Introduction to the Theory of Set Addition

October 6th – 10th 2014, Freie Universität Berlin

What is set addition and why should one learn the basics of this theory?

The first question is easy to answer. The word 'addition' is mentioned so there must be an ambient commutative group. The word 'set' is mentioned so we must add sets.

The *sumset* or *Minkowski sum* of two sets A and B in a commutative group is defined to be

$$A + B = \{a + b : a \in A, b \in B\}.$$

Adding a singleton to another set is translation so we will use the standard notation

$$\{a\} + B = a + B.$$

The iterated sumset h-fold hA is defined recursively by

$$hA = (h-1)A + A.$$

The *difference set* naturally is

$$A - B = \{a + b : a \in A, b \in B\}.$$

By $kA - \ell A$ we mean the set

$$kA - \ell B = \{a_1 + \cdots + a_k - b_1 - \cdots - b_\ell : a_j \in A, b_i \in B\}.$$

The second questions is trickier. To begin to answer it, let us introduce a concept you may actually not have heard before: that of a set of small doubling. The *doubling constant* of a finite set A is the ratio

$$\text{doubling constant of } A := \frac{|A + A|}{|A|}.$$

One can think of the doubling constant as a measure of "additive structure". Finite subgroups, which are closed under addition and in general have very rich structure, have doubling one, while a finite set A of generators of a free commutative group has maximum doubling $\binom{|A|+1}{2}$.

The doubling constant also allows one to study questions that are otherwise almost meaningless. For example, given a finite non-empty set A in a commutative group, what can be said about the cardinality of $A+A+A$? Well, not much. The bounds

$$|A| \leq |A+A+A| \leq \binom{|A|+2}{3}$$

are easy to prove and sharp: the lower bound is attained when A is a subgroup and the upper bound when A is a et of generators of free commutative group.

Once a condition on the doubling constant is inserted, the question becomes more precise, more difficult to answer and also more useful. The archetypical question we will study in the first couple of days is as follows.

How large can $|A+A+A|$ be, when $|A+A| \leq \alpha|A|$?

Later on in the Block Course you will see a rather precise characterisation of sets of small doubling. This is a celebrated theorem that has influenced additive number theory in the 21st century considerably. As you will see, many of the basic techniques and results we will learn this week are featured in the study of sets of small doubling.

They also appear in many famous results of famous mathematicians: Ruzsa's proof of Freiman's theorem, Gowers' proof of Szemerédi's theorem, Bourgain's contribution to the Kakeya problem, the Bourgain-Katz-Tao sum-product theorem for finite fields and Helfgott's result about growth and generation in $SL_2(\mathbb{Z}/p\mathbb{Z})$.

Moreover, there are sound educational reasons for studying this subject. Many particularly useful combinatorial techniques are applied: double-counting, working with extreme quantities, simple probabilistic reasoning and the Cauchy-Schartz inequality. I hope that in this first week you will see how one can do a lot by using very little.

Acknowledgement. In preparing these handouts, I relied on various material of Ben Green, Tim Gowers and Imre Ruzsa.

1 Cardinality inequalities

Let us begin with a gentle exercise.

Real time exercise. For each of the following sets determine the desired quantities.

(i) $A = \{1, \dots, n\} \subset \mathbb{Z}$. Find $A - A$.

(ii) $A = \{1, \dots, n\} \times \{1, \dots, n\} \subset \mathbb{Z}^2$. Find $A + A$ and the doubling constant.

(iii) $A = \{\mathbf{e}_1, \dots, \mathbf{e}_d\} \subset \mathbb{R}^d$. Find $A + A$ and the doubling constant. $\{\mathbf{e}_i\}$ is the standard basis.

Solution.

From now on all sets are finite, non-empty subsets of a commutative group

Our first topic is to study what the doubling constant of a finite set tells us about the cardinality of sum-and-difference sets like the ones defined above. We begin with a remarkable inequality of Ruzsa.

Lemma 1.1 (Ruzsa's triangle inequality)**.** *Let X, Y, Z be finite non-empty sets in a commutative group. Then*

$$|X||Y - Z| \leq |Y - X||X - Z|.$$

Sketch of proof.

