Part III – Introduction to Approximate Groups (Ongoing course)

Based on lectures by Dr M. Tointon
Notes taken by Bhavik Mehta

Lent 2019

Contents

0 Introduction

Lecture 1

A subgroup $H < G$ is a non-empty set closed under products and inverses. Roughly, an 'approximate subgroup' is a subset that is only 'approximately closed' under products. (Will make this precise soon). Such sets arise naturally in a number of branches of mathematics, and as such approximate groups have had a broad range of applications. In this course, we will look in detail, for example, at applications to *polynomial growth* (fundamental in geometric group theory) and touch on construction of expander graphs (important in theoretical computer science).

1 Small doubling

To start with, we will look at a preliminary notion of approximate closure called *small doubling*. In this course, G is always a group, arbitrary unless specified otherwise.

Notation. Given $A, B \subset G$, write

$$\begin{aligned} AB &\coloneqq \{ab \mid a \in A, b \in B\} \quad \text{'Product sets'} \\ A^n &= \underbrace{A \cdot A \cdots A}_{n \text{ times}} \\ A^{-1} &= \{a^{-1} \mid a \in A\} \\ A^{-n} &= (A^{-1})^n \end{aligned}$$

When G is abelian, often switch to additive notation, e.g. $A + B$, nA, $-A$, $-nA$, called 'Sum sets'.

To say A is closed is to say $A^2 = A$. If A is finite, one way to say that A is 'approximately closed' is to say that

$$|A^2| \text{ is 'not much bigger' than } |A|.$$

This is the notion of approximate closure that arises when studying polynomial growth or expansion, for example.

To get a feel for what this should mean, let's look at the possible values of $|A^2|$. Trivially, $|A| \leq |A^2| \leq |A|^2$. Both bounds are attained. However, although the quadratic upper bound on $|A^2|$ in terms of $|A|$ is extremal, in a strict sense, it should not be seen as atypical for the size of A^2. We will see, for example, in Example Sheet 1 that if A is a set of size n chosen uniformly from $\{1, \dots, n^{100}\}$, then $\mathbb{E}(|A + A|)$ is close to $\frac{1}{2}|A|^2$ (about as large as it can be, because abelian). Therefore, we can view sets satisfying

$$|A^2| = o\big(|A|^2\big) \tag{1.1}$$

as being 'exceptional', and so condition (1.1) can already be seen as a form of 'approximate closure'. In this course, we will concentrate on the strongest form of (1.1), where $|A^2|$ is *linear* in $|A|$, in the sense that

$$|A^2| \leq K|A| \tag{1.2}$$

for some $K \geq 1$ fixed a priori.

Since such sets are 'far from random' we can expect (1.2) to impose a significant restriction on A. The main aim of this course is to work out how significant.

Definition. Given $A \subset G$, the ratio $\frac{|A^2|}{|A|}$ is called the **doubling constant** of A. If A satisfies (1.2), we'll say that A has **doubling** at most K, or simply **small doubling**.

Example (Some simple examples)**.**

- (Empty set)
- A a finite subgroup ($K = 1$)
- $|A| \leq K$
- $A \subset \mathbb{Z}$, $A = \{-n, \dots, n\}$, $|A + A| \leq 2|A|$.

This last example is especially important as it shows the theory does not just reduce to subgroups and 'small' sets. We'll develop these examples later in the course.

One main aim will be to prove theorems along the lines of:

A has small doubling $\Rightarrow$ A has a certain structure.

When K is very small, this is quite easy, as follows:

Theorem 1.1 (Freiman; proof due to Tao)**.** Let $K < \frac{3}{2}$. Suppose $A \subset G$ and $|A^2| \leq K|A|$. Then there is a subgroup $H < G$ with $|H| = |A^2| (\leq K|A|)$ such that

$$A \subset aH = Ha \quad \forall a \in A$$

(i.e. A is a large portion of a coset of a finite subgroup).

Remark. Converse: If $A \subset xH = Hx$ for $x \in G$, with $H < G$ and $|H| \leq K|A|$ then $|H^2| \leq K|A|$. So this is a complete classification of sets of very small doubling.

Lemma 1.2 (Identify H)**.** If $|A^2| < \frac{3}{2}|A|$ then $H = A^{-1}A$ is a subgroup. Moreover, $A^{-1}A = AA^{-1}$ and $|H| < 2|A|$.

