lemma (K=1)

Let A be a finite subset in a group G. Suppose $|AA| = |A|$. Then:

- *$A = aH$ for some finite subgroup H of G and some (all) $a \in A$,*
- *H is normalized by every element of A.*

A proof:

- $\forall a, a' \in A$, $a'A = aA$. So $a^{-1}a'A = A$ and $A^{-1}AA = A$.
- Let $H := A^{-1}A$. Then $H = H^{-1}$, $e_G \in H$, and $HA = A$.
- So $H^n A = A$ for all $n \in \mathbb{N}$. And $\langle H \rangle := \cup_n H^n$ is a finite subgroup.
- Since $|A| \leqslant |H| \leqslant |H^n| \leqslant |A|$, it must be that $H = \langle H \rangle$ is a subgroup.
- and $HA = A$, so $Ha = A$ for all $a \in A$.

Lemma (K=1)

Let A be a finite subset in a group G. Suppose $|AA| = |A|$. Then:

- *$A = aH$ for some finite subgroup H of G and some (all) $a \in A$,*
- *H is normalized by every element of A.*

A proof:

- $\forall a, a' \in A$, $a'A = aA$. So $a^{-1}a'A = A$ and $A^{-1}AA = A$.
- Let $H := A^{-1}A$. Then $H = H^{-1}$, $e_G \in H$, and $HA = A$.
- So $H^nA = A$ for all $n \in \mathbb{N}$. And $\langle H \rangle := \cup_n H^n$ is a finite subgroup.
- Since $|A| \leqslant |H| \leqslant |H^n| \leqslant |A|$, it must be that $H = \langle H \rangle$ is a subgroup.
- and $HA = A$, so $Ha = A$ for all $a \in A$.
- Since $H = A^{-1}A$, we conclude that $a^{-1}Ha = H$ for every $a \in A$.

Under the $K = 2$ threshold: Only groups!

Under the $K = 2$ threshold: Only groups!

Lemma (Freiman $\frac{3}{2}$ lemma (1960's))

If $|AA| < \frac{3}{2}|A|$, then $A \subset aH$, for some finite subgroup H of G normalized by A with $|H| < \frac{3}{2}|A|$.

This is sharp! take $A := \{0, 1\}$ in $\mathbb{Z}$.

Under the $K = 2$ threshold: Only groups!

Lemma (Freiman $\frac{3}{2}$ lemma (1960's))

If $|AA| < \frac{3}{2}|A|$, then $A \subset aH$, for some finite subgroup H of G normalized by A with $|H| < \frac{3}{2}|A|$.

This is sharp! take $A := \{0, 1\}$ in $\mathbb{Z}$.

Lemma (Hamidoune's $2 - \varepsilon$ result (2010))

If $|AA| < (2 - \varepsilon)|A|$, then $A \subset a_1 H \cup \ldots \cup a_N H$, for some finite subgroup H of G, with $|H| < \frac{2}{\varepsilon}|A|$ and $N < \frac{2}{\varepsilon}$.

The case when $G = \mathbb{Z}$: Freiman's classification theorem:

Theorem (Freiman's theorem (1960's))

Suppose $A \subset \mathbb{Z}$ and $|AA| \leqslant K|A|$. Then

$$A \subset X + P,$$

where

- $|X| = O_K(1)$,
- P *is multi-dimensional progression* P *of dimension* $d = O_K(1)$.
- $|P| \leqslant O_K(1)|A|$.

The case when $G = \mathbb{Z}$: Freiman's classification theorem:

Theorem (Freiman's theorem (1960's))

Suppose $A \subset \mathbb{Z}$ and $|AA| \leqslant K|A|$. Then

$$A \subset X + P,$$

where

- $|X| = O_K(1)$,
- *P is multi-dimensional progression P of dimension $d = O_K(1)$.*
- $|P| \leqslant O_K(1)|A|$.

Remark: A subset $P \subset G$ is called a multi-dimensional progression if $P = \pi(B)$, where B is a box $\prod_{i=1}^{r}[-N_i, N_i] \subset \mathbb{Z}^d$, and $\pi : \mathbb{Z}^d \to \mathbb{Z}$ is a homomorphism.

Green and Ruzsa generalized Freiman's theorem to arbitrary *abelian* groups:

Theorem (Green-Ruzsa 2006)

Suppose G is abelian and $A \subset G$ has $|AA| \leqslant K|A|$. Then

$$A \subset X + H + P,$$

where

- $|X| = O_K(1)$,
- *P is multi-dimensional progression P of dimension $d = O_K(1)$.*
- *H is a finite subgroup of G,*
- $|H + P| \leqslant O_K(1)|A|$.

