Additive combinatorics

Ana E. de Orellana
Analysis Reading Group

Contents

These notes were taken during a reading group at the University of St Andrews during autumn of the 2023-2024 academic year. In each meeting a member of the group would present a topic from the book [TV06]. Any errors in these notes are due to me.

1. First meeting - Jonathan Fraser

Throughout these notes, our ambient space, will be an abelian additive group Z, for most applications it will be one of $\mathbb{Z}$ or $\mathbb{Z}_n$, and A, B, C will be subsets of Z. The idea will be to relate the additive structure of A and B with that of $A+B$ and $A-B$, where

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

1.1. **Motivation.** Being a group of analysts, we immediately think: Why are we interested in studying additive combinatorics? It seems like something we should leave for group theorists.

Often, A and B will be discretisations at scale $\delta > 0$ of some compact space $\boldsymbol{X} \subset [0,1]$. In such way that the covering number of $\boldsymbol{X}$ is $N_\delta(\boldsymbol{X}) \approx |A|$. In this case, our ambient space would be $\delta\mathbb{Z}$.

The first analysis example where additive combinatorics takes place is orthogonal projections. Given two sets A and B, the projection into the 45 degree line of their product is $P_{(1,1)}(A \times B) = A + B$, simply by taking the dot product of $(a,b) \in A \times B$ with $(1,1)$. All of a sudden, the size of $A + B$ seems very important.

1.2. **Bounds for sumsets.** Back to additive combinatorics. Let's talk about $|A + B|$, where $|\cdot|$ stands for cardinality. $A + B$ will contain translations of A by elements in B, translations obviously don't change cardinality. Also, $A + B$ will have at most as many elements as $A \times B$, these two facts give

$$|A| \leqslant |A + B| \leqslant |A||B|.$$

Can these bounds improve if we now consider $A + A$? The lower bound will remain the same, but for the upper bound we can think of the choices we make when adding two elements together. To do $x + y$ we first choose x, we have $|A|$ options for this. Then, to choose y different from x we will have $|A| - 1$ options, but because $x + y = y + x$ (Z is abelian), then we are counting everything twice, adding the diagonal to that yields

$$|A + A| \leqslant \frac{|A|\big(|A| - 1\big)}{2} + |A| = \frac{|A|\big(|A| + 1\big)}{2}.$$

Similarly, for $A - A$ we first choose x from a pool of $|A|$ options, then y from $|A| - 1$ options. However, now we're not counting twice because substraction is not commutative, noting that the diagonal will always give 0 we have

$$|A - A| \leqslant |A|\big(|A| - 1\big) - 1.$$

1.3. **Equalities.** A natural question at this point is. When is $\leqslant$ actually $=$? Let's start with the case $|A| = |A + B|$, without loss of generality we may assume $0 \in B$ (otherwise just translate B), then $A \subset A + B$, which implies that $A + B = A$. Then, A can be written as

$$A = \bigcup_{b \in B} (A + b),$$

that is, a covering by union of cosets. Then $B \subset \mathrm{sym}(A) = \{t \in Z : t + A = A\}$ and

$$A = \bigcup_{a \in A} (a + B).$$

Essentially, what $|A + B| = |A|$ tells us is that studying A is like studying pure group theory.

On the other extreme, if $|A + A| = \frac{|A|(|A|+1)}{2}$, then we're saying that all pairs of elements of A add up to different things, this type of sets are called Sidon sets. So a set is a Sidon set if, whenever $x + y = z + w$, $\{x, y\} = \{z, w\}$. Let's see some properties about this type of sets.

Let $A \subset \mathbb{Z} \cap [0, N]$ be a Sidon set that is not contained in any other Sidon set (A is maximal with respect to the property of being Sidon). Easily we have $A + A \subset \mathbb{Z} \cap [0, 2N]$ and $|A| \leqslant c\sqrt{N}$. Less trivially we have the fact that $|A| \geqslant CN^{1/3}$. To prove this use that since A is a maximal Sidon set, then for every $t \in \mathbb{Z}[0, N] \backslash A$, $A \cup \{t\}$ is not Sidon. Then there exist $x, y, z \in A$ such that $x + t = y + z$, so $t = y + z - x$, which implies that $\mathbb{Z} \cap [0, N] \subset A + A - A$. Remembering that $|A + A - A| \leqslant |A|^3$ yields that $N \leqslant |A|^3$.

