

A BRIEF INTRODUCTION TO APPROXIMATE GROUPS

EMMANUEL BREUILLARD

1. APPROXIMATE GROUPS AND THEIR CLASSIFICATION

A finite subgroup of a group G is a finite subset stable under product. It is tempting to investigate what happens if we consider finite subsets that are almost stable under products. Are they close to genuine subgroups in some meaningful sense? Before answering this question, we need to make precise what we mean by “almost stable”. The subject of approximate groups first attempts to do just that, and then tackles the more general problem of classifying such objects.

The formal definition of an approximate group given below (see Definition 1.2) was introduced by T. Tao in [53] and was in part motivated by its use in the ground-breaking work of Bourgain and Gamburd [2] on super-strong approximation for Zariski dense subgroups of $\mathrm{SL}(2, \mathbb{Z})$. However the origins of the concept can be traced much earlier and people have been studying approximate groups much before they were even defined. A significant part of additive number theory as it developed in the last fifty years, and in particular the study of sets of integers with small doubling (e.g. Freiman’s theorem, see Theorem 1.9 below), was precisely about understanding abelian approximate groups. Similarly the sum-product phenomenon (see Theorem 2.5), which played a key role in super-strong approximation especially in the early developments of the subject (e.g. in Helfgott’s work [28]), is equivalent to classifying approximate subgroups of the affine group $\{x \mapsto ax + b\}$.

1.1. 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 1.2 (Approximate groups, Tao 2005 [53]). *Let $K \geq 1$ 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*

- (1) $1 \in A$,
- (2) A is symmetric: $A = A^{-1}$,
- (3) 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.

Tao’s definition of a K -approximate subgroup is only one of several natural candidates. The following result says that all these notions are roughly equivalent.

Proposition 1.3 (Balog-Szemerédi-Gowers-Tao). *There is an absolute constant $C > 0$ such that the following conditions on a finite set A in an ambient group G and parameter $K \geq 1$*

- (1) $|AA| \leq K|A|$
- (2) $|AAA| \leq K|A|$

- (3) $|\{(a, b, c, d) \in A \times A \times A \times A | ab = cd\}| \geq \frac{|A|^3}{K}$
 (4) $|\{(a, b) \in A \times A | ab \in A\}| \geq \frac{|A|^2}{K}$
 (5) A is a K -approximate subgroup of G .

are roughly equivalent in the sense that, for every $i, i' = 1, \dots, 4$, if condition (i) holds for A with a constant K , then condition (i') will hold for a set $A' \subset G$ such that $|A \cap A'| \geq \frac{1}{CK^C} \max\{|A|, |A'|\}$ with constant $K' \leq CK^C$ (where C is an absolute constant).

Condition (1) (resp. (2)) is the small doubling (resp. tripling) condition. Conditions (3) and (4) are statistical in nature. The rough equivalence above was proved by Tao in [53], but it relies¹ on a tricky yet extremely useful graph theoretical result of Balog and Szemerédi, which was later improved (yielding the polynomial bound CK^C in the above statement) by Gowers. See the book by Tao-Vu [55] or Green's Part III Cambridge lecture notes for a proof of the Balog-Szemerédi-Gowers lemma.

This proposition also gives a hint at what kind of equivalence between sets one would like to impose when dealing with attempting to *classify* approximate groups. For example, passing to a large (say $\geq 1/CK^C$) proportion of a set A is allowed and does not significantly alter the structure of A (at least for our purposes).

Remark. It is often the case in various mathematical problems that one has to confront approximate versions of some well-known mathematical notion, namely objects that satisfy the usual axioms only most of the time, or perhaps just part of the time. When it happens most of the time, people say that we are in the 99% regime, while if the axioms are satisfied only part of the time, we are in the 1% regime. This distinction makes sense for approximate groups when using the statistical definitions (3) or (4) above. Approximate groups in the 99% regime are easily seen to be very close to genuine subgroups (see Propositions 1.7 below and the remark after it) and much of the subject of approximate groups concentrates on the 1% regime.

Tao's approximate groups are easier to handle than the other notions (1) to (4) defined in this proposition. In fact it is fair to say that Tao's definition is tailored so as to reduce to a maximum the appearance of purely additive combinatorial arguments in the proofs, so that classifying sets satisfying either of the conditions (1) to (4) above in a given group G is reduced to understanding approximate groups in Tao's sense. This usually boils down to more familiar algebraic or geometric problem about the ambient group where combinatorics play a minor role.

