MINI-COURSE ON APPROXIMATE GROUPS

EMMANUEL BREUILLARD

Abstract. These are notes from a 2-hour minicourse I gave at the hot topics workshop on Super-strong approximation at MSRI, Berkeley, in February 2012

1. Lecture 1, A definition, a problem and some theorems

1.1. **Motivation: why study approximate groups ?** One of the main motivations for the subject of approximate groups and its recent fast development is its connection with super-strong approximation[1] as was first made clear in the 2005 work of Bourgain-Gamburd [2] on $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$.

Super-strong approximation is the topic of this workshop, so I will not attempt here to give the state of the art on this theorem (for this see the talk by Alireza Salehi-Golsefidy and [41]) nor will I talk about the wonderful applications of this theorem as we have already heard about many of them this week. Let me however recall the following typical instance of super-strong approximation: let $\Gamma \leqslant \mathrm{SL}_d(\mathbb{Z})$ be a Zariski dense subgroup. Then strong approximation for Γ says that for every large enough prime number p, the subgroup Γ surjects onto $\mathrm{SL}_d(\mathbb{Z}/p\mathbb{Z})$ (see Rapinchuk's talk and [35, 37]), while *super-strong approximation* asserts that given any fixed generating set S of Γ, the sequence of Cayley graphs $Cay(\mathrm{SL}_d(\mathbb{Z}/p\mathbb{Z}), S \bmod p)$ forms a family of ε-expanders, for some $\varepsilon = \varepsilon(S) > 0$.

Up until 2005, the main tool for constructing such families of expanders was representation theory. This started with Margulis [34] in the 70s and his use of Kazhdan's property (T) to give the first construction of expander graphs, then was continued in the work of Lubotzky-Phillips-Sarnak on Ramanujan graphs [33], and many others later on. This approach applied only to lattices Γ and was essentially based on a transfer principle between the representation theory of $\mathbb{L}^2(G/\Gamma)$ and that of Γ.

A consequence of the expander property is that the simple random walk on Γ, when projected onto the finite quotients, becomes equidistributed very fast, typically in logarithmic time (in the size of the quotient). In the representation theoretic approach, this fast equidistribution follows from the spectral gap. However it is not difficult to prove (see the survey by Hoory-Linial-Wigderson) that the spectral gap is in fact equivalent to the fast equidistribution of the random walk. In 2005 Bourgain-Gamburd [2] reversed

Date: February 14th 2012.

[1] or simply 'super-approximation' as was suggested by Alex Kontorovich at this workshop.

the idea: they proved the fast equidistribution of the random walk by combinatorial methods, then deduced the spectral.

For this, the strategy is to control the random walk on the finite quotients $\mathrm{SL}_d(\mathbb{Z}/p\mathbb{Z})$ in three stages:

(i) For short times (typically $t < c \log p$, $c > 0$ small constant), one needs to show that the random walk *escapes proper subgroups*, i.e. is not too concentrated on any proper subgroup of $\mathrm{SL}_d(\mathbb{Z}/p\mathbb{Z})$.

(ii) For medium times (with $c \log p < t < C \log p$, $c < C$), one shows that the walk *escapes from approximate subgroups*. This is sometimes phrased in terms of probability measures as the "ℓ^2-flattening" lemma.

(iii) For long times one uses *quasi-randomness* (i.e. the Frobenius/Landazuri-Seitz bounds on the dimension of complex linear representations of finite simple groups) to show that the walk covers the whole group very quickly.

The hard parts of this strategy are (1) and (2). In their original paper Bourgain-Gamburd dealt only with $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ whose subgroup structure is very simple, so item (1) in this case was a simple consequence of Kesten's thesis [30] (on the decay of the probability of return to the identity of simple random walks on groups). Currently there are two (related) known methods to deal with (1) in higher rank: to use ping-pong and produce a free subgroup which has small intersection with every proper algebraic subgroup (see Varju [48] and Salehi-Varju [41]), or to use the theory of products of random matrices à la Furstenberg-Guivarc'h (see the further work of Bourgain-Gamburd [4, 3]).

Item (2) is the subject of this mini-course and amounts to understanding approximate subgroups of the finite quotients. This was first done in a famous paper of Helfgott [25] for $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, which then allowed Bourgain-Gamburd to implement their strategy in the SL_2 case. In my second lecture, I will explain how Helfgott's result generalizes to higher rank and sketch a proof of the classification of approximate subgroups of simple algebraic groups over an arbitrary field (finite or not).

1.2. **Approximate groups: the definition.** Given sets A, B in a group G, write $AB = \{ab, a \in A, b \in B\}$ and more generally $A^{n+1} = A^n A$. Also $|A|$ denotes the cardinality of A.

Definition 1.3 (Approximate groups, Tao 2005 [45])**.** *Let $K \geqslant 1$ be a parameter, G be a group and $A \subset G$ a finite subset. We say that A is a K-approximate subgroup of G if*

(i) $1 \in A$,
(ii) *A is symmetric:* $A = A^{-1}$,

(iii) *There is a symmetric set X of size at most K such that $AA \subset XA$.*

Remark. Observe that if $K = 1$, then we recover the definition of a finite subgroup of G. Namely 1-approximate subgroups are just genuine finite subgroups.

This definition arose in a very different context from that of super-approximation. Tao was largely motivated by a different problem, coming from additive number theory and combinatorics, which is known as the:

Freiman inverse problem: Given a group G and a parameter $K \geqslant 1$, describe the "structure" of finite subsets A of G such that $|AA| \leqslant K|A|$.

Sets with $|AA| \leqslant K|A|$ are said to have *doubling at most* K, and the ratio $\frac{|AA|}{|A|}$ is often called the *doubling constant* of A. Note that K-approximate groups are examples of sets with doubling at most K.

Later in the talk, I will state a recent theorem of Green, Tao and myself [11], which provides an answer to Freiman's inverse problem for general groups. For the applications to super-approximation however (i.e. for step (2) of the Bourgain-Gamburd strategy outlined above) this general theorem is not enough, because it provides no explicit bounds in terms of the parameter K. However it treats the general case while for these applications one only cares about approximate subgroups of linear groups (i.e. subgroups of GL_d for some fixed d). In the linear setting one has an entire set of tools and techniques (in particular algebraic geometry) that can be exploited and it turns out that one can indeed give explicit (even polynomial bounds) for the Freiman inverse problem as I will explain in this mini-course.

Many people have contributed to the Freiman inverse problem in recent years in the non-commutative case. To name a few:

- Bourgain-Katz-Tao [6] (2003) proved the *sum-product* theorem for finite fields.
- Helfgott (2005) breakthrough result [25] for $\mathrm{SL}_2(\mathbb{F}_p)$ using the sum-product.
- Tao (2005) transposed to the non-commutative setting most of the apparatus of additive number theory previously used to tackle Freiman's problem in abelian groups and defined approximate groups [45].
- Helfgott for $\mathrm{SL}_3(\mathbb{F}_p)$ [26] then partial results for $\mathrm{SL}_d(\mathbb{F}_p)$ by Gill-Helfgott [17].
- Dinai $\mathrm{SL}_2(\mathbb{F}_q)$ [15].
- Tao : general solvable subgroups with a bounded on the solvability length [46].
- Breuillard-Green [9]: torsion-free nilpotent groups and compact Lie groups.
- Bourgain-Gamburd-Sarnak $\mathrm{SL}_2(\mathbb{Z}/q\mathbb{Z})$ with q square-free integer [5].
- Hrushovski (2009): progress towards the general Freiman inverse problem and the higher rank GL_d case using model theory [27].
- Pyber-Szabo, Breuillard-Green-Tao (2010) generalization of Helfgott's theorem to higher rank simple algebraic groups over arbitrary fields [38, 12].

