

LECTURES ON APPROXIMATE GROUPS AND HILBERT'S 5TH PROBLEM

EMMANUEL BREUILLARD

ABSTRACT. This paper gathers four lectures, based on a mini-course at IMA in 2014, whose aim was to discuss the structure of approximate subgroups of an arbitrary group, following the works of Hrushovski and of Green, Tao and the author. Along the way we discuss the proof of the Gleason-Yamabe theorem on Hilbert's 5th problem about the structure of locally compact groups and explain its relevance to approximate groups. We also present several applications, in particular to uniform diameter bounds for finite groups and to the determination of scaling limits of vertex transitive graphs with large diameter.

CONTENTS

1. Additive combinatorics on groups	1
2. The structure of approximate groups and geometric applications	6
3. Hilbert's fifth problem and approximate groups	11
4. Applications to diameter bounds and scaling limits of finite groups	21
References	27

1. ADDITIVE COMBINATORICS ON GROUPS

1.1. Introduction. A key idea of Geometric Group Theory as initiated by Gromov and others in the seventies and eighties is to study infinite groups as geometric objects via their Cayley graphs. Endowed with the graph distance, the Cayley graphs are naturally metric spaces. Typically we look at a group Γ generated by a finite symmetric set S and define the associated Cayley graph and word metric:

$$d_S(g, h) := \inf\{n \geq 0, g^{-1}h \in S^n\},$$

where $S^n := S \cdot \dots \cdot S$ is the product set of n copies of S . In particular the ball of radius n around the identity $B_S(e, n)$ is nothing other than S^n . Usually people are interested in properties that are independent of the choice of S , and look at very large values of n . So S is of bounded size and n is large.

Additive Combinatorics on groups on the other hand is concerned with product sets $A^n := A \cdot \dots \cdot A$, where n is of bounded size, but A is a very large finite subset of an ambient group G . Traditionally, combinatorialists and number theorists have been interested in studying large finite subsets of integers that do not grow much under addition. This is an old and well-developed field of mathematics (much older than Geometric Group Theory) with applications to many number theoretical questions (such as unique factorization in rings of algebraic integers, arithmetic progressions in primes, Goldbach's problem, Waring's problem, etc).

Only fairly recently did people start looking at similar questions on non-abelian groups, only to find out that many of the tools developed in the commutative context could also be applied in a non-commutative setting.

1.2. Examples of results from additive combinatorics. To fix ideas, let us recall a sample of landmark results from additive combinatorics:

Theorem 1.1 (Sum-product theorem, Bourgain-Katz-Tao [8], Bourgain-Glibichuk-Konyagin [7]). *Given $\varepsilon > 0$, there is $\delta > 0$ such if p is a prime and $A \subset \mathbb{F}_p$ is a subset of the field $\mathbb{F}_p$ with p elements, then either $|A + A| > |A|^{1+\delta}$ or $|AA| > |A|^{1+\delta}$ or $|A| > p^{1-\varepsilon}$.*

In other words a subset of a prime field must grow either by addition or by multiplication unless it is almost all of the field. This can be viewed as a quantitative version of the fact that there are no non-trivial subrings in $\mathbb{F}_p$. Of course it is easy to construct large subsets A of $\mathbb{F}_p$ that do not grow much under addition, or under multiplication: take a finite arithmetic progression, or geometric progression; then $|AA| \leq 2|A|$, but $|A|$ can be of arbitrary cardinality inside $\mathbb{F}_p$.

By now pretty good quantitative estimates have been obtained on the exponent $\delta(\varepsilon)$, see e.g. [36, 37, 66] and references therein.

Theorem 1.2 (Freiman-Ruzsa-Chang theorem [32, 67, 23]). *Let $A \subset \mathbb{Z}$ be a finite subset such that $|A + A| \leq K|A|$. Then A is $C(K)$ -commensurable to a d -dimensional arithmetic progression P with $d = O(\log K)$.*

Here we used the following terminology:

Definition 1.3 (K-commensurability). Two finite subsets A and B of an ambient group G are called K -commensurable if

$$|A \cap B| \geq \frac{1}{K} \max\{|A|, |B|\}.$$

and

Definition 1.4 (Multidimensional arithmetic progression). A d -dimensional arithmetic progression in an ambient group G is a finite subset of the form $P := \pi(B)$, where $\pi : \mathbb{Z}^d \rightarrow G$ is a group homomorphism and $B := \prod_{i=1}^d [-L_i, L_i]$ is a “box” with side-lengths $L_i \in \mathbb{N}$.

Remarks:

a) It is easy to see that P as above satisfies $|PP| \leq 2^d|P|$ because $B + B$ is contained in at most 2^d translates of B .

b) The proof of the Freiman-Ruzsa-Chang theorem is based on harmonic analysis on $\mathbb{Z}/p\mathbb{Z}$ for some suitably chosen prime p . We refer the reader to [5], [74] and [41] for nice accounts with proofs. The constant $C(K)$ given by these authors was historically of order $e^{O(K^{O(1)})}$. Tom Sanders recently gave much better, almost polynomial, bounds. See [70] for a recent survey. Conjecturally (“Polynomial Freiman-Ruzsa conjecture”, see [42]) one ought to be able to take $C(K)$ to be of order $O(K^{O(1)})$.

In this theorem and its applications, the quality of the bounds (i.e. their dependence on K) are important.

Non-commutative analogues of the above results have started to draw the attention of a number of people in the past ten years. For example, the sum-product theorem can be reformulated as a Freiman type theorem in the affine group of the line (see [51]). The main goal of these lectures is to present a generalization of Freiman’s theorem to arbitrary groups, following [54] and [14]. See [15] for another survey on this topic. Proofs were completely avoided in [15]. Our intent in these lectures is not to provide

a complete treatment, but rather to give some ideas regarding the proofs, a rather complete outline and even the details of some steps, while remaining as informal as possible. All details can be found in the original paper [14] and full proofs are also given in Tao's recent book [73]. For yet another account, we recommend Van den Dries' Bourbaki report [29]. Also part of our focus here is also on the geometric applications, especially in the last lecture, where the main ones are given full proofs.

We refer the reader to [58, 33, 10, 47, 81, 48] for some older results about the general non-commutative case, mostly dealing with the small K regime. In the arbitrary K regime in the non-commutative context, early papers include [30, 59, 71, 50]. One of the first results in this direction is due to Razborov [64] and deals with finite subsets of the free group. Razborov proved that if F is a non-abelian free group and $A \subset F$ a finite subset, then

$$|AAA| \geq |A|^2 / (\log |A|)^c$$

for some positive c independent of A and F , unless A lies in a cyclic subgroup. The exponent 2 is best possible here, as is clear by considering for example $A := \{x\} \cup \{y^i; -N < i < N\}$ in $F_2 := \langle x, y \rangle$.

S. R. Safin recently improved this and showed:

Theorem 1.5 (Safin [68]). *There is $c \in (0, 1)$ such that if F is a free group, then for every $n \geq 3$ and every finite subset A in F*

$$|A^n| \geq c^n |A|^{\lfloor \frac{n+1}{2} \rfloor}$$

unless A generates a cyclic group.

Safin's proof gives an explicit lower bound on c . One can take $c = \frac{1}{62}$. Again the same example shows that the exponent is sharp for each n . See [22] for further generalizations of the Razborov-Safin results to free products and HNN extensions.

Remark: When G is an abelian group, then $|AA| \leq K|A|$ implies that $|A^n| \leq O_{K,n}(1)|A|$ for every $n \geq 2$, according to the Plünnecke-Ruzsa inequalities (see [74]). This is still the case in the non-abelian context, but when starting with the assumption $|AAA| \leq K|A|$ (see §2.2 below). A set A consisting of a subgroup H and another element x with $H \cap xHx^{-1} = \{1\}$ yields an example with small $|AA|$ and large $|AAA|$. This justifies the consideration of three-fold product sets in non-commutative groups. See §2.2 below for more on this issue.

1.3. The Freiman inverse problem. The general problem ("Freiman inverse problem" as advertised in particular by T. Tao in his blog several years ago) is to describe the structure of large subsets A of an arbitrary ambient group G that satisfy $|AA| \leq K|A|$ for some fixed constant K .

The value $|AA|/|A|$ is usually called the *doubling constant* of A , equivalently we say that A has *doubling at most K* .

For example we easily have:

Proposition 1.6. *Let G be an arbitrary group. Suppose $|AA| = |A|$. Then there is a finite subgroup H of G and $A = aH = Ha$ for every $a \in A$.*

Proof. Pick $a \in A$ and set $H := Aa^{-1}$. The set H contains the identity, so $A \subset AH$. But $|AH| = |AHa| = |AA| = |A|$, hence $A = AH$. Iterating $A = AH^n$ for every $n \geq 1$ and it follows that the semigroup $\cup_n H^n$ is finite and contained in $a^{-1}A$. But a finite semigroup inside a group is a finite group. So the subgroup generated by H satisfies $\langle H \rangle \subset a^{-1}A$. In particular $|\langle H \rangle| \leq |A| = |H|$. Hence $\langle H \rangle = H$. It follows that $A = Ha$ and that $H = AA^{-1}$. Finally $|H| = |A| = |AA| = |HaHa| = |HaH| = |a^{-1}HaH|$. But $a^{-1}HaH/H \simeq a^{-1}Ha/(a^{-1}Ha \cap H)$. Hence $a^{-1}Ha = H$ and we are done. $\square$

Slightly trickier is the following:

Proposition 1.7. *Let G be an arbitrary group. Suppose $|AA| \leq 1.1|A|$. Then there is a finite subgroup H of G and $a \in A$ such that $aHa^{-1} = H$, $|H| \leq 1.2|A|$ and $A \subset aH$.*

Proof. Let 1_A be the indicator function of A and $\|f\|_1 = \sum_{g \in G} |f(g)|$ the ℓ^1 -norm. We will prove that $H := AA^{-1}$ is stable under multiplication using the following observation: if $\|1_A - 1_{gA}\|_1 < 2|A|$, then $g \in H$. First we show that $H = A^{-1}A$ and that $|H| \leq 1.2|A|$.

Note that $\forall x, y \in G$, $\|1_{xA} - 1_{yA}\|_1 = |xA \Delta yA| = 2(|A| - |xA \cap yA|)$. But if $x, y \in A$, then $|xA \cup yA| = 2|A| - |xA \cap yA| \leq |A^2| \leq 1.1|A|$. Hence $\forall x, y \in A$, $|xA \cap yA| \geq 0.9|A|$ and

$$\|1_A - 1_{x^{-1}yA}\|_1 \leq 0.2|A|. \quad (1.1)$$

Since $|xA \cap yA| > 0$ we conclude that $xa = yb$ for some $a, b \in A$, i.e. $x^{-1}y \in AA^{-1}$. Hence $A^{-1}A = H = AA^{-1}$. In fact $xa = yb$ for at least $0.9|A|$ pairs (a, b) in $A \times A$. Therefore $|H| = |A^{-1}A| \leq |A|^2/0.9|A| \leq 1.2|A|$.

To see that $HH \subset H$ we write:

$$\|1_A - 1_{z^{-1}wx^{-1}yA}\|_1 \leq \|1_A - 1_{z^{-1}wA}\|_1 + \|1_{z^{-1}wA} - 1_{z^{-1}wx^{-1}yA}\|_1,$$

we get from (1.1)

$$\|1_A - 1_{z^{-1}wx^{-1}yAA}\|_1 \leq 0.4|A|$$

for every $x, y, z, w \in A$. Hence $HH \subset H$. Hence H is a subgroup and $A \subset Ha$ for all $a \in A$, so $H = A^{-1}A \subset a^{-1}Ha$ and a normalizes H . $\square$

Remark 1.8. The above proof can be pushed with little effort to yield that if $|AA| < \frac{3}{2}|A|$, then $H = AA^{-1} = A^{-1}A$ is a finite subgroup of size $< \frac{3}{2}|A|$ which is normalized by A . This is a theorem of G. Freiman, see [34]. Clearly $3/2$ is sharp, take $A = \{0, 1\} \in \mathbb{Z}$.

Remark 1.9. An immediate consequence of the above lemma is the following general fact: if S is a symmetric generating subset of a finite group G with $|S| \geq \alpha|G|$ for some $\alpha \in (0, 1)$, then $S^n = G$ for some $n \leq O(\log(\frac{1}{\alpha}))$. Indeed $|S^{2^n}| > 1.1^n|S|$ unless $|S^{2^{n-1}}| \geq |G|/1.2 > |G|/2$, in which case $S^{2^n} = G$.

Remark 1.10. One may ask: for which values of $K \geq 1$ is it true that the condition $|AA| \leq K|A|$ implies that A is contained in boundedly many (in terms of K) cosets of a finite subgroup? The answer is: this holds for all $K < 2$. This is due to Yayha Hamidoune. He showed that A is then contained in at most $\frac{1}{2-K}$ cosets of a subgroup of size at most $|A|$. See [49, Prop. 4.1]. Clearly it is sharp because the arithmetic progressions $A := \{0, 1, \dots, N\} \subset \mathbb{Z}$ have $|A + A| \leq 2|A|$.

What if we increase the parameter K beyond the $K = 2$ threshold? The next natural question to ask is: for which values of K is it true that the condition $|AA| \leq K|A|$ implies that A is contained in an extension HL , where H is a finite subgroup normalized by L a d -dimensional arithmetic progression? Clearly such a set has doubling at most 2^d .

However this question is ill-posed, because there are sets of doubling say 2^4 which are not of this form: take a ball S^n of large radius n in the discrete Heisenberg group

$$H_3(\mathbb{Z}) := \left\{ \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}; x, y, z \in \mathbb{Z} \right\}$$

Here 4 is the homogeneous asymptotic dimension of the Heisenberg group, namely $|S^n| \simeq n^4$ up to multiplicative constants, for any given finite generating set S of $H_3(\mathbb{Z})$.