Corollary 1.2 (From sums to differences)**.** *Let $\alpha \in \mathbb{R}$ and A be a finite no-empty set in a commutative group. Suppose that $|A+A| \leq \alpha|A|$. Then $|A-A| \leq \alpha^2|A|$.*

Proof.

□

This simple lemma is a remarkable result: it is easy to state, easy to prove, essentially sharp and with many applications!

The exponent of α is sharp. There are examples of arbitrarily large values of α where $|A+A| = \alpha|A|$ and $|A-A| \geq c\frac{\alpha^2}{\sqrt{\log(\alpha)}}|A|$, for some absolute constant c. Absolute means a genuine constant: independent of A (and hence of α).

Application 1.3 (From three to many summands)**.** *Let $\beta \in \mathbb{R}$ and A be a finite no-empty set in a commutative group. Suppose that $|A+A-A| \leq \beta|A|$. Then $|A+A+A+A| \leq \beta^2|A|$.*

Proof.

□

Bounds on $\lvert A \pm A \pm A\rvert$ imply bounds on $\lvert kA - \ell A\rvert$

Real time exercise. Let $\alpha \in \mathbb{R}$ and A be a finite no-empty set in a commutative group. Suppose that $|A+A| \leq \alpha|A|$. What bound can you put on $|A+A+A|$?

Solution.

Lemma 1.4 (From two to many summands)**.** *Let A, B be finite non-empty sets in a commutative group. Let $\emptyset \neq X \subseteq A$ be a non-empty subset of A that minimises the quantity $|Z+B|/|Z|$ over all non-empty subsets of A. Then for all non-empty sets C in the ambient group*

$$|X||X+B+C| \leq |X+B||X+C|.$$

Proof.

□

At the heart of the proof of the lemma lies *submodularity*: for any two sets S and T we have

$$|X + (S \cup T)| + |X + (S \cap T)| \leq |X + S| + |X + T|.$$

To verify the above inequality note

$$|X+S|+|X+T| = |(X+S)\cup(X+T)|+|(X+S)\cap(X+T)| \geq |X+(S\cup T)|+|X+(S\cap T)|.$$

It is noteworthy that the Cauchy–Davenport and Kneser inequalities, which offer basic lower bounds on the cardinality of sumsets, are also related to submodularity.

Theorem 1.5 (Plünnecke's inequality)**.** *Let $\alpha \in \mathbb{R}$ and A and B be finite non-empty sets in a commutative group. Suppose that $|A+B| \leq \alpha|A|$. There exists a non-empty subset $\emptyset \neq X \subseteq A$ such that for all positive integers h*

$$|X + hB| \leq \alpha^h |X|.$$

In particular, if $|A + A| \leq \alpha|A|$, then $|hA| \leq \alpha^h|A|$.

Proof.

□

Remarks. In general it is not possible to replace X by the whole of A. Note the order of the quantifiers: there is an X that works for all h.

Theorem 1.6 (The Plünnecke–Ruzsa inequalities)**.** *Let $\alpha \in \mathbb{R}$, k and ℓ be positive integers, and A be a finite non-empty set in a commutative group. Suppose that $|A+A| \leq \alpha|A|$. Then*

$$|kA - \ell A| \leq \alpha^{k+\ell}|A|.$$

Proof. □

Bounds on $\lvert A \pm A\rvert$ imply bounds on $\lvert kA - \ell A\rvert$

Lemma 1.7 (Ruzsa's twin to the triangle inequality)**.** *Let A, B, C be finite non-empty sets in a commutative group. Then*

$$|A||B+C| \leq |A+B||A+C|.$$

Proof. □

Lemma 1.8 (Another cardinality inequality of Ruzsa)**.** *Let A, B, C be finite non-empty sets in a commutative group. Then*

$$|A+B+C|^2 \leq |A+B||B+C||C+A|.$$

No proof given here. Note that the above inequality bounds the whole of $|A+B+C|$ and not just $|X+B+C|$ for some suitably chosen X.

Let us compare the range of α for which the bound above beats that of Plünnecke's inequality. Setting $A = B = C$ yields $|A+A+A| \leq \alpha^{3/2}|A|^{3/2}$. This is superior to $\alpha^3|A|$ when $\alpha \geq |A|^{1/3}$.