- Varju (2010) $\mathbf{G}(\mathbb{Z}/q\mathbb{Z})$, q square free [48].
- Bourgain-Varju (2011) [7] handled $\mathrm{SL}_d(\mathbb{Z}/n\mathbb{Z})$ for arbitrary modulus n.
- Salehi-Varju (2011) [41] handled the case $\mathbf{G}$ perfect with square free modulus.
- Gill-Helfgott (2011) [18]: solvable algebraic subgroups over $\mathbb{F}_p$.
- Breuillard-Green-Tao (2011) : general groups with no explicit bounds [11].

1.4. **Some examples of approximate groups.** Having given the definition of approximate groups and stated Freiman's inverse problem, I will now discuss some simple instances of this problem and give some examples of approximate groups.

Remark. Suppose A is a finite set of an ambient group G. Then requiring $|A| = |AA|$ is equivalent to saying that A is a *normalizing coset* of a finite subgroup, namely that $A = aH$ for some $a \in G$ and some finite subgroup H in G such that $aH = Ha$ (a simple exercise).

This remark answers completely Freiman's inverse problem when the doubling constant K equals 1. What if K is slightly bigger than 1 ? Then the following is an old result of Freiman (see Tao's blog or Freiman's recent note about it [16], or [8]).

Proposition 1.5. *(Freiman inverse problem for $K < \frac{3}{2}$) Let A be a finite subset of an ambient group G such that $|AA| < \frac{3}{2}|A|$. Then there exists a finite subgroup H of G and $a \in G$ such that $aH = Ha$ and $A \subset aH$ with $|A| > \frac{2}{3}|H|$. The converse is clear.*

In other words if A has doubling $< \frac{3}{2}$, then A is contained in a coset of a genuine subgroup which is not much larger than A itself. This is certainly an instance of the Freiman problem, because starting only from a small doubling assumption, we have exhibited structure: there is a genuine subgroup that hangs around.

If $K > 3/2$, Freiman's problem is more tricky. However as long as $K < 2$, it will remain the case that doubling at most K implies that A is contained in a bounded number of cosets of a genuine finite subgroup, which is itself not much bigger than A. This is a recent result of Y. Hamidoune [24], which answered a question of Tao.

It is clear that such a thing no longer holds if $K \geqslant 2$, because of the following other well-known example of set of small doubling (besides finite subgroups), namely arithmetic progressions: the subset $A := [-N, N] \subset \mathbb{Z}$ has doubling at most 2.

This brings about the following family of approximate groups:

Example 1.6 (Symmetric generalized arithmetic progressions)**.** *Let $N_1, ..., N_d$ be positive integers and consider the box $B = \prod_1^d [-N_i, N_i] \subset \mathbb{Z}^d$ with side lengths $N_1, ...N_d$. Let $\pi : \mathbb{Z}^d \to G$ be a group homomorphism. Then $A := \pi(B)$ is called a (symmetric) d-dimensional (generalized) arithmetic progression. It is easy to see that A is a 2^d-approximate group and in particular $|AA| \leqslant 2^d|A|$.*
$\diamond$

Generalized arithmetic progressions can be generalized further (!) to the setting of nilpotent groups. Basically any homomorphic image of a "box" in a finitely generated nilpotent group will have small doubling. This leads to the notion of **nilprogression** or nilpotent progression. It was investigated in Breuillard-Green [9] as well as in Tao's paper on solvable groups [46]. There are several natural definitions of nilprogressions which are all roughly equivalent. One can define them as the homomorphic image of a "box" in the free nilpotent group $N_{r,k}(\mathbb{Z})$ of step r and rank k. A natural definition for the "box" can be to take all elements that can be written as a word in the generators $e_1, ..., e_k$ of $N_{r,k}(\mathbb{Z})$ with e_i appearing at most N_i times. Another more geometric possible notion of "box" is to take the integer points in the Lie group $N_{r,k}(\mathbb{R})$ that lie in the ball of radius 1 for the left-invariant Carnot-Caratheodory metric induced on $N_{r,k}(\mathbb{R})$ by the norm $\|(x_1, ..., x_k)\| = \sum \frac{|x_i|}{N_i}$ on the abelianization $\mathbb{R}^k$ of $N_{r,k}(\mathbb{R})$. The two notions lead to two essentially equivalent notions of nilprogressions, see [9, 11, 8].

Let us leave the general case for a moment and say a word about approximate subgroups of $G = \mathbb{Z}$, the infinite cyclic group. In this case, the inverse Freiman problem was solved by Freiman himself in the late 60s. There are no non trivial finite subgroups of $\mathbb{Z}$, so finite groups will not appear. However there are generalized arithmetic progressions. Freiman's theorem [16] says that every approximate subgroup of $\mathbb{Z}$ is roughly equivalent to a generalized arithmetic progression.

Theorem 1.7 (Freiman's theorem)**.** *Let A be a K-approximate subgroup of $\mathbb{Z}$. Then there is a d-dimensional generalized arithmetic progression P and a set X in $\mathbb{Z}$ such that*

(i) $A \subset X + P$
(ii) $|P| \leqslant C|A|$, *with* $C \leqslant O_K(1)$.
(iii) $|X| \leqslant O_K(1)$
(iv) $d \leqslant O_K(1)$

For a proof, see Ben Green's Edinburgh notes [22], or the book by Tao and Vu [47].

In the 90s Ruzsa gave a simplified proof of Freiman's theorem [40], which was improved by Chang [14] and then pushed to all abelian groups by Green and Ruzsa [23]. Ruzsa's proof gave the bounds of the form: $C \leqslant \exp(O(K^{O(1)}))$, $d \leqslant O(K^{O(1)})$ and $|X| \leqslant O(K^{O(1)})$. Note that, given the exponential bound on C, one could ignore the set X altogether by declaring it to be part of the progression P at the expense of increasing slightly the rank d of the progression. However the set X becomes important when one considers the following conjecture:

Conjecture 1.8 (Polynomial Freiman-Ruzsa conjecture)**.** *One can take $C \leqslant O(K^{O(1)})$, while keeping $|X|$ and d of size $O(K^{O(1)})$.*

Recently Tom Sanders gave almost polynomial bounds towards this conjecture (see [42]): he has $d = O(\log^6 K)$, while $C \leqslant K^3$ and $|X| = O(K^{\log^6 K})$.

1.9. **The Balog-Szemeredi-Gowers-Tao lemma: from small doubling to approximate groups.** Tao's definition of a K-approximate subgroup is only one of several natural candidates. The following result says that all these notions are essentially equivalent.

Proposition 1.10 (Balog-Szemeredi-Gowers-Tao)**.** *There is an absolute constant $C > 0$ such that the following conditions on a finite set A in an ambient group G*

(i) $|AA| \leqslant K|A|$
(ii) $|AAA| \leqslant K|A|$
(iii) $|\{(a,b,c,d) \in A \times A \times A \times A | ab = cd\}| \geqslant \frac{|A|^3}{K}$
(iv) $|\{(a,b) \in A \times A | ab \in A\}| \geqslant \frac{|A|^2}{K}$
(v) *A is a K-approximate subgroup of G.*

are roughly equivalent in the sense that if condition (i) holds for A with a constant K, then condition (i') will hold for a set $A' \subset G$ such that $|A \cap A'| \geqslant \frac{1}{CK^C} \max\{|A|, |A'|\}$ with constant $K' \leqslant CK^C$ (where C is an absolute constant).

This proposition was proved by Tao in [45], but it relies[2] on a tricky graph theoretical result of Balog and Szemeredi, which was later improved (yielding the polynomial bound CK^C in the above statement) by Gowers. See the book by Tao-Vu [47] for a proof, or Green's Part III lectures notes.

This proposition also gives a hint at what kind of equivalence between sets one would like to impose when dealing with the Freiman inverse problem and talk about the "structure" of sets of small doubling. For example, passing to a large (say $\geqslant 1/CK^C$) proportion of a set A is allowed and does not significantly alter the structure of A (at least for our purposes).

Tao's approximate groups are easier to handle than the other notions defined in this proposition. In fact it is fair to say that this definition is tailored so as to reduce to a maximum the number of combinatorial arguments in the proofs, so the inverse Freiman problem in a given group G now becomes a more familiar (at least to me) algebraic or geometric problem about the ambient group.

