Approximate Groups

Emmanuel Breuillard

Contents

1 Overview, Motivation **1**
1.1 Asymptotic finite group theory 1
1.2 Growth of finitely generated groups 2
1.3 Additive combinatorics, harmonic analysis 4
1.4 Sum-product phenomenon 4

2 Approximate groups **6**
2.1 Small doubling 6
2.2 Small tripling 7
2.3 Approximate subgroups 8
2.4 Structure theorem for approximate subgroups of simple algebraic groups 10

3 Structure theorem for approximate groups **11**

1 Overview, Motivation

1.1 Asymptotic finite group theory

1.1 Notation: Suppose G is a finite group, $G = \langle S \rangle$ for some finite generating set $1 \in S = S^{-1}$. We write $\mathrm{diam}_S(G) = \inf\{n \in \mathbb{N} : G = S^n = S \cdot S \cdot \ldots \cdot S\}$; this is the diameter of the Cayley graph of G with respect to S. We write $\mathrm{diam}(G) = \max_S \mathrm{diam}_S(G)$.

1.2 Babai's Conjecture: There exists $C > 0$, an absolute constant, such that $\mathrm{diam}(G) \leq C(\log |G|)^C$ for any arbitrary finite simple group.

1.3 Remark: $\mathrm{diam}_S(G) \geq \frac{\log |G|}{\log |S|}$ because $|S^n| \leq |S|^n$.

1.4 Partial Results:
- (Helfsott 2005) $G = PSL_2(\mathbb{F}_p)$, p prime.
- (Hrushovski 2010) G a finite simple group of Lie type (eg $PSL_d(\mathbb{F}_q)$, $q = p^*$).

1.5 Theorem: (Breuillard Green Tao, Pyben-Szabo) Babai holds with $C = C(d) > 0$ for finite simple groups of Lie type of rank at most d, $G = \mathbb{G}(\mathbb{F}_q)$.

1.6 Remark: For $G = \mathrm{alt}(n)$, Babai is open. In 2013, Helfsott-Sevess showed that $\mathrm{diam}(G) \leq (\log |G|)^{\log ??}$

1.7 Theorem: (Breuillard Tointon 2015) For all $\varepsilon > 0$, there exists $c_\varepsilon > 0$ such that $\mathrm{diam}(G) \leq c_\varepsilon |G|^\varepsilon$ for every finite simple group. (This result does not use the classification of finite simple groups.)

1.2 Growth of finitely generated groups

1.8 Notation: Let $G = \langle S \rangle$ be a fintiely generated group. The Cayley graph of G has elements of G as vertices, and an edge between x and y if there exists $s \in S$ with $x = ys$. Asymptotics for $|S^n|$: the ball of radius n in the Caylet graph around 1 is S^n.

1.9 Definition: We say G has *polynomial growth* if $|S^n| = O(n^c)$ for some $c \in \mathbb{N}$ and all $n \in \mathbb{N}$. We say that G has *exponential growth* if there exists $\rho > 1$ such that $|S^n| \geq \rho^n$ for all $n \in \mathbb{N}$.

1.10 Remark: These are well defined for G, ie they are independent of the choice of S. Exponential growth is the worst possible scenario, since there are only exponentially many words of length n.

1.11 Gigorchuck 1981: Consider $G = \langle a, b, c, d \rangle \subseteq Bij[0, 1)$, where

- $a(x) = x + 1/2$ for $x < 1/2$, $a(x) = x - 1/2$ for $x \geq 1/2$
- $b = a$ on $[0, 1/2)$, a on $[1/2, 3/4)$, e on $[3/4, 7/8)$, etc.
- $c = a$ on $[0, 1/2)$, e on $[1/2, 3/4)$, a on $[3/4, 7/8)$, etc.
- $d = e$ on $[0, 1/2)$, a on $[1/2, 3/4)$, a on $[3/4, 7/8)$, etc.

Then there exist $0 < \alpha < \beta < 1$ with $e^{n^\alpha} \leq |S^n| \leq e^{n^\beta}$, so G has *intermediate growth*, ie is in between polynomial growth and expontential growth.

1.12 Theorem: (Gromov's polynomial growth theorem) G has polynomial growth iff G is virtually nilpotent, ie there exists $G_0 \leq G$ of finite index such that G_0 is nilpotent (ie there exists $s \in \mathbb{N}$ such that $\gamma_{s+1}(G_0) = 1$, where $\gamma_{i+1}(G_0) = [G_0, \gamma_i(G_0)]$ is the central descending series).

1.13 Example: The Heisenberg group

$$G = \left\{ \begin{pmatrix} 1 & n & p \\ 0 & 1 & m \\ 0 & 0 & 1 \end{pmatrix} : n, m, p \in \mathbb{Z} \right\} = \left\langle \begin{matrix} 1 & 1 & 0 \\ 0 & 1 & 0^{\pm 1} \\ 0 & 0 & 1 \end{matrix}, \begin{matrix} 1 & 0 & 0 \\ 0 & 1 & 1^{\pm 1} \\ 0 & 0 & 1 \end{matrix} \right\rangle$$

Then $|S^n| \approx n^4$, $[G, G] = \{A \in G : n = m = 0\}$, $[G, [G, G]] = 1$.

1.14 Theorem: (Pansu, 1982) If G is nilpotent, $|S^n| \sim c(S) n^d$ for some $d \in \mathbb{N}$, then $d = \sum_{i \geq 1} i \, \mathrm{rk}_{\mathbb{Q}}(\gamma_i / \gamma_{i+1})$ where $\gamma_1 = G$.

1.15 Remark: Being of polynomial growth is invariant under finite extensions: if $\langle S \rangle = G$ then $\langle S^{2d+1} \cap G_0 \rangle = G_0$ for every subgroup G_0 of index d.

1.16 Proposition: Assuming $|S^n| = O(n^c)$, then there exist $n_1 < n_2 < \dots$ such that $|(S^{n_i})^3| \leq 4^c|S^{n_i}|$ for all i.

Proof: Suppose not. Then there exists n_0 such that for $n \geq n_0$, $|(S^n)^3| \geq 4^c|S^n|$. But then iterating this gives $|(S^{n_0})^{3^k}| \geq (4^c)^k|S^{n_0}|$. However, this violates the assumption that $|S^n| = O(n^c)$ (which implies $|(S^{n_0})^{3^k}| = O((3^k)^c) = O((3^c)^k)$.)