In 2008 Elon Lindenstrauss proposed [60] a general conjectural statement, which was subsequently proved by Ben Green and Terry Tao and the author in [14], and is the main subject of these notes:

Theorem 1.11 (Structure theorem, weak version). *Let G be a group, $K \geq 1$ a parameter and A a finite subset with $|AA| \leq K|A|$. Then there is a coset of a virtually nilpotent subgroup of G which intersects A in a subset of size $\geq |A|/C(K)$.*

Remarks.

a) Here $C(K)$ is a number depending on K only, and not on A nor G .

b) The proof also gives a uniform bound on the nilpotency class and the number of generators of the nilpotent subgroup (both in $O(\log K)$ with an absolute implied constant), although no bound can be expected on the index (e.g. take A a large finite simple group). More precisely we can take the virtually nilpotent group to be a finite-by-nilpotent group, where the nilpotent quotient satisfies $\sum_i d(C^i(N)/C^{(i+1)}(N)) = O(\log K)$, where $(C^i(N))_i$ is the lower central series and $d(\cdot)$ the number of generators.

c) However the proof gives no explicit bound on $C(K)$. The proof is not effective.

d) Stated as above the theorem says nothing about the case when G is finite. And this is enough for a number of geometric applications. However the proof does. We actually show that the virtually nilpotent subgroup can be taken to be finite-by-nilpotent where the finite normal subgroup lies in XA for some X of size $|X| \leq c(K)$ for some constant $c(K)$ depending only on K . We will give a stronger form of the theorem below, which includes this refinement.

e) The theorem had been established earlier by Tao [72] in the special case when G is assumed solvable of bounded derived length.

f) In certain situations, most notably when G is a free group (by the result of Razborov mentioned above) or when $G = GL_n(k)$ for some field k , then pretty good explicit bounds can be found on $C(K)$. For example in [13] it is shown that $C(K) = O(K^{O_n(1)})$ for $G = GL_n(\mathbb{C})$. See also [63, 39] for the positive characteristic situation.

Theorem 1.11 can be seen as a finitary version of Gromov's theorem on groups with polynomial growth. And indeed, as we now show, it easily implies Gromov's theorem.

Theorem 1.12 (Gromov's polynomial growth theorem). *Let $\Gamma := \langle S \rangle$ be a finitely generated group with polynomial growth (i.e. $|S^n| = O(n^D)$ for some $D > 0$ as $n \rightarrow +\infty$). Then Γ is virtually nilpotent.*

Proof that Theorem 1.11 implies Theorem 1.12. Since $|S^n| = O(n^D)$, there must be arbitrarily large n 's for which $|S^{4n}| \leq 5^D |S^n|$. Indeed, suppose not, then $|S^{4n}| > 5^D |S^n|$ for all n large enough, $n \geq n_0$ say, and hence $5^{Dk} |S^{n_0}| < |S^{4^k n_0}| = O(4^{Dk} n_0^D)$ a contradiction for large k .

Pick such an n . By Theorem 1.11 applied to $A := S^n$ and $K = 5^D$, there is a virtually nilpotent subgroup H_n such that S^n has a large intersection with a coset of H_n . In particular $|S^{2n} \cap H_n| \geq |S^n|/C(D) \geq |S^{4n}|/(5^D C(D))$. Theorem 1.12 follows by applying the following lemma with $k = 2n$.

Lemma 1.13. *In a group $\Gamma = \langle S \rangle$ if $|S^k \cap H| > |S^{2k}|/C$ for some subgroup H , some $C > 0$ and some $k \geq C$, then $[\Gamma : H] \leq C$.*

Proof. Look at the Schreier graph of Γ/H . It is connected, so either $S^k H = \Gamma$ or $|S^k H/H| > k$. Write $S^k = \cup_{i=1}^N S^k \cap g_i H$. Clearly $\cup_{i=1}^N (S^k \cap g_i H)(S^k \cap H) \subset S^{2k}$. Hence $N|(S^k \cap H)| \leq |S^{2k}| < C|S^k \cap H|$. And hence $N = |S^k H/H| < C \leq k$. Hence $S^k H = \Gamma$, and $[\Gamma : H] = N < C$. $\square$

Remark 1.14. In fact the above proves slightly more than Gromov's theorem. It shows that given $C, D > 0$ there is $n_0 = n_0(C, D)$ such that if $|S^n| \leq Cn^D$ for some $n \geq n_0$, then Γ is virtually nilpotent. Note that this is stronger than Gromov's own finitary version of his result (discussed at the end of his original paper [44]). He showed (basically just by contradiction) that his theorem implies that there is $n_0 = n_0(C, D)$ such that if $|S^n| \leq Cn^D$ holds for all $n \leq n_0$, then Γ is virtually nilpotent. So the added value here is that we need only one scale, where the doubling property occurs.

We end this lecture by giving the following equivalent form of the main theorem:

Theorem 1.15 (Structure theorem, equivalent form). *Let G be a group, $K \geq 1$ a parameter and A a finite subset with $|AA| \leq K|A|$. Then there is a subset $X \subset G$ such that $|X| \leq C(K)$ and a virtually nilpotent subgroup $\Gamma_0 \leq G$ such that $A \subset X\Gamma_0$.*

The equivalence follows immediately from the following basic combinatorial lemma by taking $B = A \cap \Gamma_0 a$, where $\Gamma_0 a$ is the coset obtained in Theorem 1.11.

Lemma 1.16 (Ruzsa covering lemma). *Suppose A, B are subsets in a group G such that $|AB| \leq K|B|$, then there is a subset $X \subset A$ of size $\leq K$ such that $A \subset XBB^{-1}$.*

Proof. Pick a maximal family of disjoint translates of B of the form $a_i B$ for $a_1, \dots, a_N \in A$. Clearly $N \leq K$. Then for every $a \in A$, aB intersects some $a_i B$ non trivially and hence $a \in a_i B B^{-1}$. Take $X = \{a_1, \dots, a_N\}$. $\square$

2. THE STRUCTURE OF APPROXIMATE GROUPS AND GEOMETRIC APPLICATIONS

In the first lecture, we saw that our structure theorem 1.11 easily implies Gromov's polynomial growth theorem. To provide further motivation for our study of the non-commutative inverse Freiman problem and of approximate groups, we begin this lecture with another geometric application.

2.1. A generalized Margulis lemma. In his book on metric structures on Riemannian and non-Riemannian spaces [45], Gromov discusses among many other things the properties of spaces with a lower curvature bound, in particular the Margulis lemma. The Margulis lemma is an important result in Riemannian geometry and hyperbolic geometry, where it is used for example to give lower bounds on the volume of closed manifolds, and to describe the geometry of cusps. Usually this lemma requires some

curvature bounds on the manifold (see e.g. the books by Buser-Karcher [20] and Burago-Zalgaller [19]). The following result, which was conjectured by Gromov in this book, shows that the lemma holds in much greater generality.

Theorem 2.1 (Generalized Margulis Lemma). *Let X be a metric space and assume that every ball of radius 4 can be covered by at most K balls of radius 1. Now let $\Gamma \leq \text{Isom}(X)$ be a discrete subgroup of isometries of X . Then there is $\varepsilon_0 > 0$ depending on K only and not on X such that for every $x \in X$ the subgroup generated by*

$$S_\varepsilon(x) := \{\gamma \in \Gamma; d(\gamma \cdot x, x) < \varepsilon\}$$

is virtually nilpotent if $\varepsilon < \varepsilon_0$.

The classical Bishop-Gromov inequalities imply that hypotheses of this theorem are fulfilled for example when X is the universal cover of a compact Riemannian n -manifold M with the parameter K depending only on n and the lower bound on the curvature of M , and $\Gamma = \pi_1(M)$.

Note that there is no properness assumption on X . However when we say that Γ is a “discrete group of isometries” we mean that the orbit maps $\Gamma \rightarrow X$, $\gamma \mapsto \gamma \cdot x$ are proper for every x , i.e. inverse images of bounded balls are finite. In fact all we need is that $S_2(x)$ is finite for each x .

Proof. Clearly, from the triangle inequality we have: $S_2(x)^2 \subset S_4(x)$. Let us prove that $|S_2(x)^2| \leq K|S_2(x)|$. Write $B(x, 4) \subset \cup_{i=1}^K B(x_i, 1)$ for a collection of K points $x_i \in X$. If $B(x_i, 1)$ intersects $S_4(x) \cdot x$, then pick $\gamma_i \in S_4(x)$ such that $\gamma_i \cdot x \in B(x_i, 1)$. Now given any $\gamma \in S_4(x)$, $\gamma \cdot x \in B(x_i, 1)$ for some i , hence $d(\gamma \cdot x, \gamma_i \cdot x) \leq 2$. This means that $\gamma_i^{-1}\gamma \in S_2(x)$. Hence we proved $S_4(x) \subset XS_2(x)$ for some set $X \subset \Gamma$ with $|X| \leq K$. In particular $|S_2(x)^2| \leq |S_4(x)| \leq K|S_2(x)|$.

Now we can apply the structure theorem (here Theorem 1.15) to $S_2(x)$ and conclude that there is a virtually nilpotent group Γ_0 such that $S_2(x) \subset X\Gamma_0$ for some finite set X with $|X| \leq C(K)$. Pick an integer n with $C(K) < n < 2C(K)$ and $\varepsilon_0 = \frac{1}{n}$. If $\varepsilon < \varepsilon_0$, then by the triangle inequality $S_\varepsilon(x)^n \subset S_2(x) \subset X\Gamma_0$. But $S_\varepsilon(x)^k\Gamma_0/\Gamma_0$ is a non-decreasing sequence of sets and if for some k $S_\varepsilon(x)^k\Gamma_0/\Gamma_0 = S_\varepsilon(x)^{k+1}\Gamma_0/\Gamma_0$, then the sequence stabilizes and $S_\varepsilon(x)^k\Gamma_0/\Gamma_0 = \langle S_\varepsilon(x) \rangle \Gamma_0/\Gamma_0$. Since $n > |X|$ it follows that $S_\varepsilon(x)^n\Gamma_0/\Gamma_0 = \langle S_\varepsilon(x) \rangle \Gamma_0/\Gamma_0$ and $[\langle S_\varepsilon(x) \rangle : \langle S_\varepsilon(x) \rangle \cap \Gamma_0] \leq n \leq 2C(K)$. Hence $\langle S_\varepsilon(x) \rangle$ is virtually nilpotent. $\square$

Here again the nilpotent subgroup can be taken to have at most $O(\log K)$ generators and be of nilpotency class $O(\log K)$.

The best constant $\varepsilon_0(X)$ is usually called the *Margulis constant* of X .

Yet another application of the structure theorem is the fact, first proved by Gromov, that the fundamental groups of almost flat manifolds are virtually nilpotent. This was later extended by Fukaya-Yamaguchi to almost non-negatively curved manifolds and by Cheeger-Colding and Kapovich-Wilking to Ricci almost non-negatively curved manifolds. We can recover this last result from the structure theorem by a simple application of the Bishop-Gromov volume comparison estimates (see [14])

Theorem 2.2 (Almost non-negatively curved manifolds). *Given d there is $\varepsilon(d) > 0$ such that if M is a Riemannian d -manifold with diameter 1 and Ricci curvature bounded below by $-\varepsilon(d)$, then $\pi_1(M)$ is virtually nilpotent.*

2.2. Approximate groups and the additive combinatorics toolkit. We now return to additive combinatorics and describe a few combinatorial tricks and useful tools that one uses all the time when one deals with sets of small doubling. The first one is the so-called Ruzsa triangle inequality. Given two finite subsets A, B in a group G let

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

Clearly $d(A, B) = d(B, A)$ and $d(A, B) \geq 0$ because $|AB^{-1}| \geq |A|, |B|$. What is remarkable is the following:

Lemma 2.3 (Ruzsa triangle inequality). *Given three finite subsets A, B, C in G , the triangle inequality holds*

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

Hence $d(A, B)$ is called the *Ruzsa distance*¹ between A and B . The proof is very easy:

Proof. Consider the map $AC^{-1} \times B \rightarrow AB^{-1} \times BC^{-1}$, which sends (x, b) to $(a_x b^{-1}, b c_x^{-1})$, 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 $d(A, C) \leq d(A, B) + d(B, C)$. $\square$

As a consequence:

$$\frac{|AA^{-1}|}{|A|} = e^{d(A, A)} \leq e^{d(A, A^{-1}) + d(A^{-1}, A)} = \left(\frac{|AA|}{|A|}\right)^2.$$

Using the triangle inequality one can also prove ([71, 50, 62]):

Lemma 2.4 (Small tripling lemma). *If A is any finite subset in a group G , and $n \geq 3$, then*

$$\frac{|A^n|}{|A|} \leq \left(\frac{|A^3|}{|A|}\right)^{n-2}$$

Dealing with conditions like $|AA| \leq K|A|$, or $|A^{-1}A| \leq K|A|$ can be cumbersome at times and it is easy to run into unessential technical difficulties that hide the real ones. This is why Terry Tao came up with another set of axioms for a subset A , closely related to the small doubling condition, which is much easier to handle. He coined the following definition ([71]):

Definition 2.5 (Approximate subgroup). Let G be a group and $K \geq 1$ a parameter. A subset A of G is called an K -approximate subgroup if

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

Note: this makes sense for A infinite as well. But we will be mainly concerned with finite sets and by abuse of language A will always be assumed finite in the sequel.

¹note that $d(A, B) = 0$ does not imply $A = B$, but only (this is an exercise similar to Proposition 1.6) $A = aH$ and $B = bH$ for some finite subgroup H and some $a, b \in G$.

Clearly a K -approximate subgroup has doubling at most K . The converse is not true of course, but we have the following partial converse:

Proposition 2.6 (Tao 2007 [71]). *Suppose A is a finite subset of an ambient group G such that $|AA| \leq K|A|$. Then there is an $O(K^{O(1)})$ -approximate subgroup H of G such that $A \subset XH \cap HY$ for some subsets X, Y of size at most $O(K^{O(1)})$ and $|H| \leq O(K^{O(1)})|A|$.*

The implied constants in this result are absolute. This proposition essentially reduces the study of large sets of bounded doubling to that of approximate groups. In a similar flavor one shows that if $|A^3| \leq K|A|$, then $(A \cup A^{-1} \cup \{1\})^2$ is a $O(K^{O(1)})$ -approximate subgroup, and that if $|AA| \leq K|A|$, then A has a subset of size $\geq |A|/O(K^{O(1)})$ which has tripling at most $O(K^{O(1)})$.