I will now present some of the basic properties of approximate groups. This basic yoga of approximate groups relies of the following guiding principle which will remain our slogan for the remainder of these lectures:

Philosophy: group theoretical arguments (at least those not involving divisibility properties of the order of the group) can often be successfully transfered to approximate groups.

[2]at least for the conditions involving (iii) and (iv); the rough equivalence between (i), (ii) and (v) are easier.

1.11. **Basic properties of approximate groups.** As Tao observed, many combinatorial arguments from additive number theory actually work without modification in the non-commutative setting. This is the case for the celebrated *Ruzsa triangle inequality* which asserts that the *Ruzsa distance*

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

for any finite subsets A, B of an ambient group G satisfies the triangle inequality

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

The proof of the Ruzsa triangle inequality is just a few lines (see the book by Tao and Vu [47]) and is comparatively much easier than the Balog-Szemeredi-Gowers-Tao result stated above. Applying only the Ruzsa triangle inequality one can prove the following (e.g. see [8]):

Lemma 1.12. *Let A be a finite subset of a group G.*

- *If $|A^3| \leqslant K|A|$, then $|A^n| \leqslant K^{2n}|A|$ for all $n \geqslant 1$.*
- *If $|A^3| \leqslant K|A|$, then $B := (A \cup A^{-1} \cup \{1\})^2$ is a $O(K^{O(1)})$-approximate group.*
- *If A is a K-approximate subgroup and B an L-approximate subgroup, then $A^2 \cap B^2$ is a $(KL)^2$-approximate subgroup.*

Beware: small doubling is not enough to guarantee small tripling! If $A = H \cup \{x\}$ for some finite subgroup H and such that $xHx^{-1} \cap H = \{1\}$ (this situation can arise), then $AA = H \cup xH \cup Hx \cup \{x^2\}$ (a set of size at most $3|A|$) while AAA contains HxH, which has size $|H|^2$.

The polynomial bounds in Proposition 1.10 and Lemma 1.12 are crucial for the applications to super-approximation.

Also crucial to the classification of approximate subgroups of simple algebraic groups that we are about to describe is the following approximate version of the orbit-stabilizer lemma for group actions.

Lemma 1.13 (Approximate orbit-stabilizer lemma)**.** *Suppose a group G acts on a set X and let A be a K-approximate subgroup of X. Let $k \geqslant 2$, then*

$$|A| \leqslant |A \cdot x| \cdot |Stab(x) \cap A^k| \leqslant K^{k+1}|A|$$

Observe that this lemma applies in particular to the action by left translations on the coset space G/H for any subgroup H. It follows from the lemma applied to this action that the size of $A^k \cap H$ is roughly (i.e. up to a factor K^k) independent of $k \geqslant 2$. See Pyber's talk, where this feature is exploited a lot: growth in a subgroup implies growth of the set.

Proofs of the two lemmas above can be found in my lecture notes [8] for instance.

1.14. **Classification of approximate groups and the Helfgott-Lindenstrauss conjecture.** We have seen two chief examples of approximate groups: finite subgroups, and generalized arithmetic progressions. We also mentioned that the latter is only a special case of the notion of nilprogression.

Furthermore one can build extensions of approximate groups: if A normalizes a finite subgroup H and A is an approximate subgroup, then AH is again an approximate subgroup. In particular any set of the form HL, where H is a finite subgroup normalized by L and L is a finite subset such that $H\backslash HL$ is a nilprogression is an approximate subgroup. Such HL sets are called *coset nilprogressions*.

The following conjecture and theorem say that every approximate group is roughly equivalent to an HL set as above. The conjecture was formulated by E. Lindenstrauss in a private communication. It is also implicit in Helfgott's $\mathrm{SL}_3(\mathbb{Z}/p\mathbb{Z})$ paper [26], because it coincides with his description of an arbitrary approximate subgroup of $\mathrm{SL}_3(\mathbb{Z}/p\mathbb{Z})$.

Conjecture 1.15 (Helfgott-Lindenstrauss)**.** *Let G be an arbitrary group. Let A be a K-approximate subgroup of G. Then there is a finite subset P of G ("a coset nilprogression") and $X \subset G$ such that*

(i) $A \subset XP$
(ii) $|X| \leqslant O_K(1)$
(iii) $|P| \leqslant O_K(1)|A|$
(iv) *$P = HL$, where H is a finite subgroup of G and L a finite subset lying in the normalizer $N_G(H)$ of H in G such that $H\backslash HL$ generates a nilpotent subgroup of $H\backslash N_G(H)$ with complexity $O_K(1)$ (i.e. number of generators and nilpotency class are $O_K(1)$).*

This conjecture is now a theorem:

Theorem 1.16 (B-Green-Tao, 2011 [11])**.** *The Helfgott-Lindenstrauss conjecture holds. Moreover one can take $P \subset A^4$ and P a coset nilprogression of complexity $O_K(1)$.*

Note that the theorem not only proves the conjecture, but also generalizes Freiman's classification of approximate subgroups of $\mathbb{Z}$ (see Theorem 1.7), because nilprogressions in $\mathbb{Z}$ are just generalized arithmetic progressions. In fact our proof of Theorem 1.16 gives a new proof of Freiman's theorem.

The theorem also gives a strengthening of Gromov's polynomial growth theorem and has several applications to Riemannian geometry and non-negative curvature. Gromov's theorem can be deduced in only a few lines from Theorem 1.16.

The reader interested in the proof of Theorem 1.16 should look at our arXiv preprint [11] and at Tao's blog posts in the past few months. The basic strategy was inspired by a 2009 preprint of Hrushovski [27], which outlines a way to tackle the Freiman inverse problem for general groups using model theory to construct limits of sequences

of approximate groups. In particular Hrushovski showed that every infinite sequence of K-approximate groups (K fixed) yields a certain locally compact group in a certain model theoretic limit. Studying this locally compact group, and in particular applying the Gleason-Montgomery-Zippin-Yamabe structure theorem (Hilbert 5th problem), already gets you a long way towards the above theorem and indeed Hrushovski was also able to improve on Gromov's polynomial growth theorem using these ideas. In [11] we delve into the proof of the Gleason-Montgomery-Zippin-Yamabe structure theorem and manage to transfer some of the group theoretic arguments there to approximate groups in order to exhibit the coset nilprogression P.

The proof of Theorem 1.16 does not give any explicit bounds on the complexity of the coset nilprogression[3] nor on the size of X. This is due to the inherently non explicit nature of the proof, which makes use of ultrafilters to take limits.

In view of the polynomial Freiman-Ruzsa conjecture (see Conjecture 1.8 above) it is reasonable to expect that these bounds can be made polynomial in K.

We will see in the second lecture that this polynomiality of the bounds can be proven for approximate subgroups of GL_d with exponents depending on the dimension d. But can they be made independent of d ? – this was asked in Pyber's lecture. For approximate subgroup of GL_d one can even hope to find a P which is normalized by A (this is what happens in Helfgott $\mathrm{SL}_3(\mathbb{Z}/p\mathbb{Z})$ theorem). One should however bear in mind the following example due to Laci Pyber (see also the end of his preprint with E. Szabo):

Example 1.17. *Let $G = \mathcal{S}_{2n+1}$ be the symmetric group on $2n+1$ objects. Let H be the subgroup generated by all transpositions $(i, i+1)$ for $i = 1, ..., n$. Let σ be the shift $i \mapsto i+2$ mod $2n+1$. Let $A := H \cup \{\sigma^{\pm 1}\}$. Then A is a 10-approximate group which generates G. While it is contained in at most 10 cosets of H, it does not normalize any proper subgroup of G (except A_{2n+1}), because $\mathcal{S}_{2n+1}$ has no non trivial normal subgroup (apart from A_{2n+1}).*

◇

In this example, the approximate group is roughly equivalent to a large finite subgroup which is *almost normalized* by A, but A does not normalize any subgroup (except trivial ones, which are either much smaller of much larger than A).

[3]if one does not require $P \subset A^4$, then our proof does give a $O(\log K)$ bound on the dimension of P.

