# Introduction to Approximate Groups

January 24, 2019

# Contents

# 0 Introduction

—Lecture 1—

Example classes: 12 Feb, 5 Mar, 2-3pm.
Venue will be confirmed later.
Examinable material is exactly what is on board (as usual).
No plan for printed notes (as usual).

After 3.5 years of tripos, we finally know what a subgroup is: a *subgroup* $H < G$ is a non-empty set closed under products and inverses.
We would then expect an *approximate subgroup* to be a subset that is only *approximately* closed under products. We'll make this precise soon. Such sets arise naturally in a number of branches of maths, and as such approximate groups have had broad range of applications. In this course we'll 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 CS).[1]

[1] Lecturer actually spent the time to write all this on board, probably implying a slower-paced course than category theory! But every course is slower than category theory.

# 1 Small Doubling

To start with, we'll look at a preliminary notion of approximate closure called *small doubling*.
In this course, $G$ is always a group, arbitrary unless specified otherwise. Given $A, B \subset G$, we write

$$AB = \{ab : a \in A, b \in B\}$$

called the product set,

$$A^n = \underbrace{A \cdot ... \cdot A}_{n \text{ times}}$$

$$A^{-1} = \{a^{-1} : a \in A\}$$

$$A^{-r} = (A^{-1})^n$$

When $G$ is abelian, we often switch to additive notion, for example $A+B, nA, -A, -nA$ in place of the above (*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 $|A^2|$ 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 we have $|A| \leq |A^2| \leq |A|^2$, and 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 $A^2$.[2] Therefore, we can view sets $A$ satisfying

$$|A^2| = o(|A|^2) \quad (1.1)$$

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

$$|A^2| \leq K|A| \quad (1.2)$$

for some constant $K \geq 1$ fixed a priori.
Obviously, such sets are very far from random, and we can expect (1.2) to impose a significant restriction on $A$. The main aim of the course is to work out how significant the restriction is.

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

[2] We will see in sheet 1 that random $A$ have quadratic size for $|A^2|$, in the sense of: if $A$ is a set of size $n$ chosen uniformly at random from $\{1, ..., n^{100}\}$ (we'd like to choose from all integers, but there's no uniform measure there), then $\mathbb{E}(|A+A|)$ is *closed to* $\frac{1}{2}|A|^2$. Note that this is the largest we can get, since in an abelian group we have $a + b = b + a$.

**Example.** • $A$ a finite subgroup;
• $|A| \leq K$;
• $A \subset \mathbb{Z}, A = \{-n, ..., n\}$, $|A + A| \leq 2|A|$.

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

Our main aim will be to prove theorems along the lines of: if $A$ has small doubling, then $A$ has a certain structure. When $K$ is very small, this is quite easy, as follows.

**Theorem.** (1.1, Freiman[3])
Let $K < \frac{3}{2}$. Suppose $A \subset G$ and $|A^2| \leq K|A|$ (by writing like this, we're obviously assuming $A$ is finite). Then there is a subgroup $H < G$ with $|H| = |A^2|$ $(\leq K|A|)$ such that $A \subset aH = Ha \forall a \in A$.
(i.e., $A$ is a large portion of a coset of a finite subgroup).

**Remark.** Converse: if $A \subset xH = Hx$ for $x \in G$, $H < G$, $|H| \leq K|A|$, then $|H^2| \leq K|A|$. So this is a complete classsification 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 $> \frac{1}{2}|A|$ pairs of $(x, y) \in A \times A$ s.t. $ax = by$, i.e. $a^{-1}b = xy^{-1}$. This immediately implies $A^{-1}A \subset AA^{-1}$ (as we just needed one such pair $(x, y)$), and replacing $A$ by $A^{-1}$ we get the other inclusion; so $A^{-1}A = AA^{-1}$ as required.

Since $|A \times A| = |A|^2$, it also implies that $|A^{-1}A| \leq \frac{|A|^2}{\frac{1}{2}|A|} = 2|A|$, 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 exist $> \frac{1}{2}|A|$ pairs $(u, v) \in A \times A$ s.t. $c^{-1}d = uv^{-1}$. This means for at least one pair $(x, y)$ 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 $A^2 = aHa \ \forall a \in A$ ($H$ as before). In particlar, $|H| = |A^2|$.