Proof. Let $a, b \in A$. The hypothesis gives $|aA \cap bA| > \frac{1}{2}|A|$, so there are more than $\frac{1}{2}|A|$ pairs $(x, y) \in A \times A$ such that $ax = by$, i.e. $a^{-1}b = xy^{-1}$. This immediately gives $A^{-1}A \subseteq AA^{-1}$, and replacing A by A^{-1} gives $AA^{-1} \subseteq A^{-1}A$, so $A^{-1}A = AA^{-1}$ as required.

Since $|A \times A| = |A|^2$ it also implies that

$$\left|A^{-1}A\right| \leq \frac{|A|^2}{\frac{1}{2}|A|} = 2|A|,$$

(dividing by number of repetitions), as claimed.

Note also that $A^{-1}A$ is symmetric, so it remains to show that $A^{-1}A$ is closed under products.

Let $c, d \in A$. As above, there are more than $\frac{1}{2}|A|$ pairs $(u, v) \in A \times A$ such that $c^{-1}d = uv^{-1}$. This means that for at least one pair (x, y) as above and one pair (u, v), we have $y = u$. In particular, $a^{-1}bc^{-1}d = xv^{-1} \in AA^{-1} = A^{-1}A$. □

Lemma 1.3 (Size bound)**.** If $|A^2| < \frac{3}{2}|A|$ then $A^2 = aHa \quad \forall a \in A$ (H as before). In particular, $|H| = |A^2|$.

Proof. First, note that

$$A \subset aH \cap Ha \tag{1.3}$$

by definition of H, so certainly $A^2 \subset aHa$. For the reverse inclusion, let $z \in aHa$. Since H is a subgroup, there are $|H|$ pairs $(x, y) \in aH \times Ha$ such that $z = xy$.

Moreover, by (1.3) and the bound $|H| < 2|A|$ from Lemma 1.2, more than half of these x and more than half of these y belong to A. In particular, this means that for at least one pair x, y, both have to belong to A. Hence $z = xy \in A^2$, as required. □

Proof of Theorem 1.1. Given $a \in A$, we have $Aa^{-1} \subset aHa^{-1} \cap H$ so

$$|aHa^{-1} \cap H| \geq |A| > \frac{1}{2}|H|$$

by Lemma 1.2, but the only subgroup of H of size $> \frac{1}{2}|H|$ is H itself. Hence $aHa^{-1} = H$, so indeed $A \subset aH = Ha$ by (1.3). □

Classifying the sets of small doubling is much harder than this in general, and uses a much wider range of techniques, e.g. group theory, harmonic analysis, geometry of numbers...

2 Covering and higher sum and product sets

We introduce two techniques we'll use repeatedly: *covering* and *bounding higher product sets*. A nice way to do this is by proving the following theorem.

Theorem 2.1 (Rusza)**.** Suppose $A \subset \mathbb{F}_p^r$ satisfies $|A+A| \leq K|A|$. Then $\exists H \leq \mathbb{F}_p^r$ with

$$|H| \leq p^{K^4} K^2 |A| \quad \text{such that } A \subset H.$$

So again, like Theorem 1.1, A is a large proportion of a finite subgroup.

Remark. It is not ideal that $\frac{|A|}{|H|}$ depends on p. We will remove this dependency in a few lectures' time.

We'll start by proving the following weaker version:

Proposition 2.2. Suppose $A \subset \mathbb{F}_p^r$ satisfies $|2A-2A| \leq K|A|$. Then $\exists H < \mathbb{F}_p^r$ with

$$|H| \leq p^K |A-A| (\leq p^K K|A|) \quad \text{such that } A \subset H.$$

We'll prove this using 'covering', encapsulated by the following lemma

Lemma 2.3 (Rusza's covering lemma)**.** Suppose $A, B \subset G$ and $|AB| \leq K|B|$. Then $\exists X \subset A$ with $|X| \leq K$ such that $A \subset XBB^{-1}$. Indeed, we may take $X \subset A$ maximal such that the sets xB (for $x \in X$) are disjoint.

The term 'covering' refers to the conclusion $A \subset XBB^{-1}$, which says 'A can be covered by a few left-translates of BB^{-1}.