2. Lecture 2, Approximate subgroups of linear groups: some proofs

2.1. **Quasi-randomness and Gowers trick.** A distinctive feature of finite simple groups (as opposed to abelian groups for instance) is that they have few complex linear representations of small dimension. In fact the smallest dimension $m(G)$ of a non trivial complex linear representation must tend to infinity with the size of the finite simple group G. This fact is a simple consequence of Jordan's theorem on finite subgroups of $\mathrm{GL}_d(\mathbb{C})$ which asserts that every such group must have an abelian normal subgroup of index at most some bound which depends on d only (see e.g. [10] for some historical comments on Jordan's theorem).

This feature has played a very important role in the spectral theory of arithmetic surfaces (see the work of Sarnak-Xue [43]). It also plays an important role in the Bourgain-Gamburd proof of the spectral gap for $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ in the last step of their proof, when one derives the spectral gap from the fast decay of the probability of return to the identity of the random walk at time $C\log p$.

For finite simple groups of Lie type (as opposed to the alternating groups) a very strong lower bound on the dimension of complex linear representations is known. This goes back to Frobenius who showed that $m(\mathrm{PSL}_2(\mathbb{F}_p)) = \frac{p-1}{2}$ and was established in full generality by Landazuri and Seitz [31] in the 70s. Namely:

Fact: There is a constant $c_d > 0$ such that $m(G) \geqslant c_d|G|^{\frac{r}{d}}$ for every finite simple group of Lie type $G = \mathbf{G}(q)$ over a finite field $\mathbb{F}_q$ with dimension $d = \dim \mathbf{G}$ and rank[4] r.

In the early 2000s Tim Gowers [19] exploited this fact in order to answer a combinatorial question of Babai and Sos: does every finite group G have a product free set of size $> c|G|$? A product free set is a subset $X \subset G$ such that $XX \subset G \setminus X$. Gowers shows that answer is no for $\mathrm{PSL}_2(\mathbb{F}_p)$ and for all finite simple groups of Lie type precisely thanks to the above fact about $m(G)$. And indeed this follows directly from the following formulation (due to Nikolov-Pyber [36]) of Gowers' result (take $A = B = X$ and $C = X^{-1}$):

Lemma 2.2 (Gowers' trick)**.** *Suppose A, B, C are subsets of a finite group G such that $|A||B||C| > |G|^3/m(G)$. Then $ABC = G$.*

Gowers' proof (as well as the proof given later by Babai-Nikolov-Pyber [1]) is based on spectral analysis of bi-partite graphs. We give a seemingly different though shorter argument based on the non-abelian Fourier transform.

Proof. Let $f := 1_A * 1_B * 1_C$ be the convolution product of the indicator functions of the three subsets A, B and C. Note that the support of f is precisely the product set ABC. So in order to show that $ABC = G$ it is enough to prove that $f(g) > 0$ for every $g \in G$. To show that, the idea is very simple: expand f in Fourier.

[4]Recall that the rank of G is the dimension of a maximal torus, in particular it is $< d$.

Recall the non-abelian Fourier inversion and Parseval formulas (see Serre's book [44] on representation theory of finite groups for example). Let $d_\pi = \dim(\mathcal{H}_\pi)$ be the dimension of the irreducible representation π of G.

Parseval:

$$\sum_{g\in G} |f(g)|^2 = \frac{1}{|G|}\sum_{\pi} d_\pi \|\pi(f)\|^2$$

Fourier inversion:

$$f(g) = \frac{1}{|G|}\sum_{\pi} d_\pi \langle \pi(f), \pi(g)\rangle$$

where the sum on the right hand side extends over all irreducible complex linear representations of G, and where $\pi(f) = \sum_{g\in G} f(g)\pi(g)$ and the scalar product is defined on $End(\mathcal{H}_\pi)$ by $\langle X, Y\rangle = trace(XY^*)$.

From the Parseval formula stated above applied to 1_C and the bound $d_\pi \geqslant m(G)$ for every non trivial π, we see that $|A| = \frac{1}{|G|}\sum_\pi d_\pi \|\pi(1_A)\|^2$ and thus:

$$\|\pi(1_A)\| \leqslant \sqrt{\frac{|A||G|}{m(G)}} \tag{2.2.1}$$

for every non trivial π.

Now writing the Fourier inversion formula for f and splitting the sum into a main term (corresponding to the trivial representation) and a remainder term (corresponding to all other representations), we get:

$$f(g) \geqslant \frac{|A||B||C|}{|G|} - \frac{1}{|G|}\sum_{\pi\neq 1} d_\pi \|\pi(1_A)\| \cdot \|\pi(1_B)\| \cdot \|\pi(1_C)\|$$

Using (2.2.1) to control $\|\pi(1_A)\|$ and Cauchy-Schwartz inequality together with the Parseval identity to handle $\|\pi(1_B)\|$ and $\|\pi(1_C)\|$, we get:

$$f(g) \geqslant \frac{|A||B||C|}{|G|} - \sqrt{\frac{|A||G|}{m(G)}}\frac{1}{|G|}\sqrt{|G||B|}\cdot\sqrt{|G||C|}$$

which is > 0 as soon as $|A||B||C| > |G|^3/m(G)$ as claimed. □

In relation with approximate groups, Gowers' trick will be used in the following form.

Corollary 2.3. *Let $G = \mathbf{G}(q)$ be a finite simple group of Lie type of dimension $d = \dim \mathbf{G}$ over a finite field $\mathbb{F}_q$. There is $\delta = \delta(d) > 0$ independent of q such that $AAA = G$ for every subset $A \subset G$ such that $|A| > |G|^{1-\delta}$.*

Proof. Combine Gowers' trick with the bound on $m(G)$ mentioned above. □

Gowers calls "*quasi-random*" the finite groups G for which $m(G)$ is large. This terminology comes from the abelian case, where a quasi-random subset, say of $G = (\mathbb{F}_p, +)$, is by definition a subset $A \subset G$ such that $\chi(1_A) = \sum_{a\in A} \chi(a)$ is small compare to $|G|$ for every non trivial character χ of G. Certainly random subsets of G (chosen by flipping independent coins for each element of G) are quasi-random. The bound (2.2.1) shows that if $m(G)$ is large, then every subset of G is quasi-random in the sense that $\|\pi(1_A)\|$ is small compared to $|G|$ for every non trivial irreducible representation π.

2.4. **The sum-product theorem.** The story of approximate groups really began with a 2003 paper of Bourgain-Katz-Tao [6], which proved the following:

Theorem 2.5 (Sum-product in $\mathbb{F}_p$)**.** *Let $\mathbb{F}_p$ be the finite field with p elements (p prime). Then for every $\delta > 0$, there is $\varepsilon > 0$ such that*

$$|SS| + |S + S| \geqslant |S|^{1+\varepsilon}$$

for every subset $S \subset \mathbb{F}_p$ such that $p^\delta < |S| < p^{1-\delta}$.