*Proof.* First, note that $A \subset aH \cap Ha$ (label this 1.3) by definition of $H$ and $A^{-1}A = AA^{-1}$, so certainly $A^2 \subset aHa$. For the reverse inclusion, let $z \in aHa$. Since $H$ is a subgroup, there exists $|H|$ pairs $(x, y) \in aH \times Ha$ s.t. $z = xy$. Moreover, by (1.3) and the bound $|H| < 2|A|$ from lemma (1.2), more than half of those $x$ and half of those $y$ 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. □

[3]The proof presented here is by Tao instead of the original version. Lecturer has no way to tell if the original proof is close to this, especially because the original proof is in Russian.

Proof of theorem (1.1):

*Proof.* 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, etc.

# 2 Covering and Higher Sum and Product Sets

—Lecture 2—

Today we will 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 $A \subseteq \mathbb{F}_p^r$ satisfies $|A+A| \leq K|A|$. Then there is a subgroup $H \subseteq \mathbb{F}_p^r$ with $|H| \leq p^{K^4}K^2|A|$ s.t. $A \subseteq H$.

**Remark.** It's not ideal that $|A|/|H|$ depends on $p$. We'll remove this dependency in a few lectures' time.

We'll start by proving the following weaker version:

**Proposition.** (2.2)
Suppose $A \subseteq \mathbb{F}_p^r$ satisfies $|2A-2A| \leq K|A|$. Then there is a subgroup $H \subseteq \mathbb{F}_p^r$ with $|H| \leq p^K|A-A|$ $(\leq p^K K|A|)$ such that $A \subseteq H$.

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

**Lemma.** (2.3, Rusza's Covering Lemma)
Suppose $A, B \subseteq G$, and $|AB| \leq K|B|$. Then, $\exists X \subseteq A$ with $|X| \leq K$ s.t. $A \subseteq XBB^{-1}$. Indeed, we may take $X \subseteq A$ maximal such that the sets $xB$ $(x \in X)$ are disjoint.
The term *covering* refers to the conclusion $A \subseteq XBB^{-1}$, which says $A$ *can be covered by few left-translates of* $BB^{-1}$.

*Proof.* First, disjointness of $xB \implies |XB| = |X||B|$. Since $X \subseteq A$, $|XB| \leq |AB| \leq K|B|$, so $|X| \leq K$. Maximality implies $\forall a \in A$, $\exists x \in X$ s.t. $aB \cap xB \neq \phi$; and hence $a \in xBB^{-1}$. So $A \subseteq XBB^{-1}$. □

Now we prove some lemmas for proposition 2.2:

**Lemma.** (2.4)
Suppose $A \subseteq G$ satisfies $|A^{-1}A^2A^{-1}| \leq K|A|$. Then $\exists X \subseteq A^{-1}A^2$, $|X| \leq K$ such that $A^{-1}A^n \subseteq x^{n-1}A^{-1}A \forall n \in \mathbb{N}$.

*Proof.* Lemma 2.3 gives (as $|A| = |A^{-1}|$) the existence of an $X \subseteq A^{-1}A^2$, $|X| \leq K$ s.t. $A^{-1}A^2 \subseteq XA^{-1}A$. We then have

$$\begin{aligned} A^{-1}A^n &= A^{-1}A^{n-1}A \\ &\subseteq X^{n-2}A^{-1}A^2 \text{ by induction} \\ &\subseteq X^{n-1}A^{-1}A \end{aligned}$$

□

*Proof.* (of proposition 2.2)
Note that $\mathbb{F}_p^r$ is abelian, so we can apply Lemma 2.4 which gives the existence of $X$, $|X| \leq K$ s.t. $nA - A \subseteq (n-1)X + A - A \forall n \in \mathbb{N}$. As we are in a finite vector space, this means that $\langle A \rangle \subseteq \langle X \rangle + A - A$, so $|\langle A \rangle| \leq |\langle X \rangle||A - A| \leq p^K K|A|$, as claimed. □

To strenghthen prop 2.2 to theorem 2.1, we use the technique of bounding higher sum/product sets. The key result, at least in the abelian case, is the following:

**Theorem.** (2.5, Plünecke-Rusza)
Suppose $A \subseteq G$ (abelian) and $|A + A| \leq K|A|$, then $|mA - nA| \leq K^{m+n}|A|$ $\forall m, n \geq 0$.
This was proven intro to discrete analysis last term. We won't redo the whole proof, but we will reprove some parts of it.

