Thin groups and superstrong approximation
MSRI Publications
Volume **61**, 2013

A brief introduction to approximate groups

EMMANUEL BREUILLARD

This introduction to approximate groups highlights their connection with superstrong approximation, the Freiman inverse problem, the Helfgott–Lindenstrauss conjecture, and the classification of approximate subgroups of simple algebraic groups over finite fields.

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 in Definition 1.2 below was introduced by T. Tao [2008] and was in part motivated by its use in the groundbreaking work of Bourgain and Gamburd [2008b] on superstrong 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 superstrong approximation especially in the early developments of the subject (e.g., in [Helfgott 2008]), is equivalent to classifying approximate subgroups of the affine group $\{x \mapsto ax + b\}$.

This article intends to give a brief introduction to this subject and present some of its recent developments. Worthwhile expository readings on the same topics include [Green 2009; 2012; Breuillard et al. 2013b; Pyber and Szabó 2014].

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

Definition 1.2 (approximate groups [Tao 2008]). Let $K \geqslant 1$ be a parameter, G 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: $A = A^{-1}$, and

(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, given a finite set A in an ambient group G and parameter $K \geqslant 1$, the following conditions are roughly equivalent in a sense about to be made precise*:

(1) $|AA| \leqslant K|A|$.

(2) $|AAA| \leqslant K|A|$.

(3) $|\{(a,b,c,d) \in A \times A \times A \times A \mid ab = cd\}| \geqslant |A|^3/K$.

(4) $|\{(a,b) \in A \times A : ab \in A\}| \geqslant |A|^2/K$.

(5) *A is a K-approximate subgroup of G*,

More precisely, if any of these conditions holds for A with a constant K, the other four conditions will hold, with a constant $K' \leqslant CK^C$, for a set $A' \subset G$ such that $|A \cap A'| \geqslant 1/(CK^C) \max\{|A|, |A'|\}$.

Conditions (1) and (2) are the small doubling and tripling conditions, respectively. Conditions (3) and (4) are statistical in nature. The rough equivalence above was proved in [Tao 2008], but it relies[1] on a tricky yet extremely useful graph-theoretical result of Balog and Szemerédi, which was later improved by Gowers, yielding the polynomial bound CK^C in the statement. See [Tao and Vu 2006, Section 6.4] 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 attempting to *classify* approximate groups. 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).

[1] At least for the conditions involving (3) and (4); the rough equivalence between (1), (2) and (5) is easier.

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). Approximate groups in the 99% regime are easily seen to be very close to genuine subgroups (see Proposition 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)–(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)–(4) above in a given group G is reduced to understanding approximate groups in Tao's sense. This usually boils down to a more familiar algebraic or geometric problem about the ambient group where combinatorics play a minor role.

1.4. ***Approximate groups and superstrong approximation.*** One of the main motivations for the subject of approximate groups and its recent fast development is its connection with superstrong approximation as was first made clear in [Bourgain and Gamburd 2008b], for the case of $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$.

Superstrong approximation is the main topic of this volume and is discussed at length in [Sarnak 2014; Salehi 2014; Ellenberg 2014]. So I will not attempt here to give a detailed account of it, but let me only recall that if $\Gamma \leqslant \mathrm{SL}_d(\mathbb{Z})$ is a Zariski dense subgroup, then strong approximation for Γ is the statement that for every large enough prime number p, the subgroup Γ surjects onto $\mathrm{SL}_d(\mathbb{Z}/p\mathbb{Z})$ (see [Rapinchuk 2014; Matthews et al. 1984; Nori 1987]), while *superstrong 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 [1973] 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 and Sarnak on Ramanujan graphs [Lubotzky et al. 1988], 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 (as in applications to sieving, for example). In 2005 Bourgain and Gamburd [2008b] 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 Theorem 3.2 in [Hoory et al. 2006] or Appendix E in [Breuillard et al. 2013a]) 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*; that is, it does not give too much mass to 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 *quasirandomness* (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 and 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 [1959] 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 [Varjú 2012; Salehi and Varjú 2012]), or to use the theory of products of random matrices à la Furstenberg–Guivarc'h; see [Bourgain and Gamburd 2008a; 2009].

Item (2) is the subject of this article and amounts to understanding approximate subgroups of the finite quotients. This was first done in [Helfgott 2008] for $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ (see also [Helfgott 2011] for $\mathrm{SL}_3(\mathbb{Z}/p\mathbb{Z})$), which then allowed Bourgain and 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 cobounded 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 subgroup 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 in [Pyber

and Szabó 2010b] and independently in [Breuillard et al. 2011]. See the second part of this article as well as [Pyber and Szabó 2014] to this volume for a detailed account of this story.

1.5. ***The Freiman inverse problem.*** While in part motivated by the superstrong approximation result of Bourgain and 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 $K \geqslant 1$, 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 $|AA|/|A|$ 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 [Breuillard et al. 2012], which provides an answer to Freiman's inverse problem for general groups. For the applications to superstrong 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 Section 2.

