Approximate groups

Emmanuel Breuillard

Université Paris-Sud, Orsay, France

March 19, 2011

Plan of the talk:

1. Discussion of the non-commutative Freiman problem and related conjectural statements.
2. Hrushovski's theorems and the generalization of Gromov's polynomial growth theorem.
3. Effective "Helfgott-type" versions of Hrushovski's theorem and the growth of large sets in linear groups (joint with B. Green and T. Tao).
4. Applications to expander graphs (joint with B. Green, T. Tao and R. Guralnick).

The non-commutative Freiman problem

Let $K \geqslant 1$ be a parameter.
Let G be a group and A a finite subset. $|A|$ denotes the number of elements in A.

Question (non-commmutative Freiman problem)

What can one say about A if $|AA| \leqslant K|A|$?

- This problem was first studied in the case when G is abelian in the context of Additive Number Theory and Combinatorics (Freiman, Ruzsa, Erdos, Szemeredi, etc).
- Renewed interest took place in recent years with the Green-Tao theorem on arithmetic progression on primes, the Bourgain-Gamburd new construction of expander graphs, and the Bourgain-Gamburd-Sarnak "affine sieve theory", which made use of some partial solutions to this problem.
- Last summer, Hrushovski released a remarkable paper in which he studied this problem using tools from Model Theory and Logic, giving the first general answers valid in any group, establishing a generalization of Gromov's polynomial growth theorem and unearthing new connections between logic, group theory and combinatorics.

Examples (=exercises):

- $|AA| = |A|$ if and only if $A = aH$ is a normalizing coset of a finite subgroup H of G.
- $|AA| < \frac{3}{2}|A|$ if and only if $A \subset aH$ is contained in a normalizing coset of a finite subgroup H of G of size $|H| < \frac{3}{2}|A|$.
- If $A = \{0, ..., n\} \in \mathbb{Z}$, $A + A = \{0, ..., 2n\}$ and thus $|A + A| = 2|A| - 1 < 2|A|$.
- If A is the ball of radius n in the Cayley graph of a nilpotent group G generated by some finite set S, then $|AA| \leqslant K|A|$, where K depends only on G, S but not on n.

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

When $G = \mathbb{Z}$, the answer to the question was found by Freiman in the sixties.

Theorem (Freiman's theorem)

If $A \subset \mathbb{Z}$ and $|AA| \leqslant K|A|$, then A is contained in a generalized arithmetic progression P of rank $O(K^C)$ and size $|P| \leqslant exp(O(K^C))|A|$.

What is a *generalized arithmetic progression* of rank d ? It is a set $P = \pi(B)$, where $\pi : \mathbb{Z}^d \to \mathbb{Z}$ is an affine map (i.e. a homomorphism composed with a translation), and B is a box $B := \prod_{i=1,\dots,d}[0, L_i]$, where $L_i \leqslant 1$ are the side lengths.

A simpler proof of Freiman's theorem was found by Ruzsa later on and subsequently generalized by Green-Ruzsa to an arbitrary abelian group G.

The proofs rely on harmonic analysis and identify in A or AA a so called *Bohr set*, that is the inverse image of a neighborhood of zero under a group homomorphism $G \to (\mathbb{R}/\mathbb{Z})^d$.

A couple of years ago, with Ben Green we extended Freiman's theorem to nilpotent groups:

Theorem (Breuillard-Green '08)

If G is a f.g. torsion free s-step nilpotent group and A a finite subset with $|AAA| \leqslant K|A|$, then A is contained in an s-step nilprogression P of size $O_s(exp(O_s(K^{C_s}))|A|$ and rank $O_s(K_s^C)$.

An s-step *nilprogression* of rank d is the nilpotent analog of a generalized arithmetic. It is defined similarly as $P = \pi(B)$, where π is an affine map from the s-step free nilpotent group on d generators $N_{s,d}$ and B is a "nilbox" in $N_{s,d}$.

Approximate groups were introduced by Terence Tao a few years ago to tackle the non-commutative Freiman problem.

They are defined as follows:

Definition (Approximate (sub)groups)

Let G be a group and $K \geqslant 1$ a parameter. A finite subset A of G is said to be a K-approximate group if

- $A = A^{-1}$ (i.e. A is symmetric),
- A contains the identity $1 \in G$, and
- $AA \subset XA$, where X is a subset of G with $|X| \leqslant K$.

In particular, 1-approximate subgroups are precisely ordinary subgroups.