*Proof.* 2.5 gives that $|2A - 2A| \leq K^4|A|$, and $|A - A| \leq K^2|A|$. Then immediately it follows from prop 2.2. □

We'll spend the rest of teh lecture discussing theorem 2.5 and variants of it. We've seen that it is useful, at least in one context. To see more properly why it's useful, let's think about what the genuine closure of subgroups under products and inverse means. One useful feature is that it can be iterated: given $h_1, h_2, ... \in H$, a subgroup, this means that $h_1^{\varepsilon_1}...h_m^{\varepsilon_m} \in H \ \forall \varepsilon_i = \pm 1 \ \forall m \forall h_i \in H$. Then theorem 2.5 allows us to *iterate the approximate closure* of a set of small doubling: $a_1 + ... + a_m - a_1' - ... - a_n'$ may not belong to $A$, but at least belongs to $mA - nA$ which is (a) not too large, and (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 doesn't hold for non-abelian groups.

**Example.** (2.6)
Let $x$ generate an infinite cyclic group $\langle x \rangle$, and $H$ be a finite group. Set $G = H * \langle x \rangle$, the free product (just keep in mind that $x^{-1}Hx \neq H$). Set $A = H \cup \{x\}$, then $A^2 = H \cup xH \cup Hx \cup \{x^2\}$, 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 strenghten small doubling slightly, we can recover a form of theorem 2.5. One way is to replace it with *small tripling*, i.e. $|A^3| \leq K|A|$:

**Proposition.** (2.7)
Suppose $A \subseteq G$, $|A^3| \leq K|A|$. Then $|A^{\varepsilon_1}...A^{\varepsilon_m}| \leq K^{3(m-2)}|A|$, $\forall \varepsilon_i = \pm 1, \forall m \geq 3$.

The key ingredient is the following:

**Lemma.** (2.8, Rusza's Triangle Inequality)
Given $U, V, W \subseteq G$ all finite, $|U||V^{-1}W| \leq |UV||UW|$.

*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 $W(x) \in W$, s.t. $x = V(x)^{-1}W(x)$. Set $\varphi(u, x) = (uV(x), uW(x))$. To see injectivity, first note that $(uV(x))^{-1}(uW(x)) = x$, so $x$ is determined by $\varphi(u, x)$, then $(uV(x))(v(x)^{-1}) = u$, so $u$ is also determined by $\varphi(u, x)$. □

*Proof.* (of 2.7)
First, we'll do the case $m = 3$.
• $|A^3| = |A^{-3}| \leq K|A|$;
• apply lemma 2.8 with $U = W = A$, $V = A^2$. Get $|A||A^{-2}A| \leq |A^3||A^2| \leq K^2|A|^2$, so $|S^{-2}A| \leq K^2|A|$; • note that $(A^{-2}A)^{-1} = (A^{-1}A^2)$, so $|A^{-1}A^2||A^{-2}A| \leq K^2|A|$;
• replace $A$ by $A-1$ to get $|AA^{-2}| = |A^2A^{-1}| \leq K^2|A|$;
• Finally, apply lemma 2.8 with $U = V = A, W = AA^{-1}$, we get $|A||A^{-1}AA^{-1}| \leq |A^2||A^2A^{-1}| \leq K^3|A|^2$. So, $|A^{-1}AA^{-1}| \leq K^3|A|$. For the last case, swap $A \leftrightarrow A^{-1}$.