While the above facts require a bit of thought and are not immediate (see [71]), we can prove here a very easy variant:

Lemma 2.7. *If G is a group and A a subset such that $A = A^{-1}$ and $|A^5| \leq K|A|$, then A^2 is a K -approximate subgroup.*

Proof. Simply apply Ruzsa's covering Lemma 1.16. □

It often happens that group theoretic arguments about finite subgroups of an ambient group can be transferred or adapted to approximate groups. This has been a guiding philosophy in much of our arguments. For example one has:

Lemma 2.8. *Suppose A is a K -approximate subgroup and B an L -approximate subgroup of an ambient group G (A, B not necessarily finite). Then $A^2 \cap B^2$ is a $(KL)^3$ -approximate subgroup of G .*

Proof. Write $A^2 \subset XA$, $B^2 \subset YB$, so that $(A^2 \cap B^2)^2 \subset A^4 \cap B^4 \subset X^3A \cap Y^3B$. But every set of the form $xA \cap yB$ for $x \in X^3$, $y \in Y^3$ is contained in $z_{x,y}(A^2 \cap B^2)$ for some $z_{x,y}$ (pick any $z_{x,y}$ in $xA \cap yB$). So $(A^2 \cap B^2)^2 \subset Z(A^2 \cap B^2)$ for $Z = \{z_{x,y}\}_{x \in X, y \in Y}$ of size $\leq (KL)^3$. □

In particular if H is a subgroup of G and A a K -approximate subgroup, then $A^2 \cap H$ is again a K^3 -approximate subgroup.

2.3. Nilprogressions and Tointon's theorem. The structure theorem (Theorem 1.11) gave the key information about sets with bounded doubling, namely that they have a large intersection with a coset of a virtually nilpotent group. In order to get more precise information on the structure of these sets, or equivalently on the structure of approximate groups, we need to introduce the notion of *nilprogression*. This generalizes to nilpotent groups the d -dimensional arithmetic progressions described above.

First we make the following general definition:

Definition 2.9 (Progression in a general group). Let G be a group and $x_1, \dots, x_r$ be elements in G . Let $L_1, \dots, L_r$ be non-negative integers. The set $P = P(x_1, \dots, x_r; L_1, \dots, L_r)$ of all group elements in G which can be written as a word in the x_i 's and x_i^{-1} 's involving at most L_i letters $x_i^{\pm 1}$ for each $i = 1, \dots, r$ is called a progression of rank r and lengths $\{L_i\}_i$.

For example if $L_1 = \dots = L_r = N$, then $P = P(x_1, \dots, x_r; N, \dots, N)$ is the ball of radius N for the " ℓ^∞ -word metric" with generating set $S := \{x_1^{\pm 1}, \dots, x_r^{\pm 1}\}$, which we denote by d_S^∞ . Note that this is

closely related to the usual word metric d_S (or ℓ^1 -word metric), because obviously $d_S^\infty \leq d_S \leq rd_S^\infty$.

Similarly we define:

Definition 2.10 (Nilprogression). A progression $P(x_1, \dots, x_r; N, \dots, N)$ is said to be a nilprogression with step $\leq s$ and rank $\leq r$ if the x_i 's generate a nilpotent group with nilpotency class $\leq s$.

and:

Definition 2.11 (Coset nilprogression). A coset nilprogression is the inverse image of a nilprogression by a group homomorphism with finite kernel.

Side remark: the ball-box principle (see [46]) regarding word balls in nilpotent groups (i.e. that they are sandwiched in between two “nilpotent boxes” of comparable size) remains valid for nilprogressions. This and some routine nilpotent algebra yields:

Proposition 2.12. *There is $K = K(r, s) > 0$ such that every coset nilprogression of rank $\leq r$, step $\leq s$ and large enough side length (i.e. $L_i \geq C(r, s)$ for some constant $C(r, s) > 0$) is a K -approximate subgroup.*

For the proof, see either [73, Prop. 2.2.3] or [16, Cor. 3.6]. Following previous work of Green-Ruzsa [43] on the abelian case, Green and the author [12] on torsion-free nilpotent groups, and Tao [71] on 2-step groups, M. Tointon recently generalized the Freiman-Ruzsa-Chang theorem (Theorem 1.2) to an arbitrary nilpotent group. Using a clever lifting of approximate subgroups and induction on nilpotency class he proved:

Theorem 2.13 (Tointon's theorem [75]). *Let A be a K -approximate subgroup of a nilpotent group G with nilpotency class s . Then there is a coset nilprogression P with rank $\leq r = O_s(K^{C(s)})$ and step $\leq s$ such that $A \subset P \subset XA$ for some $X \subset G$ of size $|X| \leq O_s(K^{C(s)})$.*

2.4. Stronger form of the structure theorem. We now are in a position to state the stronger form of our structure theorem.

Theorem 2.14 (BGT strong form). *Suppose A is a K -approximate subgroup in an ambient group G . Then $A \subset XP$, where $X \subset G$ has size $|X| \leq C(K)$ and P is a coset nilprogression whose rank and step are bounded in terms of K only and such that $|P|/|A|$ is bounded in terms of K only.*

Remarks:

a) Here again $C(K)$ is some constant depending only on K , but the proof gives no explicit estimate in terms of K . It can in fact be shown that $C(K)$ is not upper-bounded by K^C for some absolute constant $C > 0$. See [16] for an example.

b) Below we derive the above strong form from the weak form given earlier in Theorem 1.15 using Tointon's theorem. Originally in [14] we proved the strong form directly (thus obtaining as a by-product a new proof of the original abelian Freiman-Ruzsa theorem) and obtained explicit bounds for the rank and step of the nilprogression and its size as well, but not on the constant $C(K)$. In fact we show in [14] that one can find a coset nilprogression P as in Theorem 2.14 with $P \subset A^{12}$ (and hence $|P| \leq K^{11}|A|$) whose rank and step are $O(K^3)$.

Proof. From the weak form of the structure theorem, more precisely Theorem 1.15, we can find a virtually nilpotent subgroup $\Gamma_0 \leq G$ such that $A \subset X\Gamma_0$ for some subset X of size $|X| \leq C(K)$. So $|A^2 \cap \Gamma_0| \geq$

$|A|/C(K)$. In fact (see Remark d) after Theorem 1.11) the proof shows that Γ_0 fits into an exact sequence $1 \rightarrow N \rightarrow \Gamma_0 \xrightarrow{\pi} L \rightarrow 1$, where L is nilpotent with bounded rank and step, and N is finite with $N \subset XA$ for some bounded set X , $|X| \leq c(K)$. By Lemma 2.8 $A^2 \cap \Gamma_0$ is a K^3 -approximate subgroup. Then $\pi(A^2 \cap \Gamma_0)$ is a K^3 -approximate subgroup of L and Tointon's theorem applies: there is a coset nilprogression Q with bounded rank and step which contains $\pi(A^2 \cap \Gamma_0)$ and is contained in boundedly many translates of $\pi(A^2 \cap \Gamma_0)$. Set $P = \pi^{-1}(Q)$. This is again a coset nilprogression with bounded rank and step. It contains $A^2 \cap \Gamma_0$, so by Ruzsa covering (Lemma 1.16) A lies in XP for some bounded X . Moreover, P is contained in boundedly many translates of A , because N is. $\square$

We now give an interesting consequence of the strong form of the theorem and in the last lecture, we will give two geometric applications, one to Cayley graphs of finite simple groups, the other to scaling limits of vertex transitive graphs, that both require this strong form.

Suppose

$$P = P(x_1, \dots, x_r; L_1, \dots, L_r)$$

is a nilprogression of rank r and step s , then for every $n \in \mathbb{N}$ the power set P^n is obviously contained in $P(x_1, \dots, x_r; nL_1, \dots, nL_r)$. Using some nilpotent algebra it can be shown (by arguments similar to those in the proof of Proposition 2.12) that if the L_i 's are large enough, it also contains $P(x_1, \dots, x_r; \frac{n}{C}L_1, \dots, \frac{n}{C}L_r)$ for some $C = C(r, s) > 0$ and that the three sets are of comparable size up to multiplicative constants depending only on r and s . In particular $|P^{2n}| \leq K|P^n|$ for some constant $K = K(r, s)$ independent of the L_i 's and independent of n . So the bound on the doubling P is inherited to all powers P^n . From this observation (proved in detail in [16]) and the strong form of the theorem it is then an exercise (similar to the derivation of Theorem 1.12 from Theorem 1.11) to derive:

Theorem 2.15 (doubling at one scale $\Rightarrow$ doubling at all scales, [16]). *Given $K > 0$ there is $n_0, C(K) > 0$ such that if S is a finite subset of a group G such that S^{n_1} is a K -approximate subgroup for some $n_1 > n_0$, then S^n is a $C(K)$ -approximate subgroup for every $n \geq n_1$.*

3. HILBERT'S FIFTH PROBLEM AND APPROXIMATE GROUPS

In this third lecture, we outline the proof of the structure theorem (Theorem 1.11). A good deal of this lecture is devoted to explaining the key step of the Gleason-Yamabe theorem on the structure theory of locally compact groups.

3.1. Introduction. Approximate subgroups of specific groups (such as linear groups, free groups, finite simple groups, etc...) had been studied by various authors relying on techniques specific to the given class of groups they were considering, often yielding explicit bounds. But no approach to tackle the general problem of understanding the structure of approximate subgroups of arbitrary groups existed prior to the work of Hrushovski [54].

In his paper [54], Hrushovski proposed an approach based on an analogy between this question and various problems and results from Stability Theory, a branch of Model Theory. His theorem, which we state below in a form that avoids the language of model theory, is the first step of the proof. For readers interested in the connection with model theory, we recommend van den Dries' Bourbaki report [29] as well as Hrushovski's own lecture notes.

Combined with the Gleason-Yamabe structure theorem for locally compact groups (Hilbert 5th problem) Hrushovski's theorem already gives non trivial information on the structure of an arbitrary approximate group. Roughly speaking Hrushovski derives from it a weaker structure theorem than Theorem

1.11 in which approximate groups are showed to admit a nested sequence $S_{n+1}^2 \subset S_n$ of large approximate subgroups S_n of A , which exhibits the following weak form of nilpotence: $[S_n, S_n] \subset S_{n+1}$, see [54, Theorem 1.1].

In order to obtain the finer structure given by our Theorem 1.11, one has to go inside the proof of the Gleason-Yamabe theorem and adapt arguments discovered there, more than sixty years ago, in the context of topological groups to the setting of approximate groups.

Going through the proof of the Gleason-Yamabe theorem in the original papers of Gleason and of Yamabe or in the subsequent exposition in the book by Montgomery and Zippin can be daunting. Nevertheless the task has been greatly eased by a number of people over the years, including I. Kaplansky [56] and especially J. Hirschfeld [53] who identified and formulated the key claims (the Gleason-Yamabe lemmas) and gave a much streamlined treatment of the proof using ultra-products (recently simplified further by model theorists L. van den Dries and I. Goldbring in a forthcoming article [28]). The whole thing is now pretty demystified, and a clear and complete modern treatment is now available in Tao's book [73].

3.2. Proof strategy. We turn to the proof of the structure theorem. As in Gromov's proof of his theorem [44] on groups with polynomial growth, one needs to pass from a discrete object (in our case a finite approximate group) to an infinite object on which we can perform analysis. While Gromov used his notion of Gromov-Hausdorff convergence to define his limit space (i.e. the asymptotic cone = the Cayley graph viewed from infinity) van den Dries and Wilkie [27] later suggested to construct this space using ultra-filters. We will follow the same route and start with a non-principal ultrafilter $\mathcal{U}$ on the set of positive integers.

Fix $K \geq 1$. Given any family of groups G_n and a family of finite K -approximate subgroups $A_n \leq G_n$, we form the ultra-product:

$$\mathbb{A} := \prod_{\mathcal{U}} A_n, \quad \mathbb{G} := \prod_{\mathcal{U}} G_n.$$

The first observation is that $\mathbb{A}$ is a K -approximate subgroup of $\mathbb{G}$. Indeed the ultra-product of a sequence of sets of cardinal at most K has cardinal at most K . We call such a set $\mathbb{A}$ an *ultra approximate group*.

The proof has essentially three main steps:

Step 1 : Build a topology.

Step 2 : Adapt the Gleason-Yamabe lemmas.

Step 3 : Conclude.

Step 1: This step is due to Hrushovski [54]. While Gromov started with a sequence of metric spaces (Cayley graphs), we do not have any distance given a priori with our sequence of sets A_n . So the first goal here is to define a notion of closeness or nearness for elements of A . One would like to say that an element g is close to the identity if the symmetric difference $gA\Delta A$ is very small in size. While this does not quite work on the nose, a variation of this idea can be implemented successfully. This "distance" being defined for each A_n , it passes to the ultra-product to give rise to a genuine left invariant pseudo-distance $d(\cdot, \cdot)$ on the group $\langle \mathbb{A} \rangle$. One then shows that $G := \langle \mathbb{A} \rangle / \{\mathfrak{a}; d(\mathfrak{a}, 1) = 0\}$ is a locally compact second countable group.

Step 2: This part consists in adapting the Gleason-Yamabe lemmas from locally compact groups to approximate groups. The Gleason-Yamabe lemmas lie at the heart of the proof of the structure theorem for locally compact groups proved by Gleason and Yamabe in the early 1950's. According to this theorem, every locally compact group has an open subgroup which is a projective limit of Lie groups, i.e. has arbitrarily small normal compact subgroups modulo which it is a Lie group with a finite number of connected components. The Gleason-Yamabe lemmas serve two purposes in the proof: they allow to reduce to the NSS case (NSS= no small subgroups) and to show that the set of one-parameter subgroups of an NSS group is a vector space, thus giving rise to a Lie algebra and a Lie structure. It turns out that under some assumptions on the finite approximate group A (which are anyway satisfied by a large approximate subgroup of A as follows from Step 1), these lemmas can be adapted almost word for word to A and yield a finite subgroup H of $\langle A \rangle$ contained in A and normalized by A , together with an element $a \in A \setminus H$ which commutes with A modulo H . This element will serve as a stem from which to build the nilprogression.