Proof. First, disjointness of xB gives that $|XB| = |X||B|$. Since $X \subset A$,

$$|XB| \leq |AB| \leq K|B|,$$

so $|X| \leq K$. By maximality, for all $a \in A$, there is $x \in X$ such that $aB \cap xB \neq \varnothing$, and hence $a \in xBB^{-1}$. Hence $A \subset XBB^{-1}$, as required. □

Lemma 2.4. Suppose $A \subset G$ satisfies $|A^{-1}A^2A^{-1}| \leq K|A|$. Then $\exists X \subset A^{-1}A^2$, with $|X| \leq K$ such that $A^{-1}A^n \subset X^{n-1}A^{-1}A$ for any $n \in \mathbb{N}$.

Proof. By Lemma 2.3, $\exists X \subset A^{-1}A^2$, $|X| \leq K$ such that

$$A^{-1}A^2 \subset XA^{-1}A. \tag{2.1}$$

We then have

$$\begin{aligned} A^{-1}A^n &= A^{-1}A^{n-1}A \\ &\subset X^{n-2}A^{-1}A^2 \quad \text{by induction} \\ &\subset X^{n-1}A^{-1}A. \quad \text{by (2.1)} \end{aligned}$$

□

Proof of Proposition 2.2. By Lemma 2.4, $\exists X$ with $|X| \leq K$ such that

$$nA - A \subset (n-1)X + A - A \quad \forall n \in \mathbb{N}.$$

This means that $\langle A \rangle \subset \langle X \rangle + A - A$, so

$$|\langle A \rangle| \leq |\langle X \rangle| \, |A-A| \leq p^K |A-A|$$

as claimed. □

To strengthen Proposition 2.2 to Theorem 2.1, we use the second technique of this section, bounding higher sum/product sets. The key result is the following, at least in the abelian case.

Theorem 2.5 (Plünnecke-Rusza)**.** Suppose $A \subset G$ for G abelian, and $|A+A| \leq K|A|$. Then for all $m, n \geq 0$,

$$|mA - nA| \leq K^{m+n}|A|.$$

This was proved in Introduction to Discrete Analysis last term. We won't redo the whole proof in lectures, but we will reprove some parts of it. See the Example Sheet for the full result.

Proof of Theorem 2.1. Using Theorem 2.5, $|2A - 2A| \leq K^4|A|$, and $|A - A| \leq K^2|A|$. Then immediate from Proposition 2.2. □

We'll spend the rest of this section discussing Theorem 2.5 and variants of it. We've seen it's useful, at least in one context. To see more philosophically why it's useful, let's think about what the genuine closure of subgroups under products and inverses means. One useful feature is that it can be iterated: given $h_1, h_2, \ldots \in H$, a subgroup, this means that $h_1^{\epsilon_1} \cdots h_m^{\epsilon_m} \in H$ $\forall \epsilon_i = \pm 1$, $\forall n, \forall h_i \in H$. Theorem 2.5 allows us to 'iterate' the 'approximate closure' of a set of small doubling: $a_1 + \cdots + a_m - a_1' - \cdots - a_n'$ may not belong to A, but at least it belongs to $mA - nA$, which is

(a) not too large ($|mA - nA| \leq K^{m+n}|A|$)

(b) itself a set of small doubling ($|2(mA - nA)| \leq K^{2m+2n}|mA - nA|$).

This is an important part of why the theory works so well.

It is therefore unfortunate that Theorem 2.5 does not hold for non-abelian groups:

Example 2.6. Let x generate an infinite cyclic group $\langle x \rangle$, H be a finite group, set $G = H * \langle x \rangle$ (the free product, which has the important property that $x^{-1}Hx \neq H$). Set $A = H \cup \{x\}$. $A^2 = H \cup xH \cup Hx \cup \{x^2\}$, so $|A^2| \leq 3|A|$. But A^3 contains HxH, which has size $|H|^2 \sim |A|^2$.

So as $|H| \to \infty$, Theorem 2.5 cannot hold.

Nonetheless, if we strengthen small doubling slightly, we can recover a form of Theorem 2.5. One way is to replace small doubling with **small tripling**: $|A^3| \leq K|A|$.

Proposition 2.7. Suppose $A \subset G$, $|A^3| \leq K|A|$. Then $|A^{\epsilon_1} \cdots A^{\epsilon_m}| \leq K^{3(m-2)}|A|$ $\forall \epsilon_i = \pm 1$, $\forall m \geq 3$.