1.17 Theorem: (Hrushovski: Stable groups and approdimate groups, 2010, JAMS) If G is any finitely generated group with a sequence of finite subsets $(A_n)_n$ such that

- $A_n \subseteq A_{n+1}$
- $\bigcap A_n = G$
- There exists $k \geq 1$ such that $|(A_n)^2| \leq k|A_{n+1}|$

Then G is virtually nilpotent. (In fact, this is an if and only if.)

1.18 Remark: This is stronger than Gromov's theorem, since if G has polynomial growth then we may take $A_n = S^n$.

1.19 Open Problem: Instead assume $|(A_n)^3| \leq k|(A_n)^2|$. Does the same conclusion hold?

1.20 Theorem: (B, Green, Tao, 2011) For all $k \geq 1$, there exists $n_0(k)$ such that if G is any finitely generated group with some finite subset A such that

- $S^{n_0} \subseteq A$ (for some generating set S of G)
- $|AA| \leq k|A|$

Then G is virtually nilpotent.

1.21 Theorem: (Gromov almost flat manifold theorem, 1978) There exists $\varepsilon = \varepsilon(d) > 0$ such that if M is any Riemannian manifold which is compact of volume 1 and dimension d such that $|k(x)| < \varepsilon$ for all $x \in M$ ($k(x)$ is the sectional curvature) then $\pi_1(M)$ (the fundamental group) is virtually nilpotent.

1.22 Theorem: (Kapovich-Wilking) This is true even assuming only $Ric(M) > -\varepsilon$.

1.23 Conjecture: (Grigorchuk) If $G = \langle Z \rangle$ is a finitely generated group such that $|S^n| \leq e^{n^\alpha}$ for some $\alpha < 1/2$ then G is virtually nilpotent.

1.24 Partial Results:

- (Shalom-Tao) If there exists $c > 0$ such that $|S^n| \leq O(n^{(\log\log n)^c})$ then G is virtually nilpotent
- The conjecture is known under the assumption that G is residually nilpotent (ie for all $g \neq 1$ there exists π such that $\pi : G \twoheadrightarrow N$, $\pi(g) \neq 1$, N nilpotent). (Grigorchuck Lubotzky Mann)
- (Bartholdi-Enshler) $|S^n| \approx e^{n^\alpha}$, $\alpha \geq 0.76$. There is no known example with $\alpha < 3/4$.

1.3 Additive combinatorics, harmonic analysis

1.25 Additive Combinatorics: The study of sum sets. For example, Goldbach, Vinogradov ($P+P+P \subseteq [n_0,\infty) \cap (2\mathbb{N}+1)$ for some $n_0 \in \mathbb{N}$). Given a set A, $A+A$ should be much larger (perhaps using some measure of density); otherwise A has strong arithmetical properties.

1.26 Definition: An *arithmetic progression* is a sequence of the form $\{a+\mathbb{N}b\} = \{a, a+b, a+2b, \ldots\}$ for $a, b \in \mathbb{N}$ ($\mathbb{Z}$?) A *generalized arithmetic progression* (GAP) is a subset of $\mathbb{Z}$ (or of an abelian group G) of the form

$$\{a +_1 b_1 + \ldots n_d b_d : a, b_i \in G, n_i \in [0, N_i] \cap \mathbb{N}\}$$

ie a transalte of a homomorphic image of a box $B = \prod_{i=1}^{d} [0, N_i] \subseteq \mathbb{Z}^d \to G$. Then $B+B = \prod_{i=1}^{d} [0, 2N_i]$, so $B+B \subseteq B+X$ with $|X| \leq 2^d$. Observe that $|A+A| \leq 2^d |A|$.

1.27 Theorem: (Freiman-Rusza) If $A \subseteq \mathbb{Z}$ is finite and $|A+A| \leq k|A|$ for some $k \in \mathbb{N}$ then there exist generalized arithmetic progressions $P \subseteq Q$ of dimension $d \leq e^{k^{O(1)}}$ such that $P \leq (A+A)-(A+A) \leq Q$ and $|Q|/|P| \leq e^{k^{O(1)}}$.

1.28 Proposition: (Rusza Covering Lemma) If $A, B \subseteq G$ are finite subsets of a group G and $|AB| \leq k|A|$ for some $k \geq 1$ then $B \subseteq A^{-1}AX$ for some $X \subseteq G$ with $|X| \leq k$.

Proof: Pick a maximal family of disjoint translates f A, say $Ab_1, \ldots, Ab_m$ with $b_i \in B$. Since $|AB| \leq k|A|$, $m \leq k$, and for all $b \in B$, $Ab \cap Ab_i \neq \emptyset$ for some i. This emans $b \in A^{-1}Ab_i$, and so we can set $X = \{b_1, \ldots, b_m\}$.

1.29 Theorem: (Green-Rusza) The same holds with coset-GAPs instead of GAPs, where a coset GAP is a set of the form HP, where $H \leq G$ is a finite subgroup and P is a GAP.

1.4 Sum-product phenomenon

1.30 Idea: (Erdos-Szemeredi) If $A \subseteq \mathbb{Z}$ is finite, then $|A+A|$ is small iff A is close to an arithmetic sequence, and $|A \cdot A|$ is small iff A is close to a geometric sequence. But these cannot both happen together; precisely, there exists $\varepsilon > 0$ such that $|A+A| + |AA| \geq |A|^{1+\varepsilon}$.

1.31 Conjecture: For all $\varepsilon > 0$, there exists $c_\varepsilon > 0$ such that for all $A \subseteq \mathbb{Z}$, $|A+A| + |AA| > c_\varepsilon |A|^{2+\varepsilon}$. ($2-\varepsilon$?)

1.32 Elekes bound: $A \subseteq \mathbb{R}$ a finite subset, then $|A+A| + |AA| \geq c|A|^{5/4}$ for some $c > 0$ (presumably c is independent of A). This is an application of the Szemeredi-Trotter incidence theorem:

1.33 Theorem: (Szemeredi-Trotter) Suppose P is a set of points in $\mathbb{R}^2$ and L is a set of lines in $\mathbb{R}^2$. Define I to be the set of incidences, ie $\{(p,l) \in P \times L : p \in l\}$. Then $|I| \leq c\left((|P||L|)^{2/3} + |P| + |L|\right)$. In particular, if $|P| = |L| = N$, then $|I| \ll N^{4/3}$.