Step 3: Performing Step 2 for each A_n , we obtain an ultra finite subgroup $\mathbb{H} := \prod_{\mathcal{U}} H_n \triangleleft \langle \mathbb{A} \rangle$ and an ultra cyclic subgroup $\langle \mathfrak{a} \rangle \leq \langle \mathbb{A} \rangle$, where $\mathfrak{a}$ is the class of $(a_n)_n$. By Step 1 and the structure theorem for locally compact groups, we may assume after passing to an open subgroup that G is a projective limit of Lie groups. Modding out by the maximal normal compact subgroup of G , we obtain a connected Lie group L . If $\dim L = 0$, then $\mathbb{A}$ is covered by finitely many translates of a compact open subgroup and this means A_n is covered by boundedly many translates of a finite subgroup for $\mathcal{U}$ -almost every n . If $\dim L > 0$, the projection of $\langle \mathfrak{a} \rangle$ to L is a central one-parameter subgroup. The rest of the proof proceeds by induction on $\dim L$, modding out $\langle \mathbb{A} \rangle$ by $\langle \mathfrak{a} \rangle$ and starting all over again. A careful treatment of this step requires the introduction of *local groups*². At the end we obtain that the A_n 's are covered by boundedly many translates of a finite-by-nilpotent subgroup, the finite part being itself contained in boundedly many translates of A_n . The theorem then follows by contradiction, picking a sequence of potential counter-examples A_n to the statement of the theorem and carefully negating the quantifiers.

N.B. In Gromov's theorem the induction in the final step is done on the exponent of polynomial growth. In his paper [54], Hrushovski also gave another proof of Gromov's theorem and even a strengthening of it (which is now a simple consequence of Theorem 1.11) using induction on $\dim L$ as in Step 3 above. The novelty of [14], say compared to [54], consists mainly in Step 2.

Below we describe Step 1 and Step 2 and refer the reader to the original paper for Step 3, whose details are a bit more technical.

3.3. Building a locally compact topology (Step 1). The goal here is to define a non-trivial topology on $\langle \mathbb{A} \rangle$ which, when a certain normal subgroup is quotiented out, turns $\langle \mathbb{A} \rangle$ into a locally compact group. We need to define a base of neighborhoods of the identity. The main tool for this is the following lemma:

Lemma 3.1 (Sanders [69], Crooot-Sisask [24], Hrushovski [54]). *If A is a K -approximate group and $k \geq 1$, then there is $S \subset A^4$ such that*

- $1 \in S$, $S = S^{-1}$,
- $S^k \subset A^4$,

²they can be avoided if one only shoots for Theorem 1.11, see the proof in [29], but seem necessary for the finer structure described in Remark d) after Theorem 1.11, and hence for the strong form Theorem 2.14.

- $|S| \geq |A|/C(K, k)$

In other words, this lemma allows to take a “square root”, or k -th root, of any given approximate group. The lemma was proved independently by Sanders using a combinatorial argument (showing the existence of a subset $B \subset A$ such that there is a non-trivial proportion of elements $g \in A^4$ such that $|gAB\Delta AB|$ is at most $\frac{1}{k}|AB|$ say), by Croot-Sisask (who use the probabilistic method to find the subset S) and by Hrushovski (using tools from Model Theory).

Using this lemma, we can define a base of neighborhoods of the identity in $\langle \mathbb{A} \rangle$ as follows. For each A_n and each $k \geq 1$ pick a subset $S_{n,k}$ as given by the above lemma. In fact a rather straightforward strengthening of the above lemma ensures that we can pick $S_{n,k}$ in such a way that $S_{n,k+1}^2 \subset S_{n,k}$ and $gS_{n,k+1}g^{-1} \in S_{n,k}$ for all $g \in A$.

Set $\mathbb{S}_k := \prod_{\mathcal{U}} S_{n,k}$. This defines a topology on $\langle \mathbb{A} \rangle$ with the $\mathbb{S}_k$ as a base of neighborhoods of the identity. Moreover the intersection $\Gamma := \bigcap_{k \geq 1} \mathbb{S}_k$, where $\mathbb{S}_k := \prod_{\mathcal{U}} S_{n,k}$ is a normal subgroup of $\langle \mathbb{A} \rangle$. We define G as the quotient of $\langle \mathbb{A}^4 \rangle / \Gamma$. In this topology $\mathbb{A} \bmod \Gamma$ is a compact neighborhood of the identity.

Given a Hausdorff topological group with a nested sequence of symmetric neighborhoods of the identity $S_{i+1}^2 \subset S_i$ a classical construction of Birkhoff and Kakutani [6, 61] yields a left invariant distance compatible with the topology (in which the S_i are essentially the balls of radius $\frac{1}{2^i}$ around the identity). We can do this here with the $\mathbb{S}_k$'s and obtain a left invariant distance d on G .

Then the local compactness of G is proven in the usual way by establishing completeness with respect to d and total boundedness (i.e. $\forall 0 < \varepsilon < r$ every ball of radius r can be covered by $\leq C(\varepsilon, r)$ balls of radius ε). This follows from the Ruzsa covering lemma. Completeness follows by the countable saturation property of ultrafilters.

In the Birkhoff-Kakutani construction of the left invariant distance d , balls can be approximated by finite products of the S_i 's. Since the $\mathbb{S}_k$'s are ultra-product sets, i.e. given by the ultra-product of subsets of A_n , we obtain that balls in G , and more generally any compact subset of G , can be approximated by ultra-product sets.

We summarize the above discussion in the following statement:

Theorem 3.2. (*Hrushovski local model theorem*, [54, Theorem 4.2.]) *There exists a locally compact group G and a group homomorphism*

$$\pi : \langle \mathbb{A} \rangle \rightarrow G$$

such that $\pi(\mathbb{A})$ is a compact neighborhood of the identity in G , and for every $F \subset O \subset \pi(\mathbb{A}^4)$ with F closed and O open subsets, there are $B_n \subset A_n^4$ such that

$$\pi^{-1}(F) \subset \mathbb{B} \subset \pi^{-1}(O),$$

where $\mathbb{B} := \prod_{\mathcal{U}} B_n$.

Remarks.

a) If G is the trivial group, then the theorem implies that the A_n 's are finite groups for almost all indices n w.r.t the ultrafilter $\mathcal{U}$. Indeed take $O = F = \{1\}$. Then according to the theorem there is

$\mathbb{B} = \prod_{\mathcal{U}} B_n \subset \mathbb{A}$ such that $B = \ker \pi = \langle A \rangle$. Thus $\mathbb{A}$ is stable under multiplication. Hence so are the A_n for $\mathcal{U}$ -almost every n .

b) Similarly if the “model group” G is totally disconnected, then we can conclude that there is a finite group $H_n \subset A_n^C$ for some bounded C such that A_n is contained in boundedly translates of H_n (exercise: this implies that H_n and A_n^2 are commensurable). Indeed a totally disconnected locally compact group contains an open compact subgroup (van Dantzig). According to the theorem it must be an ultra-product set $\mathbb{H} := \prod_{\mathcal{U}} H_n$ and the H_n must be stable under multiplication for $\mathcal{U}$ -almost every n , i.e. be finite subgroups. Since $\mathbb{A}$ is compact in projection to G , it must be finitely covered by $\mathbb{H}$.

c) Recall the Gleason-Yamabe structure theorem for locally compact groups:

Theorem 3.3 (Gleason-Yamabe [40, 80]). *If G is a locally compact group, then G has an open subgroup G' which is a “generalized Lie group” in the sense that every identity neighborhood contains a compact subgroup $H \triangleleft G'$ such that G'/H is a Lie group with finitely many connected components.*

N.B. If G is compact, the above boils down to the Peter-Weyl theorem (which is itself an application of the spectral theorem for self-adjoint convolution operators acting on $L^2(G)$). It is worth noting that the proof of Theorem 3.3 for non-compact groups is not independent of the Peter-Weyl theorem as it makes use of it in the crucial reduction step to the NSS (No Small Subgroup) case.

A consequence of this is that attached to every non-compact locally compact group there is a canonically defined non-compact connected Lie group L with no non-trivial compact normal subgroups. Indeed L is the connected component of the identity of G'/H modulo its maximal normal compact subgroup. Its isomorphism class is independent of G' and H . The connected component G^0 is compact if and only if L is trivial.

In the setting of Theorem 3.2, we call L the *Hrushovski Lie group* associated to the A_n 's. If it is trivial, then the A_n^2 are commensurable to finite groups (this is Remark b) above). In order to understand what happens if L is non-trivial, we need to go into the proof of the Gleason-Yamabe theorem. This is the aim of Step 2. At the end (Step 3) we establish that L is a simply connected nilpotent Lie group.

3.4. The Gleason-Yamabe theorem. Let us digress for a little while and discuss the proof of the Gleason-Yamabe structure theorem for locally compact groups (Theorem 3.3). At the heart of it lie the so-called Gleason-Yamabe lemmas (Lemmas 3.4 and 3.6 below). They serve a dual purpose:

- (1) reduce the structure theorem to the NSS case (i.e. the case when G has an identity neighborhood with no non-trivial subgroup).
- (2) show that if G is NSS, the set of one-parameter subgroups (i.e. homomorphisms from $(\mathbb{R}, +)$ to G) forms a vector space, thus giving rise to the sought-after Lie algebra and Lie group structure.

Historically, Gleason [40] used a construction closely related to Lemma 3.6 below to prove Theorem 3.3 in the case of NSS connected locally compact groups of finite topological dimension. It was Yamabe [79, 80] who first understood how to deal with the general (non NSS) case by reducing it to the Peter-Weyl theorem using a variant of Gleason's argument (encapsulated in Lemma 3.4). We stress that there are two important cases in which the theorem is much easier to prove: the compact case (Peter-Weyl), and the totally disconnected case (van Dantzig).

Suppose G is a locally compact group and pick a compact identity neighborhood V in G . Given a subset $Q \subset V$, let $n_V(Q)$ be the largest integer such that $1, Q, \dots, Q^{n-1}$ are all contained in V . Clearly $n_V(Q) > 1$ iff $Q \subset V$, and $n_V(Q) = +\infty$ iff the subgroup $\langle Q \rangle$ lies in V entirely. Set $n_V(g) = n_V(\{g\})$.

Lemma 3.4 (Gleason-Yamabe 1). *There is $C = C_V > 0$ such that for every $K \geq 1$, there is an identity neighborhood $U \subset V$, such that for every subset $Q \subset U$,*

- *either $n_{V^4}(Q) \geq Kn_V(Q)$,*
- *or there is $g \in Q$ such that $n_U(g) \leq KC_V n_V(Q)$.*

In other words, unless it takes a very long time for powers of Q to venture outside of V^4 after they first pop out of V , the time it takes for powers of Q to escape V is comparable to the maximal time needed for powers of individual members of Q to escape U .

A direct consequence of this is:

Corollary 3.5 (subgroup trapping). *Let G be a locally compact group. For every identity neighborhood V in G , there is an identity neighborhood $U \subset V$ such that the subgroup H generated by all subgroups contained in U is contained in V .*

Proof. Take for Q the union of all subgroups contained in U and apply Lemma 3.4. □

Proof of Theorem 3.3 : reduction to the NSS case. We claim that there exists an open subgroup G' in G and, for each compact neighbourhood V of the identity in G' , a normal subgroup $N' \triangleleft G'$ such that $N' \subset V$ and such that G'/N' is NSS. This is clearly sufficient to reduce Theorem 3.3 to the NSS case.

Up to passing to an open subgroup, we may assume that G is almost connected, in the sense that its connected component of the identity is co-compact. Van Dantzig's theorem ensures that this is possible: indeed, every totally disconnected locally compact group has an open compact subgroup, so the pre-image in G of a compact open subgroup of G/G^0 , where G^0 is the connected component of G , is an almost connected open subgroup of G .

Let V be a compact neighborhood of the identity in G . By Corollary 3.5, there is an open neighborhood of the identity $U \subset V$ such that the closure H of the subgroup generated by all subgroups contained in U is contained in V . Since H is a compact group, we may apply the Peter-Weyl theorem to it. In particular, we may find a closed normal subgroup $N \triangleleft H$ contained in U such that H/N is NSS. This means that there is an open neighborhood of the identity W_0 in G containing N such that every subgroup of H containing N and contained in W_0 is in fact a subgroup of N . We can pick a smaller identity neighborhood W of G , which contains N , and is such that $W^4 \subset W_0$. Then we see that every subgroup of H contained in W^3 must lie in N , and in particular $gNg^{-1} \subset N$ for every $g \in W$, because gNg^{-1} lies in $W^3 \subset U$ so gNg^{-1} is indeed a subgroup of H . This means that N is normalised by $\langle W \rangle$ and that $\langle W \rangle/N$ is NSS.