The key ingredient is the following:

Lemma 2.8 (Rusza's triangle inequality)**.** Given $U, V, W \subset G$, all finite, we have

$$|U||V^{-1}W| \leq |UV||UW|.$$

Proof. We'll define an injection $\varphi : U \times V^{-1}W \to UV \times UW$. First, for $x \in V^{-1}W$, set $v(x) \in V$ and $w(x) \in W$ such that $x = v(x)^{-1}w(x)$. Set $\varphi(u, x) = (uv(x), uw(x))$. To see that φ is injective, first observe

$$(uv(x))^{-1}(uw(x)) = x,$$

so x determined by $\varphi(u, x)$, and then

$$(uv(x))v(x)^{-1} = u,$$

so u is also determined by $\varphi(u, x)$. □

Proof of Proposition 2.7. First we'll do the case $m = 3$.

- $|A^3| = |A^{-3}| \leq K|A|$.
- Apply Rusza's triangle inequality with $U = W = A$, $V = A^2$:

$$|A||A^{-2}A| \leq |A^3||A^2| \leq K^2|A|^2,$$

  so $|A^{-2}A| \leq K^2|A|$.
- Note that $(A^{-2}A)^{-1} = A^{-1}A^2$, so $|A^{-1}A^2| = |A^{-2}A| \leq K^2|A|$.
- Replacing A by A^{-1} we get

$$|AA^{-2}| = |A^2A^{-1}| \leq K^2|A|.$$

- Finally, Rusza's triangle inequality with $U = V = A$, $W = AA^{-1}$ gives

$$|A||A^{-1}AA^{-1}| \leq |A^2||A^2A^{-1}| \leq K^3|A|^2.$$

  So $|A^{-1}AA^{-1}| \leq K^3|A|$.
- For the last case, swap A, A^{-1} again.

For $m \geq 4$, Rusza's triangle inequality gives

$$\begin{aligned} |A||A^{\epsilon_1} \cdots A^{\epsilon_m}| &\leq |AA^{-\epsilon_2}A^{-\epsilon_1}||AA^{\epsilon_3} \cdots A^{\epsilon_m}| \\ &\leq K^3|A|\ K^{3(m-2)}|A|. \end{aligned}$$

□

3 Approximate Groups

In the last section, we saw that assuming small tripling instead of small doubling allowed us to control higher product sets of the form $A^{\epsilon_1} \cdots A^{\epsilon_m}$. In this section, we'll see another possible strengthening of small doubling. We also saw, in the proofs of Theorem 2.1 and Proposition 2.2, an advantage of having a 'covering' condition in place of a size bound. This motivates in part the following definition.

Definition. A set $A \subset G$ is called a **K-approximate group** (or K-approximate subgroup) if $1 \in A$, $A^{-1} = A$ and $\exists X \subset G$ with $|X| \leq K$ such that $A^2 \subset XA$.

Note that A need not be finite, although in this course it almost always will be. Also, if A is finite, then $|A^2| \leq K|A|$. The conditions $1 \in A$ and $A^{-1} = A$ are convenient 'notationally': for example, this lets us write A^m instead of $A^{\epsilon_1} \cdots A^{\epsilon_m}$ and $1 \in A$ gives us that $A \subset A^2 \subset A^3 \subset \cdots$, which is also convenient at times. It's the condition $A^2 \subset XA$ that is most important.

For approximate groups, bounding higher product sets is easy:

Lemma 3.1. If A is a finite K-approximate group then $|A^m| \leq K^{m-1}|A|$.

Proof. If X is as in the definition of approximate group, in fact we have $A^m \subset X^{m-1}A$:

$$\begin{aligned} A^m &= A^{m-1}A \\ &\subset X^{m-2}A^2 \quad \text{induction} \\ &\subset X^{m-1}A \quad \text{definition of } X \end{aligned}$$

□

Another advantage of approximate groups is that if $\pi : G \to H$ is a homomorphism and $A \subset G$ is a K-approximate group then $\pi(A)$ is also trivially a K-approximate group (although we'll see that there is a version of this for small tripling).