1.4. Approximate groups and super-strong approximation. One of the main motivations for the subject of approximate groups and its recent fast development is its connection with super-strong approximation 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 main topic of this volume and is discussed at length in several articles (e.g. see the notes by Sarnak, by Salehi-Golsefidy and by Ellenberg). So I will not attempt here to give a detailed account of it, but let me only recall that if $\Gamma \leq \mathrm{SL}_d(\mathbb{Z})$ is a Zariski dense subgroup, then strong approximation for Γ is the statement that for every large

¹at least for the conditions involving (3) and (4); the rough equivalence between (1), (2) and (5) are easier.

enough prime number p , the subgroup Γ surjects onto $\mathrm{SL}_d(\mathbb{Z}/p\mathbb{Z})$ (see Rapinchuk’s notes in this volume [46] and [40, 42]), while *super-strong approximation* asserts that given any fixed generating set S of Γ , the sequence of Cayley graphs $\mathrm{Cay}(\mathrm{SL}_d(\mathbb{Z}/p\mathbb{Z}), S \bmod p)$ 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 [39] 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 [38], and many others later on. This approach applied only to arithmetic 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 (i.e. the stochastic process one gets by multiplying on the left a generator from S chosen at random uniformly among the generators), when projected onto the finite quotients, becomes equidistributed very fast, typically in logarithmic time (in the size of the quotient). And usually this fast equidistribution is the reason why one wants to prove a spectral gap (cf. the applications to sieving for example). In 2005 Bourgain-Gamburd [2] reversed the idea: they proved the fast equidistribution of the random walk by combinatorial methods, then deduced the spectral gap. Indeed it is not difficult to prove (see the survey by Hoory-Linial-Wigderson [30]) that the spectral gap is in fact equivalent to the fast equidistribution of the random walk.

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:

- (1) 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 $\mathrm{SL}_d(\mathbb{Z}/p\mathbb{Z})$.
- (2) 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.
- (3) 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 in 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 [35] (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 [57] and Salehi-Varju [48]), 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 my note and amounts to understanding approximate subgroups of the finite quotients. This was first done in a famous paper of Helfgott [28] for $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ (see also [29] for $\mathrm{SL}_3(\mathbb{Z}/p\mathbb{Z})$), which then allowed Bourgain-Gamburd to implement their strategy in the SL_2 case. Basically Helfgott's theorem says that there are no approximate subgroups of $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ except for bounded sets and co-bounded sets (i.e. sets forming a significant proportion of the whole group). Hence the random walk at stage (2) cannot remain "stuck" in an approximate group of intermediate size.

The higher rank case and the extension of Helfgott's theorem to arbitrary semisimple algebraic groups over arbitrary finite fields was done later by Pyber-Szabó in [43] and independently by Breuillard-Green-Tao in [14]. See the second part of these notes as well as Pyber and Szabó's contribution to this volume [45] for a detailed account of this story.

1.5. The Freiman inverse problem. While in part motivated by the super-strong approximation result of Bourgain-Gamburd, Tao's definition of an approximate group fitted well within a general line of thought coming from additive number theory and combinatorics, which was guided by the:

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

Sets with $|AA| \leq K|A|$ 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 this note, I will state a recent theorem of Green, Tao and myself [13], which provides an answer to Freiman's inverse problem for general groups. For the applications to super-strong-approximation however (i.e. for step (2) of the Bourgain-Gamburd strategy outlined above) this general theorem is of no use, because it provides no explicit bounds in terms of the parameter K . Nevertheless 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 entirely different set of tools and techniques (in particular algebraic geometry) that can be exploited. And they indeed yield explicit (even polynomial) bounds for the Freiman inverse problem as I will explain in part 2 of these notes.