There are several proofs of this result (see e.g. Tao-Vu [47]), most of them very combinatorial. Konyagin [29] gave a proof which does not require the $|S| > p^\delta$ assumption. We will give a more geometric proof (also not requiring the $|S| > p^\delta$ assumption) later on in this talk. All proofs require (at least some version of) the following lemma due to Katz and Tao (see [47] or [8]):

Lemma 2.6 (Katz-Tao lemma)**.** *For every $n \geqslant 1$ there is an absolute constant $C > 0$ such that for every $K \geqslant 1$ and for any set $S \subset \mathbb{F}_p$ with $|S + S| + |SS| \leqslant K|S|$, there is $\lambda \in \mathbb{F}_p^*$ and a subset $S' \subset \lambda S$ with $|S'| \geqslant |S|/CK^C$ and $|F_n(S')| \leqslant CK^C|S|$, where $F_n(S')$ denotes the set of all elements of $\mathbb{F}_p$ one can obtain from 0 by applying at most n operations (i.e. additions,subtractions, multiplications, divisions) by elements from S' or from the previously constructed elements.*

It turns out that one can recast the sum-product theorem in terms of the Freiman inverse problem, which we discussed in the first lecture. This was first observed by Helfgott in his SL_3 paper [26]. Consider the group of affine transformations of the $\mathbb{F}_p$-line, namely $\mathbb{F}_p \rtimes \mathbb{F}_p^\times$ viewed as a matrix group as

$$\{\begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix} \mid \alpha \in \mathbb{F}_p^\times, \beta \in \mathbb{F}_p\}$$

and inside this group consider the subset

$$B := \{\begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix} \mid \alpha \in S', \beta \in S'\}$$

where S' is the subset obtained from the Katz-Tao lemma (applied with $n = 4$ say). Then B satisfies

$$|BBB| \leqslant CK^C|B|$$

for some absolute constant C. So in view of Lemma 1.12 the subset $A := (B \cup B^{-1} \cup \{\mathrm{id}\})^2$ is a $O(K^{O(1)})$-approximate subgroup of the affine group. So if we knew the solution to Freiman's inverse problem for the affine group, namely a complete description (with polynomial bounds) of its approximate subgroups, then we would derive the sum-product theorem as a corollary. We will pursue this strategy to the end in the second part of the talk, but before that I would like to describe the answer to Freiman's inverse problem inside simple algebraic groups.

2.7. **The product theorem.** In his seminal 2005 paper [25], Helfgott established the following theorem

Theorem 2.8 (Helfgott's product theorem)**.** *For every $\delta > 0$ there is $\varepsilon > 0$ such that*

$$|SSS| \geqslant |S|^{1+\varepsilon}$$

for every finite generating subset of $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ such that $|S| < |\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})|^{1-\delta}$.

Approximate groups are not mentioned in this statement. The bridge between product theorems and results about the classification of approximate groups is clear however: if one has $|SSS| \leqslant |S|^{1+\varepsilon}$, then S has tripling at most K, where $K = |S|^{\varepsilon}$, and thus by Lemma 1.12 $A := (S \cup S^{-1} \cup \{\mathrm{id}\})^2$ is CK^C-approximate group. So Helfgott's theorem can be rephrased by saying that: *there are no non-trivial approximate subgroups of* $\mathrm{SL}_2(\mathbb{F}_p)$.

Helfgott's proof was based on the Bourgain-Katz-Tao sum-product theorem and explicit 2×2 matrix calculations. It appeared clearly from the proof however that a key role was played by large subsets of simultaneously diagonalizable matrices in S. This idea was further exploited in Helfgott's SL_3 paper [26].

After Helfgott's results (and also his partial results with Gill [17] on $\mathrm{SL}_n(\mathbb{Z}/p\mathbb{Z})$) it became highly plausible that a product theorem should hold in full generality for subsets of arbitrary simple algebraic groups (such as SL_d) over an arbitrary field. Moreover a proof of such a theorem should be geometric and exploit the underlying algebraic geometry of simple algebraic groups and in particular the geometry of maximal tori.

The breakthrough came with Hrushovski's 2009 preprint on "Stable groups theory and approximate subgroups" (see [27]) in which he made use of model theoretic tools to give an essentially complete classification of approximate subgroups of simple algebraic groups, albeit with no explicit bounds. One of his statements is the following:

Theorem 2.9 (Hrushovski 2009)**.** *Let $\mathbf{G}$ be a simple algebraic group over an algebraically closed field k with $\dim \mathbf{G} = d$. Let $A \subset \mathbf{G}(k)$ be a K-approximate subgroup of $\mathbf{G}(k)$. Then there exists a closed algebraic subgroup $\mathbb{H}$ of $\mathbf{G}$ such that A intersects at most $f(d, K)$ cosets of $\mathbb{H}(k)$ and*

(i) *either $\mathbb{H}$ is a proper algebraic group of $\mathbf{G}$ with at most $C = C(d)$ connected components,*

(ii) *or* A^4 *contains* $\mathbb{H}(k)$.

where $f(d,K)$ *is a number depending only on* d *and* K.

Hrushovski's interest in approximate groups was triggered by his observation of the similarity between the Freiman inverse problem and some model theoretic results, such as the Zilber stabilizer lemma, in stable group theory. His proof however (as often in model theory) gave no explicit bounds on the function $f(d,K)$ above in terms of d and K.

A few months after Hrushovski's paper appeared on the archive however Pyber-Szabo [39, 38] and independently Green-Tao and myself [13, 12] managed to give a polynomial bound on $f(K,d)$ and to improve Hrushovski's conclusion slightly as follows:

Theorem 2.10 (Classification of approximate subgroups of $\mathbf{G}(k)$, PS / BGT 2010)**.** *There is a constant* $f(d,K) \leqslant O_d(K^{O_d(1)})$ *such that for every simple algebraic group* $\mathbf{G}$ *with dimension* $d = \dim \mathbf{G}$ *which is defined over an algebraically closed field* k *and every* K*-approximate subgroup* $A \subset \mathbf{G}(k)$

(i) *either there exists a proper closed algebraic subgroup with at most* $C(d)$ *connected components such that* $A \subset \mathbb{H}(k)$
(ii) *or* $|A| \leqslant f(d,K)$
(iii) *or* $|A| \geqslant |\langle A\rangle|/f(d,K)$.

I will sketch a proof of that theorem later in the talk. An explicit bound on the implied constants in $f(d,K)$ is obtainable in principle from the proof (especially the version given by Pyber-Szabo), although it has not been worked out, mostly because tracking the constants throughout the proof would most likely not yield very sharp bounds.

It follows from the theorem that if conclusions (i) and (ii) fail, then A generates a finite subgroup. In view of that theorem of Jordan on finite linear groups in characteristic zero which we already mentioned, this implies that k is of positive characteristic. Now a deep result of Larsen and Pink [32] implies that $\langle A\rangle$ is then essentially (up to some bounded index issues) a finite simple group of Lie type. In particular the Landazuri-Seitz bound on the dimension of complex linear representations holds and Gowers' trick kicks in.

One can then easily derive the following generalization of Helfgott's product theorem.

Corollary 2.11 (The product theorem)**.** *Let* $\mathbf{G}$ *be a simple algebraic group over an algebraically closed field* k *with dimension* $d = \dim \mathbf{G}$*. There is a constant* $\varepsilon = \varepsilon(d) > 0$ *such that for every finite subset* $S \subset \mathbf{G}(k)$*,*

(i) *either* S *is contained in a proper algebraic subgroup with at most* C *connected components.*
(ii) *or*

$$|S^N| \geqslant \min\{|\langle S\rangle|, |S|^{1+\varepsilon}\}$$

where $N = N(d)$ and $C = C(d)$ are constants.

One can take $N(d) \leqslant \max\{3, |Z|\}$, where $|Z|$ is the size of the center of the simply connected cover of $\mathbf{G}$.

Sketched proof. Take $k = \overline{\mathbb{F}_p}$, set $K = |S|^\varepsilon$ and apply Theorem 2.10 to $A := (S \cup S^{-1} \cup \{\mathrm{id}\})^2$, which is a $O(K^{O(1)})$-approximate group. Then, thanks to the polynomial bound on $f(d, K)$ obtained in Theorem 2.10, item (ii) in that theorem cannot hold if ε is chosen small enough. So if (i) does not either, it must be that (iii) holds. Then $\langle A\rangle$ is finite and k has positive characteristic (because the negation of (i) is incompatible with Jordan's theorem in characteristic zero). Larsen-Pink then tell us that $\langle A\rangle$ is (after taking the commutator subgroup and moding out by the center) a finite simple group of Lie type. If ε is small enough, we can apply Gowers' trick (see Corollary 2.3 above) to $[\langle A\rangle, \langle A\rangle]$/center and the result follows. □

Finite simple groups of Lie type[5] are of form $G = \mathbf{G}(\mathbb{F}_q)$/center for some absolutely almost simple (simply connected) algebraic group $\mathbf{G}$ defined over $\mathbb{F}_q$. It can be shown that they (rather their lift to $\mathbf{G}$) are not contained in a proper algebraic group of $\mathbf{G}$ with boundedly many connected components. Moreover finite simple groups are quasi-random in the sense of Gowers (cf. the result of Landazuri-Seitz mentioned above) and Gowers' trick applies to large subsets of G. The product theorem then takes the following simple form for generating sets of finite simple groups of Lie type.