Green and Ruzsa generalized Freiman's theorem to arbitrary *abelian* groups:

Theorem (Green-Ruzsa 2006)

Suppose G is abelian and $A \subset G$ has $|AA| \leqslant K|A|$. Then

$$A \subset X + H + P,$$

where

- $|X| = O_K(1)$,
- *P is multi-dimensional progression P of dimension $d = O_K(1)$.*
- *H is a finite subgroup of G,*
- $|H + P| \leqslant O_K(1)|A|$.

Remark: Such a set of the form $H + P$ as above is called a coset multi-dimensional progression.

Gromov's theorem on groups of polynomial growth.

G = a group generated by a finite set $S := \{s_1, s_1^{-1}, \ldots, s_k, s_k^{-1}\}$,
$\mathcal{G}$ = its Cayley graph,
$B(n) = S^n$ = the balls in $\mathcal{G}$ centered at the identity.

Gromov's theorem on groups of polynomial growth.

G = a group generated by a finite set $S := \{s_1, s_1^{-1}, \ldots, s_k, s_k^{-1}\}$,
$\mathcal{G}$ = its Cayley graph,
$B(n) = S^n$ = the balls in $\mathcal{G}$ centered at the identity.

A natural problem is to ask about the growth type of G.

Growth type = asymptotics for $|B(n)|$.

Gromov's theorem on groups of polynomial growth.

G = a group generated by a finite set $S := \{s_1, s_1^{-1}, \dots, s_k, s_k^{-1}\}$,
$\mathcal{G}$ = its Cayley graph,
$B(n) = S^n$ = the balls in $\mathcal{G}$ centered at the identity.

A natural problem is to ask about the growth type of G.

Growth type = asymptotics for $|B(n)|$.

Theorem (Gromov 1982)

Every finitely generated group with polynomial growth is virtually nilpotent.

virtually nilpotent = there is a finite index subgroup which is nilpotent.
polynomial growth = $|B(n)| = O(n^C)$ for some $C > 0$.

Gromov's paper (IHES 1982) is truly amazing!

$\rightarrow$ founding paper for geometric group theory.

$\rightarrow$ the start of the proof is to argue that there are infinitely many radii n_k's for which:

$$|B(2n_k)| \leqslant K|B(n_k)|$$

for some $K > 0$ ($K = 3^C$ OK).

Gromov's paper (IHES 1982) is truly amazing!

$\rightarrow$ founding paper for geometric group theory.

$\rightarrow$ the start of the proof is to argue that there are infinitely many radii n_k's for which:

$$|B(2n_k)| \leqslant K|B(n_k)|$$

for some $K > 0$ ($K = 3^C$ OK).

$\rightarrow$ We see here a need for understanding sets of doubling $\leqslant K$ in arbitrary groups.

Main theorem, weak form

G = a group.
$A \subset G$ a finite subset.

Theorem (BGT 2011 weak form)

Assume $|AA| \leqslant K|A|$. Then there is a virtually nilpotent subgroup $\Gamma \leqslant G$ and $g \in G$ such that

$$|A \cap g\Gamma| \geqslant |A|/O_K(1).$$

Gromov's theorem on groups of polynomial growth.

From our theorem, we recover Gromov's theorem!

Theorem (Gromov 1982)

Every group with polynomial growth is virtually nilpotent.

Gromov's theorem on groups of polynomial growth.

From our theorem, we recover Gromov's theorem!

Theorem (Gromov 1982)

Every group with polynomial growth is virtually nilpotent.

Suppose $|B(r)| \leqslant r^K$ for all large r.

- There are arbitrarily large scales r such that

$$|B(2r)| \leqslant 3^K |B(r)|.$$

- By the theorem applied to $A := B(r)$ we get that $B(2r)$ intersects a virtually nilpotent group in a set of size $\geqslant |B(r)|/O_K(1)$

Gromov's theorem on groups of polynomial growth.

From our theorem, we recover Gromov's theorem!

Theorem (Gromov 1982)

Every group with polynomial growth is virtually nilpotent.

Suppose $|B(r)| \leqslant r^K$ for all large r.

- There are arbitrarily large scales r such that

$$|B(2r)| \leqslant 3^K |B(r)|.$$

- By the theorem applied to $A := B(r)$ we get that $B(2r)$ intersects a virtually nilpotent group in a set of size $\geqslant |B(r)|/O_K(1)$

Remark: the argument works assuming only that $|B(r)| \leqslant r^K$ for one large r.