However $\langle W \rangle$ is an open subgroup of the almost connected group G . Hence it has finite index in G (it contains the connected component G^0 and is open modulo G^0 in the profinite group G/G^0). Thus there are only finitely many conjugates $g_i N g_i^{-1}$ of N in G . So $N' := \cap g_i N g_i^{-1}$ is normal in G and contained in the neighborhood of the identity $W' := \cap g_i W g_i^{-1}$. Moreover any subgroup contained in W' is contained in N' , so G/N' is NSS. □

Proof of Corollary 3.5. We now derive Corollary 3.5 from Lemma 3.4. This uses Peter-Weyl's theorem one more time. Let $B(t)$ be the closed ball of radius t around the identity (for a fixed left invariant distance), let Q_t be the union of all subgroups contained in $B(t)$. Fix $s > 0$. For $t < s$, $Q_t \subset B(s)$, and $n_{B(s)}(g) = +\infty$ for $g \in Q_t$. So Lemma 3.4 implies that either $n_{B(s)}(Q_t) = +\infty$ in which case $\langle Q_t \rangle$ is relatively compact

and we are done, or $\frac{n_{B(4s)}(Q_t)}{n_{B(s)}(Q_t)}$ is unbounded as $t \rightarrow 0$. This implies that $Q_t^{n_{B(s)}(Q_t)}$ converges along a sequence of $t \rightarrow 0$ towards a compact subgroup $H_s \subset B(4s)$ not contained in $B(s/2)$. By diagonal process we obtain this way a nested family of groups $H_s \leq H_{s'}$ if $s \leq s'$. But by Peter-Weyl, since H_1 is compact, it has a closed normal subgroup N_1 such that H_1/N_1 is NSS. Now doing the above construction with $B(s)N_1$ in place of $B(s)$ we obtain a nested family of subgroups $H'_s \subset (B(s)N_1)^4 \cap H_1 \subset B(4s)N_1 \cap H_1$ such that H'_s is not contained in $B(s/2)N_1$. This contradicts the fact that H_1/N_1 is NSS. $\square$

We now pass to the second part of the Gleason-Yamabe lemmas and thus assume that G is NSS. It is then easy to see (arguing by contradiction and taking a limit) that n_U and n_V are comparable if U and V are any two small enough identity neighborhoods, i.e.

$$\frac{1}{C}n_U(Q) \leq n_V(Q) \leq Cn_U(Q) \quad (3.1)$$

for some $C = C(U, V) > 0$ and all subsets Q . We then define for $g \in G$

$$\|g\|_U := \frac{1}{n_U(g)},$$

and call it the *escape norm* associated to U .

Lemma 3.6 (Gleason-Yamabe 2). *Suppose G is a locally compact group which is NSS and V is a neighborhood of the identity. Then V contains a compact identity neighborhood U such that, for some $C = C_U > 0$, and all $g, h \in U$,*

- (1) $\|h^{-1}gh\|_U \leq C\|g\|_U$
- (2) $\|gh\|_U \leq C(\|g\|_U + \|h\|_U)$
- (3) $\|[g, h]\|_U \leq C\|g\|_U \cdot \|h\|_U$

Item 1) is clear from the definition and (3.1). Item 2) is an immediate consequence of the first Gleason-Yamabe lemma, i.e. Lemma 3.4, and of (3.1) (take $Q = \{g, h\}$). Item 3) can be proved by an argument similar that used in the proof of Lemma 3.4 (see below).

Lemma 3.6 is used to prove that the set $L(G)$ of one-parameter subgroups of G forms a vector space on which (an open subgroup of) G acts by conjugation with central kernel. From this point the end of the proof of Theorem 3.3 is fairly standard: one shows that $L(G)$ is locally compact, hence finite dimensional, thus (an open subgroup of) G embeds in $\mathrm{GL}(\mathbb{R}^n)$ modulo the center and one concludes by the Cartan-von-Neumann theorems that G is a Lie group.

The NSS assumption easily implies (taking the cyclic group generated by group elements closer and closer to the identity and passing to a limit) that $L(G)$ is non-trivial. In order to prove that $L(G)$ is a vector space, one needs to make sense of the formula:

$$\lim_{n \rightarrow +\infty} \left(X\left(\frac{t}{n}\right)Y\left(\frac{t}{n}\right) \right)^n = (X + Y)(t)$$

given two one-parameter subgroups $X, Y \in L(G)$. This is where Item 2) of Lemma 3.6 comes into play, because it allows to conclude that $(X(\frac{t}{n})Y(\frac{t}{n}))^n$ remains in a fixed compact part of G when n tends to $+\infty$ and t remains bounded. In fact, using Item 3), i.e. the commutator shrinking property, one shows that this is a Cauchy sequence (NSS groups are metrisable) and hence converges.

Finally, using Item 3) again, one proves that every small enough element of G lies on a one-parameter subgroup. Then after passing to an open subgroup of G , we see that the kernel of the adjoint representation is central. This concludes the proof of Theorem 3.3.

The proof of the Gleason-Yamabe lemmas. Having explained how the Gleason-Yamabe theorem is derived from the Gleason-Yamabe lemmas, let us now say a few words about the proof of the lemmas themselves. As said earlier Items 1) and 2) follow easily from the NSS condition and Lemma 3.4, so we are left with proving Lemma 3.4 and Item 3) of Lemma 3.6.

Before we start, it is instructive to notice that if G were a Lie group, then both statements would be easy to prove using the exponential map $\exp : L(G) \rightarrow G$, as $\|\exp(X)\|_U$ is then comparable to $\|X\|$ for any fixed norm on $L(G)$. But we are precisely trying to establish the existence of an exponential map...

We now focus on Lemma 3.4. There are two bright ideas involved here: the first, say in the setting of Lemma 3.4, is to introduce a continuous non-negative bump function ϕ , which vanishes outside V^4 and is equal to 1 at the identity, and compare $\|g\|_U$ to the sup norm $\|\partial_g \phi\|_\infty$, where $\partial_g \phi(x) := \phi(g^{-1}x) - \phi(x)$. We make the following simple observations:

- (1) We have the triangle inequality $\|\partial_{gh} \phi\|_\infty \leq \|\partial_g \phi\|_\infty + \|\partial_h \phi\|_\infty$,
- (2) If $\|\partial_g \phi\|_\infty < 1$, then $g \in \text{Supp}(\phi) \subset V^4$.

from which it follows immediately that $\|g\|_V \leq \|\partial_g \phi\|_\infty$. We cannot expect that an inequality in the other direction holds for all g , because that would imply that ϕ is invariant under every subgroup contained in V . But, for every $K \geq 1$ we will find U small enough and build a function ϕ (depending on K, V) supported in V^4 , such that $\phi(1) = 1$, and for which the following inequality holds for all $Q \subset U$, all $g \in Q$, and some $C_V > 0$

$$\|\partial_g \phi\|_\infty \leq C_V \frac{1}{n_U(g)} + \frac{1}{2K} \cdot \frac{1}{n_V(Q)}. \quad (3.2)$$

Lemma 3.4 follows easily. Indeed, by definition of $n_{V^4}(Q)$ there is a word w of length $n_V(Q)$ with letters in Q such that $w \notin V^4$. Hence $\|\partial_w \phi\|_\infty \geq 1$ by (2) above, and by the triangle inequality (1) there must be $g \in Q$ such that $\|\partial_g \phi\|_\infty \geq \frac{1}{n_{V^4}(Q)}$. Suppose $n_{V^4}(Q) \leq K n_V(Q)$, then we conclude from (3.2) that $n_U(g) \leq K C_V n_V(Q)$ as desired.

So things boil down to finding ϕ such that (3.2) holds. If we were on a Lie group and ϕ were say of class C^2 , because the second derivatives are controlled, we would have $\partial_{g^n} \phi \simeq n \partial_g \phi$ as long as $g^n \in U$ if U is small enough. This follows immediately from the Taylor expansion of ϕ near the identity, or from the following abstract form of the Taylor formula, which always holds (direct check):

$$\partial_{g^n} \phi = n \partial_g \phi + \sum_{i=0}^{n-1} \partial_{g^i} \partial_g \phi \quad (3.3)$$

The second term in the right hand side would then be negligible and it would follow that $\|\partial_g \phi\|_\infty \leq C \|g\|_U$, which is a strong form of (3.2).

This is where the second bright idea comes in: making use of a (left-) Haar measure, we can define ϕ as the convolution of two bump functions $\phi(x) := \frac{\psi_1 * \psi_2(x)}{\psi_1 * \psi_2(1)}$, where $\psi_1 * \psi_2(x) = \int \psi_1(xy) \psi_2(y^{-1}) dy$. The following simple formula allows to control the second derivatives of ϕ in terms of the first derivatives of ψ_1 and ψ_2 :

$$\partial_h \partial_g (\psi_1 * \psi_2) = \int (\partial_g \psi_1)(y) \cdot (\partial_{hy} \psi_2)(y^{-1}x) dy.$$

where $h^y = y^{-1}hy$. We take

$$\psi_1(x) := (1 - \frac{1}{n_V(Q)} \inf\{n \geq 0, x \in Q^n V\})^+$$

and

$$\psi_2(x) := (1 - \frac{1}{L} \inf\{n \geq 0, x \in W^n V\})^+,$$

where $y^+ := \max\{0, y\}$ and W is an identity neighborhood such that $W^L \subset V$ for some integer $L > 2K \text{vol}(V^3)/\text{vol}(V \cap V^{-1})$.

It is clear that ψ_1 and ψ_2 are equal to 1 on V and their supports are contained in V^2 . Hence the support of ϕ lies in V^4 , $\|\psi_1 * \psi_2\| \leq \text{vol}(V^2)$ and $\psi_1 * \psi_2(1) \geq \text{vol}(V \cap V^{-1})$. Hence

$$\|\phi\| \leq \frac{\text{vol}(V^2)}{\text{vol}(V \cap V^{-1})}$$

We also have Lipschitz control on both ψ_1 and ψ_2 , because if $g \in Q$, then $\|\partial_g \psi_1\| \leq \frac{1}{n_V(Q)}$, while if $h \in W$, then $\|\partial_h \psi_2\| \leq \frac{1}{L}$. Moreover if $g \in V$, then the support of $\partial_g \psi_1$ is contained in V^3 .

Setting $U = \cap_{y \in V^3} y^{-1}Wy$, we conclude that for all $g \in Q$ and $h \in U$:

$$\|\partial_h \partial_g (\psi_1 * \psi_2)\| \leq \text{vol}(V^3) \frac{1}{n_V(Q)} \frac{1}{L}. \quad (3.4)$$

Finally plugging (3.4) into the Taylor formula (3.3), and writing $\|\partial_{g^n} \phi\| \leq 2\|\phi\|$, we get that as long as $g^i \in U$ for all $i = 0, \dots, n$,

$$\|\partial_g \phi\| \leq \frac{\|\partial_{g^n} \phi\|}{n} + \sum_{i=0}^{n-1} \|\partial_{g^i} \partial_g \phi\| \leq C_V \frac{1}{n} + \frac{\text{vol}(V^3)}{\text{vol}(V \cap V^{-1})} \frac{1}{n_V(Q)} \frac{1}{L} \leq C_V \frac{1}{n} + \frac{1}{2Kn_V(Q)}$$

since $L > 2K \text{vol}(V^3)/\text{vol}(V \cap V^{-1})$, and where $C_V = 2 \frac{\text{vol}(V^2)}{\text{vol}(V \cap V^{-1})}$. We thus obtain (3.2) and we are done.

This concludes the proof of Lemma 3.4. The proof of the commutator shrinking property, Item 3) of Lemma 3.6, is similar and we do not include it here. We also leave out the details of the remainder of the proof of Theorem 3.3, namely the proof that the set of one-parameter subgroups is finite dimensional space on which G acts with central kernel. We refer the reader to Tao's book [73] for these missing items.

3.5. The Gleason-Yamabe lemmas for approximate groups (Step 2). We now return to our main theorem (Theorems 1.11 and 2.14) and to the second step of its proof. Here the intent is to adapt the Gleason-Yamabe lemmas to the setting of approximate groups. In much the same way as these lemmas were used in the locally compact setting to exhibit a small normal subgroup modulo which the group is Lie, the adaptation of the Gleason-Yamabe lemmas to the approximate group setting will yield a finite normal subgroup modulo which the approximate group centralizes a non-trivial subgroup.

Given g , let $n_A(g)$ be the largest integer such that $1, g, \dots, g^n$ belong to A .

In order to implement the Gleason-Yamabe lemmas in the approximate group setting, we need an assumption on the approximate group.

Definition 3.7 (Strong approximate group). A K -approximate group A is said to be a strong approximate group if

- (1) if $1, g, \dots, g^{1000} \in A^{100}$, then $g \in A$.
- (2) there is a subset $S = S^{-1} \subset A$ such that $(S^{A^4})^{10^6 K^3} \subset A$ and if $1, g, \dots, g^{10^6 K^3} \in A$, then $g \in S$.

Here S^{A^4} denotes the set of elements of the form gsg^{-1} with $s \in S$ and $g \in A^4$. Observe that, as follows from this definition, if A is a strong K -approximate subgroup of G , then

- $\forall g, n_A(g) \leq n_{A^{100}}(g) \leq 10^3 n_A(g)$,
- $10^6 K^3 n_S(g) \geq n_A(g)$.

Set

$$\|g\|_A = \frac{1}{n_A(g)}$$

the *escape norm* of g w.r.t A . Note that $\|g\|_A = 0$ iff the cyclic group $\langle g \rangle$ lies in A entirely.

Lemma 3.8 (Gleason-Yamabe lemmas, approximate group version). *Given $K \geq 1$, there is $C = C(K) > 0$ such that if A is a strong K -approximate subgroup of a group G , then $\forall g, h \in A$,*

- (1) $\|h^{-1}gh\|_A \leq C\|g\|_A$
- (2) $\|gh\|_A \leq C(\|g\|_A + \|h\|_A)$
- (3) $\|[g, h]\|_A \leq C\|g\|_A \cdot \|h\|_A$

We do not repeat the proof, which is essentially identical to the original Gleason-Yamabe lemma that we proved above. The key point here is the second item. For example it implies that if the $\langle g \rangle$ and $\langle h \rangle$ lie both in A , then the subgroup generated by gh is also contained in A .

Of course in order to be able to apply this lemma, we need to be able to produce a strong approximate subgroup out of the original approximate subgroup A . Indeed we prove:

Lemma 3.9 (existence of strong approximate subgroups). *Given $K > 0$, there is $C(K) > 0$ such that for every K -approximate subgroup A of a group G there is a strong $C(K)$ -approximate subgroup $A' \subset A^4$, such that A is contained in a most $C(K)$ left translates of A' .*

This allows to work with A' instead of A , and thus apply the Gleason-Yamabe lemmas to it. Unfortunately, we were not able to give a purely combinatorial proof of this lemma. It is a consequence of Hrushovski's local model theorem (Theorem 3.2) and of the original Gleason-Yamabe structure theorem for locally compact groups (applied to the model group G from Theorem 3.2). Consequently $C(K)$ is ineffective, and there lies the source of ineffectiveness of our main theorem.

