Approximate groups and their applications: part 1

E. Breuillard

Université Paris-Sud, Orsay

St. Andrews, August 3-10, 2013

the notion of an approximate subgroup

Let G be an ambient group with unit element 1.

Let G be an ambient group with unit element 1.
Let A be a finite subset $A \subset G$.

the notion of an approximate subgroup

Let G be an ambient group with unit element 1.
Let A be a finite subset $A \subset G$.
Here are three equivalent conditions for A to be a *subgroup* of G.

1. $AA \subset A$,
2. $|AA| = |A|$ and $1 \in A$,
3. $Proba_{a \in A, b \in A}(ab \in A) = 1$.

Let G be an ambient group with unit element 1.
Let A be a finite subset $A \subset G$.
Here are three equivalent conditions for A to be a *subgroup* of G.

1. $AA \subset A$,
2. $|AA| = |A|$ and $1 \in A$,
3. $Proba_{a \in A, b \in A}(ab \in A) = 1$.

What if we relax these conditions in some quantitative way ?

For example suppose A is a finite subset of G such that $1 \in A$ and $|AA| \leqslant (1+\varepsilon)|A|$ for some small $\varepsilon > 0$.

the notion of an approximate subgroup

For example suppose A is a finite subset of G such that $1 \in A$ and $|AA| \leqslant (1+\varepsilon)|A|$ for some small $\varepsilon > 0$.

Fact: then there is a finite subgroup H of G such that $A \subset H$ and $|A| \geqslant (1-\varepsilon)|H|$.

For example suppose A is a finite subset of G such that $1 \in A$ and $|AA| \leqslant (1+\varepsilon)|A|$ for some small $\varepsilon > 0$.

Fact: then there is a finite subgroup H of G such that $A \subset H$ and $|A| \geqslant (1-\varepsilon)|H|$.

Proof: Let $H = A^{-1}A$. We have for all $a, b \in A$,

$$|aA \cap bA| = 2|A| - |aA \cup bA| \geqslant 2|A| - |A^2| \geqslant (1-\varepsilon)|A|.$$

the notion of an approximate subgroup

For example suppose A is a finite subset of G such that $1 \in A$ and $|AA| \leqslant (1+\varepsilon)|A|$ for some small $\varepsilon > 0$.

Fact: then there is a finite subgroup H of G such that $A \subset H$ and $|A| \geqslant (1-\varepsilon)|H|$.

Proof: Let $H = A^{-1}A$. We have for all $a, b \in A$,

$$|aA \cap bA| = 2|A| - |aA \cup bA| \geqslant 2|A| - |A^2| \geqslant (1-\varepsilon)|A|.$$

So $AA^{-1} = A^{-1}A = H$ and every $x \in H$ has at least $(1-\varepsilon)$ representations of the form $x = dc^{-1}$, $d, c \in A$. Hence $|H| \leqslant \frac{1}{(1-\varepsilon)}|A|$.

the notion of an approximate subgroup

For example suppose A is a finite subset of G such that $1 \in A$ and $|AA| \leqslant (1+\varepsilon)|A|$ for some small $\varepsilon > 0$.

Fact: then there is a finite subgroup H of G such that $A \subset H$ and $|A| \geqslant (1-\varepsilon)|H|$.

Proof: Let $H = A^{-1}A$. We have for all $a, b \in A$,

$$|aA \cap bA| = 2|A| - |aA \cup bA| \geqslant 2|A| - |A^2| \geqslant (1-\varepsilon)|A|.$$

So $AA^{-1} = A^{-1}A = H$ and every $x \in H$ has at least $(1-\varepsilon)$ representations of the form $x = dc^{-1}$, $d, c \in A$. Hence $|H| \leqslant \frac{1}{(1-\varepsilon)}|A|$.
(if $\varepsilon < \frac{1}{2}$) Given $x, y \in H$, there must be representations $x = dc^{-1}$ and $y = ef^{-1}$ with $c = e$. Hence $xy \in H$.

For example suppose A is a finite subset of G such that $1 \in A$ and $|AA| \leqslant (1+\varepsilon)|A|$ for some small $\varepsilon > 0$.

Fact: then there is a finite subgroup H of G such that $A \subset H$ and $|A| \geqslant (1-\varepsilon)|H|$.

Proof: Let $H = A^{-1}A$. We have for all $a, b \in A$,

$$|aA \cap bA| = 2|A| - |aA \cup bA| \geqslant 2|A| - |A^2| \geqslant (1-\varepsilon)|A|.$$

So $AA^{-1} = A^{-1}A = H$ and every $x \in H$ has at least $(1-\varepsilon)$ representations of the form $x = dc^{-1}$, $d, c \in A$. Hence $|H| \leqslant \frac{1}{(1-\varepsilon)}|A|$.
(if $\varepsilon < \frac{1}{2}$) Given $x, y \in H$, there must be representations $x = dc^{-1}$ and $y = ef^{-1}$ with $c = e$. Hence $xy \in H$.
Done.

the notion of an approximate subgroup

More generally, let $K \geqslant 1$ be a parameter, and consider the following conditions on a finite subset A of G.