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) the *sum-product* theorem for finite fields.
- Helfgott (2005) [28] the $\mathrm{SL}_2(\mathbb{F}_p)$ case 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 [53].
- Helfgott : $\mathrm{SL}_3(\mathbb{F}_p)$ [29] then partial results for $\mathrm{SL}_d(\mathbb{F}_p)$ by Gill-Helfgott [20].
- Dinai : $\mathrm{SL}_2(\mathbb{F}_q)$ [17].
- Tao : general solvable groups with bounded solvability length [54].
- Breuillard-Green [9, 10, 11] : polynomial bounds for torsion-free nilpotent groups, solvable linear groups, 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 Freiman inverse problem for arbitrary groups; also for general linear groups (no explicit bounds) using model theory [31].
- Pyber-Szabo, Breuillard-Green-Tao (2010) : extension of Helfgott's theorem to higher rank simple algebraic groups \mathbf{G} over arbitrary fields [43, 14].
- Varju (2010) $\mathbf{G}(\mathbb{Z}/q\mathbb{Z})$, q square free, $\mathbf{G} = \mathrm{SL}_n$. [57].
- Bourgain-Varju (2011) [7] handled $\mathrm{SL}_d(\mathbb{Z}/n\mathbb{Z})$ for arbitrary modulus n .
- Salehi-Varju (2011) [48] $\mathbf{G}(\mathbb{Z}/q\mathbb{Z})$, q square free, \mathbf{G} perfect.
- Gill-Helfgott (2011) [21]: solvable algebraic subgroups over \mathbb{F}_p .
- Breuillard-Green-Tao (2011) : arbitrary groups (but no explicit bounds) [13].
- Tointon (2012) : arbitrary nilpotent groups (with polynomial bounds), see [56].
- Pyber-Szabo (2013?) : general linear groups (with polynomial bounds), see [45].

1.6. Some examples of approximate groups. Having given the definition of approximate groups and stated Freiman's inverse problem, we now discuss some simple instances of this problem and give a number of examples of approximate groups. We begin with a simple observation.

Remark. Suppose A is a finite set of an ambient group G . It is a simple exercise to prove that the requirement that $|A| = |AA|$ 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 $aH = Ha$.

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 [18], or [8]).

Proposition 1.7. (*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.

As an illustrative example, let us give a complete argument showing that if $|AA^{-1}A| \leq (1 + \varepsilon)|A|$ for some $\varepsilon < 1$, then A is close to a (left coset of a) genuine subgroup in the sense that $H := A^{-1}A$ is a genuine subgroup of cardinality at most $(1 + \varepsilon)|A|$. Indeed $H^{-1} = H$ and for every $x, y \in H$, Ax and Ay intersect non trivially, because $\varepsilon < 1$. It follows that $xy^{-1} \in H$. Hence H is stable under multiplication and hence a genuine subgroup. Note finally that $|H| \leq (1 + \varepsilon)|A|$ and $A \subset aH$ for every $a \in A$. The proof of Proposition 1.7 is more involved, but involves similar arguments.

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 [27], which answered a question of Tao (see also Tao's blog for a proof).

It is clear that such a thing no longer holds if $K \geq 2$, because of the following other well-known example of a set with 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 1.8 (Symmetric generalized arithmetic progressions). *Let N_1, \dots, N_d be positive integers and consider the box $B = \prod_1^d [-N_i, N_i] \subset \mathbb{Z}^d$. Let $\pi : \mathbb{Z}^d \rightarrow G$ be a group homomorphism. Then $A := \pi(B)$ is called a (symmetric) d -dimensional (generalized) arithmetic progression. Clearly B is a 2^d -approximate group. It follows that A too is a 2^d -approximate group and in particular $|AA| \leq 2^d|A|$.*

◇

For instance an arithmetic progression of odd length $\{a, a+r, a+2r, \dots, a+2Nr\}$ in \mathbb{Z} is nothing else than a translate of a symmetric generalized arithmetic progression of dimension $d=1$, where $N_1 = N$ and the $\pi(x) = rx$.

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 [54]. 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, \dots, e_k of $N_{r,k}(\mathbb{Z})$ with e_i appearing at most N_i times. Another more way to proceed is to take as our box 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 $\|(x_1, \dots, x_k)\| = \sum \frac{|x_i|}{N_i}$ on the abelianization \mathbb{R}^k of $N_{r,k}(\mathbb{R})$. The two definitions lead to two roughly equivalent notions of nilprogressions. See [9] the appendix to [13] and Tointon’s paper on approximate subgroups of nilpotent groups [56].

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 [19] says that every approximate subgroup of \mathbb{Z} is roughly equivalent to a generalized arithmetic progression.

Theorem 1.9 (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*

- (1) $A \subset X + P$
- (2) $|P| \leq C|A|$, with $C \leq O_K(1)$.
- (3) $|X| \leq O_K(1)$
- (4) $d \leq O_K(1)$

For a proof, see Ben Green’s Edinburgh notes [25], or the book by Tao and Vu [55].