Proof. Apply the Gleason-Yamabe structure theorem for locally compact groups to the model group G from Theorem 3.2. Up to passing to an open subgroup, we may assume (up to changing A into a commensurate approximate subgroup) that G is a projective limit of Lie groups. But it is easy to see that sufficiently small balls around the identity in exponential coordinates in a connected Lie group (say for a choice of a Euclidean metric on the Lie algebra) satisfy the strong approximate group axioms. Hence we can pull back those sets to $\mathbb{A}^4$ via Theorem 3.2, and we are done. $\square$

Note that this argument actually shows that $\{g \in A; \|g\|_A < \varepsilon\}$ is a positive proportion of A , for every $\varepsilon > 0$. So up to passing to that subset for $\varepsilon = \frac{1}{C}$, we may assume that $\|g\|_A < \frac{1}{C}$ for all $g \in A$. It is then easy to exploit the approximate group version of the Gleason-Yamabe lemmas and conclude Step 2. Indeed set $H := \{g \in A; \|g\| = 0\}$. By (1) and (2), this forms a subgroup of G , which is normalized by A . Moreover set pick $a \in A$ with $\|a\|_A$ minimal. Then (3) implies that a commutes with every element of A modulo H . This concludes Step 2.

For Step 3 and the induction on $\dim L$, we refer the reader to our original paper [14], or to Tao's book [73].

4. APPLICATIONS TO DIAMETER BOUNDS AND SCALING LIMITS OF FINITE GROUPS

4.1. Diameter of finite simple groups. A celebrated conjecture of Babai [1] proposes the following universal polylogarithmic upper bound on the diameter of all Cayley graphs of finite simple groups:

$$\text{diam}_S(G) \leq C \log(|G|)^D$$

for every finite simple group G with symmetric generating set S , where $\text{diam}_S(G) := \inf\{n \in \mathbb{N}; S^n = G\}$, and absolute constants $C, D > 0$.

All attempts to this conjecture so far are based on the classification of finite simple groups, by examining case by case various infinite families, such as the alternating groups (for which the conjecture is still open, see [52] for the best available bounds), or finite simple group of Lie type in the q large limit (such as $\text{PSL}_n(q)$ for n fixed). Actually in the latter case, when the rank is bounded, the conjecture has been solved by Helfgott [50] for $\text{PSL}_2(p)$ and by Pyber-Szabo [63], and independently Green, Tao and the author [13] in general. In fact it is conjectured that $D = 1$ for bounded rank groups ([11]). It has also been extended to some non simple perfect groups such as $\text{PSL}_n(\mathbb{Z}/q\mathbb{Z})$ with q arbitrary by Varjú [78] (see also [9]).

On the other hand, one can very easily derive from our structure theorem for approximate groups, the following weaker, but very general bound.

Theorem 4.1 (Diameter bound for finite simple groups [16]). *Given $\varepsilon > 0$, there are only finitely many non-abelian finite simple groups admitting a symmetric generating set S with diameter*

$$\text{diam}_S(G) \geq |G|^\varepsilon.$$

Proof. We argue as in the proof of Theorem 1.12, but instead of Theorem 1.11, we use the strong form of our structure theorem, i.e. Theorem 2.14. By contradiction, suppose there were infinitely many such groups. Then there would be arbitrarily large integers n and simple groups G with generating sets S , such that $|S^{5n}| \leq K|S^n|$, where $K = 5^{4/\varepsilon}$, and $n \leq \sqrt{\text{diam}_S(G)}$. For otherwise there would be $n_0 \geq 1$ independent of G, S such that $|G| \geq |S^{5^m n_0}| \geq K^m |S^{n_0}| \geq K^m$ for all m with $5^m n_0 \leq \sqrt{\text{diam}_S(G)}$, but this is not compatible with $\text{diam}_S(G) \geq |G|^\varepsilon$, when $|G|$ is large. By Lemma 2.7, S^{2n} is a K^2 -approximate subgroup. We may then apply Theorem 2.14 and conclude that $S^n \subset XP$, where $|X| \leq C(K)$ and P is a coset nilprogression of size $|P| \leq C(K)|S^{2n}|$. In particular $|S^{2n} \cap \langle P \rangle| \geq |S^{5n}|/KC(K)^2$. By Lemma 1.13, if n is large enough, $\langle P \rangle$ has index at most $KC(K)^2$ in G . But G is a non-abelian simple group, so it has no non-trivial subgroup of bounded index (for every subgroup of index d contains a normal subgroup of index at most $d!$). Hence $G = \langle P \rangle$. However, by definition, P contains a subgroup H normalized by P , such that $\langle P \rangle/H$ is nilpotent. Since G is simple, we must have $G = H$, and hence $|G| \leq |XP| \leq C(K)^2 |S^{2n}|$, and hence applying Remark 1.9 $\text{diam}_S(G) \leq O_K(n)$, which is eventually a contradiction, for $n \leq \sqrt{\text{diam}_S(G)}$. $\square$

The above argument can be strengthened to arbitrary finite groups. For example, in [16] we prove:

Theorem 4.2 ([16]). *Assume that G is a finite group with symmetric generating set S such that $\text{diam}_S(G) \geq |G|^\varepsilon$. Then G has a quotient Q with diameter at least $c_\varepsilon \text{diam}_S(G)$, which contains a cyclic subgroup of index at most C_ε . Here $c_\varepsilon, C_\varepsilon$ are positive constants depending on ε only.*

On a Cayley graph, the diameter and the first eigenvalue of the Laplacian enjoy the following general inequality (see [26] of [16, Lemma 5.1]):

$$\lambda_1 \geq \frac{1}{8 \text{diam}_S(G)^2}$$

As a consequence of this and the above theorem, we see that every Cayley graph of a finite group G satisfies a spectral gap lower bound of the form

$$\lambda_1 \geq \frac{1}{|G|^\varepsilon}$$

unless it admits a large virtually cyclic quotient with diameter comparable to that of G . Such bounds are weaker than what is required for expander graphs, but they can be useful (they can be used for example in the work of Ellenberg-Hall-Kowalski [31]). For additional results in this vein, we refer the reader to [16].

4.2. Scaling limits of vertex transitive graphs. In [3] Benjamini, Finucane and Tessera considered the problem of determining the scaling limits of finite vertex transitive graphs satisfying the volume bound (4.1) below. It turns that this problem can be analysed thanks to our structure theorem for approximate subgroups. Given constants $C, d > 0$, consider the family $\mathcal{F}_{C,d}$ of all finite, vertex transitive connected graphs X such that

$$\frac{|X|}{\deg(X)} \leq C \cdot \text{diam}(X)^d \tag{4.1}$$

where $|X|$ is the number of vertices of X and $\deg(X)$ is the number of neighbors of a given vertex in X (all vertices have the same number of neighbors, since X is assumed vertex transitive). We denote by $\widehat{X}$ the finite metric space defined on the set X by the graph distance renormalized by a factor $\frac{1}{\text{diam}(X)}$ so that $\widehat{X}$ has diameter 1. They prove:

Theorem 4.3 ([3]). *For every sequence $\{X_n\}_{n \geq 1}$ of finite graphs belonging to $\mathcal{F}_{C,d}$ for some fixed C, d , and such that $\text{diam}(X_n) \rightarrow +\infty$, there is a subsequence $\{X_{n_k}\}$ such that $\widehat{X_{n_k}}$ converges in the Gromov-Hausdorff topology towards a torus $\mathbb{R}^q/\mathbb{Z}^q$, endowed with a left-invariant Finsler metric.*

In other words: scaling limits of vertex transitive graphs with (polynomially) large diameter are flat tori equipped with a norm. We give a complete proof of Theorem 4.3 in this section. In [3] the stronger condition $|X| \leq C \cdot \text{diam}(X)^d$ is assumed, but the proof works just as well assuming the weaker bound (4.1). When $\deg(X)$ is uniformly bounded it is possible to further show that $q \leq d$ and that the limit norm is polyhedral, see [3], but we will not pursue this here.

A left-invariant Finsler metric on $\mathbb{R}^k/\mathbb{Z}^k$ is nothing but the choice of a norm $\|\cdot\|$ on $\mathbb{R}^k$, which induces a translation invariant distance on the torus $\mathbb{R}^k/\mathbb{Z}^k$ by setting $d([x], [y]) = \inf_{u \in \mathbb{Z}^k} \|x - y + u\|$.

Here is a graphic way to illustrate the above theorem: the result implies that it is impossible to approximate the Euclidean sphere S^2 by finer and finer finite vertex transitive graphs. The soccer ball

(or truncated icosahedron, which is vertex transitive) is perhaps (one of) the best attempts at this game, see [38, 2].

4.2.1. Gromov compactness criterion. The Gromov-Hausdorff metric is the natural distance on the space of compact metric spaces up to isometry extending the Hausdorff topology on compact subsets of a given metric space. We refer the reader to the books [45, 18] for background on this notion. For the moment we only recall the well-known:

Gromov compactness criterion: *A family $\mathcal{F}$ of compact metric spaces is relatively compact in the GH-topology if and only if it is uniformly bounded in diameter, and for all $\varepsilon > 0$ there is $N(\varepsilon) \in \mathbb{N}$ such that every $X \in \mathcal{F}$ can be covered by at most $N(\varepsilon)$ balls of radius ε .*

It easily follows from this criterion that the space of all compact metric spaces up to isometry is complete for the GH-metric. In fact this is the non-trivial part of the statement (it is easy to see that the above criterion is equivalent to the total boundedness of the family $\mathcal{F}$, and clearly a totally bounded subset of a complete metric space is relatively compact). Completeness is only proved for path metric spaces in Gromov's book [45, Prop 5.2], but it is folklore that it holds in general, see e.g. [65], or [73, Prop. 1.8.7] for a proof with ultraproducts.

We prove Theorem 4.3 in two stages, first showing the existence of a limit and then identifying it.

First note that pulling back the graph metric on $X \in \mathcal{F}_{C,d}$ to the group of automorphisms of the graph, we get a natural word metric on this group. To this effect pick a base point $x_0 \in X$ and consider the subset $S \subset G := \text{Aut}(X)$ of those $s \in S$ which either fix x_0 or send it to a neighbor. Since X is connected and vertex transitive G is generated by S and $S = S^{-1}$. Moreover the preimage under the orbit map $G \rightarrow X$, $g \mapsto g \cdot x_0$ of the ball $B(x_0, n)$ of radius n around x_0 is precisely S^n . In particular $\text{diam}(X) = \text{diam}_S(G)$ and

$$\frac{|S^n|}{|S|} = \frac{|B(x_0, n)|}{\deg(X)}$$

for all $n \geq 1$. This allows to easily translate the statements from X to G .

Proof of the existence of a limit in Theorem 4.3. To apply the Gromov compactness criterion above to the family $\mathcal{F} = \{\widehat{X}_n\}_{n \geq 1}$, it is enough to check that given $\varepsilon > 0$, there is $K_\varepsilon > 0$ such that every ball of radius $r \geq \varepsilon$ can be covered by at most K_ε balls of radius $\frac{r}{2}$. In fact we will show the stronger property (needed only for the identification of the limit) that K_ε can be taken to be independent of ε , if n is large enough. This follows easily from Theorem 2.15. Indeed setting $K = 9^d$ in Theorem 2.15 we get an integer $n_0 = n_0(K) \geq 1$. And we see that if $\text{diam}(X_n)$ is large enough, there must be some $n_1 \in [n_0, \varepsilon \text{diam}(X_n)]$ such that $|S^{3n_1}| \leq K|S^{n_1}|$, for otherwise $|S^{3^m n_0}| \geq 9^{dm}|S^{n_0}|$ for all m with $3^m n_0 \leq \varepsilon \text{diam}(X_n)$, and thus $|G| \geq 9^{dm}|S|$ for the maximal such m , which implies $C \text{diam}(X_n)^d \geq 9^{dm} \geq (\varepsilon \text{diam}(X_n)/3n_0)^{2d}$, a contradiction for n large. So we apply Theorem 2.15 and get that $|B(x_0, 4k)| \leq K'|B(x_0, k)|$ for all $k \geq \varepsilon \text{diam}(X_n)$ and all n large enough, for some $K' > 0$ independent of n . From this we conclude that every ball of radius $4k$ can be covered by at most K' balls of radius $2k$, and this ends the proof. $\square$

We remember from this argument, that there exists some $K = K(C, d) > 0$ such that if X is a limit of a sequence of $\widehat{X}_n$ with X_n satisfying (4.1) and with $\text{diam}(X_n) \rightarrow +\infty$, then X is K -doubling in the sense that every ball of radius $r > 0$ can be covered by at most K balls of radius $\frac{r}{2}$. It follows immediately from this that X has finite Hausdorff dimension, hence *finite topological dimension*.

4.2.2. Identification of the limit: outline. We now turn to the identification of the limit. This part is almost purely formal in that it follows from a simple combination of known facts (we differ here from the original treatment of [3]). Here is the argument. If $\widehat{X_n}$ converges to some compact metric space X , then $G := \text{Isom}(X)$ must act transitively on X , because $G_n := \text{Isom}(X_n)$ acts transitively on X_n . Moreover, X is pathwise connected and locally connected (because the balls in the graphs X_n are connected), and has finite topological dimension. From this, a lemma of Montgomery-Zippin, which is a simple consequence of the Peter-Weyl theorem, tells us that G is a (compact) Lie group. Moreover up to passing to a subsequence (equivariant GH-convergence), we may assume that there is an ε_n -representation of G_n in G , which is ε_n -dense, for some $\varepsilon_n \rightarrow 0$. A well-known result (the so-called *Ulam stability* of almost representations of finite groups in compact groups, due to Alan Turing in this setting and further generalized by Kazhdan and others) ensures that the ε_n -representation must be close to a genuine representation. Then Jordan's lemma on finite subgroups of Lie groups and the almost density of the representations imply that G^0 must be abelian, hence $X = G^0$ is a torus. The metric on $X = G^0$ is geodesic and left-invariant: all such metrics on a torus are Finsler (i.e. given by a norm).