1.4. **Some constants.** We will now define several constants, that don't have anything special in their definition. But they are useful because they provide with a manageable notation that makes obtaining bounds easier.

$$\begin{aligned}
\text{Doubling constant} \quad &\longrightarrow \quad \sigma(A) = \frac{|A+A|}{|A|} \in \big[1, (|A|+1)/2\big];\\
\text{Difference constant} \quad &\longrightarrow \quad \delta(A) = \frac{|A-A|}{|A|};\\
\text{Ruzsa distance} \quad &\longrightarrow \quad d(A,B) = \log \frac{|A-B|}{\sqrt{|A|}\sqrt{|B|}}.
\end{aligned}$$

A few things to keep in mind:

- The doubling constant measures how much a set looks like a group (if it's close to 1) or to a Sidon set (if it's close to $(|A|+1)/2$).
- Ruzsa distance is not actually a distance, it satisfies all the properties of distances except for the fact that $d(A,A) = \log \delta(A) \neq 0$. It shows how far away two sets are in terms of additive structure.

Let's prove that Ruzsa distance satisfies the triangle inequality, which is equivalent to prove

$$\begin{aligned}
\frac{|A-B|}{\sqrt{|A|}\sqrt{|B|}} &\leqslant \frac{|A-C|}{\sqrt{|A|}\sqrt{|C|}} \frac{|C-B|}{\sqrt{|B|}\sqrt{|C|}}\\
|A-B| &\leqslant \frac{|A-C||C-B|}{|C|}.
\end{aligned}$$

And this inequality is trivial after noticing that if $a \in A$, $b \in B$, then for each $c \in C$, $a-b = a-c+c-b$, meaning that we have $|C|$ representations of $a+b$.

Our aim now will be to estimate $|A-B|$ in terms of all those constants. Here we will notice the role that notation plays, the previously defined constants do not hide any difficulties, but they are very useful to obtain easy estimates like the one that follows. Using the triangle inequality for the Ruzsa distance with $-A$ in place of C we obtain

$$d(A,B) \leqslant d(A,-A) + d(-A,B),$$

or equivalently

$$\begin{aligned}
\frac{|A-B|}{\sqrt{|A|}\sqrt{|B|}} &\leqslant \frac{|A+A|}{|A|} \frac{|A+B|}{\sqrt{|A|}\sqrt{|B|}}\\
|A-B| &\leqslant \frac{|A+A||A+B|}{|A|}.
\end{aligned}$$

We now define one last constant

$$\text{Additive energy} \quad \longrightarrow \quad E(A,B) = \Big|\big\{(a,a',b,b') \in A\times A\times B\times B : a+b = a'+b'\big\}\Big|.$$

In some way, the additive energy runs in an opposite direction as the Ruzsa distance, because $d(A,B)$ is small when A and B share additive structure, but in those cases $E(A,B)$ is big. Of course, this doesn't mean that there is a direct relation between them (of the sort $d(A,B) \sim E(A,B)^{-1}$), because in that case it would be redundant having both constants defined. The constants d and E quantify the additive structure between two sets, but in a different way.

Let's see one of the properties that the additive energy satisfies, for this it is useful to consider the following equality

$$|A||B| = \sum_{x\in A+B} \big|A\cap(x-B)\big|,$$

which comes from counting the ways of writing $x = a+b$, because then $a = x-b$.

With this in mind, the additive energy can be written sort of "using that relation twice", and using the fact that, if $a+b = a'+b'$ then $a-a' = b'-b$

$$\begin{aligned}
E(A,B) &= \sum_{x\in A+B} \big|A\cap(x-B)\big|^2 \\
&= \sum_{x\in(A-A)\cap(B-B)} \big|A\cap(x+A)\big|\big|B\cap(x-B)\big| \\
&\overset{CS}{\leqslant} \Big(\sum_{x\in A-A} \big|A\cap(x+A)\big|^2\Big)^{1/2}\Big(\sum_{x\in B-B} \big|B\cap(x+B)\big|^2\Big)^{1/2} \\
&= \big[E(A,-A)E(B,-B)\big]^{1/2} \\
&= \big[E(A,A)E(B,B)\big]^{1/2}.
\end{aligned}$$

Where in the last equality we used that $E(A,-B) = E(A,B)$, because if $a-b = a'-b'$ then $a+b' = a'+b$.