2 The power trick

A very natural question is to ponder what happens when we add different sets to A. As one may expect the outlook does not change much.

Theorem 2.1 (Ruzsa's Plünnecke–type inequality for different summands)**.** *Let h be a positive integer and $A, B_1, \dots, B_h$ be finite non-empty sets in a commutative group. Suppose that $|A + B_i| \le \alpha |A|$ for all $i = 1, \dots, h$. Then*

$$|B_1 + \dots + B_h| \le \alpha^h |X|.$$

Proof.

□

A few remarks. Ruzsa in fact showed that there exists a nonempty subset $\emptyset \neq Y \subseteq A$ such that $|Y + B_1 + B_2| \leq \alpha^2 |X|$.

It is worth comparing Ruzsa's bound with that given by Lemma 1.4. Setting $B = B_1$ and $C = B_2$ in the lemma yields a non-empty $\emptyset \neq X \subseteq A$ such that

$$|X + B_1 + B_2| \leq \frac{|X + B_1|}{|X|} |X + B_2| \leq \frac{|A + B_1|}{|A|} |X + B_2| \leq \alpha |X + B_2|.$$

No information is known about $|X + B_2|$, so we bound it by $|A + B_2| \leq \alpha |A|$. Putting everything together gives

$$|X + B_1 + B_2| \leq \alpha^2 |A|.$$

While this is a strictly speaking worse bound than that given by Ruzsa. In practice, however, the difference between having $|X|$ and $|A|$ on the right side is not important.

The careful reader will have noted that we in fact gave a simpler proof of the lemma.

3 Covering lemmas

So far have seen that if $|A+B|$ is "small" compared to $|A|$, then we can say something about the cardinality of higher sum-and-difference sets.

Now want to do a little more: starting from the condition that $|A+B|$ is "small", we want to cover B by "few translates of A". What does cover a set by translates of another set mean?

Definition. Let A and B be sets in a commutative group. B is *covered* by k translates of A if there exist elements $s_1, \dots, s_k$ in the ambient group such that

$$B \subseteq \bigcup_{i=1}^{k} (s_i + A) \text{ or equivalently } B \subseteq S + A, \text{ where } S = \{s_1, \dots, s_k\}.$$

Real time exercise. For each of the following you are given two sets A and B. Find a set S of least cardinality such that $B \subseteq S + A$.

(i) $A = \{1, \dots n\}$ and $B = \{1, \dots, n+1\}$.

(ii) $A = \{1, \dots n\} \times \{0\}$ and $B = \{1, \dots, n\} \times \{1, \dots, n\}$.

(iii) $A = \{1, \dots n\}$ and $B = \{n^2, 2n^2, \dots, n^3\}$.

Let's see what is going on. Set $\alpha = |A+B|/|A|$.

(i) $\alpha = 2$ and we needed 2 translates.

(ii) α is about $2n$ and we needed n translates.

(iii) α is about n and we needed n translates.

Your conjecture is:

Consider now one more example.

(iv) A is a random subset of $\{1, \ldots, n\}$ and $B = \{1, \ldots, n\}$.

What is a random subset of $\{1, \ldots, n\}$? For each $i = 1, \ldots, n$ flip a coin; if you get H put i in A and if you get T do not put i in A. Formally: each integer between 1 and n is included in A with uniform probability $1/2$ independent of all the others.

In this case α is about 4:

An exercise in probabilistic arguments shows that B cannot be covered by fewer than $\log(n)$ translates of A.

Note however, that $A - A$ is very likely to include $\{-\lceil n/3 \rceil, \ldots, \lceil n/3 \rceil\}$:

So B can be covered by α translates of A.

Difference sets are nice sets – they have few holes

Lemma 3.1 (Ruzsa's covering lemma)**.** *Let $\alpha \in \mathbb{R}$ and A, B be finite non-empty sets in a commutative group. Suppose that $|A + B| \leq \alpha |A|$. Then $B \subseteq S + A - A$ where $S \subseteq B$ satisfies $|S| \leq \lfloor \alpha \rfloor$.*

Proof.

□