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

- Bourgain, Katz and Tao [Bourgain et al. 2004]: the *sum-product* theorem for finite fields (2003).
- Helfgott [2008]: the $\mathrm{SL}_2(\mathbb{F}_p)$ case using the sum-product (2005).
- Tao [2008] transposed to the noncommutative setting most of the apparatus of additive number theory previously used to tackle Freiman's problem in abelian groups and defined approximate groups (2005).
- Helfgott [2011]: $\mathrm{SL}_3(\mathbb{F}_p)$ then partial results for $\mathrm{SL}_d(\mathbb{F}_p)$ in [Gill and Helfgott 2011].
- Dinai [2010]: $\mathrm{SL}_2(\mathbb{F}_q)$.
- Tao [2010]: general solvable groups with bounded solvability length.
- Breuillard and Green [2011a; 2011b; 2012]: polynomial bounds for torsion-free nilpotent groups, solvable linear groups, compact Lie groups.

- Bourgain, Gamburd and Sarnak [2010]: $\mathrm{SL}_2(\mathbb{Z}/q\mathbb{Z})$ with q square-free integer.
- Hrushovski [2012b]: progress towards the Freiman inverse problem for arbitrary groups; also for general linear groups (no explicit bounds) using model theory.
- Pyber and Szabó [2010b]; Breuillard, Green and Tao [Breuillard et al. 2011]: $\mathbf{G}(\mathbb{F}_q)$, $\mathbf{G}$ a simple algebraic group over a finite field $\mathbb{F}_q$ (with polynomial bounds).
- Varjú [2012]: $\mathbf{G}(\mathbb{Z}/q\mathbb{Z})$, q square free, $\mathbf{G} = \mathrm{SL}_n$.
- Bourgain and Varjú [2012]: handled $\mathrm{SL}_d(\mathbb{Z}/n\mathbb{Z})$ for arbitrary modulus n.
- Salehi and Varjú [2012]: $\mathbf{G}(\mathbb{Z}/q\mathbb{Z})$, q square free, $\mathbf{G}$ perfect.
- Gill and Helfgott [2010]: solvable algebraic subgroups over $\mathbb{F}_p$.
- Breuillard, Green, and Tao [Breuillard et al. 2012]: arbitrary groups (but no explicit bounds).
- Tointon [2012]: arbitrary nilpotent groups (with polynomial bounds).
- Pyber and Szabó [2014]: general linear groups (with polynomial bounds).

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? Here is an old result of Freiman, first published in [Freiman 1973a]:

Proposition 1.7 (Freiman inverse problem for $K < \frac{3}{2}$; see [Tao 2009], [Freiman 2012], or [Breuillard 2011b]). *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 $|AA^{-1}A| \leqslant (1+\varepsilon)|A|$ 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 nontrivially, because $\varepsilon < 1$. It follows that $xy^{-1} \in H$. Hence H is stable under multiplication and hence a genuine subgroup. Note finally that $|H| \leqslant (1+\varepsilon)|A|$ and $A \subset aH$ for every $a \in A$. The proof of Proposition 1.7 is more involved, but makes use of similar arguments.

If $K > \frac{3}{2}$, 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 [2013], which answered a question of Tao (see also [Tao 2011] for a proof).

It is clear that such a thing no longer holds if $K \geqslant 2$, 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 $\pi : \mathbb{Z}^d \to G$ 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 $|AA| \leqslant 2^d|A|$.

For instance, $\{a, a+r, a+2r, \dots, a+2Nr\}$, an arithmetic progression of odd length in $\mathbb{Z}$, is nothing other 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 and Green 2011a] as well as in Tao's paper on solvable groups [2010]. 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 geometric 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 $\|(x_1, \dots, x_k)\| = \sum |x_i|/N_i$ on the abelianization $\mathbb{R}^k$ of $N_{r,k}(\mathbb{R})$.

The two definitions lead to two roughly equivalent notions of nilprogressions. See [Breuillard and Green 2011a], the appendix to [Breuillard et al. 2012], and Tointon's paper [2012] on approximate subgroups of nilpotent groups.

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 1960s. There are no nontrivial finite subgroups of $\mathbb{Z}$, so finite groups will not appear. However there are generalized arithmetic progressions. Freiman's theorem [1973b] 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) $|P| \leqslant C|A|$, *with* $C \leqslant O_K(1)$,

(3) $|X| \leqslant O_K(1)$,

(4) $d \leqslant O_K(1)$.

For a proof, see [Green 2002] or [Tao and Vu 2006].

Ruzsa [1994] gave a simplified proof of Freiman's theorem, which was improved by Chang [2002] and then pushed to all abelian groups by Green and Ruzsa [2007]. Ruzsa's proof gave 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 1.10 (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 [2012] gave almost polynomial bounds towards this conjecture: he has $d = O(\log^6 K)$, while $C \leqslant K^3$ and $|X| = O(K^{\log^6 K})$. See also his excellent recent survey [Sanders 2013], where these bounds are further improved.