2. Second meeting - István Kolossváry

To summarise the previous meeting, let us start with a few examples of sets A to be able to know more about $A+A$ and $A-A$. We know that the doubling constant satisfies $\sigma(A)\in[1,(|A|+1)/2]$. The case where it's close to 1 is because the set is approximately a group and the other extreme is when A is a Sidon set. But what do we have in the middle?

If A is an arithmetic progression, say $A = \{a, a+r, a+2r, \dots, a+(N-1)r\}$, then $A+A = 2a+\{(i+j)r : 1\leqslant i\leqslant j\leqslant N+1\}$. In this case we have $|A| = N$ and $|A+A| = 2N-1$, thus $\sigma(A) = 2+1/N$, this number is in the middle of the interval, but it's rather small. Freiman's theorem deals with things that lay more towards the middle of the interval.

One would expect $|A+A|$ to be similar to $|A-A|$. However, not only this is not the case, the following examples will show us that we can define sets for which $|A-A|$ is much larger than $|A+A|$, and vice versa.

Define the set $A = \{0,1,3\}$, then $A+A = \{0,1,2,3,4,6\}$, $|A+A| = 6$, and also $A-A = \{-3,-2,-1,0,1,2,3\}$ with $|A-A| = 7$. A difference of 1 may not seem like much. However, if now we turn this into a higher dimensional problem redefining A as A^d for some $d\in\mathbb{N}$, then the difference becomes 7^d-6^d, which gets very large.

To build the other example define the set

$$A = \big\{(0,0),(1,0),(2,0),(3,1),(4,0),(5,1),(6,1),(7,0),(8,1),(9,1)\big\}\subset\mathbb{Z}_{10}\times\mathbb{Z}_2.$$

In this case we have $|A+A| = 20$ and $|A-A| = 19$, again, considering the set A^d, $|A+A|$ becomes much larger than $|A-A|$.

These examples show us that if there is some kind of relation between $|A+A|$ and $|A-A|$, then it's definitely very strange. However, we will see that it is still possible to obtain something.

2.1. **A meaningful inequality.** In this section we will try to prove the inequality

$$\delta(A)^{1/2} \leqslant \sigma(A) \leqslant \delta(A)^3,$$

this is, in some sense, an answer to the posed problem, given that $\delta(A) = |A-A|/|A|$ and $\sigma(A) = |A+A|/|A|$.

Let us prove the first inequality: $\delta(A)^{1/2} \leqslant \sigma(A)$, for this we shall use the triangle inequality of the Ruzsa distance d and that $d(A,A) = \log \delta(A)$ and $d(A,-A) = \log \sigma(A)$.

$$\log \delta(A) = d(A,A) \leqslant d(A,-A) + d(-A,A) = 2\log \sigma(A),$$

from this, the desired inequality follows immediately.

Instead or proving the second inequality, $\sigma(A) \leqslant \delta(A)^3$, we shall prove a more general statement: $d(A,-B) \leqslant 3d(A,B)$, using $B = A$ we'd obtain the desired inequality. For this we need to use the following facts:

(1) There exists $x \in A+B$ such that $\big|A \cap (x-B)\big| \geqslant E(A,B)/(|A||B|)$.
The proof for this statement follows from the alternate definition for the additive energy $E(A,B) = \sum_{x\in A+B} \big|A\cap(x-B)\big|^2 \leqslant$, taking the maximum in the sum and using the fact that $|A||B| = \sum_{x\in A+B} \big|A\cap(x-B)\big|$.

(2) For every $x \in A+B$, $\big|A\cap(x-B)\big| \leqslant \frac{|A-B|^2}{|A+B|}$. This statement is equivalent to having

$$\big|\{(a,b,c) \in A\times B\times(A+B) : a+b=x\}\big| \leqslant \big|(A-B)\times(A-B)\big|,$$

where c is an element in $A+B$, so in some sense, this is like multiplying the fibers by $A+B$. To prove this statement notice that given $c \in A+B$, there exist $a_c \in A$ and $b_c \in B$ such that $c = a_c + b_c$, this representation may not be unique, but we can just pick a representant. Now to prove the inequality in the cardinality of sets, define the mapping $(a,b,c) \mapsto \big((a-b_c),(a_c-b)\big)$ and prove that it is injective. This is direct once one realises that c can be written as $c = x-(a-b_c)+(a_c-b)$.