Corollary 2.12 (Product theorem for finite simple groups of Lie type)**.** *Let $G = \mathbf{G}(q)$ be a finite simple group of Lie type over a finite field $\mathbb{F}_q$ with $d = \dim \mathbf{G}$. Let A be any generating set for G. Then*

$$|SSS| \geqslant \min\{|G|, |S|^{1+\varepsilon}\}$$

for some constant $\varepsilon = \varepsilon(d) > 0$.

I am now going to talk about the proof of Theorem 2.10. I will give an essentially complete proof, modulo the Larsen-Pink inequality for which I will refer to our original paper. Before doing so, I want to give a geometric proof of the sum-product theorem (Theorem 2.5), because we will see that this geometric proof can easily be transformed into a proof of Theorem 2.10.

2.13. **A geometric proof of the sum-product theorem.** In this paragraph I give a proof of Theorem 2.5. I keep the notation of that theorem and of the discussion following it. In particular $G = \mathbb{F}_p \rtimes \mathbb{F}_p^\times$ is the group of affine transformations of the line over the finite field $\mathbb{F}_p$. In matrix notation

$$G = \{\begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix} \mid \alpha \in \mathbb{F}_p^\times, \beta \in \mathbb{F}_p\}$$

This group admits two remarkable actions:

[5]except the Suzuki and Ree families, which arise slightly differently and can also be handled similarly.

(a) its action on itself by conjugation $g^h := hgh^{-1}$,

(b) its action on the affine line $\mathbb{F}_p$ by affine transformations $g \cdot x := \alpha x + \beta$.

In case (b) the stabilizers of a point $x \in \mathbb{F}_p$ are the *tori* T_x made of all homotheties fixing the point x. In case (a) the stabilizers are centralizer subgroups. Note that if g is a non trivial homothety (i.e. fixes a point x and is not the identity), then its centralizer $C_G(g)$ is precisely the torus T_x. Finally note that $gT_xg^{-1} = T_{g\cdot x}$.

The sum-product theorem is a consequence of the tension between these two actions. The proof relies on the orbit-stabilizer lemma for approximate groups (i.e. Lemma 1.13) applied to both actions. The approximate group in consideration is obtained from the set S in the way that was described earlier, namely $A := (B \cup B^{-1} \cup \{\mathrm{id}\})^2$, where B is the set:

$$B := \{\begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix} \mid \alpha \in S', \beta \in S'\}$$

and S' is the subset obtained from the Katz-Tao lemma applied with $n = 6$ say and with $K = |S|^\varepsilon$ for some small ε to be determined later. Then B satisfies $|BBB| \leqslant CK^C|B|$ and by Lemma 1.12 A is a $O(K^{O(1)})$-approximate subgroup of G. Moreover $|S'| = |B|^{\frac{1}{2}} \geqslant |S|/O(K^{O(1)})$.

Let us apply the orbit-stabiliser lemma two both actions:

Action (a) : suppose $g \in A^2 \cap T_x$ for some $x \in \mathbb{F}_p$ and $g \neq 1$, then computing the matrix g^h for $h \in A$, we see that $|g^A| \leqslant O(K^{O(1)})|S|$ because (cf. Katz-Tao lemma) the translation part of that matrix is an algebraic expression of small length involving only elements from S'. From the orbit-stabilizer lemma, we conclude:

$$|A^2 \cap T_x| \geqslant \frac{|S|}{O(K^{O(1)})}$$

Action (b) : we clearly have $|A \cdot x| \geqslant |S'| \geqslant \frac{|S|}{O(K^{O(1)})}$ for every $x \in \mathbb{F}_p$, for example because A contains many translations. From the orbit-stabilizer lemma applied to this action, we conclude:

$$|A^2 \cap T_x| \leqslant O(K^{O(1)})|S|.$$

Conclusion: For every $x \in \mathbb{F}_p$, if $A^2 \cap T_x \neq \{1\}$, then $|A^2 \cap T_x| \asymp_K |S|$,

where I have used the following shorthand $|A_1| \asymp_K |A_2|$ if $|A_1| \geqslant |A_2|/O(K^{O(1)})$ and vice-versa.

This is where the miracle happens: if $A^2 \cap T_x$ has one non trivial element, then it has many! Everything will follow easily from this. Let $\mathcal{T}$ be the set of tori T_x which intersect A^2 non trivially (the so-called "involved tori" in the terminology of [13]). We have:

Key claim: If $|S'| \geqslant CK^C$ for some absolute constant C, then $\mathcal{T}$ is invariant under conjugation by A (and hence by the subgroup $\langle A \rangle$ generated by A).

Proof. Recall again the orbit stabilizer lemma (Lemma 1.13) and its extra feature that $|A^k \cap Stab(x)|$ is roughly of the same size as $|A^2 \cap Stab(x)|$ for any given $k \geqslant 2$. So we may write:

$$|A^2 \cap aT_x a^{-1}| = |a^{-1}A^2 a \cap T_x| \asymp_K |a^{-1}A^4 a \cap T_x| \geqslant |A^2 \cap T_x|$$

If the $T_x \in \mathcal{T}$, then the right handside is large. Hence the left handside too is large, and is in particular > 1, so $aT_x a^{-1} \in \mathcal{T}$ as claimed. □

Note from the way we defined A that A contains a non trivial translation (e.g. of the form $b_1^{-1}b_2$, where b_1 and b_2 have the same top-left matrix entry). Since p is prime, $\mathbb{Z}/p\mathbb{Z}$ has no non-trivial proper subgroup and it follows that $\langle A \rangle$ contains all translations. Therefore every torus T_x belongs to $\mathcal{T}$, and $|\mathcal{T}| = p$.

To finish the proof it only remains to count A^2 by slicing it into different tori. Since tori are disjoint (except for the fact that they all contain the identity), we may write

$$\bigcup_{T_x \in \mathcal{T}} (A^2 \cap T_x \setminus \{1\}) \subset A^2,$$

thus

$$|\mathcal{T}| \frac{|S|}{O(K^{O(1)})} \leqslant \sum_{T_x \in \mathcal{T}} |A^2 \cap T_x \setminus \{1\}| \leqslant |A^2| \leqslant K|A| = O(K^{O(1)})|S|^2$$

hence

$$|S| \geqslant \frac{|\mathcal{T}|}{O(K^{O(1)})} = \frac{p}{O(K^{O(1)})}$$

Thus (remember that $K = |S|^{\varepsilon}$) choosing ε small enough ($\varepsilon \leqslant \frac{\delta}{O(1)}$ will do) we obtain $|S| > p^{1-\delta}$ as claimed.

2.14. **A proof of the product-theorem and the Larsen-Pink inequality.** The proof of the product theorem (in the form of the classification theorem for approximate subgroups, i.e. Theorem 2.10) follows exactly the same path as the above geometric proof of the sum product theorem. There will be here also two different actions of the group and the tension between these two actions, via the orbit-stabilizer lemma for approximate groups (Lemma 1.13), will yield the proof.

It turns out that in order to implement this strategy, one needs one further ingredient, which was already present in a crucial way in Hrushovski's proof of Theorem 2.9 (although used differently). This is the celebrated Larsen-Pink dimension inequality, which was devised by Larsen and Pink in their 1995 preprint on finite subgroups of linear groups (the same work which we already cited and has now appeared as [32]) and then subsequently investigated in the model theoretic framework by Hrushovski and Wagner in this article [28].