1.11. ***The combinatorial toolbox of approximate groups.*** As Tao has observed, many combinatorial arguments from additive number theory actually work without modification in the noncommutative 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

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

The proof of the Ruzsa triangle inequality is just a few lines, which I cannot resist including here. Note first that obviously

$$|AB^{-1}| \geqslant |A| \quad \text{and} \quad |AB^{-1}| \geqslant |B|,$$

so that $|AB^{-1}|^2 \geqslant |A||B|$, yielding $d(A, B) \geqslant 0$ always. Next consider the map $AC^{-1} \times B \to AB^{-1} \times BC^{-1}$, 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 $|B||AC^{-1}| \leqslant |AB^{-1}||BC^{-1}|$, which is another way to phrase the triangle inequality $d(A, C) \leqslant d(A, B) + d(B, C)$. QED.

Clearly this proof is much easier than that of the Balog–Szemerédi–Gowers lemma mentioned on page 24. Applying only the Ruzsa triangle inequality one can prove the following (see, e.g., [Tao 2008] or [Breuillard 2011b]):

Lemma 1.12. *Let A be a finite subset of a group G and $K \geqslant 1$ be a parameter.*

- *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.*

Note. 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 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 superstrong 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 $K \geqslant 1$. For every integer $k \geqslant 2$, and $x \in X$, we have*

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

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 and Szabó 2014], 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 [Breuillard 2011b]; see also [Tao and Vu 2006; Tao 2008; Helfgott 2008]. They form the basic toolkit 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 this article:

Philosophy. Group-theoretical arguments can often be successfully transferred to approximate groups.

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 [2011], 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 are finite subsets $P, X \subset G$ satisfying the following conditions*:

(1) $A \subset XP$.

(2) $|X| \leqslant O_K(1)$.

(3) $|P| \leqslant O_K(1)|A|$.

(4) *P is a coset nilprogression; that is, $P = HL$, 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 was proved by Green, Tao and myself:

Theorem 1.16 [Breuillard et al. 2012]. *The Helfgott–Lindenstrauss conjecture holds. In it, one can take $P \subset A^4$, 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 nonnegative curvature. Gromov's theorem can be deduced in only a few lines from Theorem 1.16.

A proof of Theorem 1.16 can be found in [Breuillard et al. 2012]. The basic strategy was inspired by the preprint version of [Hrushovski 2012b], 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 fifth 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 [Breuillard et al. 2012], 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 readers with a taste for model theory, we also recommend Hrushovski's beautiful lecture notes [2012a], 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 nilprogression[2] nor on the size of X. This is due to the inherently nonexplicit nature of the proof, which makes use of ultrafilters to take limits.

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

In view of the polynomial Freiman–Ruzsa conjecture (Conjecture 1.10) it is reasonable to expect that these bounds can be made polynomial in K.

We will see in Section 2 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 by László Pyber at his workshop lecture (see also [Pyber and Szabó 2014]). 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's $\mathrm{SL}_3(\mathbb{Z}/p\mathbb{Z})$ theorem. One should however bear in mind the following example due to Pyber (see also the end of [Pyber and Szabó 2010b]).

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 $i \mapsto i+2 \bmod 2n+1$. 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 nontrivial 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 remainder of the article, we give an introduction to the works [Breuillard et al. 2011] and [Pyber and Szabó 2010b], which classify approximate subgroups of simple algebraic groups over finite fields. We will give complete proofs save for the Larsen–Pink-type nonconcentration estimate (Theorem 2.15 below), whose proof we only briefly sketch as it is rather more involved.

A key tool is the use of quasirandomness 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 nonabelian 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. ***Quasirandomness 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 nontrivial 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 nontrivial 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., [Breuillard 2011a] for some historical comments on Jordan's theorem).

This feature has played a very important role in the spectral theory of arithmetic surfaces; see [Sarnak and Xue 1991]. 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 $m(\mathrm{PSL}_2(\mathbb{F}_p)) = \frac{1}{2}(p-1)$, and was established in full generality as follows:

Fact (Landazuri–Seitz bound [1974]). *There is a constant $c_d > 0$ such that $m(G) \geqslant c_d|G|^{r/d}$ 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*[3] *r.*

In the early 2000s, Tim Gowers [2008] exploited this fact in order to answer a combinatorial question of Babai and Sós: 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 and Pyber in [2011]) 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 and Pyber [Babai et al. 2008]) is based on spectral analysis of bipartite graphs. We give a seemingly different argument based on the nonabelian Fourier transform.