In the 90s Ruzsa gave a simplified proof of Freiman’s theorem [47], which was improved by Chang [16] and then pushed to all abelian groups by Green and Ruzsa [26]. Ruzsa’s proof

gave bounds of the form: $C \leq \exp(O(K^{O(1)}))$, $d \leq O(K^{O(1)})$ and $|X| \leq O(K^{O(1)})$. 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 1.10 (Polynomial Freiman-Ruzsa conjecture). *One can take $C \leq O(K^{O(1)})$, while keeping $|X|$ and d of size $O(K^{O(1)})$.*

Recently Tom Sanders gave almost polynomial bounds towards this conjecture (see [49]): he has $d = O(\log^6 K)$, while $C \leq K^3$ and $|X| = O(K^{\log^6 K})$. See also his excellent recent survey [50], where these bounds are further improved.

1.11. The combinatorial toolbox 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*

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

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

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

The proof of the Ruzsa triangle inequality is just a few lines, which I cannot resist including here. Note first that quite obviously $|AB^{-1}| \geq |A|$ and $|AB^{-1}| \geq |B|$, so that $|AB^{-1}|^2 \geq |A||B|$, yielding $d(A, B) \geq 0$ always. Next consider the map $AC^{-1} \times B \rightarrow AB^{-1} \times BC^{-1}$, which sends (x, b) to $(a_x b^{-1}, bc_x^{-1})$, where we made a choice of $a_x \in A$ and $c_x \in C$ for each $x \in AC^{-1}$. Then quite obviously this map is injective. Hence $|B||AC^{-1}| \leq |AB^{-1}||BC^{-1}|$, which is another way to phrase the triangle inequality $d(A, C) \leq d(A, B) + d(B, C)$. QED.

Clearly the proof of Ruzsa's inequality is comparatively much easier than that of the Balog-Szemerédi-Gowers lemma mentioned 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 and $K \geq 1$ be a parameter,*

- *If $|A^3| \leq K|A|$, then $|A^n| \leq K^{2n}|A|$ for all $n \geq 1$.*
- *If $|A^3| \leq K|A|$, 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: Although the two notions are roughly equivalent in the sense of Proposition 1.3, 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 1.3 and Lemma 1.12 are crucial for the applications to super-strong-approximation and to the classification of approximate subgroups of simple

algebraic groups that we are about to describe. Also crucial 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 G for some $K \geq 1$. For every integer $k \geq 2$, and $x \in X$, we have*

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

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 $k \geq 2$. See Pyber and Szabó's contribution to these proceedings [45], where this feature is exploited with great skill: growth in a subgroup implies growth of the set.

Proofs of the two lemmas above can be found in my lecture notes [8], see also [55, 53, 28]. They form the basic tool-kit of approximate groups. Their use is widespread in the proofs of many classification results regarding approximate groups. They also allow to make many group theoretical arguments (as used in classical group theory; at least those not involving divisibility properties of the order of the group) work in the approximate groups setting. And indeed the following principle will remain our slogan for the remainder of these notes:

Philosophy: group theoretical arguments can often be successfully transferred to approximate groups.

1.14. The 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 $\text{SL}_3(\mathbb{Z}/p\mathbb{Z})$ paper [29], because it coincides with his description of an arbitrary approximate subgroup of $\text{SL}_3(\mathbb{Z}/p\mathbb{Z})$.

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

- (1) $A \subset XP$
- (2) $|X| \leq O_K(1)$
- (3) $|P| \leq O_K(1)|A|$

- (4) $P = HL$, 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 [13]). *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 1.9), 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 paper [13] and at Tao's various blog posts on the matter. The basic strategy was inspired by a 2009 preprint of Hrushovski [31], 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 [13] 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 . For the readers with a taste for model theory, we also recommend Hrushovski's beautiful set of lecture notes [32], where the proof of Theorem 1.16 is presented in full from a model-theoretic viewpoint.

The proof of Theorem 1.16 does not give any explicit bounds on the complexity of the coset nilprogression² 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 1.10 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 only on the dimension d . But can they be made independent of d ? – this was asked in Pyber's lecture at this workshop (see also [45]). For approximate subgroups 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 [43]):

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 $i = 1, \dots, n$. Let σ be the shift $i \mapsto i + 2$*

²if one does not require $P \subset A^4$, then our proof does give a $O(\log K)$ bound on the dimension of P .

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 or much larger than A).

2. APPROXIMATE SUBGROUPS OF LINEAR GROUPS: SOME PROOFS

In the second part of these notes, we give an introduction to the works [14] and [43], which classify approximate subgroups of simple algebraic groups over finite fields. We will give a complete proof save for the Larsen-Pink-type non-concentration estimate (Theorem 2.15 below), whose proof we only briefly sketch as it is rather more involved.