For $m \geq 4$, lemma 2.8 gives $|A||A^{\varepsilon_1}...A^{\varepsilon_m}| \leq |AA^{-\varepsilon_2}A^{-\varepsilon_1}||AA^{\varepsilon_3}...A^{\varepsilon_m}| \leq K^3|A|K^{3(m-3)}|A|$ by induction. □

# 3 Approximate groups

—Lecture 3—

Last time we saw that assuming small tripling instead of small doubling allowed us to control higher product sets of the form $A^{\varepsilon_1}...A^{\varepsilon_m}$. In this lecture, we'll see another possible strengthening of small doubling. We also saw, in the proofs of theorem 2.1 and proposition 2.2, that the advantage of having a *covering* condition in place of a size bound. This motivates the following definition:

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

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, we can write $A^m$ in stead of $A^{\varepsilon_1}...A^{\varepsilon_m}$, and $1 \in A \implies A \subset A^2 \subset A^3 \subset ...$, 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 definition of approximate group, in fact we have $A^m \subset X^{m-1}A$:

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

□

Another advantage is that if $\pi : G \to H$ is a homomorphism and $A$ is a $K$-approximate group, then $\pi(A)$ is also trivially a $K$-approximate group (although we'll see that there exists 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 exists $O(K^{12})$-approximate groups $B$ 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 part is just lemma 3.1. For the converse, set $\hat{A} = A \cup \{1\} \cup A^{-1}$, and note that $A^2 = \{1\} \cup A \cup A^{-1} \cup A^2 \cup A^{-1}A \cup AA^{-1} \cup A^{-2}$. Each set in this

union has size $\leq K^2|A|$, by prop 2.7, so $|B| \leq 7K^3|A|$, as claimed. Similarly,

$$A^4 = \bigcup_{\varepsilon_i=\pm 1, 0 \leq m \leq 4} A^{\varepsilon_1}...A_{\varepsilon_m}$$

and the sets in this union have size $\leq K^6|A|$. It follows that $|\hat{A}^4| \leq O(K^6)|\hat{A}|$. Lemma 2.4 then tells us that $\exists X \subset G$, $|X| \leq O(K^6)$ s.t. $\hat{A}^n \subset X^{n-2}\hat{A}^2$ for every $n \geq 2$.
In particular, $|X^2| \leq O(K^{12})$, and $\hat{A}^4 = (\hat{A}^2)^2 \subset X^2\hat{A}^2$, so $\hat{A}^2$ is an $O(K^{12})$-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 (but not tripling)? 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 $\exists U \subset A$ with $|U| \geq \frac{1}{K}|A|$ s.t. $|U^m| \leq K^{m-1}|U|$ $\forall m \in \mathbb{N}$.

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

Tao proved a version of theorem 3.3 when he introduced the definition of approximate groups. We'll use instead a lemma of Petridis, which he proved when proving the Plünnecke-Ruzsa 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 every finite $C \subset G$, we have $|CUB| \leq R|CU|$.

*Proof.* It's trivial if $C = \phi$, so we may assume $\exists x \in C$. Defining $C' = C\{x\}$, we may also assume by inducion that $|C'UB| \leq R|C'U|$.
Set $W = \{u \in U : xu \in C'U\}$. Then $CU = C'U \cup (xU \setminus xW)$ is a disjoint union, so in particular

$$|CU| = |C'U| + |U| - |W| \quad (3.1)$$

We also have $xWB \subset C'UB$ by definition of $W$, so $CUB \subset C'UB \cup (xUB \setminus xWB)$, and hence

$$|CUB| \leq |C'UB| + |UB| - |WB| \quad (3.2)$$

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

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

□

*Proof.* (of 3.3)
Set $U \subset A$ to be non-empty, minimizing $|UA|/|U|$, and write $R = |UA|/|U|$, noting that $R \leq K$ by minimality (since $U$ must have beaten $A$). Also, $U$ non-empty implies $|UA| \geq |A|$, 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 $|U^m| \leq K^{m-1}|U|$. □

Non-examinable: 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.** (3.5, Tao, Petridis)
If $|A^2| \leq K|A|$, and $|AxA| \leq K|A| \ \forall x \in A$, then $|A^m| \leq K^{O(m)}|A| \ \forall m \geq 3$.

Also non-examinable (it's in intro to DA, but lecturer thought it's was showing):

**Theorem.** (2.5')
After writing a few words, lecturer decided that there's not enough time, and we have written enough this lecture, so wiped everything out from the board.

Check example sheets at *tointon.neocities.org*; they'll be up some time this afternoon.