Approximate groups, definition

Definition (Approximate subgroups)

Let $K \geqslant 1$. A subset A of a group G is said to be a K-approximate subgroup of G if
(i) $e_G \in A$,
(ii) $A = A^{-1}$,
(iii) $\exists X \subset G$, $|X| \leqslant K$, such that

$$AA \subset XA$$

Remark:
We will be mainly interested in *finite* approximate groups, although considering infinite ones as well is crucial to our proof.

Of course every K-approximate group has doubling at most K.

Of course every K-approximate group has doubling at most K. Conversely,

Proposition (Ruzsa, Tao)

If $|AA| \leqslant K|A|$, then there is $A_1 \subset (A \cup A^{-1} \cup \{1\})^2$ such that:
(i) A_1 is a $O(K^{O(1)})$-approximate group, $|A_1| \leqslant O_K(1)|A|$,
(ii) Moreover A is contained in $\leqslant O(K^{O(1)})$ (left) translates of A_1.

Of course every K-approximate group has doubling at most K. Conversely,

Proposition (Ruzsa, Tao)

If $|AA| \leqslant K|A|$, then there is $A_1 \subset (A \cup A^{-1} \cup \{1\})^2$ such that:
(i) A_1 is a $O(K^{O(1)})$-approximate group, $|A_1| \leqslant O_K(1)|A|$,
(ii) Moreover A is contained in $\leqslant O(K^{O(1)})$ (left) translates of A_1.

Remark:

This essentially reduces the study of sets of small doubling to that of finite approximate groups.

Examples of approximate groups

- a finite group is a 1-approximate group.
- a d-dimensional progression is a 2^d-approximate group.
- a small ball around the identity in a Lie group (not a finite approximate group though!).
- a nilprogression of rank r and step s is a $O_{r,s}$-approximate group.
- "extensions" of such.

Basic properties

Finite approximate groups have many of the basic properties of groups. They are:
(i) stable under intersection ($A^2 \cap B^2$ is an approximate group if A, B are)
(ii) stable under quotients ($\pi(A)$ is an approximate group if π is a homomorphism)

Basic properties

Finite approximate groups have many of the basic properties of groups. They are:
(i) stable under intersection ($A^2 \cap B^2$ is an approximate group if A, B are)
(ii) stable under quotients ($\pi(A)$ is an approximate group if π is a homomorphism)

Examples of approximate groups

- a nilprogression of rank r and step s is a $O_{r,s}$-approximate group.
- "extensions" of such (so-called *coset nilpgrogressions*).

What is a nilprogression ?

Examples of approximate groups

- a nilprogression of rank r and step s is a $O_{r,s}$-approximate group.
- "extensions" of such (so-called *coset nilpgrogressions*).

What is a nilprogression ?

"Nilprogression" $=$ a homomorphic image $P = \pi(B)$ of a box B in the free nilpotent group of rank r and step s.

Examples of approximate groups

- a nilprogression of rank r and step s is a $O_{r,s}$-approximate group.
- "extensions" of such (so-called *coset nilpgrogressions*).

What is a nilprogression ?

"Nilprogression" $=$ a homomorphic image $P = \pi(B)$ of a box B in the free nilpotent group of rank r and step s.

"Box" means: ball for a left invariant Riemannian (or CC) metric on the free nilpotent Lie group.

What is a <u>nilprogression</u> ?

"Nilprogression" = a homomorphic image $P = \pi(B)$ of a box B in the free nilpotent group of rank r and step s.

"Box" means: ball for a left invariant Riemannian (or CC) metric on the free nilpotent Lie group.

Example: If $N, M \in \mathbb{N}$, set

$$A := \left\{ \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} ; |x|, |y| \leqslant N; |z| \leqslant M \right\}$$

It is a "box" if $M \simeq N^2$. It is a nilprogression of step 2 and rank $\leqslant 3$ if $M \geqslant N^2$.

Main theorem, strong form

$G =$ a group.
$K \geqslant 1$

Theorem (BGT strong form: structure of approximate groups)

Assume $A \subset G$ a finite K-approximate subgroup. Then

$$A \subset XP,$$

where

- $|X| \leqslant O_K(1)$,
- *P is a coset nilprogression of rank and step $O_K(1)$,*
- $P \subset A^4$.

coset-nilprogression = finite set of the form $P = HL$, where H is a finite group normalized by L and $H \backslash HL$ is a nilprogression.