With these two facts we know that

$$\frac{E(A,B)}{|A||B|} \leqslant \frac{|A-B|^2}{|A+B|},$$

then, using Jensen's inequality we get

$$\begin{aligned}\frac{E(A,B)}{|A-B|} &= \sum_{x\in A-B} \frac{1}{A-B}\big|A\cap(x+B)\big|^2 \\ &\geqslant \Big(\sum_{x\in A-B} \frac{1}{|A-B|}\big|A\cap(x+B)\big|\Big)^2 \\ &= \frac{1}{|A-B|^2}|A||B||A||B|.\end{aligned}$$

Third meeting - Ana E. de Orellana

Covering lemmas such as the ones we will study might be convenient to allow the computation of iterated sums. If we happen to know that $A+B \subset A+X$ for some set $X \subset B$ much smaller than B, then by induction $A+nB \subset A+nX$ for all $n \geqslant 0$, which can be much more easy to calculate.

2.2. **Covering lemmas.** The first lemma we will see is fairly simple, it states that there exists a set $X \subset B$ such that $B \subset X + A - A$, where $|X| \leqslant (|A + B|)/|A|$. The way we obtain X is rather boring, we just take it as the maximal subset of the following family

$$\mathcal{B} = \big\{X \subset B : \{A + x : x \in X\} \text{ are all disjoint}\big\}.$$

The existence of X is trivial when B is finite, and when this isn't the case then it just exists from Zorn's lemma. Since X is maximal then for every $a + b \in A + B$, there exist $a' + x \in A + X$ such that $a + b = a' + x$ (if not then X wouldn't be maximal), this implies that $b = a' - a + x$ and so $B \subset A - A + X$. Also, from the definition of X we have that $A + x$ are all disjoint,

$$|A + X| = \sum_{x \in X} |A + x| = \sum_{x \in X} |A| = |A||X|.$$

Therefore,

$$|X| = \frac{|A + X|}{|A|} \leqslant \frac{|A + B|}{|X|}.$$

Which finishes the proof.

The idea of the next covering lemma will be to build a set X such that $|A + X|$ is big, because of this the algorithm will stop rather soon. It's some sort of "greedy algorithm".

Lemma 2.1. *Let $A, B \subset Z$. Then there exists $X \subset B$ with $|X| \leqslant 2\frac{|A+B|}{|A|} - 1$ such that for every $y \in B$ there are at least $|A|/2$ representations of y in $A - A + X$.*

Proof. We will initialise $X = \varnothing$, then $A - A + X = \varnothing$. Now choose an element $y \in B$ such that

$$\big|\big\{(A + y) \cap (A + X)\big\}\big| \leqslant \frac{|A|}{2}.$$

If we can find such y, add it to X, if not then finish the algorithm. Basically what we are doing is add y to X if there are less than $|A|/2$ ways of representing it in $A - A + X$.

Let y be the element we added to X at a given step and call the previous X (the one without y) X_p, then

$$|A + X| \geqslant |A + X_p| + \frac{|A|}{2},$$

this is because $X = X_p \cup \{y\}$ and so $X + A = (X_p + A) \cup (y + A)$, $|y + A| = |A|$ and at most $|A|/2$ elements in $y + A$ are in $X_p + A$, so at least $|A|/2$ elements in $y + A$ are new.

Also, $A + X \subset A + B$, letting n be the number of iterations, we have

$$\begin{aligned} |A + X| &\leqslant |A + B| \\ \frac{|A|}{2}(n + 1) &\leqslant |A + B| \\ n &\leqslant 2\frac{|A + B|}{|A|} - 1. \end{aligned}$$

Finally, after finishing the algorithm, given $y \in B \backslash X$,

$$\big|\big\{(A + y) \cap (A + X)\big\}\big| > \frac{|A|}{2},$$

so $y + A$ has at least $|A|/2$ representations in $A + X$, and so does y in $X + A - A$. Therefore, $B \subset X + A - A$. □

Examples of this algorithm are tricky, usually what happens is that either the set B is too small, and we end up having $X = B$, or it has a lot of additive structure, and we also get $X = B$. So if B is big and has a lot of additive structure, this can be a problem. Luckily, usually we will try and cover sets B that have low additive structure, so that we can actually gain some from doing $A - A + X$.