Basic properties of approximate groups

Approximate groups enjoy many nice properties that are often the approximate counterparts to basic group-theoretic properties. For example:

- (Inheritance to subgroups) If $H \leqslant G$ is a subgroup and A is a K-approximate group, then $A^2 \cap H$ is a K^3-approximate group.
- (Inheritance to quotients) If $\pi : G \to Q$ is a homomorphism and A is a K-approximate group, then $\pi(A)$ is a K-approximate group of $\pi(G)$.

In dealing with K-approximate groups, it is often instructive to first consider the limit case $K \to 1$, which reduces to pure group theoretic arguments, and try to then "perturb" these arguments to the approximate setting.

Relation between approximate groups and the non-commutative Freiman problem

Let A be a finite subset of an ambient group G.

Proposition

1. *If* $|AAA| \leqslant K|A|$, *then* $|A^n| \leqslant K^{2n-2}|A|$ *for every* $n \in \mathbb{N}$. *Moreover* $(A \cup A^{-1} \cup 1)^2$ *is a* CK^C*-approximate group.*
2. *If* $|AA| \leqslant K|A|$, *then* A *contains a subset* A_0 *with* $|A_0| \geqslant |A|/CK^C$, *such that* $|A_0A_0A_0| \leqslant DK^D|A_0|$, *where* C, D *are absolute constants.*

Consequence : in the non-commutative Freiman problem, we may assume that A is an approximate group.

What comes in the proof of this proposition ?
In item 1) one makes use of a remarkable combinatorial tool : the Ruzsa distance on finite subsets of a group:

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

it satisfies the triangle inequality !

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

Item 2) is an instance of an important combinatorial result called the Balog-Szemeredi-Gowers-Tao lemma.

Helfgott-Lindenstrauss conjecture

The following may be considered the most optimistic answer to the non-commutative Freiman problem:

Conjecture

Given $K \geqslant 1$, there are $K_1, K_2 \geqslant 1$ such that any K-approximate subgroup A (in any group) is contained in at most K_1 cosets of a HL-set of size $|HL| \leqslant K_2|A|$ and nilpotency class and rank $\leqslant K_2$.

What is an HL-set ?
A set of the form $H \cdot L$, where H is a finite subgroup of the ambient group G, and L a finite subset of G lying in the normalizer $N_G(H)$ such that $H \backslash HL$ is a *nilprogression* of rank at most K_2 and step at most K_2 (in particular, it generates a nilpotent group of nilpotency class at most K_2 and with at most K_2-generators).

Hrushovski's theorems

A year ago, Udi Hrushovski released a remarkable paper.

He used model-theoretic tools to tackle the non-commutative Freiman problem and the above conjecture.

Hrushovski's theorems

We now briefly describe some of his methods and results. Fix $K \geqslant 1$.
Let G_n a sequence of groups and A_n be a sequence of K-approximate subgroups of G_n.
One may form the ultraproduct $\hat{G} := \prod_{\mathcal{U}} G_n$ and $\hat{A} := \prod_{\mathcal{U}} A_n$.
Then $\hat{G}$ is a group and $\hat{A}$ is still a K-approximate group (though $\hat{A}$ can be infinite).
Using model theory, Hrushovski was able to construct a certain subgroup H of $\hat{G}$ such that:

- $H \subset \hat{A}^4$,
- H is normal in $\langle \hat{A} \rangle$.
- $\langle \hat{A} \rangle / H$ is endowed with a natural *topology* ; this topology is *locally compact*.

Hrushovski's theorems

Hrushovski then applies to $\langle \hat{A} \rangle / H$ the Gleason-Montgomery-Zippin results on the structure of locally compact groups (Hilbert's 5th problem) to deduce the following results.

Theorem (Hrushovski 1)

Given $K \geqslant 1$ there is $K_1 \geqslant 1$ such that for any K-approximate group A (in any group), there is $X_1 \subset A^4$ such that $|X_1| \geqslant |A|/K_2$ and $[X_1, X_1] \subset X_1$.

In fact Hrushovski finds an arbitrarily long nested sequence $X_n \subset X_{n-1} \subset .... \subset X_1 \subset A^4$, with $X_i^2 \subset X_{i-1}$ and $[X_i, X_j] \subset X_{\max\{i,j\}+1}$ and $|X_i| \gg_n |X_{i-1}|/K_1$.
These X_i can be interpreted as "non-commutative Bohr-sets" as they are the "pull-backs" to A of a base of neighborhoods of the identity in the locally compact group $\langle \hat{A} \rangle / H$.

Hrushovski's theorems

Applying this machine to the case when $G_n = \mathbf{G}(k_n)$ is an algebraic group over a field k_n, Hrushovski gets the following complete answer to the HL conjecture in the case of simple algebraic groups.