1. $AA \subset XA$, for some set X with $|X| \leqslant K$.

More generally, let $K \geqslant 1$ be a parameter, and consider the following conditions on a finite subset A of G.

1. $AA \subset XA$, for some set X with $|X| \leqslant K$.
2. $|AA| \leqslant K|A|$,

the notion of an approximate subgroup

More generally, let $K \geqslant 1$ be a parameter, and consider the following conditions on a finite subset A of G.

1. $AA \subset XA$, for some set X with $|X| \leqslant K$.
2. $|AA| \leqslant K|A|$,
3. $Proba_{a \in A, b \in A}(ab \in A) \geqslant \frac{1}{K}$.

More generally, let $K \geqslant 1$ be a parameter, and consider the following conditions on a finite subset A of G.

1. $AA \subset XA$, for some set X with $|X| \leqslant K$.
2. $|AA| \leqslant K|A|$,
3. $Proba_{a \in A, b \in A}(ab \in A) \geqslant \frac{1}{K}$.

Proposition

There is an absolute constant $C > 0$ such that: If condition (i) holds for A and K, then condition (i') holds for some subset A' with $|A|/K' \leqslant |A'| \leqslant K'|A|$, $|A \cap A'| \geqslant |A|/K'$, and $K' \leqslant CK^C$.

More generally, let $K \geqslant 1$ be a parameter, and consider the following conditions on a finite subset A of G.

1. $AA \subset XA$, for some set X with $|X| \leqslant K$.
2. $|AA| \leqslant K|A|$,
3. $Proba_{a \in A, b \in A}(ab \in A) \geqslant \frac{1}{K}$.

Proposition

There is an absolute constant $C > 0$ such that: If condition (i) holds for A and K, then condition (i') holds for some subset A' with $|A|/K' \leqslant |A'| \leqslant K'|A|$, $|A \cap A'| \geqslant |A|/K'$, and $K' \leqslant CK^C$.

Proof: Balog-Szemeredi-Gowers-Tao.

We will say that two finite subsets A, A' of an ambient group G are *K-roughly equivalent* if

$$|A \cap A'| \geqslant \frac{\max\{|A|, |A'|\}}{K}$$

We will say that two finite subsets A, A' of an ambient group G are *K-roughly equivalent* if

$$|A \cap A'| \geqslant \frac{\max\{|A|, |A'|\}}{K}$$

In 2005, T. Tao introduced the following:

Definition (Approximate subgroup)

A (finite) subset A in an ambient group G, is called a K-approximate subgroup if:

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

Approximate groups and their applications

Motivations for studying approximate groups:

- construction of new families of expander graphs, (Bourgain-Gamburd, Bourgain-Gamburd-Sarnak, Varju, BGT, etc).
- extending additive combinatorics to the non-commutative setting (Freiman, Ruzsa, Gowers, Tao, BGT, etc.)
- new applications in analytic number theory (sieving) and counting primes in orbits (Bourgain-Gamburd-Sarnak, Salehi-Sarnak, Kowalski, Lubotzky-Meiri,...)
- connection with Model Theory and Stability theory (Hrushovski),
- new results for finite simple groups (Waring type problems: Liebeck, Nikolov, Shalev, etc).
- applications to growth of groups (improvements of Gromov's theorem, counting conjugacy classes), to Riemannian geometry (almost flat manifolds, structure of large transitive graphs)

- J. Bourgain. N. Katz, T. Tao, *A sum-product estimate for finite fields, and applications*, Geom. Func. Anal. **14** (2004), 27–57.
- T. C. Tao and V. H. Vu, *Additive Combinatorics*, CUP 2006.
- 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.
- T. Tao, *Product set estimates in noncommutative groups*, Combinatorica **28** (2008), 547–594.
- H. Helfgott, *Growth and generation in* $SL_2(\mathbb{Z}/p\mathbb{Z})$, Ann. of Math. 167 (2008), 601–623.

- E. Hrushovski, *Stable group theory and approximate subgroups*, J. Amer. Math. Soc. 25 (2012), no. 1, 189–243.
- L. Pyber, E. Szabó, *Growth in finite simple groups of Lie type*, preprint (2010) arXiv:1001.4556
- E. Breuillard, B. Green and T. Tao, *Approximate subgroups of linear groups*, Geom. Funct. Anal. 21 (2011), no. 4, 774–819.
- E. Breuillard, B. Green and T. Tao, *The structure of approximate groups*, Publ. Inst. Hautes Études Sci., **116**, Issue 1, 115–221, (2012)

Sets with small doubling and the Freiman inverse problem

A finite subset $A \subset G$ of an ambient group G is said to have doubling at most K if

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

Sets with small doubling and the Freiman inverse problem

A finite subset $A \subset G$ of an ambient group G is said to have doubling at most K if

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

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

Sets with small doubling and the Freiman inverse problem

A finite subset $A \subset G$ of an ambient group G is said to have 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 $\rightarrow AA = A$. 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.*

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* $|A + A| \leqslant K|A|$. *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 $|A + A| \leqslant K|A|$. 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.