Theorem 2.15 (Larsen-Pink inequality)**.** *Let* $\mathbf{G}$ *be a simple algebraic group over an algebraically closed field* k*. Let* $M \geqslant 1$*. Let* A *be a* K*-approximate subgroup of* $\mathbf{G}(k)$ *and suppose that* A *is not contained in a proper algebraic subgroup of* $\mathbf{G}$ *with at most* M *connected components. Then for every closed algebraic subvariety* $\mathcal{V}$ *of* $\mathbf{G}$ *with degree at most* M*,*

$$|A \cap \mathcal{V}| \leqslant O(K^{O(1)})|A|^{\frac{\dim \mathcal{V}}{\dim \mathbf{G}}}$$

where the implied constants depend on M *and* $\dim \mathbf{G}$ *only.*

Larsen and Pink proved this inequality in [32] in the case when A is a genuine finite subgroup of $\mathbf{G}(k)$. Hrushovski and Wagner [28] then gave a model theoretic proof (as well as a vast generalization) and Hrushovski [27] used this generalized version in his proof of Theorem 2.9. In turns out that the proof in the approximate group case is no more difficult than in the group case and this is a very good example where the philosophy of transfering group theoretical arguments to the approximate group setting is particularly successful.

A word on the proof. There are at least two cases where the inequality is obvious: when $\dim \mathcal{V} = 0$, because then $\mathcal{V}$ is finite and its degree is its number of elements; and when $\dim \mathcal{V} = \dim \mathbf{G}$, obviously. Now the proof proceeds by a double induction on the dimension of $\dim \mathcal{V}$. Starting with two possible counter-examples, one of smallest possible dimension $\mathcal{V}_-$ and one of largest possible dimension $\mathcal{V}_+$ one uses the assumption on A (that A is "sufficiently Zariski-dense", or "sufficiently general" in the Larsen-Pink terminology) and the simplicity of $\mathbf{G}$ to deduce that there is $a \in A^k$, where k depends only on the degree bound, such that $\mathcal{V}_- a \mathcal{V}_+$ has dimension $\dim \mathcal{V}_+ + 1$ at least. Indeed assuming as we may that $\mathcal{V}_-$ and $\mathcal{V}_+$ are irreducible, an equality between the dimensions $\dim \mathcal{V}_- a \mathcal{V}_+ = \dim \mathcal{V}_+$ for all $a \in A^k$ would imply that A^k is contained in the proper (because $\mathbf{G}$ is simple) subvariety of bounded degree $\{g \in \mathbf{G}(k) \mid g^{-1} {\mathcal{V}_-}^{-1} \mathcal{V}_- g \subset Stab(\mathcal{V}_+)\}$, where $Stab(\mathcal{V}_+)$ is the subgroup $\{g \in \mathbf{G}(k) | g\mathcal{V}_+ = \mathcal{V}_+\}$. Then one can use the induction hypothesis on $\mathcal{V}_- a \mathcal{V}_+$ to deduce a contradiction (it will have too many points in A^{k+2}).

In the proof of the product theorem Theorem 2.15 will be applied to only three kinds of subvarieties $\mathcal{V}$, all of them of bounded degree (maximal tori and their normalizers, conjugacy classes of regular semisimple elements, and the set of non-regular semisimple elements).

We now move on to the proof of Theorem 2.10, which as we already said, is just a matter of adapting the above geometric proof of the sum-product theorem. At this point I only have to point out the words that need to be changed in order to turn the above into a proof of Theorem 2.10. At the blackboard this was very easy to do by simply erasing and replacing a couple of words here and there with a colored chalk. I cannot do this in these notes, so let me briefly describe what remains to be done.

The group now is $G = \mathbf{G}(k)$ and as above we consider two actions of this group:

(a) the action of G on itself by conjugation, $g^h := hgh^{-1}$

(b) the action of G on the variety of maximal tori $G/N_G(T)$, $g \cdot T := gTg^{-1}$.

Recall that maximal tori in G (i.e. maximal connected subgroups made of semisimple elements) are all conjugate to each other (k is algebraically closed), so the stabilizer of a maximal torus T in action (b) equals its normalizer $N_G(T)$. Moreover recall that $N_G(T)/T$ is finite (the Weyl group) and independent of k.

Now the stabilizers of action (a) are the centralizers of elements. Elements $g \in G$ such that the (connected component of the) centralizer of $g \in G$ is a maximal torus are called *regular semisimple* (e.g. the elements with distinct eigenvalues in case $\mathbf{G} = \mathrm{SL}_n$). They form a Zariski-open subset of G as well as of every maximal torus T (in a maximal torus non regular semisimple elements are contained in a union of boundedly many proper subtori, the *root tori*). So here, in order to define a notion of involved torus T, we need to require A^2 to intersect T not only non trivially, but in such a way that $A^2 \cap T$ contains a regular element. Denote by T_{reg} the regular semisimple elements of T. Then define

$$\mathcal{T} := \{T \text{ maximal torus } |A^2 \cap T_{reg} \neq \varnothing\}$$

We can now apply the orbit-stabilizer lemma (Lemma 1.13) in combination with the Larsen-Pink inequality to both action (a) and action (b).

Action (a) : suppose $g \in A^2 \cap T_{reg}$. The Larsen-Pink inequality applied to $\mathcal{V} = g^G$ the conjugacy class of g (it is a closed variety of bounded degree and of dimension $\dim \mathbf{G} - \dim T$ because g is regular semisimple) yields $|g^A| \leqslant |A^3 \cap \mathcal{V}| \leqslant O(K^{O(1)})|A|^{1-\frac{\dim T}{\dim \mathbf{G}}}$. So by the orbit-stabilizer lemma, we conclude[6]:

$$|A^2 \cap T| \geqslant \frac{|A|^{\frac{\dim T}{\dim \mathbf{G}}}}{O(K^{O(1)})}$$

[6]Note that $[C_G(g) : C_G(g)^\circ]$ is bounded independently of the regular semisimple element g.

Action (b) : we can apply directly the Larsen-Pink inequality to the variety $\mathcal{V} = T$ and conclude that:

$$|A^2 \cap T| \leqslant O(K^{O(1)})|A|^{\frac{\dim T}{\dim \mathbf{G}}}.$$

Since non-regular elements form a proper Zariski closed subset of bounded degree, another application of the Larsen-Pink inequality yields $|A^2 \cap (T \setminus T_{reg})| \leqslant O(K^{O(1)})|A|^{\frac{\dim T}{\dim \mathbf{G}}-1}$ and thus:

Conclusion: For every maximal torus T, if $A^2 \cap T_{reg} \neq \varnothing$, then $|A^2 \cap T_{reg}| \asymp |A|^{\frac{\dim T}{\dim \mathbf{G}}}$.

where as above we have used the shorthand $|A_1| \asymp_K |A_2|$ if $|A_1| \geqslant |A_2|/O(K^{O(1)})$ and vice-versa.

Then precisely the same proof as in the sum-product theorem above yields the analogous

Key claim: If $|A| \geqslant CK^C$ for some absolute constant C, then $\mathcal{T}$ is invariant under conjugation by A (and hence by the subgroup $\langle A \rangle$ generated by A).

Finally the end of the proof is also the same: one can slice A^2 into different maximal tori and write, noting that $T_{reg} \cap T'_{reg} = \varnothing$ for two different tori T and T',

$$\bigcup_{T \in \mathcal{T}} (A^2 \cap T_{reg}) \subset A^2,$$

thus

$$|\mathcal{T}| \frac{|A|^{\frac{\dim T}{\dim \mathbf{G}}}}{O(K^{O(1)})} \leqslant \sum_{T \in \mathcal{T}} |A^2 \cap T_{reg}| \leqslant |A^2| \leqslant K|A|$$

hence

$$|A|^{1-\frac{\dim T}{\dim \mathbf{G}}} \geqslant \frac{|\mathcal{T}|}{O(K^{O(1)})}. \tag{2.15.1}$$

However by the key claim and the orbit-stabilizer lemma (the original one for groups this time!) we have for any $T \in \mathcal{T}$

$$|\mathcal{T}| \geqslant |T^{\langle A \rangle}| = \frac{|\langle A \rangle|}{|\langle A \rangle \cap N_G(T)|}$$

Finally another application of the Larsen-Pink inequality (this time the original one for genuine subgroups) gives $|\langle A \rangle \cap N_G(T)| \leqslant O(K^{O(1)})|\langle A \rangle|^{\frac{\dim T}{\dim \mathbf{G}}}$. So combining this with (2.15.1) we obtain the desired conclusion:

$$|A| \geqslant \frac{|\langle A\rangle|}{O(K^{O(1)})}.$$

This ends the proof of the product theorem.