A key tool is the use of quasi-randomness through Gowers' trick, which shows that large subsets of a finite simple group of Lie type grow quickly. We include a proof of that via non-abelian Fourier analysis of finite groups.

We also include a presentation of the sum-product phenomenon and give a geometric proof of it, which is run in parallel with the proof of the classification of approximate subgroups of simple algebraic groups, emphasizing the parentage between the two problems.

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. 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 $c(d)$ which depends on d only. Indeed, since G is simple, any non-trivial linear representation of G must be faithful, hence the abelian normal subgroup must be trivial, and G must have cardinality at most $c(d)$ (see e.g. [12] 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 [51]). 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 [36] in the 70s. Namely:

Fact: There is a constant $c_d > 0$ such that $m(G) \geq c_d |G|^{\frac{r}{d}}$ 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 rank³ r .

³Recall that the rank of G is the dimension of a maximal torus, in particular it is $< d$.

In the early 2000s Tim Gowers [22] 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 (first observed by Nikolov-Pyber in [41]) of Gowers' result (take $A = B = X$ and $C = X^{-1}$ to answer the Babai-Sos question negatively):

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 argument based on the non-abelian Fourier transform.

Recall that the convolution of two functions f_1, f_2 on a finite group G is defined by

$$f_1 * f_2(x) = \sum_{a,b \in G, ab=x} f_1(a)f_2(b).$$

The convolution product is associative so that $(f_1 * f_2) * f_3 = f_1 * (f_2 * f_3)$. For a subset A in G we denote by 1_A the indicator function of A , namely $1_A(x) = 1$ if $x \in A$ and $1_A(x) = 0$ if $x \notin A$.

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.

Recall the non-abelian Fourier inversion and Parseval formulas (see Serre's book [52] 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 $\mathrm{End}(\mathcal{H}_\pi)$ by $\langle X, Y \rangle = \mathrm{trace}(XY^*)$.

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

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

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:

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

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

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

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

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. \square

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 $\varepsilon > 0$ independent of p such that*

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

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 [55]), most of them quite combinatorial. Konyagin [34] 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 note. All proofs require (at least some version of) the following lemma due to Katz and Tao (see [55] or [8]):

Lemma 2.6 (Katz-Tao lemma). *For every $n \geq 1$ there is a constant $C = C(n) > 0$ such that for every $K \geq 1$ and for any set $S \subset \mathbb{F}_p$ with $|S + S| + |SS| \leq K|S|$, there are $\lambda \in \mathbb{F}_p^*$ and a subset $S' \subset \lambda S$ with $|S'| \geq |S|/CK^C$ and $|F_n(S')| \leq CK^C|S|$, 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 [29]. 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

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

and inside this group consider the subset

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

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

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

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, 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 [28], Helfgott established the following theorem

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

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

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 $|SSS| \leq |S|^{1+\varepsilon}$, 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 a CK^C -approximate group. So Helfgott's theorem can be rephrased (somewhat abusively) as 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 [29].

After Helfgott's results (and also his partial results with Gill [20] on $\mathrm{SL}_d(\mathbb{Z}/p\mathbb{Z})$) 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 group theory and approximate subgroups” (see [31]) 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, [31, Theorem 1.3]*) *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 subgroup \mathbb{H} of $\mathbf{G}(k)$ such that A intersects at most $f(d, K)$ cosets of \mathbb{H} and*

- (1) *either \mathbb{H} is a proper connected algebraic subgroup of \mathbf{G} ,*
- (2) *or \mathbb{H} is finite and contained in A^4 .*

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 [44, 43] and independently Green-Tao and myself [15, 14] 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 $\mathbf{G}(k)$). *There are constants $C(d)$ independent of K, k , and $f(d, K) \leq O_d(K^{O_d(1)})$, 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 $A \subset \mathbf{G}(k)$*

- (1) *either there exists a proper closed algebraic subgroup with at most $C(d)$ connected components such that $A \subset \mathbb{H}(k)$*
- (2) *or $|A| \leq f(d, K)$*
- (3) *or $|A| \geq |\langle A \rangle|/f(d, K)$.*

Note that if we are in cases (1) or (2) of Theorem 2.10, then we are in case (1) of Theorem 2.9. While if we are in case (3) of Theorem 2.10, then $\langle A \rangle$ is finite and not much larger than A , a condition which is close to condition (2) in Theorem 2.9, yet not exactly the same (see however Corollary 2.12 below).