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

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

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

The convolution product is associative: $(f_1 * f_2) * f_3 = f_1 * (f_2 * f_3)$. 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 nonabelian Fourier inversion and Parseval formulas (see [Serre 1977] 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. Then

$$\textit{Parseval}: \qquad \sum_{g\in G} |f(g)|^2 = \frac{1}{|G|}\sum_{\pi} d_\pi \|\pi(f)\|^2,$$

$$\textit{Fourier inversion}: \qquad f(g) = \frac{1}{|G|}\sum_{\pi} d_\pi \langle \pi(f), \pi(g)\rangle.$$

Here we have written $\pi(f) = \sum_{g\in G} f(g)\pi(g)$, where π is an irreducible complex linear representation of G, and the sums on the right extend over all such representations; moreover the scalar product is defined on $\mathrm{End}(\mathcal{H}_\pi)$ by $\langle X, Y\rangle = \mathrm{trace}(XY^*)$.

From the Parseval formula applied to 1_A and the bound $d_\pi \geqslant m(G)$ for every nontrivial π, we see that $|A| = (1/|G|)\sum_\pi d_\pi \|\pi(1_A)\|^2$, and thus

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

for every nontrivial 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–Schwarz inequality together with the Parseval identity to handle $\|\pi(1_B)\|$ and $\|\pi(1_C)\|$, we get

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

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

Combining Gowers' trick with the bound on $m(G)$ mentioned above, we obtain this result for approximate groups:

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 $|A| > |G|^{1-\delta}$.*

Gowers calls *quasirandom* a finite group G for which $m(G)$ is large. This terminology comes from the abelian case, where a quasirandom 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 nontrivial character χ of G. Certainly random subsets of G (chosen by flipping independent coins for each element of G) are quasirandom. The bound (2.2.1) shows that if $m(G)$ is large, then every subset of G is quasirandom in the sense that $\|\pi(1_A)\|$ is small compared to $|G|$ for every nontrivial irreducible representation π.

2.4. ***The sum-product theorem.*** The story of approximate groups really began when Bourgain, Katz and Tao proved the following:

Theorem 2.5 (sum-product in $\mathbb{F}_p$; see [Bourgain et al. 2004]). *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*

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

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 and Vu 2006]), most of them quite combinatorial. Konyagin [2003] gave a proof that does not require the $|S| > p^\delta$ assumption. We will give a more geometric proof (also not requiring the $|S| > p^\delta$ assumption) below. All proofs require some version of the following result:

Lemma 2.6 (Katz and Tao; see [Tao and Vu 2006] or [Breuillard 2011b]). *For every $n \geqslant 1$ there is a constant $C = C(n) > 0$ such that for every $K \geqslant 1$ and for any set $S \subset \mathbb{F}_p$ with $|S + S| + |SS| \leqslant K|S|$, there are $\lambda \in \mathbb{F}_p^*$ 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 [2011]. 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

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

and inside this group consider the subset

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

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

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

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, 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 2005, Helfgott established a seminal result:

Theorem 2.8 (product theorem [Helfgott 2008]). *For every $\delta > 0$ there is $\varepsilon > 0$ (independent of p) 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 a CK^C-approximate group. So Helfgott's theorem can be rephrased (somewhat abusively) as saying that: *there are no nontrivial 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 [2011].

After Helfgott's results (and also the partial results on $\mathrm{SL}_d(\mathbb{Z}/p\mathbb{Z})$ in [Gill and Helfgott 2011]) 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 in 2009, with the preprint of [Hrushovski 2012b], where use was made of model-theoretic tools to give an essentially complete classification of approximate subgroups of simple algebraic groups, albeit with no explicit bounds. One statement is the following:

Theorem 2.9 [Hrushovski 2012b, 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* $\mathbf{G}(k)$ *and a number* $f(d, K)$ *depending only on* d *and* K *satisfying the following conditions*:

(i) A *intersects at most* $f(d, K)$ *cosets of* $\mathbb{H}$.

(ii) *Either* $\mathbb{H}$ *is a proper connected algebraic subgroup of* $\mathbf{G}$, *or* $\mathbb{H}$ *is finite and contained in* A^4.

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 arXiv, however, Pyber and Szabó [2010a; 2010b] and independently Green, Tao and myself [Breuillard et al. 2010; 2011] 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* $f(d, K) \leqslant O_d(K^{O_d(1)})$, *such that for every simple algebraic group* $\mathbf{G}$ *of dimension* $d = \dim \mathbf{G}$ *defined over an algebraically closed field* k *and every* K*-approximate subgroup* $A \subset \mathbf{G}(k)$, *we are in one of the following situations*:

(1) *There exists a proper closed algebraic subgroup* $\mathbb{H}$ *with at most* $C(d)$ *connected components and such that* $A \subset \mathbb{H}(k)$.

(2) $|A| \leqslant f(d, K)$.

(3) $|A| \geqslant |\langle A \rangle| / f(d, K)$.

In cases (1) or (2), the first alternative in Theorem 2.9(ii) holds. If we are in case (3) of Theorem 2.10, then $\langle A \rangle$ is finite and not much larger than A, a condition that is close to the condition in the second branch of Theorem 2.9(ii), yet not exactly the same (see however Corollary 2.12 below).