Theorem (Hrushovski 2)

Let $d \geqslant 1$. There is a function $f : \mathbb{R}_+ \to \mathbb{R}_+$ with $\lim_{x \to +\infty} f(x) = +\infty$ such that if $\mathbf{G}$ is an almost simple algebraic group of dimension $\leqslant d$ over a field k. Then for any subset A of $\mathbf{G}(k)$:

- *either A is contained in a proper algebraic subgroup $\mathbf{H}$ of $\mathbf{G}$ with at most $C(d)$-connected components,*
- *or $|AAA| \geqslant \min\{|\langle A \rangle|, |A| f(|A|)\}$*

Using this Hrushovski also obtains a complete proof of the HL conjecture for approximate subgroups of $GL_d(\mathbb{C})$ (fixed d).

Hrushovski's theorems

Using a similar conjugation trick as Gromov did in his celebrated polynomial growth theorem, Hrushovski gets:

Theorem (Hrushovski 3, generalization of Gromov's theorem)

Let $K \geqslant 1$ and let Γ be a finitely generated group and let A_n be an increasing sequence of finite subsets with $\bigcup A_n = \Gamma$ and $|A_n A_n| \leqslant K|A_n|$. Then Γ is virtually nilpotent.

Helfgott type product theorems

In joint work with Green and Tao, we found a different proof of Hrushovski 2, giving an effective *polynomial* bound on f, i.e. $f(x) = x^{\epsilon}$, for some $\epsilon > 0$. Namely:

Theorem (Breuillard-Green-Tao I)

Let $\mathbf{G}$ *be an almost simple algebraic group of dimension at most* d *over an algebraically closed field* k*. Then for any subset* A *of* $\mathbf{G}(k)$*:*

- *either* A *is contained in a proper algebraic subgroup* $\mathbf{H}$ *of* $\mathbf{G}$ *with at most* $C(d)$*-connected components,*
- *or* $|AAA| \geqslant \min\{|\langle A\rangle|, |A|^{1+\epsilon}\}$*,*

where $\epsilon > 0$ *depends only on* d*.*

Additionally, we obtain a complete proof of the HL conjecture for approximate subgroups of $\mathrm{GL}_d(\mathbb{C})$ with effective *polynomial* bounds.

Remarks

- This theorem was proved independently by Pyber and Szabo in the case when $k = \overline{\mathbb{F}_p}$, and A is assumed to generate some $\mathbf{G}(\mathbb{F}_q)$ for q some power of a prime p. This is in fact the hardest case.
- The result extends prior work of Helfgott and Gill, which dealt with the special cases of $\mathrm{SL}_2(\mathbb{F}_p)$ and $\mathrm{SL}_3(\mathbb{F}_p)$ and of $\mathrm{SL}_n(\mathbb{F}_p)$ for sets A of small size and p a prime.
- In joint work with Ben Green, we obtained a completely different proof of this result for compact Lie groups, which relies on the geometry of compact Lie groups and a Besicovitch covering argument.

Proofs

The proof consists in making A act on the variety of tori $\mathbf{G}/N(T)$ of G. It splits in three steps:

1. We prove a Larsen-Pink type non-concentration estimate: if $\mathcal{V}$ is an algebraic subvariety of $\mathbf{G}$, and A a K-approximate subgroup of $\mathbf{G}(k)$, then $|\mathcal{V} \cap A| \ll_{\mathcal{V}} K^{C_d} |A|^{\frac{\dim \mathcal{V}}{\dim \mathbf{G}}}$.
2. Applying the above to $\mathcal{V} = T$, for T a maximal torus of $\mathbf{G}$, and $\mathcal{V} = \mathrm{Conj}(a)$ a conjugacy class of a regular element a, we show that the set of maximal tori T such that $A^2 \cap T$ contains a regular element is invariant under conjugation by $\langle A \rangle$.
3. If $|AAA| \ll |A|^{1+\varepsilon}$, this already forces $|A| \gg |\langle A \rangle|^{1-\varepsilon'}$. We use the fact that $\langle A \rangle$ has no non trivial complex linear representation of dimension $< |\langle A \rangle|^{\epsilon''}$ to conclude.

Other known instances of the HL conjecture

In the following cases the HL conjecture is known to hold:

- Free groups (Razborov, Safin) : a much stronger result holds, namely $\forall n \geqslant 1$, $|A^n| \geqslant (|A|/1000)^{[\frac{n}{2}]}$ for every finite subset A not contained in a cyclic subgroup.
- Hyperbolic groups and more generally uniformly non-amenable groups (Breuillard-Green-Tao) : every K-approximate subgroup is contained in at most $O_K(1)$-cosets of an amenable subgroup.
- Quotients of the free Burnside group of exponent m (Hrushovski) : every K-approximate subgroup is contained in $O_{K,m}(1)$-cosets of a finite subgroup.