It turns out that sets of small tripling and approximate groups are essentially equivalent, in the following sense:

Proposition 3.2. Let $A \subset G$ be finite. If A is a K-approximate group then $|A^3| \leq K^2|A|$. Conversely if $|A^3| \leq K|A|$ then there is a $\mathcal{O}(K^{12})$-approximate group B with $A \subset B$ and $|B| \leq 7K^3|A|$ ('A is a large proportion of an approximate group'). In fact, we may take $B = (A \cup \{1\} \cup A^{-1})^2$.

Proof. First bit is just Lemma 3.1. For the converse, set $\hat{A} = A \cup \{1\} \cup A^{-1}$, and note that

$$B = \hat{A}^2 = \{1\} \cup A \cup A^{-1} \cup A^2 \cup A^{-1}A \cup AA^{-1} \cup A^{-2}.$$

Each set in this union has size $\leq K^3|A|$ by Proposition 2.7, so $|B| \leq 7K^3|A|$, as claimed. Similarly,

$$\hat{A}^k = \bigcup_{\substack{\epsilon_i = \pm 1 \\ 0 \leq m \leq 4}} A^{\epsilon_1} \cdots A^{\epsilon_m},$$

and the sets in this union have size $\leq K^6|A|$. It follows that $|\hat{A}^4| \leq \mathcal{O}(K^6)|A|$.

So, Lemma 2.4 implies $\exists X \subset G$ with $|X| \leq \mathcal{O}(K^6)$ such that $\hat{A}^n \subset X^{n-2}\hat{A}^2$ for every $n \geq 2$. In particular, $|X^2| \leq \mathcal{O}(K^{12})$ and $\hat{A}^4 = (\hat{A}^2)^2 \subset X^2\hat{A}^2$, so $\hat{A}^2$ is an $\mathcal{O}(K^{12})$-approximate group, as claimed. □

This is all well and good, but what if we are faced with a set like that from Example 2.6 which only has small doubling? In that specific example, a large proportion of A was a set of small tripling, namely H. Rather helpfully, that turns out to be a general phenomenon:

Theorem 3.3. If $A \subset G$ satisfies $|A^2| \leq K|A|$ then there is $U \subset A$ with $|U| \geq \frac{1}{K}|A|$ such that $|U^m| \leq K^{m-1}|U|$ $\forall m \in \mathbb{N}$.

So small doubling reduces to small tripling, which reduces to approximate groups. In Example Sheet 1, we'll see a direct reduction from small doubling to approximate group.

Tao proved a version of Theorem 3.3 when he introduced the definition of approximate groups. We will use instead a lemma of Petridis, which he proved when proving the Plünnecke-Rusza inequalities.

Lemma 3.4 (Petridis)**.** Suppose $A, B \subset G$ are finite, let $U \subset A$ be non-empty, chosen to minimise the ratio $|UB|/|U|$, and write $R = |UB|/|U|$. Then for any finite $C \subset G$, we have

$$|CUB| \leq R|CU|.$$

Proof. Trivial if $C = \varnothing$, so we may assume $\exists x \in C$. Defining $C' = C \setminus \{x\}$, we may also assume by induction that $|C'UB| \leq R|C'U|$. Set $W = \{u \in U \mid xu \in C'U\}$. Then

$$CU = C'U \cup (xU \setminus xW)$$

is a disjoint union, so in particular

$$|CU| = |C'U| + |U| - |W|. \tag{3.1}$$

We also have $xUB \subset C'UB$ by definition of W, so

$$CUB \subset C'UB \cup (xUB \setminus xWB)$$

and hence

$$|CUB| \leq |C'UB| + |UB| - |WB|. \tag{3.2}$$

We have $|C'UB| \leq R|C'U|$ by the induction hypothesis, $|UB| = R|U|$ by definition of R, and $|WB| \geq R|W|$ by minimality in the definition of U. So

$$\begin{aligned} |CUB| &\leq R(|C'U| + |U| - |W|) \quad \text{by (3.2)} \\ &= R|CU| \quad \text{by (3.1).} \end{aligned}$$

□

Proof of Theorem 3.3. Set $U \subset A$ to be non-empty minimising $|UA|/|U|$, and write R for this ratio, noting that $R \leq K$ by minimality. Also, U non-empty, so $|UA| \geq |A|$, so $|U| \geq \frac{|A|}{K}$, as required. Lemma 2.4 also implies that $|U^m A| \leq K|U^m|$ $\forall m$ (taking $C = U^{m-1}$) and since $U \subset A$, this gives $|U^{m+1}| \leq K|U^m|$ $\forall m$, so $|U^m| \leq K^{m-1}|U|$. □