I will sketch a proof of Theorem 2.10 further below. An explicit bound on the implied constants $f(d, K)$ and $C(d)$ 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 (1) and (2) fail, then A generates a finite subgroup. In view of Jordan’s lemma 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 [37] 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 $\varepsilon = \varepsilon(d) > 0$, independent of the field k , such that for every finite subset $S \subset \mathbf{G}(k)$,*

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

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

where $N = N(d)$ and $C = C(d)$ are constants independent of the field k .

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

Sketched proof. Set $K = |S|^\varepsilon$ and apply Theorem 2.10 to $A := (S \cup S^{-1} \cup \{\text{id}\})^2$, 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 (2) in that theorem cannot hold if ε is chosen small enough. So if (1) does not hold either, it must be that (3) holds. Then $\langle A \rangle$ is finite and k has positive characteristic (because the negation of (1) is incompatible with Jordan's lemma 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 of bounded rank. If ε is small enough, we can apply Gowers' trick (see Corollary 2.3 above) to $[\langle A \rangle, \langle A \rangle]/\text{center}$ and the result follows. \square

Finite simple groups of Lie type⁴ are of form $G = \mathbf{G}(\mathbb{F}_q)/\text{center}$ 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 S be any generating set for G . Then*

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

for some constant $\varepsilon = \varepsilon(d) > 0$ independent of the field \mathbb{F}_q .

I will now pass to 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 [14]. 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.

⁴except the Suzuki and Ree families, which arise slightly differently and can also be handled similarly.

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

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

This group admits two remarkable actions:

- (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 $A := (B \cup B^{-1} \cup \{\text{id}\})^2$, where B is the set:

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

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 $|BBB| \leq CK^C|B|$ and by Lemma 1.12 A is a $O(K^{O(1)})$ -approximate subgroup of G . Moreover $|S'| = |B|^{\frac{1}{2}} \geq |S|/O(K^{O(1)})$.

Let us apply the orbit-stabiliser lemma (Lemma 1.13) to 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 $|g^A| \leq O(K^{O(1)})|S|$ 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:

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

Action (b) : we clearly have $|A \cdot x| \geq |S'| \geq \frac{|S|}{O(K^{O(1)})}$ 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:

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

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 $|A_1| \geq |A_2|/O(K^{O(1)})$ 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 [15]). We have:

Key claim: If $|S'| \geq CK^C$ 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 $|A^k \cap \text{Stab}(x)|$ is roughly of the same size as $|A^2 \cap \text{Stab}(x)|$ for any given $k \geq 2$. So we may write:

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

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 $aT_xa^{-1} \in \mathcal{T}$ as claimed. \square

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, since $gT_xg^{-1} = T_{g \cdot x}$, 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

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

hence

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

Thus (remember that $K = |S|^\varepsilon$) choosing ε small enough ($\varepsilon \leq \frac{\delta}{O(1)}$ 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. Here too there will be 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 (which has now appeared as [37]) and then subsequently investigated in the model theoretic framework by Hrushovski and Wagner in [33].

Theorem 2.15 (Larsen-Pink inequality). *Let \mathbf{G} be a (connected) simple algebraic group over an algebraically closed field k . Given $M \geq 1$, there is $C = C(M, \dim \mathbf{G}) > 0$ independent of k such that the following holds. If A denotes a finite K -approximate subgroup of $\mathbf{G}(k)$, then either A is contained in some proper algebraic subgroup \mathbf{H} of \mathbf{G} such that $[\mathbf{H}, \mathbf{H}^0] \leq C$, or for every closed algebraic subvariety \mathcal{V} of \mathbf{G} with degree at most M ,*

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

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

When $k = \overline{\mathbb{F}_p}$, which is the case of interest in the applications to approximate groups, if A generates a subgroup of the form $\mathbf{G}(\mathbb{F}_q)$, for some large enough $q = p^n$, then the first possibility that A may be contained in some proper algebraic subgroup with a bounded number of connected components is automatically ruled out.