1.34 Remark: If we think of the sets of points and lines as a graph (in the graph-theory sense), there is a naive bound in the $|P| = |L| = N$ case of $|I| \ll N^2$. But there is at most one line through any two points, from which a Cauchy-Schwartz argument gives a bound of $|I| \ll N^{3/2}$. The $|I| \ll N^{5/4}$ bound of the theorem is much better than $3/2$, and is in fact a sharp bound.

Proof: (Of Elekes bound) Suppose $A \subseteq \mathbb{R}$ is finite, $P = \{(a+b, cd) : a, b, c, d \in A\}$, and $L = \{y = a(x-b) : a, b \in A\}$. Then $|L| = A^2$ and $|P| = |A+A| \cdot |AA|$. But every line in L contains at least $|A|$ points from P, so $|I| \geq |L||A| = |A|^3$. Applying Szemeredi-Trotter, we get

$$|A|^3 \leq |I| \ll (|P||L|+|P|+|L|)^{2/3} = (|AA||A+A||A|^2+|AA||A+A|+|A|^2)^{2/3} << (|AA||A+A|)^{2/3}|A|^{4/3}$$

and hence $\max\{|A+A|, |AA|\}^2 \geq |A+A||AA| >> |A|^{5/2}$.

1.35 Theorem: (Bourgain-Katz-Tao, 2004; Konyagin-Glibichuk) For every δ, there exists $\varepsilon > 0$ such that for any prime p and any $A \subseteq \mathbb{F}_p$, if $|A| \leq p^{1-\delta}$,

$$|A+A| + |AA| \geq |A|^{1+\varepsilon}.$$

1.36 Open Problem: Suppose $f \in \mathbb{F}_p[x, y]$. Then either

- $f = Q(u_1(x) + u_2(y))$,
- $f = Q(u_1(x)u_2(y))$, or
- for every δ there exists ε such that for all $A \subseteq \mathbb{F}_p$ with $|A| < p^{1-\delta}$ we have $|f(A, A)| \geq |A|^{1+\varepsilon}$.

Bukh-Tsimerman have shown this with the additional assumption that $|A| \geq p^{15/16}$; their result has since been improved by Tao.

1.37 Lemma: (An easy but crucial part of the proof of the theorem) Set $Alg_n(A) = \{\frac{a_1 \pm \ldots \pm a_n}{b_1 \pm \ldots \pm b_n} : a_i, b_i \in (A \cup A^{-1})^n\}$. Then for all $\varepsilon > 0$ there exists $\delta > 0$ such that for all $A \subseteq \mathbb{F}_p$, $|A| < p^{1-\delta}$, we have $|Alg_3(A)| \geq |A|^{1+\varepsilon}$.

Proof: Follows from the observation that if $\phi_x : A \times A \to \mathbb{F}_p$ is the map $(a, b) \mapsto ax + b$, then ϕ_x is injective unless $x \in B = \frac{A-A}{A-A}$. Indeed, if there exist $(a, b) \neq (c, d)$ such that $ax + b = cx + d$ then $a \neq c$ and $x = \frac{d-b}{a-c} \in B$.

For contradiction, suppose $|Alg_3(A)| \leq |A|^{1+\varepsilon}$. We claim that this implies B is a subring. To show $x, y \in B$ implies $xy \in B$ and $x + y \in B$, it is enough to show that ϕ_{xy} and ϕ_{x+y} are not injective. This follows since $\phi_{x+y}(A \times A), \phi_{xy}(A \times A) \subseteq Alg_3(A)$. If the maps were injective, then their image would have cardinality $|A|^2$, which is impossible by assumption. Thus, the maps are not injective, and B is a subring. But the only subring of $\mathbb{F}_p$ is $\mathbb{F}_p$ itself, and this should be enough to prove the result.

1.38 Remark: From this baby version of the sum-product, using Rusza covering lemma multiple times gives $|AA + A| \geq |A|^{1+\varepsilon}$ unless $|A| > p^{1-\delta}$.

1.39 References:

- Tao-Wu additive combinatorics (CUP)
- St. Andrews group theory congress (2013)

- Minnesota IMA meeting (2014)
- MSRI proceedings (2012)

1.40 Definition: Given $\delta > 0$ and $A \subseteq \mathbb{R}$, define $N_\delta(A)$ to be the minimum number of intervals of length δ needed to cover A. If A is "very discrete", $N_\delta(A) \approx |A|$ for small values of δ, since very few points will share intervals.

1.41 Theorem: (Bourgain - Discretized sum-product in $\mathbb{R}$) For all $\sigma, \kappa > 0$, there exist $\varepsilon, \beta > 0$ such that for every scale $\delta > 0$ and bounded subset $A \subseteq \mathbb{R}$, if

- $N_\delta(A) \leq \delta^{-(1-\sigma)}$
- Non-concentration: For every interval I of length at least δ, $N_\delta(A \cap I) \leq \left(\frac{|I|}{\delta}\right)^\kappa \delta^{-\varepsilon}$

Then $\max\{N_\delta(A+A), N_\delta(AA)\} \geq N_\delta(A)^{1+\beta}$.

1.42 Corollary: (Erdos ring conjecture) Every measurable subring of $(\mathbb{R}, +, \cdot)$ is either $\mathbb{R}$ itself or has Hausdorff dimension zero.

1.43 Corollary: (Bourgain-Gambura) If $a, b \in SO(3, \overline{\mathbb{Q}})$ and $\langle a, b\rangle$ is Zariski-dense, then there is a spectral gap $T_{a,b} : L^2_0(SO(3,\mathbb{R})) \to L^2_0(SO(3,\mathbb{R}))$ with $f \mapsto \frac{1}{4}(f \circ a + f \circ a^{-1} + f \circ b + f \circ b^{-1})$ with $\|T_{a,b}\| < 1$.

1.44 Remark: Benoist-de Saxcé (?) extended this to any semi-simple compact Lie group. The proof is based on a non-abelian version of Bourgain's sum-product theorem (de Saxcé's thesis).