*Bonus content

The reason A in Example 2.6 failed to have small tripling was the existence of $x \in A$ with AxA large. It turns out that this is the only obstruction to small doubling having small tripling:

Theorem (Tao; Petridis)**.** If $|A^2| \leq K|A|$ and $|AxA| \leq K|A|$ $\forall x \in A$ then

$$|A^m| \leq K^{\mathcal{O}(m)}|A| \ \forall m \geq 3.$$

4 Stability of approximate closure under basic operations

Two familiar properties of genuine subgroups are that they behave well under quotients and intersections: if $H < G$ and $\pi : G \to \Gamma$ is a homomorphism, then $\pi(H) < \Gamma$, and if $H_1, H_2 < G$ then $H_1 \cap H_2 < G$. In this lecture, we'll see versions of these properties for approximate groups and sets of small tripling.

It's trivial that if $A \subset G$ is a K-approximate group then $\pi(A)$ is also a K-approximate group. The following is the corresponding result for sets of small tripling.

Lemma 4.1 (Stability of small tripling under homomorphisms)**.** Let $A \subset G$ be finite, symmetric containing the identity. Suppose $\pi : G \to H$ is a homomorphism. Then

$$\frac{|\pi(A)^m|}{|\pi(A)|} \leq \frac{|A^{m+2}|}{|A|} \quad \forall m \in \mathbb{N}.$$

In particular, if $|A^3| \leq K|A|$ then $|\pi(A)^3| \leq K^9|\pi(A)|$ by Proposition 2.7. We can prove this using an argument of Helfgott. We'll start with a simple observation that we'll use repeatedly in the course.

Lemma 4.2. Let $H < G$, let $A \subset G$ be finite, and let $x \in G$. Then

$$|A^{-1}A \cap H| \geq |A \cap xH|.$$

Proof. We have $(A \cap xH)^{-1}(A \cap xH) \subset A^{-1}A \cap H$. □

Remark. Most of the lemmas and propositions in this section will have familiar/trivial analogues for genuine subgroups. It is a useful exercise to think about what they are.

Lemma 4.3. Let $H < G$, write $\pi : G \to G/H$ for the quotient map, let $A \subset G$ be finite. Then

$$|A^{-1}A \cap H| \geq \frac{|A|}{|\pi(A)|}.$$

Note that H is not assumed normal, so G/H is just the space of left cosets xH, not necessarily a group.

Proof. The pigeonhole principle gives $\exists x \in G$ such that $|A \cap xH| \geq |A|/|\pi(A)|$. Then apply Lemma 4.2. □

Lemma 4.4. Let $H < G$, write $\pi : G \to G/H$ for the quotient map, and let $A \subset G$ be finite. Then

$$|\pi(A^m)||A^n \cap H| \leq |A^{m+n}| \ \forall m, n \geq 0.$$

Proof. Define $\varphi : \pi(A^m) \to A^m$ by picking arbitrarily for each $x \in \pi(A^m)$ some $\varphi(x)$ such that $\pi(\varphi(x)) = x$. Then the cosets $\varphi(x)H$ for $x \in \pi(A^m)$ are all distinct by definition, so

$$|\varphi(\pi(A^m))|\,|(A^n \cap H)| = |\pi(A^m)|\,|A^n \cap H|\,.$$

But also, $\varphi(\pi(A^m))(A^n \cap H) \subset A^{m+n}$. □

Proof of Lemma 4.1. Take $H = \ker \pi$. Lemma 4.4 gives

$$|\pi(A^m)| \leq \frac{|A^{m+2}|}{|A^2 \cap H|}.$$

Lemma 4.3 gives

$$|A^2 \cap H| \geq \frac{|A|}{|\pi(A)|}.$$

The proposition follows by combining these inequalities. □

Now we'll look at intersections.

Proposition 4.5 (Stability of small tripling under intersections with subgroups)**.** Let $A \subset G$ be finite, symmetric, contain 1. Let $H < G$. Then

$$\frac{|A^m \cap H|}{|A^2 \cap H|} \leq \frac{|A^{m+1}|}{|A|}.$$

In particular, by Proposition 2.7, if $|A^3| \leq K|A|$ then $\left|(A^m \cap H)^3\right| \leq K^9 |A^m \cap H|$ for any $m \geq 2$.