Larsen and Pink proved this inequality in [37, Theorem 4.2] in the case when A is a genuine finite subgroup of $\mathbf{G}(k)$ (namely when $K = 1$). Hrushovski and Wagner [33] then gave a model theoretic proof as well as a vast generalization, which was subsequently used by Hrushovski [31] in his proof of Theorem 2.9. It 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 transferring 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 \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 $\{g \in \mathbf{G}(k) \mid g^{-1} \mathcal{V}_-^{-1} \mathcal{V}_- g \subset \text{Stab}(\mathcal{V}_+)\}$, where $\text{Stab}(\mathcal{V}_+)$ is the subgroup $\{g \in \mathbf{G}(k) \mid g \mathcal{V}_+ = \mathcal{V}_+\}$. 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 geometric proof of the sum-product theorem that was given above. At this point I only have to point out the words that need to be changed in order to turn it 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 point stabilizers in 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

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

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 subvariety of bounded degree and of dimension $\dim \mathbf{G} - \dim T$ because g is regular semisimple) yields $|g^A| \leq |A^3 \cap \mathcal{V}| \leq O(K^{O(1)})|A|^{1 - \frac{\dim T}{\dim \mathbf{G}}}$. So by the orbit-stabilizer lemma, we conclude⁵:

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

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

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

⁵Note that $[C_G(g) : C_G(g)^\circ]$ is bounded above by a constant depending only on $\dim \mathbf{G}$ and not on g nor k .

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

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

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

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

Key claim: If $|A| \geq CK^C$, for some constant C depending on $\dim \mathbf{G}$ only, 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 $T_{reg} \cap T'_{reg} = \emptyset$ for two different tori T and T' ,

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

thus

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

hence

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

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

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

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

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

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. I am also grateful to Hee Oh and to Nicolas de Saxcé for their careful reading of the manuscript.

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 $SL_2(\mathbb{F}_p)$* , Ann. of Math. **167** (2008), no. 2, 625–642.
- [3] J. Bourgain, A. Gamburd, *Expansion and random walks in $SL_d(\mathbb{Z}/p^n\mathbb{Z})$ 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 $SL_d(\mathbb{Z}/p^n\mathbb{Z})$ 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 $SL_d(\mathbb{Z}/q\mathbb{Z})$, q arbitrary*, preprint arXiv:1006.3365.
- [8] E. Breuillard, *Lectures on Approximate Groups*, see <http://www.math.u-psud.fr/~breuilla>
- [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, B. Green, *Approximate groups II : the solvable linear case*, Quarterly Journal of Math 62(3): 513–521, (2011).
- [11] E. Breuillard, B. Green, *Approximate groups III: the unitary case*, Turkish J. Math. 36 (2012), no. 2, 199–215.
- [12] E. Breuillard, *An exposition of Jordan’s original proof of his theorem on finite subgroups of $GL_n(\mathbb{C})$* , see <http://www.math.u-psud.fr/~breuilla>
- [13] E. Breuillard, B. Green and T. Tao, *The structure of approximate groups*, Publ. Math. IHES **116**, Issue 1, pp 115–221, (2012).
- [14] E. Breuillard, B. Green and T. Tao, *Approximate subgroups of linear groups*, Geom. Funct. Anal., **21** (2011) 774–819.
- [15] E. Breuillard, B. Green, T. Tao, *Linear approximate groups*, Electron. Res. Announc. Math. Sci. 17 (2010), 5767
- [16] M. C. Chang, *A polynomial bound in Freiman’s theorem*, Duke Math. J. 113 (2002), no. 3, 399419.
- [17] O. Dinai, *Expansion properties of finite simple groups*, arXiv:1001.5069, preprint.
- [18] G.A. Freiman, *On finite subsets of non-abelian groups with small doubling*, Proc. Amer. Math. Soc., 140(9), 2997–3002, 2012.
- [19] G. A. Freiman, *Foundations of a structural theory of set addition*, AMS, 1973, Translated from the Russian, Translations of Mathematical Monographs, Vol 37.
- [20] N. Gill and H. Helfgott, *Growth of small generating sets in $SL_n(\mathbb{Z}/p\mathbb{Z})$* , Int. Math. Res. Not. IMRN (2011), no. 18, 42264251.
- [21] N. Gill and H. Helfgott, *Growth in solvable subgroups of $GL_r(\mathbb{Z}/p\mathbb{Z})$* , preprint arXiv:1008.5264.
- [22] W. T. Gowers, *Quasirandom groups*, Combin. Probab. Comput. **17** (2008), no. 3, 363–387
- [23] B. J. Green, *Approximate groups and their applications: work of Bourgain, Gamburd, Helfgott and Sarnak*, preprint.
- [24] B. J. Green, *What is... an approximate group*, Notices of the AMS.
- [25] 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.
- [26] B. J. Green and I. Ruzsa, *Freiman’s theorem in an arbitrary abelian group*, J. Lond. Math. Soc. (2) 75 (2007), no. 1, 163175.
- [27] Y. O. Hamidoune, *Two inverse results*, preprint arXiv:1006.5074
- [28] H. A. Helfgott, *Growth and generation in $SL_2(\mathbb{Z}/p\mathbb{Z})$* , Ann. of Math. (2) 167 (2008), no. 2, 601–623.
- [29] H. A. Helfgott, *Growth in $SL_3(\mathbb{Z}/p\mathbb{Z})$* , J. Eur. Math. Soc., **13** No. 3 (2011), 761–851.
- [30] S. Hoory, N. Linial and A. Wigderson, *Expander graphs and their applications*, Bull. Amer. Math. Soc. (N.S.) **43** (2006), no. 4, 439–561.
- [31] E. Hrushovski, *Stable group theory and approximate subgroups*, J. Amer. Math. Soc. 25 (2012), no. 1, 189243, 03C45 (11P70)