1.45 Theorem: (de Saxcé) If G is a semi-simple real Lie group (eg $SL_n(\mathbb{R})$, $SO(n,\mathbb{R})$) then any measurable dense dsubgroup of G is either G or has Hausdorff-dimension zero.

2 Approximate groups

2.1 Small doubling

2.1 Definition: Let G be a group, $k \geq 1$. A finite subset $A \subseteq G$ has *doubling at most k* or *bounded doubling* (if k is arbitrary) if $|AA| \leq k|A|$.

2.2 Freiman Inverse Problem: Describe thes tructure of subsets of bounded doubling.

2.3 Examples: ("Baby cases")

1. $|AA| = |A|$ iff there exists $H \leq G$ (a finite subgroup) and $a \in G$ such that $A = aH = Ha$.
2. Suppose $k < 3/2$. Then $|AA| \leq k|A|$ iff there exists $H \leq G$ with $|H| \leq k|A|$ such that $aH = Ha$ for all $a \in A$ and $A \subseteq aH$.

Proof:

1. The reverse direction is obvious. Assume $|AA| = |A|$; since G is a group, left multiplication is injective, so $|aA| = |A|$ for all $a \in A$. Since $aA \subseteq AA$, this means $aA = AA$ for all $a \in A$, and hence $aA = bA = Aa = Ab = AA$ for all $a, b \in A$. Then $a^{-1}bA = A$ for all $a, b \in A$, so $H = A^{-1}A$ satisfies $HA = A$, and hence $|H| \leq |A|$. But clearly $|H| \geq |A|$, and hence $|H| = |A|$. Moreover, $a^{-1}A \subseteq H$, so $a^{-1}A = b^{-1}A = H$ for all $a, b \in A$. We also have $HA = A$ implies $HHA = A$, and so $|HH| \leq |A| = |H|$, which means $|HH| = |H|$. But $1 \in H$, so $H \subseteq HH$, so $H = HH$. Hence H is stable under multiplication and is finite, which means H is a subgroup. From $HA = A$, we get $Ha = A$ for all $a \in A$, and similarly $aH = A$.

2. Again, the reverse direction is obvious. Assume $|AA| \leq k|A|$, and set $H = A^{-1}A$. Observe that for all $a, b \in A$,

$$|aA \cap bA| = |aA| + |bA| - |aA \cup bA| > 2|A| - \frac{3}{2}|A| \geq \frac{1}{2}|A| > 0$$

so for all $a, b \in A$ there exist $c, d \in A$ with $ac = bd$, ie $b^{-1}a = dc^{-1}$. Thus $H = A^{-1}A = AA^{-1}$. Note further that if $x \in H$, then

$|Ax \cap A| = |\langle (a, b) \in A \times A : bx = a \text{ ie } x = b^{-1}a \rangle| =$ the number of ways to write x as $b^{-1}a, a, b \in A$

and similarly for $|xA \cap A|$; both are at least $\frac{1}{2}|A|$. Then for ally $x, y \in H$, there exist at least $\frac{1}{2}|A|$ representations of x as ab^{-1} and at least $\frac{1}{2}|A|$ representations of y as cd^{-1}, $a, b, c, d \in A$. Then for all $x, y \in H$, there exist $a, b, c, d \in A$ with $x = ab^{-1}$, $y = cd^{-1}$ with $b = c$ (pidgeonhole principle) and so $xy = ab^{-1}cd^{-1} = ad^{-1} \in H$, and hence $HH \subseteq H$, which means H is a subgroup. The rest of the proof is an exercise.

2.4 Remark: If $A = [0, n] \subseteq (\mathbb{Z}, +)$ then $|A + A| = 2|A| - 1 < 2|A|$, but A is not close to any finite subgroup (since the only finite subgroup of $\mathbb{Z}$ is the trivial group).

2.5 Theorem: (Hamidoune) If $|AA| \leq k|A|$ and $k < 2$, then $A \subseteq XH$ where $|X| \leq \frac{2}{2-k}$ and H is a subgroup with $|H| \leq k|A|$.

2.2 Small tripling

2.6 Question: Suppose $|AA| \leq k|A|$. Is it ture that $|A^n| \leq f(k, n)|A|$ for all $n \geq 2$? The answer is no.

For example, suppose G is a finite group, $H \leq G$ a subgroup with $|H|$ large such that there exists $x \in G$ such that $H \cap xHx^{-1} = 1$. Set $A = H \cup \{x\}$. Then $AA = Hcup Hx \cup xH \cup \{x^2\}$, so $|AA| \leq 3|H| + 1 < 3|A|$. However, $AAA \supseteq HxH$ is the disjoint union of Hxh for all $h \in H$, and so $|AAA| \geq |H|^2 \geq (|A| - 1)^2$.

For a more concrete example, take $G = S_{2n}$, the symmetric group on n elements, and $H = \langle \sigma \rangle$ where $\sigma = (1\ 2 \ldots n)$. Take x to be $x(i) = n + i$ for $i = 1, \ldots, n$. Then $xHx^{-1} \cap H = \{1\}$, and so the details above follow with this choice of H and x.

2.7 Lemma: (small tripling lemma) If $|A^3| \leq k|A|$ then $|A^n| \leq k^{n-1}|A|$ and even $|(A \cup A^{-1})^n| \leq k^{O(n)}|A|$ for all $n \geq 2$.

2.8 Remark: In these arguments, we're taking k independent of everything else: A, the ambient group, etc.

2.9 Definition: Given finite subsets A, B of a group, we define the Rusza distance to be

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

Note that $d(A,A) = \log\left(\frac{|AA^{-1}|}{|A|}\right)$.

2.10 Lemma: (Rusza triangle inequality) $d(B,A) = d(A,B) \leq d(A,C) + d(C,B)$.

Proof: This is equivalent to $|AB^{-1}||C| \leq |AC^{-1}||CB^{-1}|$. Given $x \in AB^{-1}$, pick $a \in A$, $b \in B$, such that $x = a_x b_x^{-1}$. Consider the map $\phi : AB^{-1} \times C \to AC^{-1} \times CB^{-1}$ given by $(x,c) \mapsto (a_x c^{-1}, cb_x^{-1})$. We claim that this map is injective. Indeed, $a_x c^{-1} = a_y d^{-1}$ and $cb_x^{-1} = db_y^{-1}$ implies (by multiplying) that $a_x b_x^{-1} = a_y b_y^{-1}$, and hence $x = y$ and $c = d$.