4.2.3. Montgomery-Zippin lemma. We now pass to the details. Set $G := \text{Isom}(X)$. We already know that X is pathwise connected, locally connected, G -transitive, and finite dimensional. We have the following well-known lemma:

Lemma 4.4. *If G is a compact group acting faithfully and transitively on a finite-dimensional, connected and locally connected topological space, then G is a Lie group with finitely many connected components.*

Proof. The lemma holds for locally compact groups in general and is due to Montgomery-Zippin (see [61, §6.3, p. 243]). It easily follows from the Gleason-Yamabe theorem. In the case of compact groups, only Peter-Weyl is needed: we include the proof for the reader's convenience.

According to the Peter-Weyl theorem, there is a nested sequence of closed normal subgroups N_i in G such that G/N_i is a Lie group and $\bigcap_i N_i = \{1\}$. We have to show that N_i is trivial for i large. Let $X_i := X/N_i$ be the quotient space under the action of N_i . The space X is naturally a projective limit of the X_i 's, i.e. $X = \varprojlim X_i$. Note that the X_i 's are manifolds: they are homogeneous spaces of the compact Lie group G/N_i . Since X is finite dimensional as a topological space, we must have $\dim(X_i) = \dim(X_{i_0})$ when i is larger than some i_0 . This implies that N_{i_0}/N_i is zero-dimensional if $i \geq i_0$. Being a compact Lie group, it must be finite. Therefore X_i is a finite normal cover of X_{i_0} with finite group of deck transformations N_{i_0}/N_i . The group N_{i_0} is a projective limit of finite groups, i.e. it is profinite.

We claim that N_{i_0} is finite. This follows from the local connectedness of X . Indeed, by covering theory, the universal cover of X_{i_0} is a cover of each X_i , $i \geq i_0$. Therefore, given $x \in X_{i_0}$ there exists an open neighborhood U of x such that $\pi_i^{-1}(U)$ is a disjoint union of open subsets of X_i each homeomorphic to U and permuted by the action of N_{i_0}/N_i for $i \geq i_0$. Hence $\Omega := \varprojlim \pi_i^{-1}(U)$ is homeomorphic to $U \times N_{i_0}$. Note that since $X = \varprojlim X_i$, Ω is also an open subset of X , which is not locally connected at any point, unless N_{i_0} is finite. This ends the proof. $\square$

Note in passing that the hypothesis that X be locally connected is important to avoid examples such as the solenoid $(\mathbb{R} \times \mathbb{Q}_2)/\mathbb{Z}[\frac{1}{2}]$, which is a connected and finite dimensional compact group, but not a Lie group.

Note also that, since X is connected, the connected component of the identity G^0 in G acts transitively on X .

4.2.4. *Ulam stability and almost representations.* We now recall the notion of almost representation. Given a target group G , endowed with a left-invariant distance d making it a metric space, a mapping ϕ from a group Γ to G , is called an ε -representation if for every $x, y \in \Gamma$,

$$d(\phi(xy), \phi(x)\phi(y)) \leq \varepsilon.$$

We say moreover that ϕ is ε -dense if for each $g \in G$ there is $x \in \Gamma$ such that $d(g, \phi(x)) \leq \varepsilon$.

Ulam stability (see [77]) is the general problem of determining to what extent an ε -representation of Γ is $\delta(\varepsilon)$ -close to a genuine group homomorphism, i.e. does there exist a group homomorphism $\rho : \Gamma \rightarrow G$ such that $d(\phi(x), \rho(x)) \leq \delta(\varepsilon)$, for some $\delta(\varepsilon)$ tending to 0 as $\varepsilon \rightarrow 0$. A little known and recently rediscovered [3, 38] 1938 paper of Alan Turing [76] deals precisely with this problem in the case when Γ is a finite group and G a connected Lie group (endowed with a left-invariant Riemannian metric):

Theorem 4.5 (Turing's theorem). *Suppose G is a connected compact Lie group, then there is $C > 0$ such that every ε -dense ε -representation of some finite group into G is $C\varepsilon$ -close to a group homomorphism. In particular, if there is a sequence of finite groups Γ_n and ε_n -representations $\phi_n : \Gamma_n \rightarrow G$ that are ε_n -dense in G for some $\varepsilon_n \rightarrow 0$, then G is a compact abelian Lie group.*

The second part of the statement follows immediately from the combination the first and of Jordan's theorem on finite subgroups of Lie groups: that they contain an abelian subgroup of bounded index ([55, 25, 17]). The first part actually holds without the assumption of ε -density (we do not need this refinement for the proof of Theorem 4.3), as follows from the following more general result of Kazhdan [57, Theorem 1]. Let $G = \mathcal{U}(\mathcal{H})$ be the unitary group of a separable Hilbert space, endowed with the bi-invariant distance $d(g, h) := \|g - h\|$.

Theorem 4.6 (Ulam stability of amenable groups). *Every ε -representation ϕ of an amenable group Γ into G is ε -close to a genuine representation ρ , i.e. $d(\phi(\gamma), \rho(\gamma)) \leq \varepsilon$ for all $\gamma \in \Gamma$.*

Note that every finite group is amenable, so this applies uniformly to all finite groups Γ , and also note that every compact Lie group is a subgroup³ of the unitary matrices $\mathcal{U}(\mathbb{C}^n)$ for some n (the above distance being bi-Lipschitz to any left-invariant Riemannian metric), so the result applies to this situation as well and implies Turing's theorem.

For a very short proof of Kazhdan's theorem, as well as a modern view on Ulam stability, we refer the reader to the paper [21], in particular Theorem 3.2 there.

4.2.5. *Equivariant GH convergence.* When each term of a sequence of compact metric spaces comes equipped with a group action by isometries, one can strengthen the Gromov compactness theorem and argue that under the same hypotheses, one can find a subsequence which converges in an almost equivariant way. Namely we have:

Equivariant Gromov-Hausdorff compactness: *Let $(X_n, d_n) \rightarrow (X, d)$ be a converging sequence of compact metric spaces. Let $\Gamma_n := \text{Isom}(X_n)$. Then there is a closed subgroup of isometries G of X and subsequence $\{X_{n_k}\}$, such that $\{(X_{n_k}, d_{n_k})\}$ equivariantly GH converges to (X, G) , in other words, there*

³Ulam stability may fail for certain target groups other than $\mathcal{U}(\mathcal{H})$, for example it fails for G the p -adic integers, see [57, Prop 1.]

are maps $f_k : X_{n_k} \rightarrow X$ and $\phi_k : \Gamma_{n_k} \rightarrow G$ with ε_k -dense image in X and G respectively (where $\varepsilon_k \rightarrow 0$), such that

$$\sup_{x \in X_{n_k}, \gamma \in \Gamma_{n_k}} d(f_k(\gamma x), \phi_k(\gamma) f_k(x)) \xrightarrow{k \rightarrow +\infty} 0 \quad (4.2)$$

This is a classical fact, which holds more generally for locally compact metric spaces and pointed GH convergence, see for example [35, Prop. 3.6]. We give a proof for convenience.

Proof. By definition there are almost isometries $f_n : X_n \rightarrow X$ and $g_n : X \rightarrow X_n$ such that $f_n \circ g_n$ and $g_n \circ f_n$ are both uniformly close to the identity. Pick a nested sequence of ε_k -dense finite subsets F_k in X , where $\varepsilon_k \rightarrow 0$. The restrictions of elements in $f_n \Gamma_n g_n$ to F_k form a compact set of maps from F_k to X . By the usual diagonal process we can extract a subsequence of $(X_n)_n$ such that these compact sets converge as n tends to infinity for every given k . Let G_k be the limit. The restriction map $G_{k+1} \rightarrow G_k$ is surjective. The projective limit $G := \varprojlim G_k$ is a compact set of maps on $\cup_k F_k$. Maps in G_k are distance preserving, hence so are maps in G . Thus maps in G extend by continuity to isometries of X .

Given k there is n_k such that G_k is ε_k -close to the restriction of $f_n \Gamma_n g_n$ to F_k for $n = n_k$. Thus we may find for each $\gamma \in \Gamma_{n_k}$ an element $\phi_k(\gamma)$ in G_k (hence also one in G) such that $f_{n_k} \gamma g_{n_k}$ is $3\varepsilon_k$ -close to $\phi_k(\gamma)$ on X . Similarly the image of ϕ_k is $3\varepsilon_k$ -dense in G . It is then straightforward to check (4.2) and that G is indeed a subgroup. $\square$

Note that it follows directly from (4.2) that ϕ_{n_k} is a δ_k -representation of Γ_{n_k} inside G for some $\delta_k \rightarrow 0$.

By Lemma 4.4, in the setting of Theorem 4.3, the limit group G is a compact Lie group and the groups Γ_n are finite. Therefore Turing's theorem (or the combination of Kazhdan and Jordan) implies that G^0 is an abelian compact Lie group, i.e. a torus $\mathbb{R}^k/\mathbb{Z}^k$. We have $X = G^0/H$ for some closed subgroup H . But since G^0 acts faithfully on X (it is a subgroup of isometries) and G^0 is abelian, we must have $H = 1$, i.e. $X = G^0$.

4.2.6. Invariant length metrics on Lie groups. To conclude the proof of Theorem 4.3 it remains to identify the metric on the limit space X . We know that it is a *length metric* a.k.a intrinsic metric, i.e. the distance between two points coincides with the infimum of the length of paths between two points. This is so, because X is a GH limit of graphs and the graph metric is a length metric. Since $X = \mathbb{R}^k/\mathbb{Z}^k$, the distance on X lifts naturally to a length metric on $\mathbb{R}^k$, which is invariant under translations. So the last part of Theorem 4.3 is now a consequence of the following simple and well-known lemma, of which we give a proof for convenience.

Lemma 4.7. *If d is a translation invariant length metric on $\mathbb{R}^k$, then there is a norm $\|\cdot\|$ on $\mathbb{R}^k$ such that $d(x, y) = \|x - y\|$ for all x, y .*

Proof. Set $\|x\| := \limsup_{t \rightarrow 0} \frac{1}{t} d(0, tx)$. Clearly, by translation invariance and the triangle inequality $d(0, x) \leq nd(0, \frac{x}{n})$ for every $n \in \mathbb{N}$. It follows that $d(0, x) \leq \|x\|$. It is also straightforward to verify that $\|x + y\| \leq \|x\| + \|y\|$ and that $\|\lambda x\| = \lambda \|x\|$ if $\lambda > 0$. Hence $\|x\|$ is a norm on $\mathbb{R}^k$. Moreover we also have $\|x\| := \liminf_{t \rightarrow 0} \frac{1}{t} d(0, tx)$. Indeed if not there would be some $\beta < 1$ and arbitrarily small s, t such that $\frac{1}{s} d(0, sx) \leq \beta \frac{1}{t} d(0, tx)$. If s is chosen much smaller than t , say $t = ns + s'$, $0 \leq s' \leq s$, $n \geq 1$, then by the triangle inequality and translation invariance $d(0, tx) \leq nd(0, sx) + d(0, s'x)$, which eventually contradicts the previous inequality.

So $\|x\| := \lim_{t \rightarrow 0} \frac{1}{t} d(0, tx)$. By local compactness of $\mathbb{R}^k$, this limit is uniform over x with $\|x\| = 1$. From this it is easy to conclude that $\|x\| = d(0, x)$. Indeed if not, then $d(0, x) \leq (1 - \varepsilon)\|x\|$ for some x and $\varepsilon > 0$. Moreover given any $\delta > 0$, there are points $x_0 = 0, \dots, x_n = x$ such that $d(x_i, x_{i+1}) < \delta$ and $d(x_0, x_1) + \dots + d(x_{n-1}, x_n) \leq (1 - \frac{\varepsilon}{2})\|x\|$. However $d(x_i, x_{i+1})$ is uniformly very close to $\|x_i - x_{i+1}\|$, but $\|x\| \leq \|x_0 - x_1\| + \dots + \|x_{n-1} - x_n\|$ by the triangle inequality. A contradiction. $\square$

This lemma is a special case of the following much more general result of Berestovski, which gives a complete characterization of left invariant length metrics on Lie groups.

Before we state Berestovski's theorem, let us give a general construction of left invariant length metrics on a Lie group. Pick a norm on the Lie algebra $\mathfrak{g}$ of the Lie group G and use it to define the length of piecewise differential paths in exactly the same way as left invariant Riemannian metrics on G are defined, except that the norm is now arbitrary instead of Euclidean. This obviously gives rise to a left invariant (Finsler) length metric on G . More generally, we may consider a norm on a vector subspace V of $\mathfrak{g}$, which generates $\mathfrak{g}$ as a Lie algebra. Similarly this allows to define the length of piecewise differentiable *horizontal* paths, that is paths whose derivative, once translated back to the origin, everywhere belongs to V . The property of V that it generates $\mathfrak{g}$ can be shown (this is the Chow-Rachevski theorem from subriemannian geometry) to imply that every two points in G can be joined by a horizontal piecewise differentiable continuous path. Hence this yields a well-defined length metric on G . Metrics arising from the above construction are called left invariant Carnot-Caratheodory-Finsler metrics.

When G is abelian, then every subspace of $\mathfrak{g}$ is a subalgebra, so this refinement does not produce new examples of left invariant metrics. But if G is nilpotent (e.g. the Heisenberg group), then many new length metrics arise this way. In fact it can be shown ([4]) that G abelian and $G = \mathbb{R} \ltimes \mathbb{R}^n$, where $\mathbb{R}$ acts by homotheties, are the only Lie groups in which all Carnot-Caratheodory-Finsler metrics are Finsler. We can now state:

Theorem 4.8 (Berestovski [4]). *Every left invariant length metric on a connected Lie group is Carnot-Caratheodory-Finsler.*

This ends our discussion of Theorem 4.3.