2.3. **An application and the tensor power trick.** Let us now work on an application of this covering lemma to bound $|2B - 2B|$, by $16(|A + B|^4|A - A|)/|A|^4$. For this, take $X \subset B$ as in Lemma 2.1, we know that elements of B have at least $|A|/2$ representations in $A - A + X$, therefore if we take $z \in B - B$, $z = b_1 - b_2$ there will exist at least $|A|/2$ triplets in $X \times A \times A$ such that $z = b_1 - a_1 + a_2 - x$. That is,

$$\big|\big\{(x, a_1, a_2) \in X \times A \times A : z = b_1 - a_1 + a_2 - x\big\}\big| \geqslant \frac{|A|}{2},$$

letting $c = a_2 + b_1 \in A + B$ we have

$$\big|\big\{(x, c, a_1) \in X \times (A + B) \times A : z = c - a_1 - x\big\}\big| \geqslant \frac{|A|}{2},$$

thus,

$$\begin{aligned}\big|\big\{(x, x', c, x', a_1, a_1') \in X \times X \times (A + B)(A + B) \times A \times A :& \\ z = c - a_1 + x \text{ and } z' = c' - a_1' - x'\big\}\big| \geqslant \frac{|A|^2}{4}.&\end{aligned}$$

Now let $d = a_1 - a_1' \in A - A$, we have

$$z - z' = c - a_1 - x - c' + a_1' - x' = c - d - x + x',$$

this implies

$$\begin{aligned}\big|\big\{(x, x', c, c', d) \in X \times X \times (A + B) \times (A + B) \times (A - A) :& \\ z - z' = c - c' - d - x - x'\big\}\big| \geqslant \frac{|A|^2}{4}.&\end{aligned}$$

But $z - z \in 2B - 2B$, so elements in $2B - 2B$ have at least $|A|^2/4$ representations of the form $c - c' - d - x + x'$, therefore,

$$\begin{aligned}|2B - 2B| &\leqslant 4\frac{|X \times X \times (A + B) \times (A + B) \times (A - A)|}{|A|^2} \\ &\leqslant 4\frac{|X|^2|A + B|^2|A - A|}{|A|^2} \\ &\leqslant 16\frac{|A + B|^4|A - A|}{|A|^4}.\end{aligned}$$

We now will improve this bound using a tool called the "tensor power trick", the idea behind it is to get rid of constants such as the 16 in the previous bound. For this suppose that we were able to prove $|A| \leqslant C|B|$. If we also prove that for every M, $|A|^M \leqslant C|B|^M$, then we have $|A| \leqslant |B|$, just taking the M-th root and $M \to \infty$.

To apply this "trick" in the previous bound notice that, denoting $A^{\oplus M} = A \times A \times \cdots \times A$, it's trivial to see

$$2B^{\oplus M} - 2B^{\oplus M} = (2B - 2B)^{\oplus M};$$
$$A^{\oplus M} + B^{\oplus M} = (A + B)^{\oplus M};$$
$$A^{\oplus M} - A^{\oplus M} = (A - A)^{\oplus M}.$$

Then applying the previous inequality to $A^{\oplus M}$ and $B^{\oplus M}$ we have

$$|2B - 2B|^M \leqslant 16\frac{|A + B|^{4M}|A - A|^M}{|A|^{4M}},$$

and this is valid for every $M \in \mathbb{N}$.

The tensor power trick can be very useful in areas outside of additive combinatorics. For example, we can use it to prove the convexity of L^p norms: If we have some function $f : \mathbb{R} \to \mathbb{R}$ such that $\int |f|^p \leqslant 1$ and $\int |f|^q \leqslant 1$ for all $0 < p < q < \infty$, then $\int |f|^r \leqslant 1$ for every $p < r < q$.

To prove this we would use the fact that, if $|f(x)| \geqslant 1$ then $|f(x)|^r \leqslant |f(x)|^q$ and if $|f(x)| \leqslant 1$, then $|f(x)|^r \leqslant |f(x)|^p$. Thus,

$$\int |f(x)|^r \, dx \leqslant \int |f(x)|^p + |f(x)|^q \, dx \leqslant 2.$$

Which is not what we want to prove. However, by defining $f^{\oplus M} : \mathbb{R}^M \to \mathbb{R}$ as $f^{\oplus M}(x_1, \ldots, x_M) = f(x_1) \ldots f(x_M)$ we have by Fubini's theorem

$$\int |f^{\oplus M}|^p \, dx = \left(\int |f|^p \, dx \right)^M \leqslant 1,$$

and

$$\int |f^{\oplus M}|^q \, dx = \left(\int |f|^q \, dx \right)^M \leqslant 1.$$

Therefore,

$$\left(\int |f|^r \right)^M = \int |f^{\oplus M}|^r \leqslant \int |f^{\oplus M}|^p + |f^{\oplus M}|^q \, dx \leqslant 2,$$

taking the M-th root and letting $M \to \infty$ we have the result.