Proof: (of Small tripling lemma) $|A^{n+1}| = |A^{n-1}A^2|$, and so (taking $B = A^{-2}$ and $C = A^{-1}$), we have

$$(*) \qquad |A^{n+1}||C| \leq |A^{n-1}C^{-1}||CB^{-1}| \leq |A^n||A^{-1}A^2|$$

by the Rusza triangle inequality. Now

$$|A^{-1}A^2||C| \leq |A^{-1}C^{-1}||CA^2|$$

so, using $|C| = |A^{-1}| = |A|$,

$$|A^{-1}A^2||A| \leq |A^{-2}||A^3| = |A^2||A^3| \leq |A^3|^2 \leq k^2|A|^2$$

and so $|A^{-1}A^2| \leq k^2|A|$. Plugging this back into $(*)$, we get $|A^{n+1}| \leq k^2|A^n|$.

To get $|(A \cup A^{-1})| \leq k^{O(n)}|A|$, it is enough by what we did to show that $|A \cup A^{-1}|$ has tripling $\leq k^{O(n)}$, ie we need to bound AAA^{-1}, $AA^{-1}A$, and $A^{-1}AA$. All are $\leq k^{O(1)}|A|$ by a a similar use of Rusza's triangle inequality.

2.11 Remark: If instead $|A^3| < k|A|$ assume $|A^2A^{-1}| < k|A|$ or $|A^{-1}A^2| < k|A|$; then the same conclusion holds.

2.3 Approximate subgroups

2.12 Definition: A k-approximate subgroup of G is a subset $A \subseteq G$ such that

- $1 \in A$, $A^{-1} = A$
- $AA \subseteq XA$ for a subset X of size $|X| \leq k$

2.13 Remarks:

- This definition works for infinite groups, but we will generally be interested in finite approximate subgroups.
- $A^n \subseteq X^{n-1}A$, so $|A^n| \leq k^{n-1}|A|$
- $AA \subseteq XA \cap AX^{-1}$, so it doesn't matter in the definition whether we take XA or AX.

2.14 Lemma: If $A \subseteq G$ is any symmetric (ie $A = A^{-1}$) finite subset such that $|A^5| \leq k|A|$ then A^2 is a k-approximate subgroup.

Proof: Follows directlyl from the Ruzsa covering lemma: $|A^4 A| \leq k|A|$, and so $A^4 \subseteq XA^{-1}A = XA^2$ for some $|X| \leq k$.

2.15 Definition: Two symmetric sets A, B are *k-commensurable* if there exists X such that $|X| \leq k$, $A \subseteq XB$, and $B \subseteq XA$.

2.16 Lemma: If $A \subseteq G$ is finite such that $|A^3| \leq k|A|$ then $B = (A \cup A^{-1})^2$ is a $O(k^{O(1)})$-approximate subgroup which is $O(k^{O(1)})$-commensurable to AA^{-1} and $A^{-1}A$. In particular, $|B| \leq O(k^{O(1)})|A|$.

Proof: $|(A \cup A^{-1})^5| \leq O(k^{O(1)})|A|$ by the small tripling lemma. Then B is an $O(k^{O(1)})$-approximate subgroup, and so applying Rusza's covering lemma gives $|AB| \leq O(k^{O(1)})|A|$, which implies $B \subseteq XA^{-1}A$.

2.17 Lemma: (Petridis, 2011) If $A, B \subseteq G$ are two subsets and $|AB| \leq k|A|$ then there exists $X \subseteq A$ such that for every finite $C \subseteq G$, $|CXB| \leq k|CX|$.

2.18 Remark: When $A = B$, we get that $|AA| \leq k|A|$ implies there exists $X \subseteq A$ with $|X^3| \leq k^3|X|$ and $|X| \geq |A|/k$ (taking $C = X$, $C = 1$ respectively). Proof:

$$|X^3| \leq |XXA| \leq k|XX| \leq k|AA| \leq k^2|A| \leq k^3|X|$$

2.19 Corollary: If $|AA| \leq k|A|$ then there exists $A' \subseteq A$, $|(A')^3| \leq k^3|A'|$, $|A'| \geq |A|/k$, and $A^{-1}A$ and AA^{-1} are $O(k^{O(1)})$-commensurable to a $O(k^{O(1)})$-approximate subgroup.

Proof: (of Petridis's lemma) Pick $X \subseteq A$ with $\frac{|XB|}{|X|}$ minimal; note that $\frac{|XB|}{|X|} \leq \frac{|AB|}{|A|} = k$. The proof then goes by induction on $|C|$. Suppose $|CXB| \leq k|CX|$ for some C, and set $C' = C \cup \{g\}$ for an arbitrary $g \in G$. Then

$$\begin{aligned}
|C'XB| &= |CXB| + |gXB| - |CXB \cap gXB| \\
&\leq |CXB| + |XB| - |X'B| && \text{where } X' = CX \cap gX \\
&\leq k_0|CX| + k_0|X| - |X'B| && \text{where } k_0 = \frac{|XB|}{|X|} \\
&\leq k_0|CX| + k_0|X| - k_0|X'| && \text{by minimality of } k_0
\end{aligned}$$

And this is equal to

$$k_0(|CX| + |gX| - |CX \cap gX|) = k_0|C'X|$$

and then the induction follows from the fact that k_0 is minimal, and in particular $k_0 \leq k$.

2.20 Consequence: (Plunnecke-Rusza Inequalities) Suppose G is abelian and $A \subseteq G$. If $|A+A| \leq k|A|$ then for all n, m, $|nA - mA| \leq k^{n+m}|A|$.

Proof: Pick X as in Petridis's Lemma. Then $|C + X + A| \leq k|C + X|$ for all C. Set $C = nA$. Then $|(n+1)A + X| \leq k|nA + X|$, so by induction, $|nA + X| \leq k^n|A + X|$. The Rusza triangle inequality then gives

$$|X||nA - mA| \leq |nA + X||mA + X| \leq k^{n+m}|X|^2 \leq k^{n+m}|X||A|$$

and dividing by $|X|$ gives the result.