I will sketch a proof of Theorem 2.10 below. (For a beautiful exposition of this proof in the framework of model theory, we refer the reader to [Hrushovski 2013].) 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 and Szabó), 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 [2011] 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 (page 35) 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, or*

(2) $|S^N| \geqslant \min\{|\langle S\rangle| : |S|^{1+\varepsilon}\}$, *where* $N = N(d)$ *and* $C = C(d)$ *are constants independent of the field* k.

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

Sketch of proof. 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 (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 modding 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 $[\langle A\rangle, \langle A\rangle]$/center and the result follows. □

Finite simple groups of Lie type[4] are of form $G = \mathbf{G}(\mathbb{F}_q)$/center for some absolutely almost simple (simply connected) algebraic group $\mathbf{G}$ defined over $\mathbb{F}_q$.

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

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 quasirandom in the sense of Gowers (compare the Landazuri–Seitz bound, page 35) 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*

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

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

I will now turn 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 [Breuillard et al. 2011]. I will start with a geometric proof of the sum-product theorem (Theorem 2.5), because this 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

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

This group admits two remarkable actions:

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

(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 nontrivial 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

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

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 $|BBB| \leqslant CK^C|B|$ 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-stabilizer 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 $h \in A$, the Katz–Tao lemma implies that $|g^A| \leqslant O(K^{O(1)})|S|$ because 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 that

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

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 that

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

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

Here the shorthand $|A_1| \asymp_K |A_2|$ signifies that $|A_1| \geqslant |A_2|/O(K^{O(1)})$ and vice versa.

This is where the miracle happens: if $A^2 \cap T_x$ has one nontrivial 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 nontrivially (the so-called *involved tori* in the terminology of [Breuillard et al. 2010]).

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 $|A^k \cap \mathrm{Stab}(x)|$ is roughly of the same size as $|A^2 \cap \mathrm{Stab}(x)|$ for any given $k \geqslant 2$. So we may write:

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

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

Note from the way we defined A that A contains a nontrivial 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 nontrivial 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

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

thus

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

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 — $\varepsilon \leqslant \dfrac{\delta}{O(1)}$ 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, that is, 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 dimension inequality of Larsen and Pink, devised in their 1995 preprint on finite subgroups of linear groups (which has now appeared as [Larsen and Pink 2011]) and then investigated in [Hrushovski and Wagner 2008] in the model-theoretic framework.

Theorem 2.15 (Larsen–Pink inequality). *Let* $\mathbf{G}$ *be a* (*connected*) *simple algebraic group over an algebraically closed field* k. *Given* $M \geqslant 1$, *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* $[\mathbf{H}, \mathbf{H}^0] \leqslant C$, *or for every closed algebraic subvariety* $\mathscr{V}$ *of* $\mathbf{G}$ *with degree at most* M,

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

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 [2011, Theorem 4.2] in the case when A is a genuine finite subgroup of $\mathbf{G}(k)$ (namely when $K = 1$). Hrushovski and Wagner [2008] then gave a model theoretic proof as well as a vast generalization, which was subsequently used in [Hrushovski 2012b] to prove 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 $\dim \mathscr{V} = 0$, because then $\mathscr{V}$ is finite and its degree is its number of elements; and when $\dim \mathscr{V} = \dim \mathbf{G}$, obviously. Now the proof proceeds by a double induction on the dimension of $\mathscr{V}$. Starting with two possible counterexamples, one of smallest possible dimension $\mathscr{V}_-$ and one of largest possible dimension $\mathscr{V}_+$ 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 $\mathscr{V}_- a \mathscr{V}_+$ has dimension $\dim \mathscr{V}_+ + 1$ at least. Indeed assuming as we may that $\mathscr{V}_-$ and $\mathscr{V}_+$ are irreducible, an equality between the dimensions $\dim \mathscr{V}_- a \mathscr{V}_+ = \dim \mathscr{V}_+$ 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 $\{g \in \mathbf{G}(k) \mid g^{-1}\mathscr{V}_-{}^{-1}\mathscr{V}_- g \subset \mathrm{Stab}(\mathscr{V}_+)\}$, where $\mathrm{Stab}(\mathscr{V}_+)$ is the subgroup $\{g \in \mathbf{G}(k) | g\mathscr{V}_+ = \mathscr{V}_+\}$. Then one can use the induction hypothesis on $\mathscr{V}_- a \mathscr{V}_+$ 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 $\mathscr{V}$, all of them of bounded degree (maximal tori and their normalizers, conjugacy classes of regular semisimple elements, and the set of nonregular 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 this article, 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 nonregular 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 nontrivially, 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

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

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

Action (a): Suppose $g \in A^2 \cap T_{\mathrm{reg}}$. 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

$$|g^A| \leqslant |A^3 \cap \mathcal{V}| \leqslant O(K^{O(1)})|A|^{1-\frac{\dim T}{\dim \mathbf{G}}}.$$

So, by the orbit-stabilizer lemma, we conclude that[5]

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

[5]Note 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.