3. Fourth meeting - Luke Derry

Using Ruzsa's covering lemma with $B = 2A - A$ and $A = A$ we get the existence of $X_- \subset B$ such that $2A - A \subset A - A + X_-$,

$$|X_-| \leqslant \frac{|A - B|}{|A|} = \frac{|2A - 2A|}{|A|} \leqslant \frac{|A - A|^4|A - A|}{|A||A|^4} = \delta[A]^5,$$

then

$$|2A - A| \leqslant \delta[A]^5|A - A|.$$

The book uses this to get $|mA - nA| \leqslant \delta[A]^{5(m+n-2)}|A|$, but we'll see that we can drop the 5 and the 2 with Plünnecke's inequality.

Lemma 3.1. *If $|A + B| \leqslant K|A|$, then there exists $X \subset A$, $K' \leqslant K$ such that for all $C \in Z$, $|X + B + C| \leqslant K'|X + C|$.*

Proof. Choose $X \subset A$ that maximises $|X+B|/|X|$, as $K' \leqslant K$, then for $X' \subset X$ we have $|X'+B| \geqslant K'|X'|$. We continue by induction on the size of C.

If $C = \varnothing$, $|X+B| \leqslant K'|X+\varnothing|$. Suppose it's valid for C and take $C \cup \{d\}$ for some $d \in Z \backslash C$

$$X + (C \cup \{d\}) = (X+C) \cup (X \backslash X' + \{d\}),$$

with $X' = \{x \in X : x + d \in X + C\}$. Then

$$|X + C \cup \{d\}| = |X+C| + |X \backslash X' + \{d\}|.$$

Also,

$$\big(X + B + (C \cup \{d\})\big) \subset (X+B+C) \cup_{\text{disj}} (X+B+\{d\}) \backslash (X'+B+\{d\}),$$

using that the union is disjoint we get

$$\begin{aligned} \big|X+B+(C\cup\{d\})\big| &\leqslant |X+B+C| + |X+B+\{d\}| - |X'+B+\{d\}| \\ &= |X+B+C| + |X+B| - |X'+B| \\ &\leqslant K'|X+C| + K'|X| - K'|X'| \\ &= K'\big(|X+C| + |X| - |X|\big) \\ &= K'\big(|X+C| + |X \backslash X'|\big). \end{aligned}$$

□

Corollary 3.2. *If $|A+B| \leqslant K|A|$ then there exists $X \subset A$ such that $|X+nB| \leqslant K^n|X|$ for every $n \in \mathbb{N}$. (In particular $|nA| \leqslant K^n|A|$ and if we put $B = A$ or $-A$, then we get $|nA| \leqslant \sigma[A]^n|A|$ and $|nA| \leqslant \delta[A]^n|A|$)*

Proof. From the lemma, there exists $X \subset A$, $K' \leqslant K$ such that

$$|A + B + (n-1)B| \leqslant K'|X + (n-1)B|,$$

we apply the lemma inductively to get the result. □

Theorem 3.3 (Plünnecke's inequality)**.** *If $|A+B| \leqslant K|A|$ then $|nB - mB| \leqslant K^{m+n}|A|$.*

Proof. By the corollary there exists $X \subset A$ such that

$$|X+B| \leqslant K'|X| \leqslant K|X|,$$

and

$$|X + nB| \leqslant (K')^n|X| \quad \forall n \in \mathbb{N}.$$

Let $Y = -X$, $|-X - mB| = |Y - mB| = |X + mB|$, then

$$|Y - mB| \leqslant (K')^m|X|. \tag{3.1}$$

From Ruzsa's distance triangle inequality we know that

$$|X - C||B| \leqslant |A - B||B - C|.$$

Using this in (3.1) with $A = nB$, $B = Y$, $C = mB$ we get

$$\begin{aligned} |nB - mB||Y| &\leqslant |nB - Y||Y - mB| \\ &\leqslant (K')^n|X|(K')^m|X|, \end{aligned}$$

then

$$|nB - mB| \leqslant (K')^{n+m}|X| \leqslant (K')^{n+m}|A| \leqslant K^{n+m}|A|.$$