Remark. We'll see in Example Sheet 1 that even if A has small tripling, $A \cap H$ need not. So $m \geq 2$ really is important for this last conclusion.

Proof. Take $\pi : G \to G/H$ as before. Lemma 4.4 gives

$$|A^m \cap H| \leq \frac{|A^{m+1}|}{|\pi(A)|}.$$

Lemma 4.3 gives

$$|A^2 \cap H| \geq \frac{|A|}{|\pi(A)|}.$$

Combine these two inequalities. □

Proposition 4.6 (Stability of approximate groups under intersections with subgroups)**.** Let $H < G$, let $A \subset G$ be a K-approximate group. Then $A^m \cap H$ is covered by $\leq K^{m-1}$ left-translates of $A^2 \cap H$. In particular, $A^m \cap H$ is a K^{2m-1}-approximate group (since $A^2 \cap H \subset A^m \cap H$ and $(A^m \cap H)^2 \subset A^{2m} \cap H$).

Proof. By definition, $\exists X \subset G$ with $|X| = K^{m-1}$ such that $A^m \subset XA$. In particular,

$$A^m \cap H \subset \bigcup_{x \in X} (xA \cap H).$$

For each $xA \cap H$ that is not empty, $\exists h = xa \in H$ for some $a \in A$. This means that

$$xA \cap H \subset h(a^{-1}A \cap H) \subset h(A^2 \cap H).$$

Hence each set $xA \cap H$ in this union is contained in a single left translate of $A^2 \cap H$. □

In Introduction to Discrete Analysis, we saw that when studying small doubling or tripling there is a more general notion of homomorphism that comes into play: the Freiman homomorphism. To motivate this, consider two sets $A = \{-n, \dots, n\} \subset \mathbb{Z}/p\mathbb{Z}$, and $B = \{-n, \dots, n\} \subset \mathbb{Z}/q\mathbb{Z}$ for p, q two primes $\geq 10n$, say. These two sets are intuitively 'isomorphic' from the perspective of $A + A$ or $B + B$, but there is no way of encoding this with a group homomorphism $\mathbb{Z}/q\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$. Freiman homomorphisms give us a way to encode this.

Definition. Let $m \in \mathbb{N}$, let A, B be subsets of groups.

- A map $\varphi : A \to B$ is a **Freiman m-homomorphism** if $\forall x_1, \dots, x_m, y_1, \dots, y_m \in A$,
$$x_1 \cdots x_m = y_1 \cdots y_m \implies \varphi(x_1) \cdots \varphi(x_m) = \varphi(y_1) \cdots \varphi(y_m).$$
- If $1 \in A$ and $\varphi(1) = 1$ then we say that φ is **centered**.
- If φ is injective and its inverse $\varphi(A) \to A$ is also a Freiman m-homomorphism then we say $\varphi : A \to \varphi(A)$ is a **Freiman m-isomorphism**.

– We often simply write that φ is a 'Freiman homomorphism' when it is a Freiman 2-homomorphism.

Remark.

(1) Every map is trivially a 1-homomorphism, so we only care about the cases $m \geq 2$.

(2) This definition gets stronger as m increases: we may assume $A \neq \varnothing$, and then, picking $a \in A$ arbitrarily, if $x_1 \cdots x_k = y_1 \cdots y_k$ for $k \leq m$ then

$$x_1 \cdots x_k \underbrace{a \cdots a}_{m-k} = y_1 \cdots y_k \underbrace{a \cdots a}_{m-k}.$$

(3) If φ is a centered m-homomorphism and $a, a^{-1} \in A$ then exercise to check that $\varphi(a^{-1}) = \varphi(a)^{-1}$ (for $m \geq 2$).

Lemma 4.7. Suppose $\varphi : A \to \Gamma$ is a Freiman m-homomorphism. Then

$$|\varphi(A)^m| \leq |A^m|.$$

In particular, if φ is injective then

$$\frac{|\varphi(A)^m|}{|\varphi(A)|} \leq \frac{|A^m|}{|A|},$$

and if φ is a Freiman m-isomorphism then

$$\frac{|\varphi(A)^m|}{|\varphi(A)|} = \frac{|A^m|}{|A|}.$$

Proof. Exercise. □

Index