- [32] E. Hrushovski, *Notes on Hilbert's 5th problem and approximate groups*, see <http://www.ma.huji.ac.il/~ehud/>
- [33] 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).
- [34] S. Konyagin, *A sum-product estimate in fields of prime order*, arXiv math.NT/0304217.
- [35] H. Kesten, *Symmetric random walks on groups*, Trans. Amer. Math. Soc., **92** (1959), 336–354.
- [36] V. Landazuri, G. Seitz, *On the minimal degrees of projective representations of the finite Chevalley groups*, J. Algebra **32** (1974), 418–443
- [37] M. Larsen, R. Pink, *Finite subgroups of algebraic groups*, J. Amer. Math. Soc. 24 (2011), no. 4, 11051158.
- [38] A. Lubotzky, R. Phillips, and P. Sarnak, *Ramanujan graphs*, in Combinatorica 8 (1988), no. 3, 261277.
- [39] G. A. Margulis, *Explicit constructions of expanders*, Problemy Peredaci Informacii, **9** No. 4, (1973), 71–80.
- [40] 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
- [41] N. Nikolov, L. Pyber, *Product decomposition of quasirandom groups and a Jordan type theorem*, J. Eur. Math. Soc. (JEMS) 13 (2011), no. 4, 10631077.
- [42] M. V. Nori, *On subgroups of $GL_n(\mathbb{F}_p)$* , Invent. math., **88** (1987), 257–275.
- [43] L. Pyber, E. Szabó, *Growth in finite simple groups of Lie type of bounded rank*, preprint (2011) arXiv arXiv:1005.1858.
- [44] L. Pyber, E. Szabó, *Growth in finite simple groups of Lie type*, preprint (2010) arXiv:1001.4556.
- [45] L. Pyber, E. Szabó, *Growth in Linear groups*, in this volume.
- [46] A. Rapinchuk, *On Strong Approximation for Algebraic groups*, this volume.
- [47] I. Z. Ruzsa, *Generalised arithmetic progressions and sumsets*, Acta. Math. Hungar. **65** (1994), no. 4, 379–388.
- [48] A. Salehi-Golsefidy and P. Varju, *Expansion in perfect groups*, preprint arXiv:1108.4900.
- [49] T. Sanders, *On the Bogolyubov-Ruzsa lemma*, Anal. PDE 5 (2012), no. 3, 627655.
- [50] T. Sanders, *The structure theory of set addition revisited*, Bull. Amer. Math. Soc. 50 (2013), 93127
- [51] P. Sarnak and X. X. Xue, *Bounds for multiplicities of automorphic representations*, Duke Math. J., **64** no. 1, (1991), 207–227.
- [52] J.P. Serre, *Linear representations of finite groups*, Graduate Texts in Mathematics, Vol. 42. Springer-Verlag, 1977. x+170 pp.
- [53] T. Tao, *Product set estimates in noncommutative groups*, Combinatorica **28** (2008), 547–594.
- [54] T. Tao, *Freiman's theorem for solvable groups*, Contrib. Discrete Math. 5 (2010), no. 2, 137-184.
- [55] T. Tao, V. Vu, *Additive Combinatorics*, Cambridge University Press (2006).
- [56] M. Tointon, *Freiman's theorem in an arbitrary nilpotent group*, preprint (2012) arXiv:1211.3989.
- [57] 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`