Approximate subgroups and small doubling

Recall our definition:

Definition (Approximate subgroup)

A (finite) subset A in an ambient group G, is called a K-approximate subgroup if:

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

Approximate subgroups and small doubling

Recall our definition:

Definition (Approximate subgroup)

A (finite) subset A in an ambient group G, is called a K-approximate subgroup if:

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

Proposition (Tao)

If A is a finite subset of G with $|AA| \leqslant K|A|$, then there is $A' \subset A$ s.t. $|A'| \geqslant |A|/CK^C$, and $B := (A' \cup A'^{-1} \cup \{1\})^3$ is a CK^C-approximate subgroup with $|B| \leqslant CK^C|A|$ and $A \subset XB$ for some set X with $|X| \leqslant CK^C$.

Approximate subgroups and small doubling

Recall our definition:

Definition (Approximate subgroup)

A (finite) subset A in an ambient group G, is called a K-approximate subgroup if:

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

Proposition (Tao)

If A is a finite subset of G with $|AA| \leqslant K|A|$, then there is $A' \subset A$ s.t. $|A'| \geqslant |A|/CK^C$, and $B := (A' \cup A'^{-1} \cup \{1\})^3$ is a CK^C-approximate subgroup with $|B| \leqslant CK^C|A|$ and $A \subset XB$ for some set X with $|X| \leqslant CK^C$.

In particular any subset with doubling at most K is CK^C-roughly equivalent to a CK^C-approximate subgroup.

Approximate subgroups and small doubling

Definition (Approximate subgroup)

A (finite) subset A in an ambient group G, is called a K-approximate subgroup if:

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

Proposition (Tao)

If A is a finite subset of G with $|AA| \leqslant K|A|$, then there is $A' \subset A$ s.t. $|A'| \geqslant |A|/CK^C$, and $B := (A' \cup A'^{-1} \cup \{1\})^3$ is a CK^C-approximate subgroup with $|B| \leqslant CK^C|A|$ and $A \subset XB$ for some set X with $|X| \leqslant CK^C$.

$\to$ it is enough to characterize *approximate subgroups*. They are easier to handle.

Approximate subgroups and small doubling

Definition (Approximate subgroup)

A (finite) subset A in an ambient group G, is called a K-approximate subgroup if:

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

Proposition (Tao)

If A is a finite subset of G with $|AA| \leqslant K|A|$, then there is $A' \subset A$ s.t. $|A'| \geqslant |A|/CK^C$, and $B := (A' \cup A'^{-1} \cup \{1\})^3$ is a CK^C-approximate subgroup with $|B| \leqslant CK^C|A|$ and $A \subset XB$ for some set X with $|X| \leqslant CK^C$.

Remark: If $|AAA| \leqslant K|A|$, we can assume $A' = A$. In particular $A \subset B$.

Basic properties of approximate groups

Here are some simple properties:

- (powers) If A is a K-approximate subgroup and $n \geqslant 1$, then A^n is a K^n-approximate subgroup which is K^n-roughly equivalent to A.
- (intersection) If A and B are K-approximate subgroups, then $A^2 \cap B^2$ is a K^6-approximate subgroup.
- (sub-approximate group) If A is a K-approximate group and $H \leqslant G$ a subgroup, then $A^2 \cap H$ is a K^2-approximate subgroup.
- (quotient) If $\pi : G \to H$ is a group homomorphism, and A is a K-approximate group, then $\pi(A)$ is a K-approximate group.
- (group action) If G acts on a set X, and A is a K-approximate subgroup, then for each $n \geqslant 1$,

$$|A| \leqslant |A \cdot x| \cdot |A^n \cap Stab(x)| \leqslant K^n |A|$$

- (approximate partition into orbits) X can be decomposed into approximate A-orbits, $A \cdot x$, i.e. $X = \cup_Y A^2 \cdot y$, $A \cdot y$, $y \in Y$ disjoint.

Here is a surprisingly successful principle: when trying to prove a result about approximate subgroups, try to adapt a known argument valid in the classical setting of group theory.

Basic properties of approximate groups

Here is a surprisingly successful principle: when trying to prove a result about approximate subgroups, try to adapt a known argument valid in the classical setting of group theory.

For example: adapt the group theoretical arguments needed to understand the subgroup structure of a given group in order to classify its approximate subgroups.

Basic properties of approximate groups

Here is a surprisingly successful principle: when trying to prove a result about approximate subgroups, try to adapt a known argument valid in the classical setting of group theory.

For example: adapt the group theoretical arguments needed to understand the subgroup structure of a given group in order to classify its approximate subgroups.

Caveat: any group theoretical argument using divisibility properties of the order of a finite group will not have any approximate analogue...