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

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

Since nonregular elements form a proper Zariski closed subset of bounded degree, another application of the Larsen–Pink inequality yields

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

Conclusion. *For every maximal torus T, if $A^2 \cap T_{\mathrm{reg}} \neq \varnothing$, then*

$$|A^2 \cap T_{\mathrm{reg}}| \asymp_K |A|^{\frac{\dim T}{\dim \mathbf{G}}},$$

Precisely the same argument as in the proof of the sum-product theorem given above yields the analogous claim:

Key claim. *If $|A| \geqslant CK^C$, for some constant C depending on* $\dim \mathbf{G}$ *only, then $\mathscr{T}$ is invariant under conjugation by A (and hence by the subgroup $\langle A\rangle$ generated by A).*

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

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

thus

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

hence

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

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

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

Finally another application of the Larsen–Pink inequality (this time the original one for genuine subgroups) gives

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

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 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 Nicolas de Saxcé for their careful reading of the manuscript.

References

[Babai et al. 2008] L. Babai, N. Nikolov, and L. Pyber, "Product growth and mixing in finite groups", pp. 248–257 in *Proceedings of the Nineteenth Annual ACM-SIAM Symposium on Discrete Algorithms* (San Francisco, CA, 2008), ACM, New York, 2008.

[Bourgain and Gamburd 2008a] J. Bourgain and A. Gamburd, "Expansion and random walks in $\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$. I", *J. Eur. Math. Soc.* (*JEMS*) **10**:4 (2008), 987–1011.

[Bourgain and Gamburd 2008b] J. Bourgain and A. Gamburd, "Uniform expansion bounds for Cayley graphs of $\mathrm{SL}_2(\mathbb{F}_p)$", *Ann. of Math.* (2) **167**:2 (2008), 625–642.

[Bourgain and Gamburd 2009] J. Bourgain and A. Gamburd, "Expansion and random walks in $\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$. II", *J. Eur. Math. Soc.* (*JEMS*) **11**:5 (2009), 1057–1103.

[Bourgain and Varjú 2012] J. Bourgain and P. P. Varjú, "Expansion in $\mathrm{SL}_d(\mathbf{Z}/q\mathbf{Z})$, q arbitrary", *Invent. Math.* **188**:1 (2012), 151–173.

[Bourgain et al. 2004] J. Bourgain, N. Katz, and T. Tao, "A sum-product estimate in finite fields, and applications", *Geom. Funct. Anal.* **14**:1 (2004), 27–57.

[Bourgain et al. 2010] J. Bourgain, A. Gamburd, and P. Sarnak, "Affine linear sieve, expanders, and sum-product", *Invent. Math.* **179**:3 (2010), 559–644.

[Breuillard 2011a] E. Breuillard, "An exposition of Jordan's original proof of his theorem on finite subgroups of $\mathrm{GL}_n(\mathbb{C})$", preprint, 2011, http://www.math.u-psud.fr/~breuilla/Jordan.pdf.

[Breuillard 2011b] E. Breuillard, "Lectures on approximate groups", lecture notes, 2011, http://www.math.u-psud.fr/~breuilla/ClermontLectures.pdf.

[Breuillard and Green 2011a] E. Breuillard and B. Green, "Approximate groups, I: The torsion-free nilpotent case", *J. Inst. Math. Jussieu* **10**:1 (2011), 37–57.

[Breuillard and Green 2011b] E. Breuillard and B. Green, "Approximate groups, II: The solvable linear case", *Q. J. Math.* **62**:3 (2011), 513–521.

[Breuillard and Green 2012] E. Breuillard and B. Green, "Approximate groups, III: The unitary case", *Turkish J. Math.* **36**:2 (2012), 199–215.

[Breuillard et al. 2010] E. Breuillard, B. Green, and T. Tao, "Linear approximate groups", *Electron. Res. Announc. Math. Sci.* **17** (2010), 57–67.

[Breuillard et al. 2011] E. Breuillard, B. Green, and T. Tao, "Approximate subgroups of linear groups", *Geom. Funct. Anal.* **21**:4 (2011), 774–819.

[Breuillard et al. 2012] E. Breuillard, B. Green, and T. Tao, "The structure of approximate groups", *Publ. Math. IHES* **116**:1 (2012), 115–221.

[Breuillard et al. 2013a] E. Breuillard, B. Green, R. Guralnick, and T. Tao, "Expansion in finite simple groups of Lie type", preprint, 2013. arXiv 1309.1975

[Breuillard et al. 2013b] E. Breuillard, B. J. Green, and T. Tao, "Small doubling in groups", preprint, 2013. To appear in and Erdös centennial volume. arXiv 1301.7718

[Chang 2002] M.-C. Chang, "A polynomial bound in Freiman's theorem", *Duke Math. J.* **113**:3 (2002), 399–419.