2.4 Structure theorem for approximate subgroups of simple algebraic groups

2.21 Main Theorem: (qualitative Hrushovski, quantitative B-Green-Tau, variant Pyber-Szabo) Let $\mathbb{G}$ be a simple linear algebraic group, K an algebraically closed field, and $A \subseteq \mathbb{G}(K)$ a finite k-approximate subgroup. Assume $(*)$: A is not contained in a proper algebraic subgroup of positive dimension. Then A is $O(k^{O(1)})$-commensurable to a finite subgroup. In fact, either $|A| = O(k^{O(1)})$ or $|\langle A\rangle| \leq O(k^{O(1)})|A|$.

2.22 Corollary: (Product Theorem) Fix $\mathbb{G}$ simple algebraic. Then for all $\delta > 0$ there exists $\varepsilon = \varepsilon(\delta, \dim \mathbb{G})$ (ie ε independent of the field) such that for all fields K and all $A \subseteq \mathbb{G}(K)$ satisfying $(*)$, if $|A| \leq |\langle A\rangle|^{1-\delta}$ ($|\langle A\rangle|$ could be infinite) then $|AAA| \geq |A|^{1+\varepsilon}$.

Proof: (Assuming the Main Theorem holds) We have $|AAA| \leq k|A|$ with $k = |A|^{\varepsilon}$, $\varepsilon = \varepsilon(\dim \mathbb{G})$. This works because we have polynomial bounds on k in the main theorem.

2.23 Corollary: (For finite fields) There exists $\varepsilon = \varepsilon(\dim \mathbb{G})$ such that for all finite fields K and all generating subsets $A \subseteq \mathbb{G}(K)$, $|AAA| \geq \min\{|A|^{1+\varepsilon}, |\mathbb{G}(K)|\}$.

2.24 Corollary: (Diameter bound) For all generating sets S of $\mathbb{G}(\mathbb{F}_q)$,

$$\operatorname{diam}_S(\mathbb{G}(\mathbb{F}_q)) \leq O(\log q)^{O(1)}$$

and the implied constants depend only on $\dim \mathbb{G}$.

2.25 Lemma: (Larsen-Pink inequality) If $\mathbb{G}$ is a simple linear algebraic group over K, V a subvariety of $\mathbb{G}$, A a k-approximate subgroup of $\mathbb{G}(K)$ satisfying $(*)$. Then $|A \cap V| \leq O(k^{O(1)})|A|^{\dim V/\dim \mathbb{G}}$.

2.26 Definition: *Proof:* (of Main Theorem) Follows from Larsen-Pink, looking at maximal tori. We say that a maximal torus T is *involved in* A if $A^2 \cap T_{reg} \neq \emptyset$, where $T_{reg} = T \cap \mathbb{G}_{reg}$ and $\mathbb{G}_{reg} = \{g \in \mathbb{G} : \text{multiplicity of 1 as an eigenvalue of } \mathrm{Ad}(g) \text{ is minimal}\}$.

Claim: 1. If T is an involved (in A) torus then

$$|A|^{\dim T/\dim \mathbb{G}} \ll_k |T \cap A^2| \ll_k |A|^{\dim T/\dim \mathbb{G}}$$

where $x \ll_k y$ means $x \ll O(k^{O(1)})y$.

Proof: The upper bound follows from Larsen-Pink. For the lower bound, pick $a_0 \in A^2 \cap T_{reg}$, and look at $A \to Cl(a_0) = \{ga_0g^{-1} : g \in \mathbb{G}\}$. We have

$$|A| \leq |A^3 \cap Cl(a_0)||A^2 \cap C_G(a_0)|$$

where $C_G(a_0)$ is the centralizer of a_0. Then $C_G(a_0)^O = T$ since a_0 is regular. Apply Larsen-Pink with $V = \overline{Cl(a_0)}$; so $\dim V = \dim \mathbb{G} - \dim T$. Then $|A^2 \cap T| \gg |A|^{\dim T/\dim G}$.

Claim: 2. If T is involved in A so is aTa^{-1} for all $a \in A$, provided $|A| \gg k^{O(1)}$.

Proof: Exercise.

Let $\mathcal{C}$ be the set of involved tori; $\mathcal{C}$ is finite because A is. Then $\mathcal{C}$ is $\langle A\rangle$-invariant by conjugation, and so $\langle A\rangle$ is finite and

$$|\mathcal{C}| \geq |T^{\langle A\rangle}| = \frac{|\langle A\rangle|}{|\langle A\rangle \cap T|} \geq |\langle A\rangle|^{1-\dim T/\dim G}.$$

Moreover,

$$|\mathcal{C}| \leq \frac{|A^2|}{|A|^{\dim T/\dim G}} \approx_k |A|^{\dim T/\dim G}$$

and comparing the inequalities gives

$$|\langle A\rangle| \ll_k |A|.$$

3 Structure theorem for approximate groups

3.1 Last Time: Regarding the Freiman Inverse Problem (ie classifying sets of doubling at most k):

- We've shown if $k < 2$ then only subgroups appear (A is commensurable to a subgroup)
- We've described GAP of dimension $\leq d$ (examples: approximate groups with $k \leq 2^d$), *not* commensurable to subgroups)
- Coset GAP: HP with $P \subseteq N_G(H)$, P a GAP, $H \leq G$ a subgroup
- Freiman-Green-Rusza Theorem: If G is abelian then any approximate group is commensurable to GAP
- We've classified approximate subgroups of simple algebraic groups with polynomial bounds, A is $O(k^{O(1)})$-commensurable to a subgroup.

3.2 Open Problems:

- Extend the theorem for simple algebraic groups to any algebraic group.
- Is it true that if $A \subseteq G$ is a subset such that $|A^3| \leq k|A^2|$ then A^2 is $C(k)$-commensurable to an approximate subgroup?
- Infinite approximate subgroups: G lcoally compact, A bounded open set (ie contained in a compact subset of G), classify approximate subgroups (looked at by a student of Tao's). Also interesting is a discretized or entropy version, $N_\delta(A)$, δ a small scale
- Consider a specific group, and try to get good bounds. For example, Razborov-Safin showed that if G is a free group, $A \subseteq G$ finite, then $|AAA| \geq |A|^2/100$ provided A is not contained in a cyclic subgroup.

