Part III – Introduction to Approximate Groups (Unfinished 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 $\{1, \ldots, n^{100}\}$, 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

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

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 (Small doubling)**.** 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 ($K = 1$)
- $|A| \leq K$

- $A \subset \mathbb{Z}$, $A = \{-n, \ldots, n\}$, $|A + A| \leq 2|A|$.

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:

$$A \text{ has small doubling} \Rightarrow A \text{ has a certain structure.}$$

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 $x \in G$, $H < G$, $|H| \leq K|A|$ then $|H^2| \leq K|A|$. So this is a complete classification of sets of very small doubling.

Lemma 1.2 (Identify H)**.** If $|A^2| \leq \frac{3}{2}|A|$ 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 $\geq \frac{1}{2}$ 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, $\exists > \frac{1}{2}|A|$ pairs $(u, v) \in A \times A$ such that $c^{-1}d = uv^{-1}$. This means that for at least one pair (x, y) from 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...

Index