[Dinai 2010] O. Dinai, "Expansion properties of finite simple groups", preprint, 2010. MR 1001: 5069

[Ellenberg 2014] J. S. Ellenberg, "Superstrong approximation for monodromy groups", pp. 51–71 in *Thin groups and superstrong approximation*, edited by H. Oh and E. Breuillard, Math. Sci. Res. Inst. Publ. **61**, Cambridge Univ. Press, Cambridge, 2014.

[Freiman 1973a] G. Freiman, "Number-theoretic studies in the Markov spectrum and in the structural theory of set addition", pp. 175–183 in *Groups and the inverse problems of additive number theory*, Kalinin. Gos. Univ., Moscow, 1973. in Russian.

[Freiman 1973b] G. A. Freiman, *Foundations of a structural theory of set addition*, Transl. Math. Monogr. **37**, Amer. Math. Soc., Providence, 1973.

[Freiman 2012] G. A. Freiman, "On finite subsets of nonabelian groups with small doubling", *Proc. Amer. Math. Soc.* **140**:9 (2012), 2997–3002.

[Gill and Helfgott 2010] N. Gill and H. A. Helfgott, "Growth in solvable subgroups of $\mathrm{GL}_r(\mathbb{Z}/p\mathbb{Z})$", preprint, 2010. arXiv 1008.5264

[Gill and Helfgott 2011] N. Gill and H. A. Helfgott, "Growth of small generating sets in $\mathrm{SL}_n(\mathbb{Z}/p\mathbb{Z})$", *Int. Math. Res. Not.* **2011**:18 (2011), 4226–4251.

[Gowers 2008] W. T. Gowers, "Quasirandom groups", *Combin. Probab. Comput.* **17**:3 (2008), 363–387.

[Green 2002] B. J. Green, "Structure theory of set addition", notes from the ICMS Instructional Conference in Combinatorial Aspects of Mathematical Analysis(Edinburgh), 2002, https://www.dpmms.cam.ac.uk/∼bjg23/papers/icmsnotes.pdf.

[Green 2009] B. J. Green, "Approximate groups and their applications: work of Bourgain, Gamburd, Helfgott and Sarnak", preprint, 2009. arXiv 0911.5681

[Green 2012] B. Green, "What is... an approximate group?", *Notices Amer. Math. Soc.* **59**:5 (2012), 655–656.

[Green and Ruzsa 2007] B. Green and I. Z. Ruzsa, "Freiman's theorem in an arbitrary abelian group", *J. Lond. Math. Soc.* (2) **75**:1 (2007), 163–175.

[Hamidoune 2013] Y. O. Hamidoune, "Two inverse results", *Combinatorica* **33** (2013), 217–230.

[Helfgott 2008] H. A. Helfgott, "Growth and generation in $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$", *Ann. of Math.* (2) **167**:2 (2008), 601–623.

[Helfgott 2011] H. A. Helfgott, "Growth in $\mathrm{SL}_3(\mathbb{Z}/p\mathbb{Z})$", *J. Eur. Math. Soc.* (*JEMS*) **13**:3 (2011), 761–851.

[Hoory et al. 2006] S. Hoory, N. Linial, and A. Wigderson, "Expander graphs and their applications", *Bull. Amer. Math. Soc.* (*N.S.*) **43**:4 (2006), 439–561.

[Hrushovski 2012a] E. Hrushovski, "Notes on Hilbert's 5th problem and approximate groups", 2012, http://www.ma.huji.ac.il/∼ehud/notesH5-BGT.pdf.

[Hrushovski 2012b] E. Hrushovski, "Stable group theory and approximate subgroups", *J. Amer. Math. Soc.* **25**:1 (2012), 189–243.

[Hrushovski 2013] E. Hrushovski, "On pseudo-finite dimensions", in *Proceedings of a model theory conference* (Oléron, France, 2011), 2013. to appear in *Notre Dame J. Formal Logic*.

[Hrushovski and Wagner 2008] E. Hrushovski and F. Wagner, "Counting and dimensions", pp. 161–176 in *Model theory with applications to algebra and analysis, II*, edited by Z. Chatzidakis et al., London Math. Soc. Lecture Note Ser. **350**, Cambridge Univ. Press, 2008.

[Kesten 1959] H. Kesten, "Symmetric random walks on groups", *Trans. Amer. Math. Soc.* **92** (1959), 336–354.

[Konyagin 2003] S. Konyagin, "A sum-product estimate in fields of prime order", preprint, 2003. arXiv math.NT/0304217

[Landazuri and Seitz 1974] V. Landazuri and G. M. Seitz, "On the minimal degrees of projective representations of the finite Chevalley groups", *J. Algebra* **32** (1974), 418–443.

[Larsen and Pink 2011] M. J. Larsen and R. Pink, "Finite subgroups of algebraic groups", *J. Amer. Math. Soc.* **24**:4 (2011), 1105–1158.

[Lubotzky et al. 1988] A. Lubotzky, R. Phillips, and P. Sarnak, "Ramanujan graphs", *Combinatorica* **8**:3 (1988), 261–277.