3.3 Theorem: (BGT structure theorem - weak form) Suppose G is a group, $k \geq 1$, $A \subseteq G$ finite such that $|AA| \leq k|A|$. Then there exists $X \subseteq G$ with $|X| \leq C(k)$, and a virtually nilpotent subgroup H of G such that $A \subseteq XH$.

3.4 Corollary: (Gromov's Theorem) Every finite group of polynomial growth is virtually nilpotent.

Proof: (assuming weak structure theorem) Let S be a generating set for G with $1 \in S = S^{-1}$. We know that $|S^n| = O(n^c)$. Recall the remark that there exist $n_1 < n_2 < \dots$ such that $|S^{2n_k}| \leq 3^C |S^{n_k}|$. Then applying the theorem gives $S^{n_k} \subseteq X_k H_k$ where $|X_k| \leq C'$ and H_k virtually nilpotent.

> **Claim:** If $G = \langle S \rangle$, $1 \in S = S^{-1}$, and $H \leq G$ has infinite index, then S^n must intersect at least n cosets of H.
>
> *Proof:* Look at the Schreier graph of G/H, with vertices elements in G/H and $xH \sim sxH$ if $s \in S$. Then this graph is connected (since S is a generating set) and so as soon as $n_k > c'$, we must have $[G : H_k] < \infty$.

3.5 Example: (of a set of bounded doubling in a nilpotent group) The Heisenberg group is

$$\left\{ \begin{matrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{matrix} : x, y, z \in \mathbb{Z} \right\}.$$

Consider the subset

$$A = \left\{ \begin{matrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{matrix} : |x| \leq N_1, |y| \leq N_2, |z| \leq N_3,\ N_1, N_2, N_3 \in \mathbb{N} \right\}.$$

If $N_1, N_2 \leq N_3$, then $|AA| \leq 2^4 |A|$ (exercise).

3.6 Definition: (Progressions) Let G be a group, $x_1, \dots, x_r \in G$, $N_1, \dots, N_r \in \mathbb{N}$, and consider the set P of all products of x_i and x_i^{-1}, $i = 1, \dots, r$, with at most N_i copies of x_i or x_i^{-1}. Then $P = P(x_1, \dots, x_r; N_1, \dots, N_r)$ is the progression with base $x_1, \dots, x_r$ and side lengths $N_1, \dots, N_r$; clearly P is finite. We call r the *rank* of P.

A progression $P = P(x_1, \dots, x_r; N_1, \dots, N_r)$ is called a *nilprogression* if $\langle P \rangle = \langle x_1, \dots, x_r \rangle$ is nilpotent. We say that P has rank at most r and step at most s if $\langle P \rangle$ has nilpotency class at most s.

3.7 Example: The set A in the previous example is commensurable to the nilpotent progression $P(a, b, c; N_1, N_2, N_3)$, where

$$a = \begin{matrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{matrix} \quad b = \begin{matrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{matrix} \quad c = \begin{matrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{matrix}$$

3.8 Definition: A *coset nilprogression* is a finite subset of G of the form HP, where $H \leq G$, P is a nilprogression, and $P \subseteq N_G(H)$. Note that every nilprogression is a coset nilprogression, taking $H = \{1\}$.

3.9 Proposition: There exists $k = k(r, s)$ such that every coset nilprogression of rank at most r and step at most s (and side lengths $N_i \geq C(r, s)$) is a k-approimate subgroup.

3.10 Theorem: (Tointon) If G is nilpotent of step s and A is a k-approximate subgroup then A is $e^{O_s(k^{O_s(1)})}$-commensurable to a coset nilprogression of step $\leq s$ and rank $\leq O_s(k^{O_s(1)})$.

3.11 Theorem: (Strong Form) Suppose G is a group, $k \geq 1$, and A a k-approximate subgroup. Then A is $C(k)$-commensurable to a coset nilprogression of step and rank $\leq C'(k)$.

3.12 Warning: We have that $C'(k)$ is $O(k^{O(1)})$, but we have no explicit bound on $C(k)$.

3.13 Lemma: (Stabilizer Theorem - Hrushovski, Sanders, Croot-Sisask, independently). If G, k, A as in the theorem and $l \in \mathbb{N}$, then there exists $S \subseteq A^4$ such that

- $1 \in S = S^{-1}$
- $|S| \geq |A|/C(k,l)$
- $S^l \subseteq A^4$

3.14 Lemma: (Gleason-Yamabe Theorem, 1981) Any locally compact group has an open subgroup G', which is a generalized Lie group. Ie, for every neighbourhood U of the identity in G', there is a compact subgroup $K \subseteq U$ which is normalized by G' and such that G'/K is a connected Lie group.

Proof: If G is compact, this is called the Peter-Weyl theorem (proof relies on the spectral theorem for convolution operators $f \mapsto \phi * f$ on $L^2(G)$). For the non-compact setting, we use the Gleason norms: if $U \subseteq G$ is a neighbourhood of the identity, set $n_U(g) = \inf\{n \in \mathbb{N} : g^n \notin U\}$ and $\|g\|_U = (n_U(g))^{-1}$.

We can then apply the Gleason Lemma: There exist U and $c > 0$ so that

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

Now take $K = \{g : \|g\|_U = 0\}$ (this is a subgroup by (2) and normal by (1), and observe that G/K has no small subgroups.

Proof: (of Strong theorem) The proof breaks down into three steps.

Step 1: For contradiction, suppose $A_n \leq G_n$ are all k-approximate subgroups. Form the ultraproduct $\mathbb{A} = \prod_{\mathcal{U}} A_n \subseteq \mathbb{G} = \prod_{\mathcal{U}} G_n$. Then $\mathbb{A}\mathbb{A} \subseteq X\mathbb{G}$ for some $X \subseteq \mathbb{G}$ with $|X| \leq k$, so $\mathbb{A}$ is an (infinite) k-approximate subgroup of $\mathbb{G}$. Apply the stabilizer theorem to each A_n to get $S_{l,n}$ such that $(S_{l,n})^l \subseteq A_n^4$; we can assume that $(S_{l+1,n})^2 \subseteq S_{l,n}$. Then let $\mathbb{S}_l = \prod_{\mathcal{U}} S_{l,n}$, and set $\Gamma = \bigcap \mathbb{S}_l$.