Acknowledgements. I would like to thank Lior Silberman and Jitendra Bajpai, for sharing with me their notes of my lectures. This helped me a lot in preparing this text.

References

[1] L. Babai, N. Nikolov, L. Pyber, *Product growth and mixing in finite groups*, Proceedings of the Nineteenth Annual ACM-SIAM Symposium on Discrete Algorithms, 248–257, ACM, New York, 2008.
[2] 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.
[3] J. Bourgain, A. Gamburd, *Expansion and random walks in* $\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$ *II, With an appendix by Bourgain*, J. Eur. Math. Soc. (JEMS) 11 (2009), no. 5, 1057–1103.
[4] J. Bourgain, A. Gamburd, *Expansion and random walks in* $\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$ *I*, J. Eur. Math. Soc. (JEMS) 10 (2008), no. 4, 987–1011.
[5] J. Bourgain, A. Gamburd, P. Sarnak, *Affine linear sieve, expanders, and sum-product*, Invent. Math. 179 (2010), no. 3, 559644.
[6] J. Bourgain. N. Katz, T. Tao, *A sum-product estimate for finite fields, and applications*, Geom. Func. Anal. **14** (2004), 27–57.
[7] J. Bourgain, P. Varju, *Expansion on* $\mathrm{SL}_d(\mathbb{Z}/q\mathbb{Z})$*, q arbitrary*, preprint arXiv:1006.3365.
[8] E. Breuillard, *Lectures on Approximate Groups*, downloadable from my webpage.
[9] E. Breuillard and B. Green, *Approximate groups. I: The torsion-free nilpotent case*, J. Inst. Math. Jussieu 10 (2011), no. 1, 3757.
[10] E. Breuillard, *An exposition of Jordan's original proof of his theorem on finite subgroups of* $\mathrm{GL}_n(\mathbb{C})$., preprint available on my webpage.
[11] E. Breuillard, B. Green and T. Tao, *The structure of approximate groups*, preprint arXiv:1110.5008.
[12] E. Breuillard, B. Green and T. Tao, *Approximate subgroups of linear groups*, Geom. Funct. Anal., **21** (2011) 774–819.
[13] E. Breuillard, B. Green, T. Tao, *Linear approximate groups*, Electron. Res. Announc. Math. Sci. 17 (2010), 5767
[14] M. C. Chang, *A polynomial bound in Freimans theorem*, Duke Math. J. 113 (2002), no. 3, 399419.
[15] O. Dinai, *Expansion properties of finite simple groups*, preprint.
[16] G. Freiman, *On finite subsets of non-abelian groups with small doubling*, preprint 2010.
[17] N. Gill and H. Helfgott, *Growth of small generating sets in* $\mathrm{SL}_n(\mathbb{Z}/p\mathbb{Z})$, Int. Math. Res. Not. IMRN (2011), no. 18, 42264251.
[18] N. Gill and H. Helfgott, *Growth in solvable subgroups of* $\mathrm{GL}_r(\mathbb{Z}/p\mathbb{Z})$, preprint arXiv:1008.5264.
[19] W. T. Gowers, *Quasirandom groups*, Combin. Probab. Comput. **17** (2008), no. 3, 363–387
[20] B. J. Green, *Approximate groups and their applications: work of Bourgain, Gamburd, Helfgott and Sarnak*, preprint.
[21] B. J. Green, *What is... an approximate group*, Notices of the AMS.
[22] B. J. Green, *Structure Theory of Set Addition, Notes by B. J. Green*, ICMS Instructional Conference in Combinatorial Aspects of Mathematical Analysis, Edinburgh March 25-April 5 2002, available on the author's webpage.
[23] B. J. Green and I. Ruzsa, *Freiman's theorem in an arbitrary abelian group*, J. Lond. Math. Soc. (2) 75 (2007), no. 1, 163175.
[24] Y. O. Hamidoune, *Two inverse results*, preprint arXiv:1006.5074

[25] H. A. Helfgott, *Growth and generation in* $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, Ann. of Math. (2) 167 (2008), no. 2, 601–623.
[26] H. A. Helfgott, *Growth in* $SL_3(\mathbb{Z}/p\mathbb{Z})$, J. Eur. Math. Soc., **13** No. 3 (2011), 761–851.
[27] E. Hrushovski, *Stable group theory and approximate subgroups*, J. Amer. Math. Soc. 25 (2012), no. 1, 189243, 03C45 (11P70)
[28] E. Hrushovski and F. Wagner, *Counting and dimensions* in Model theory with applications to algebra and analysis, Vol. 2, 161176, London Math. Soc. Lecture Note Ser., 350, Cambridge Univ. Press, (2008).
[29] S. Konyagin, *A sum-product estimate in fields of prime order*, arXiv math.NT/0304217.
[30] H. Kesten, *Symmetric random walks on groups,* Trans. Amer. Math. Soc., **92** (1959), 336–354.
[31] V. Landazuri, G. Seitz, *On the minimal degrees of projective representations of the finite Chevalley groups*, J. Algebra **32** (1974), 418–443
[32] M. Larsen, R. Pink, *Finite subgroups of algebraic groups*, J. Amer. Math. Soc. 24 (2011), no. 4, 11051158.
[33] A. Lubotzky, R. Phillips, and P. Sarnak, *Ramanujan graphs*, in Combinatorica 8 (1988), no. 3, 261277.
[34] G. A. Margulis, *Explicit constructions of expanders*, Problemy Peredaci Informacii, **9** No. 4, (1973), 71–80.
[35] C. R. Matthews, L. N. Vaserstein, B. Weisfeiler, *Congruence properties of Zariski-dense subgroups. I*, Proc. London Math. Soc. (3) **48** (1984), no. 3, 514–532
[36] N. Nikolov, L. Pyber, *Product decomposition of quasirandom groups and a Jordan type theorem*, J. Eur. Math. Soc. (JEMS) 13 (2011), no. 4, 10631077.
[37] M. V. Nori, *On subgroups of* $GL_n(\mathbb{F}_p)$, Invent. math., **88** (1987), 257–275.
[38] L. Pyber, E. Szabó, *Growth in finite simple groups of Lie type of bounded rank*, preprint (2011) arXiv arXiv:1005.1858.
[39] L. Pyber, E. Szabó, *Growth in finite simple groups of Lie type*, preprint (2010) arXiv:1001.4556.
[40] I. Z .Ruzsa, *Generalised arithmetic progressions and sumsets,* Acta. Math. Hungar. **65** (1994), no. 4, 379–388.
[41] A. Salehi-Golsefidy and P. Varju, *Expansion in perfect groups*, preprint arXiv:1108.4900.
[42] T. Sanders, *On the Bogolyubov-Ruzsa lemma*, preprint arXiv:1011.0107.
[43] P. Sarnak and X. X. Xue, *Bounds for multiplicities of automorphic representations*, Duke Math. J., **64** no. 1, (1991), 207–227.
[44] J.P. Serre, *Linear representations of finite groups*, Graduate Texts in Mathematics, Vol. 42. Springer-Verlag, 1977. x+170 pp.
[45] T. Tao, *Product set estimates in noncommutative groups*, Combinatorica **28** (2008), 547–594.
[46] T. Tao, *Freiman's theorem for solvable groups*, preprint.
[47] T. Tao, V. Vu, *Additive Combinatorics*, Cambridge University Press (2006).
[48] P. Varjú, *Expansion in* $SL_d(\mathcal{O}_K/I)$*, I squarefree,* preprint arXiv:1001.3664.

Laboratoire de Mathématiques, Bâtiment 425, Université Paris Sud 11, 91405 Orsay, FRANCE

E-mail address: emmanuel.breuillard@math.u-psud.fr