[Margulis 1973] G. A. Margulis, "Explicit constructions of expanders", *Problemy Peredači Informacii* **9**:4 (1973), 71–80. In Russian; translated in *Probl. Inf. Transm.* **9**:4 (1973), 325–332 (1975).

[Matthews et al. 1984] C. R. Matthews, L. N. Vaserstein, and B. Weisfeiler, "Congruence properties of Zariski-dense subgroups. I", *Proc. London Math. Soc.* (3) **48**:3 (1984), 514–532.

[Nikolov and Pyber 2011] N. Nikolov and L. Pyber, "Product decompositions of quasirandom groups and a Jordan type theorem", *J. Eur. Math. Soc.* (*JEMS*) **13**:4 (2011), 1063–1077.

[Nori 1987] M. V. Nori, "On subgroups of $\mathrm{GL}_n(\mathbf{F}_p)$", *Invent. Math.* **88**:2 (1987), 257–275.

[Pyber and Szabó 2010a] L. Pyber and E. Szabó, "Growth in finite simple groups of Lie type", preprint, 2010. arXiv 1001.4556

[Pyber and Szabó 2010b] L. Pyber and E. Szabó, "Growth in finite simple groups of Lie type of bounded rank", preprint, 2010. arXiv 1005.1858

[Pyber and Szabó 2014] L. Pyber and E. Szabó, "Growth in linear groups", pp. 253–268 in *Thin groups and superstrong approximation*, edited by H. Oh and E. Breuillard, Math. Sci. Res. Inst. Publ. **61**, Cambridge Univ. Press, Cambridge, 2014.

[Rapinchuk 2014] A. Rapinchuk, "Strong approximation for algebraic groups", pp. 269–298 in *Thin groups and superstrong approximation*, edited by H. Oh and E. Breuillard, Math. Sci. Res. Inst. Publ. **61**, Cambridge Univ. Press, Cambridge, 2014.

[Ruzsa 1994] I. Z. Ruzsa, "Generalized arithmetical progressions and sumsets", *Acta Math. Hungar.* **65**:4 (1994), 379–388.

[Salehi 2014] A. Salehi Golsefidy, "Affine sieve and expanders", pp. 325–342 in *Thin groups and superstrong approximation*, edited by H. Oh and E. Breuillard, Math. Sci. Res. Inst. Publ. **61**, Cambridge Univ. Press, Cambridge, 2014.

[Salehi and Varjú 2012] A. Salehi Golsefidy and P. P. Varjú, "Expansion in perfect groups", *Geom. Funct. Anal.* **22**:6 (2012), 1832–1891.

[Sanders 2012] T. Sanders, "On the Bogolyubov–Ruzsa lemma", *Anal. PDE* **5**:3 (2012), 627–655.

[Sanders 2013] T. Sanders, "The structure theory of set addition revisited", *Bull. Amer. Math. Soc.* (*N.S.*) **50**:1 (2013), 93–127.

[Sarnak 2014] P. Sarnak, "Notes on thin matrix groups", pp. 343–362 in *Thin groups and superstrong approximation*, edited by H. Oh and E. Breuillard, Math. Sci. Res. Inst. Publ. **61**, Cambridge Univ. Press, Cambridge, 2014.

[Sarnak and Xue 1991] P. Sarnak and X. X. Xue, "Bounds for multiplicities of automorphic representations", *Duke Math. J.* **64**:1 (1991), 207–227.

[Serre 1977] J.-P. Serre, *Linear representations of finite groups*, Graduate Texts in Mathematics **42**, Springer, New York, 1977.

[Tao 2008] T. Tao, "Product set estimates for non-commutative groups", *Combinatorica* **28**:5 (2008), 547–594.

[Tao 2009] T. Tao, "An elementary non-commutative Freiman theorem", blog entry, 2009, http://tinyurl.com/tao-freiman.

[Tao 2010] T. Tao, "Freiman's theorem for solvable groups", *Contrib. Discrete Math.* **5**:2 (2010), 137–184.

[Tao 2011] T. Tao, "Hamidoune's Freiman–Kneser theorem for nonabelian groups", blog entry, 2011, http://tinyurl.com/tao-hamidoune.

[Tao and Vu 2006] T. Tao and V. Vu, *Additive combinatorics*, Cambridge Studies in Advanced Mathematics **105**, Cambridge University Press, 2006.

[Tointon 2012] M. Tointon, "Freiman's theorem in an arbitrary nilpotent group", preprint, 2012. arXiv 1211.3989

[Varjú 2012] P. P. Varjú, "Expansion in $\mathrm{SL}_d(O_K/I)$, I square-free", *J. Eur. Math. Soc.* (*JEMS*) **14**:1 (2012), 273–305.

emmanuel.breuillard@math.u-psud.fr *Laboratoire de Mathématiques, Université Paris Sud 11, Bâtiment 425, 91405 Orsay, France*