Applications to expanders: the Bourgain-Gamburd machine

Motivation to get polynomial bounds in Hrushovski's theorem 2 came in fact before Hrushovski's work and was triggered by a 2005 breakthrough paper of Bourgain and Gamburd, which proved the following :

Theorem (Bourgain-Gamburd '05)

Let $\mathbf{G} = \mathrm{SL}_2$. *Let* Γ *be a Zariski-dense subgroup of* $\mathbf{G}(\mathbb{Z})$ *generated by a finite set* S. *Then the family of Cayley graphs* $\mathcal{G}(\mathbf{G}(\mathbb{Z}/p\mathbb{Z}), S_p)$ *is an expanding family (where* $S_p = S \mod p$*).*

Their method was based on a random walk argument on the Cayley graph of the finite group $\mathbf{G}(\mathbb{F}_p)$: the expansion property is equivalent to the fast decay of the probability of return to the identity of the simple random walk.
It was making key use of the above product theorem (i.e. Breuillard-Green-Tao I), which had been discovered and proved by Helfgott for $\mathrm{SL}_2(\mathbb{F}_p)$ in 2005.

Applications to expanders: the Bourgain-Gamburd machine

Given our product theorem (i.e. Breuillard-Green-Tao I), the Bourgain-Gamburd method now gives:

Theorem

The Bourgain-Gamburd theorem holds for all simple Chevalley groups $\mathbf{G}$.

These results were recently generalized by Varju and Salehi-Golsefidy to perfect groups $\mathbf{G}$ and to square-free non prime p.

Applications to expanders: random expansion

A few years ago, Kassabov, Lubotzky and Nikolov showed that the family of all finite simple groups can be turned into a family of expanders (with fixed number of generators) except perhaps for the class of Suzuki groups $\mathbf{Suz}(q)$. (the problem being that Suzuki groups do not contain any $\mathrm{SL}_2(q')$ since their order is not a multiple of 3)

Using our product theorem, we managed to show that $\mathbf{Suz}(q)$ also can be made a family of expanders, in fact:

Theorem (Breuillard-Green-Tao II)

There $\varepsilon > 0$ such that the following holds. Let a, b be chosen at random in the finite simple group $\mathbf{Suz}(q)$ (Suzuki group over $\mathbb{F}_q$). Then with probability tending to 1 as q tends to infinity, the pair a, b generates $\mathbf{Suz}(q)$ and its Cayley graph is an ε-expander.

Applications to expanders: random expansion

Together with Bob Guralnick, we recently extended the previous result to all finite simple groups of Lie type of given rank, namely:

Theorem (Breuillard-Green-Guralnick-Tao)

Given $r \geqslant 1$, there is $\varepsilon_r > 0$ such that the following holds. Let a, b be chosen at random in the finite simple group of Lie type $\mathbf{G}(q)$ of rank r. Then with probability tending to 1 as q tends to infinity, the pair a, b generates $\mathbf{G}(q)$ and its Cayley graph is an ε-expander.

The proof follows the original Bourgain-Gamburd strategy in proving expansion by showing that the probability of return to the identity of the simple random walk on the Cayley graph of $\mathbf{G}(q)$ decays fast (i.e. becomes less that $1/|\mathbf{G}(q)|^{1-\varepsilon}$ in less than $O(\log |\mathbf{G}(q)|)$ steps.
In order to perform this, our product theorem (i.e. Breuillard-Green-Tao I), is used in the later stages, already after $O(\log |\mathbf{G}(q)|)$ steps of the walk.

Applications to expanders: random expansion

The difficulty lies chiefly in the early stages (when the walk begins), and we have to show that the Cayley graph has large girth or at least very few short loops and, more generally, that it does not concentrate on proper subgroups. In order to achieve this, we prove the following result, which is of independent interest.

Theorem (B-G-G-T, Existence of strongly dense free subgroups)

Suppose that $\mathbf{G}(k)$ *is a semisimple algebraic group over an algebraically closed field* k*, and suppose that* k *has transcendence degree at least* $2\dim(\mathbf{G})$ *over the field* k_0 *of definition of* $\mathbf{G}$*. Then there exists a non-abelian free subgroup* Γ *of* $\mathbf{G}(k)$ *on two generators which is strongly dense.*

A free subgroup of an algebraic group is said to be **strongly dense** if all of its subgroups are either trivial, cyclic, or themselves Zariski-dense.

We first prove this for $\mathbf{G} = \mathrm{SL}_d$ and then do a case by case study for each simple group arising from the various root systems.

Thank you!