Then Γ is a subgroup of $\mathbb{G}$, and in fact, we can make sure that $(S_l^l)^{A^l} \subseteq A^4$, so $\Gamma \lhd \mathbb{G}' = \langle \mathbb{A} \rangle$. We can show that $\mathbb{G}'/\Gamma$ is locally compact and $\pi(\mathbb{A})$, the image of $\mathbb{A}$ under the canonical projection, is a compact neighbourhood of the identity in $\mathbb{G}'/\Gamma$. Then for all $F \subseteq U \subseteq \mathbb{G}'/\Gamma$, with F closed and U open, there exists $B_n \subseteq A_n$ such that $\pi^{-1}(F) \subseteq \prod_{\mathcal{U}} B_n \subseteq \pi^{-1}(U)$.

Step 2: Apply the Gleason-Yamabe theorem; somehow A takes the place of U and H takes the place of K.

Step 3: We have shown that there exists $e \in A \setminus \{1\}$ such that $[e,g] = 1$ for (almost all?) $g \in A$. This will be the base of the nilprogression.

Proof: (of Stabilizer Theorem, due to Croot-Sisask) For $\varepsilon > 0$, set

$$S_\varepsilon = \{g \in G : \|1_A * 1_A - g(1_A * 1_A)\|_2 < \varepsilon \|1_A * 1_A\|_2\}$$

where $f * g(x) = \sum_{y \in G} f(xy^{-1})g(y)$; note that $\mathrm{supp}(f * g) = (\mathrm{supp}\, f)(\mathrm{supp}\, g)$. It is clear that $1 \in S_\varepsilon = S_\varepsilon^{-1}$ and $S_\varepsilon^{[1/\varepsilon]} \subseteq A^4$: if $s_1, \ldots, s_l \in S$ then (for ε sufficiently small)

$$\|1_A * 1_A - (s_1 - s_l)1_A * 1_A\|_2 \leq \sum_{i=1}^{k} \|1_A * 1_A - s_i(1_A * 1_A)\|_2 < \varepsilon l \|1_A * 1_A\|_2 < \|1_A * 1_A\|_2$$

so $A^2 = \mathrm{supp}(1_A * 1_A)$ must intersect $(s_1 - s_l)\,\mathrm{supp}(1_A * 1_A)$, so $s_1 - s_l \in A^4$. All that remains to show is that S_ε is large, ie that $|S_\varepsilon| \geq |A|/C(k, \varepsilon)$.

Let $Tf = f * 1_A = \sum_{z \in G} f(z)1_{zA}$. If $\mathrm{supp}(f) \subseteq A^2$ then $\frac{Tf}{|A^2|} = \frac{1}{|A^2|}\sum_{z \in A^2} f(z)1_{zA}$, ie it is a weighted average of the 1_{zA} for $z \in A^2$.

Idea (probalistic method) Pick m independent random variables uniformly in A^2, ie $z_1, \ldots, z_m$ are uniform in A^2, ie $P(z_i = z) = \frac{1}{|A^2|}$ for $z \in A^2$. Set $\frac{Rf}{|A^2|}$ to be $\frac{1}{m}\sum_{i=1}^{m} f(z_i)1_{z_i A}$.

Claim: 1. With > 0 probability (ie there exist $z_1, \ldots, z_m \in A^2$) there are at least $|A|/2$ gs in A such that

$$\|R1_{gA} - T1_{gA}\|_2 < \frac{2k^{3/2}}{\sqrt{m}}\|T1_A\|_2$$

Proof: Follows from claim 2; indeed, if claim 1 fails then with probability 1, there exists $\geq |A|/2$ gs in A such that

$$\|R1_{gA} - T1_{gA}\|_2 \geq \frac{2k^{3/2}}{\sqrt{m}}\|T1_A\|_2$$

so

$$\frac{1}{|A|}\sum_{g \in A} \|R1_{gA} - T1_{gA}\|_2^2 \geq \frac{2k^{3/2}}{\sqrt{m}}\|T1_A\|_2^2$$

but taking expected value, this contradicts claim 2.

Claim: 2. For all $g \in A$, $E(\|R1_{gA} - T1_{gA}\|_2^2) \leq \frac{k^3}{m}\|T1_A\|_2^2$, where $E(\ldots)$ is the expected value.

Proof: Let $f = 1_{gA}$, and note that $\|1_A * 1_A\|_1 = |A|^2$, so (since $|A^2| \subseteq XA$), Cauchy-Schwartz tells us that

$$\|1_A * 1_A\| \leq \sqrt{|\,\mathrm{supp}(1_A * 1_A)|}\sqrt{\|1_A * 1_A\|_2}$$

so $\|T1_A\|_2 = \|1_A * 1_A\|_2 \geq \frac{|A|^{3/2}}{\sqrt{k}}$. Now

$$E(\|Rf - Tf\|_2^2 = E(\|Rf\|^2) + \|Tf\|^2 - 2E\langle Rf, Tf\rangle = E\|Rf\|^2 - \|Tf\|^2.$$

But $E(Rf) = Tf$, so $Rf = |A^2|\frac{1}{m}\sum f(z_i 1_{z_i A})$ so the expectation is

$$= \frac{m^2 - m}{m^2}\|Tf\|^2 + \frac{|A^2|^2}{m}E(f(z_i)^2)|A| - \|Tf\|^2 \leq \frac{k^2|A|^3}{m} \leq \frac{k^3}{m}\|T1_A\|_2^2$$

Assume the claim holds. Then

$$R1_{gA} = \sum_{i=1}^{m} 1_{gA}(z_i)\frac{|A^2|}{m}1_{z_iA}.$$

This is a linear combination of m functions taking values in $\{0,1\}$, so there are only 2^m such functions. Then there exists $A'' \subseteq A$ with $|A''| \geq |A|/2^{m+1}$ such that $R1_{gA} = R1_{hA}$ for all $g, h \in A''$. Then

$$\|T1_{gA} - T1_{hA}\|_2 = \|g1_A * 1_A - h1_A * 1_A\|_2 < \frac{4k^{3/2}}{\sqrt{m}}\|1_A * 1_A\|_2$$

Pick m such that $\frac{4k^{3/2}}{\sqrt{m}} = \varepsilon 10$, and we are done.