Acknowledgement. These lectures were prepared for the workshop on *Additive and Analytic Combinatorics* held at the IMA in Minneapolis from September 29 to October 3, 2014. Due to a health problem, I was unfortunately not able to give the lectures. I am very grateful to Terry Tao, who replaced me on the spot. I also thank T. Tao, R. Tessera and M. Tointon for their valuable comments on the text. The author is partially supported by ERC grant no. 617129.

REFERENCES

- [1] L. Babai and A. Seress, *On the diameter of Cayley graphs of the symmetric group*, Journal of combinatorial theory, Series A 49, 175–179 (1988).
- [2] I. Benjamini, *Coarse geometry and randomness*, Lecture notes from the 41st Probability Summer School held in Saint-Flour, 2011, Lecture Notes in Mathematics, Springer, Cham, 2013. viii+129 pp.
- [3] I. Benjamini, H. Finucane and R. Tessera, *On the scaling limit of finite vertex transitive graphs with large diameter*, arXiv:1203.5624, to appear in Combinatorica.
- [4] V.N. Berestovski, *Homogeneous manifolds with intrinsic metric*, Sibirskii Matematicheskii Zhurnal, Vol. 29, No. 6, pp. 17–29 November-December, 1988.
- [5] Y. Bilu, *Structure of sets with small sumset*, in Structure theory of set addition, Astérisque 258 (1999), 77–108.

- [6] G. Birkhoff, *A note on topological groups*, Compositio Math. 3 (1936), 427–430.
- [7] Bourgain, J., A. A. Glibichuk and S. V. Konyagin, *Estimates for the number of sums and products and for exponential sums in fields of prime order*, Journal of the London Mathematical Society (2) 73 (2006): 380398
- [8] Bourgain, J., N. Katz, and T. Tao, *A sumproduct estimate in finite fields and their applications*, Geometric and Functional Analysis 14, no. 1 (2004): 2757.
- [9] H. Bradford, *New Uniform Diameter Bounds in Pro- p Groups*, arXiv preprint 1410.3007.
- [10] L.V. Brailovsky, G.A. Freiman, *On a product of finite subsets in a torsion-free group*, J. Algebra 130 (1990), no. 2, 462–476.
- [11] E. Breuillard, *Diophantine geometry and uniform growth of finite and infinite groups*, Proceedings of the International Congress of Mathematicians, 2014 ICM (Seoul).
- [12] E. Breuillard and B. J. Green, *Approximate groups. I. The torsion-free nilpotent case*, J. Inst. Math. Jussieu 10(1) (2011), 37–57.
- [13] E. Breuillard, B. Green and T. Tao, *Approximate subgroups of linear groups*, Geom. Funct. Anal. **21** (2011), no. 4, 774–819.
- [14] E. Breuillard, B. Green and T. Tao, *The structure of approximate groups*, Publ. Inst. Hautes Études Sci., **116**, Issue 1, 115–221, (2012)
- [15] E. Breuillard, B. Green, and T. Tao, *Small doubling in groups*, Erds centennial, 129–151, Bolyai Soc. Math. Stud., 25, Jnos Bolyai Math. Soc., Budapest, 2013.
- [16] E. Breuillard and M. Tointon, *Nilprogressions and groups with moderate growth*, arXiv preprint 1506.00886.
- [17] E. Breuillard, *An exposition of Camille Jordan’s original proof of his theorem on finite subgroups of invertible matrices*, notes available at <http://www.math.u-psud.fr/~breuilla/cour.html>.
- [18] Dmitri Burago, Yuri Burago, and Sergei Ivanov, *A course in metric geometry*, Graduate Studies in Mathematics, vol. 33, American Mathematical Society, Providence, RI, 2001. MR MR1835418 (2002e:53053)
- [19] Y. Burago and V.A. Zalgaller, *Geometric inequalities*, Translated from the Russian by A. B. Sosinski. Grundlehren der Mathematischen Wissenschaften, 285. Springer Series in Soviet Mathematics. Springer-Verlag, Berlin, 1988. xiv+331
- [20] P. Buser and H. Karcher, *Gromov’s almost flat manifolds*, Astérisque, 81. Société Mathématique de France, Paris, 1981. 148 pp.
- [21] M. Burger, N. Ozawa and A. Thom, *On Ulam stability*, Israel J. Math. 193 (2013), no. 1, 109–129.
- [22] J.O. Button, *Explicit Helfgott type growth in free products and in limit groups*, J. Algebra 389 (2013), 61–77.
- [23] M. C. Chang, *A polynomial bound in Freiman’s theorem*, Duke Math. J. 113 (2002), no. 3, 399–419.
- [24] E. Croot and O. Sisask, *A probabilistic technique for finding almost-periods of convolutions*, Geom. Funct. Anal. 20 (2010), no. 6, 1367–1396.
- [25] C.W. Curtis and I. Reiner, *Representation Theory of Finite Groups and Associative Algebras*, (Interscience, New York) (1962).
- [26] P. Diaconis and L. Saloff-Coste, *Comparison techniques for random walk on finite groups*, Ann. Probab. **21**(4) (1993), 2131–2156.
- [27] L. van den Dries and Wilkie, *Gromov’s theorem on groups of polynomial growth and elementary logic*, J. Algebra 89 (1984), 349–374.
- [28] L. van den Dries and I. Goldbring, *Hilbert’s 5th problem*, preprint, to appear in l’Enseig. Math.
- [29] L. van den Dries, *Approximate Groups*, Séminaire Bourbaki, Exposé 1077, Astérisque 367-368 (2015), 79–113.
- [30] G. Elekes and Z. Király, *On the combinatorics of projective mappings*, J. Algebraic Combin., 14(3):183–197, 2001
- [31] J. S. Ellenberg, C. Hall and E. Kowalski, *Expander graphs, gonality and variation of Galois representations*, Duke Math. J. **161**(7) (2012), 1233–1275.
- [32] G. A. Freiman, *Foundations of a structural theory of set addition*, Translations of Mathematical Monographs 37, Amer. Math. Soc., Providence, RI, USA, 1973.
- [33] G.A. Freiman, *Groups and the inverse problems of additive number theory*, Number-theoretic studies in the Markov spectrum and in the structural theory of set addition, pp. 175183. Kalinin. Gos. Univ., Moscow, 1973.
- [34] G. A. Freiman, *On finite subsets of nonabelian groups with small doubling*, Proc. Amer. Math. Soc. 140 (2012), no. 9, 2997–3002.
- [35] K. Fukaya and T. Yamaguchi, *The fundamental groups of almost non-negatively curved manifolds*, Ann. of Math. (2) 136 (1992), no. 2, 253–333.
- [36] M. Z. Garaev, *An explicit sumproduct estimate in $\mathbb{F}_p$* , International Mathematics Research Notices, 2007, no. 11.

- [37] M. Z. Garaev, *The sum-product estimates for large subsets of prime fields*, Proceedings of the American Mathematical Society 137, no. 8 (2008): 2735–9.
- [38] T. Gelander, *Limits of finite homogeneous metric spaces*, Enseign. Math. (2) 59 (2013), no. 1-2, 195–206.
- [39] N. Gill and H. Helfgott, *Growth in solvable subgroups of $GL_r(\mathbb{Z}/p\mathbb{Z})$* , Math. Ann. 360 (2014), no. 1–2, 157–208.
- [40] A. M. Gleason, *Groups without small subgroups*, Ann. of Math. (2), 56:193–212, 1952.
- [41] A. Granville, *An introduction to additive combinatorics*, Additive combinatorics, 1–27, CRM Proc. Lecture Notes, 43, Amer. Math. Soc., Providence, RI, 2007.
- [42] B. J. Green, *The polynomial Freiman-Ruzsa conjecture*, Open Problems in Mathematics [Online], Volume 2 (2014).
- [43] Green, Ben; Ruzsa, Imre Z. *Freiman's theorem in an arbitrary abelian group*, J. Lond. Math. Soc. (2) 75 (2007), no. 1, 163–175.
- [44] M. Gromov, *Groups of polynomial growth and expanding maps*, Publ. Inst. Hautes Études Sci., **53**, 53–73, (1981).
- [45] M. Gromov, *Metric structures for Riemannian and non-Riemannian spaces*, Modern Birkhäuser Classics, (2007), Based on the 1981 French original.
- [46] M. Gromov, *Carnot-Carathodory spaces seen from within*, in Sub-Riemannian geometry, 79–323, Progr. Math., 144, Birkhäuser, Basel, 1996.
- [47] Y. Hamidoune, A. S. Lladó, O. Serra, *On subsets with small product in torsion-free groups*, Combinatorica 18 (1998), no. 4, 529–540.
- [48] , Y. Hamidoune, *On small subset product in a group*, Structure theory of set addition. Astrisque No. 258 (1999), xivxv, 281–308.
- [49] Y. Hamidoune, *Two inverse results*, Combinatorica, April 2013, Volume 33, Issue 2, pp 217–230
- [50] H. A. Helfgott, *Growth and generation in $SL_2(\mathbb{Z}/p\mathbb{Z})$* , Ann. of Math. (2) **167** (2008), no. 2, 601–623.
- [51] H. A. Helfgott, *Growth and generation in $SL_3(\mathbb{Z}/p\mathbb{Z})$* , J. Eur. Math. Soc. 13(3), 761851 (2011).
- [52] H. A. Helfgott, A. Seress, *On the diameter of permutation groups*, Ann. of Math. (2) 179 (2014), no. 2, 611–658.
- [53] J. Hirschfeld. *The nonstandard treatment of Hilbert's fifth problem*. Trans. Amer. Math. Soc., 321(1):379–400, 1990.
- [54] E. Hrushovski, *Stable group theory and approximate subgroups*, J. Amer. Math. Soc. 25 (2012), no. 1, 189–243.
- [55] C. Jordan, *Mémoire sur les équations différentielles linéaires à intégrale algébrique*, J. Reine Angew. Math. 84 (1878), 89–215.
- [56] I. Kaplansky, *Lie algebras and locally compact groups*, The University of Chicago Press, Chicago, Ill.-London 1971 xi+148 pp.
- [57] D. Kazhdan, *On ε -representations*, Israel J. Math., 43 (1982), pp. 315–323.
- [58] J.H.B. Kemperman, *On complexes in a semigroup*, Nederl. Akad. Wetensch. Proc. Ser. A. 59 = Indag. Math. 18 (1956), 247–254.
- [59] E. Lindenstrauss, *Pointwise theorems for amenable groups*, Invent. Math. 146 (2001), no. 2, 259–295.
- [60] E. Lindenstrauss, *personal communication* 2007.
- [61] D. Montgomery and L. Zippin. *Topological transformation groups*. Interscience Publishers, New York-London, 1955.
- [62] G. Petridis, *New proofs of Plünnecke-type estimates for product sets in groups*, Combinatorica **32**(6) (2012), 721–733.
- [63] L. Pyber and E. Szabó, *Growth in finite simple groups of Lie type*, to appear in *J. Amer. Math. Soc.*
- [64] A.A. Razborov, *A product theorem in free groups*, Annals of Math., Volume 179 (2014), Issue 2, 405–429.
- [65] J. Rouyer, *Generic properties of compact metric spaces*, Topology Appl. 158 (2011), no. 16, 2140–2147.
- [66] M. Rudnev, *An improved sum-product inequality in fields of prime order*, Int. Math. Res. Not. IMRN 2012, no. 16, 3693–3705.
- [67] I. Z. Ruzsa, *Generalized arithmetical progressions and sumsets*, Acta Math. Hungar. 65 (1994), no. 4, 379388.
- [68] S.R. Safin, *Powers of subsets of free groups*, Mat. Sb. 202 (2011), no. 11, 97–102; translation in Sb. Math. 202 (2011), no. 11-12, 1661–1666.
- [69] T. Sanders, *On a nonabelian Balog-Szemerédi-type lemma*, J. Aust. Math. Soc. 89 (2010), no. 1, 127–132.
- [70] T. Sanders, *The structure theory of set addition revisited*, Bull. Amer. Math. Soc. **50** (2013), 93–127.
- [71] T. Tao, *Product set estimates for non-commutative groups*, Combinatorica, 28(5), 547–594, (2008).
- [72] T. Tao, *Freiman's theorem for solvable groups*, Contrib. Discrete Math. 5(2), 137–184 (2010)
- [73] T. Tao, *Hilbert's fifth problem and related topics*, Graduate Studies in Mathematics, 153. American Mathematical Society, Providence, RI, 2014. xiv+338
- [74] T. Tao and V. Vu, *Additive combinatorics*, volume 105 of Cambridge Studies in Advanced Mathematics, Cambridge University Press, (2006).

- [75] M. C. H. Tointon, *Freiman's theorem in an arbitrary nilpotent group*, Proc. London Math. Soc. **109** (2014), 318–352.
- [76] A. M. Turing, *Finite approximations to Lie groups*, Ann. of Math. (2) 39 (1938), no. 1, 105–111.
- [77] S. M. Ulam, *A Collection of Mathematical Problems*, Interscience Publishers, New York, 1960.
- [78] P. P. Varjú, *Random walks in compact groups*, Doc. Math. 18 (2013), 1137–1175
- [79] H. Yamabe. *A generalization of a theorem of Gleason*. Ann. of Math. (2), 58:351–365, 1953.
- [80] H. Yamabe. *On the conjecture of Iwasawa and Gleason*. Ann. of Math. (2), 58:48–54, 1953.
- [81] G. Zémor, *A generalisation to noncommutative groups of a theorem of Mann*, Discrete Math. 126 (1994), no. 1-3, 365–372.

LABORATOIRE DE MATHÉMATIQUES, BÂTIMENT 425, UNIVERSITÉ PARIS SUD 11, 91405 ORSAY, FRANCE
E-mail address: `emmanuel.breuillard@math.u-psud.fr`