In 1978 Gromov proved that almost flat manifolds are finitely covered by nilmanifolds, in particular they have virtually nilpotent fundamental group. This last fact was later generalized by Fukaya-Yamaguchi, then Cheeger-Colding, Kapovitch-Wilking, to almost non-negatively curved (sectional or Ricci) manifolds. We recover this:

Corollary

There is $\varepsilon = \varepsilon(n) > 0$ such that every closed n-manifold with diameter 1 and Ricci curvature $\geqslant -\varepsilon$ has virtually nilpotent π_1.

More applications: a generalized Margulis lemma

The following was conjectured by Gromov:

Theorem (Generalized Margulis Lemma)

Suppose X is a metric space in which every ball of radius 4 can be covered by K balls of radius 1. Then there is $\varepsilon = \varepsilon(K) > 0$ such that, given any discrete group of isometries Γ of X, and $x \in X$, the subgroup generated by

$$\{\gamma \in \Gamma; d(x, \gamma \cdot x) \leqslant \varepsilon\}$$

is virtually nilpotent.

Pick any sequence of finite vertex transitive graphs G_n satisfying $|G_n| \leqslant C(diam G_n)^d$.

Theorem (Benjamini-Finucane-Tessera)

After renormalizing to diameter 1, the G_n's have a subsequence converging (in Gromov-Hausdorff topology) to a torus $\mathbb{R}^k/\mathbb{Z}^k$ of dimension $k \leqslant d$ equipped with a translation invariant distance.

In particular the round sphere cannot be very well approximated by such graphs...

More applications: diameter of finite groups

Here is another application of the main theorem, this time to finite groups!

$$G = \text{ a finite group,}$$
$$\mathcal{G} = \text{ its Cayley graph,}$$
$$B(n) = \text{ the ball of radius } n \text{ in } \mathcal{G}.$$
$$D = diam(\mathcal{G}) \text{ the diameter of } \mathcal{G}.$$

Here is another application of the main theorem, this time to finite groups!

$$G = \text{a finite group},$$
$$\mathcal{G} = \text{its Cayley graph},$$
$$B(n) = \text{the ball of radius } n \text{ in } \mathcal{G}.$$
$$D = diam(\mathcal{G}) \text{ the diameter of } \mathcal{G}.$$

Theorem (Structure of large diameter groups)

$\forall \varepsilon, \delta > 0$, $\exists C > 0$ s.t. if $D \geqslant |G|^{\varepsilon}$, there is

- *A subgroup $G_0 \leqslant G$ of index $\leqslant C$,*
- *A normal subgroup H of G_0 s.t. $H \subset B(D^{\delta})$, and s.t.*
- *G_0/H is nilpotent with of nilpotency class $\leqslant C$ and number of generators $\leqslant C$.*

More applications: diameter of finite groups

Corollary (Diameter of finite simple groups)

$\forall \varepsilon > 0 \; \exists C_\varepsilon > 0$ *s.t.*

$$diam(\mathcal{G}) \leqslant C_\varepsilon |G|^\varepsilon,$$

for every Cayley graph $\mathcal{G}$ of every finite simple group G.

More applications: diameter of finite groups

Corollary (Diameter of finite simple groups)

$\forall \varepsilon > 0\ \exists C_\varepsilon > 0$ s.t.

$$diam(\mathcal{G}) \leqslant C_\varepsilon |G|^\varepsilon,$$

for every Cayley graph $\mathcal{G}$ of every finite simple group G.

Babai's conjecture $= \exists C > 0$ s.t.

$$diam(\mathcal{G}) \leqslant C(\log |G|)^C,$$

for some absolute constant $C > 0$.

More applications: diameter of finite groups

Corollary (Diameter of finite simple groups)

$\forall \varepsilon > 0 \; \exists C_\varepsilon > 0$ s.t.

$$diam(\mathcal{G}) \leqslant C_\varepsilon |G|^\varepsilon,$$

for every Cayley graph $\mathcal{G}$ of every finite simple group G.

Babai's conjecture $= \exists C > 0$ s.t.

$$diam(\mathcal{G}) \leqslant C(\log|G|)^C,$$

for some absolute constant $C > 0$.

Our proof does not use CFSG !

Babai's conjecture is still open even using CFSG.

Helfgott 2005 : true for the family $PSL_2(p)$.

Pyber-Szabo, BGT 2010 : true for all finite simple groups of Lie type $G(q)$ with C depending on the rank of G only.

$\rightarrow$ the proof consists in a classification theorem (with sharper constants) for K-approximate subgroups of $G(q)$.

Helfgott-Seress 2011 : $diam(A_n) = exp(O(\log\log|A_n|)^C)$

Dziękuję Bardzo!