□

Using $B = -A$ in Plünnecke's inequality we obtain

$$|nA - mA| \leqslant \delta[A]^{n+m}|A|$$

whereas in the book we would've obtained

$$|nA - mA| \leqslant \delta[A]^{5(n+m-1)}|A|.$$

4. Fifth meeting - Alex Rutar

Given $G \subset A \times B$, we define the partial sumset as

$$A \overset{G}{+} B = \{a + b : (a, b) \in G\},$$

we can think about this as the projection of a part of the product set. The idea is getting info about partial sumsets into info about the sumset, we do this by controlling large pieces of the sumset.

Theorem 4.1 (Balog, Szemerédi, Gowers)**.** *Given $A, B \subset Z$, if $G \subset A \times B$ is such that*

$$|G| \geqslant \frac{|A||B|}{K}; \qquad |A \overset{G}{+} B| \leqslant K'|A|^{1/2}|B|^{1/2}$$

(in some way we're saying that G is a large proportion of A and B)

Then there exists $A' \subset A$, $B' \subset B$ with

$$|A'| \geqslant \frac{|A|}{4\sqrt{2}K}; \qquad |B'| \geqslant \frac{|B|}{4K},$$

such that

$$|A' + B'| \leqslant 2^{12}K^4(K')^3|A|^{1/2}|B|^{1/2} \quad \textit{(a polynomial on } K \textit{ and } K')$$

Example: Suppose $B = A = S \cup P$, where S is a Sidon set and P an arithmetic progression with $|S| = |P| = N$. If we take $G = P \times P$. Then

$$|A||B| = 4N^2;$$
$$|G| = N^2,$$

in this case we'd be having $K = 4$. If we take the partial sumset, we'd be only adding the elements in the arithmetic progression, then

$$|A \overset{G}{+} B| = 2N - 1,$$
$$|A + B| = N^2 + 2N - 1 \approx N^2.$$

This example shows that A' and B' will in general be different from A and B.

Proposition 4.2 (Additive energy " $\Longleftrightarrow$ " Partial sumsets)**.**

(1) $E(A, B) \geqslant \frac{|G|}{|A \overset{G}{+} B|}$ for all $G \subset A \times B$.

(2) Suppose $E(A, B) \geqslant \frac{|A|^{3/2}|B|^{3/2}}{K}$ then there exists $G \subset A \times B$ such that

$$G \geqslant \frac{|A||B|}{K} \quad \textit{and} \quad |A \overset{G}{+} B| \leqslant 2K|A|^{1/2}|B|^{1/2}.$$

Proof.

(1) Remember that

$$E(A,B) = \sum_{x\in A+B} \big|\{(a,b)\in A\times B : a+b=x\}\big|^2.$$

Then

$$\begin{aligned}|G|^2 &= \Big(\sum_{x\in A+B} \big|\{(a,b)\in G : a+b=x\}\big|\Big)^2\\ &\leqslant \Big[\sum_{x\in A+B} \big|\{(a,b)\in G : a+b=x\}\big|^2\Big]|A\overset{G}{+}B|\\ &\leqslant E(A,B)|A\overset{G}{+}B|.\end{aligned}$$

(2) Recall that $|A||B| \leqslant E(A,B) \leqslant \min\{|A|^2|B|, |A||B|^2\}$. Define the set

$$S = \{x\in A+B : |A\cap(x-B)| \geqslant \tfrac{|A|^{1/2}|B|^{1/2}}{2K}\}.$$

Let $G = \{(a,b)\in A\times B : a+b\in S\}$. We're taking G to carry most of the additive structure of A and B.

Fact 1:

$$\begin{aligned}\sum_{x\in S}\big|A\cap(x-B)\big|^2 &= E(A,B) - \sum_{x\notin S}\big|A\cap(x-B)\big|^2\\ &\geqslant \frac{|A|^{3/2}|B|^{3/2}}{K} - \frac{|A||B||A|^{1/2}|B|^{1/2}}{2K}\\ &\geqslant \frac{|A|^{3/2}|B|^{3/2}}{2K}.\end{aligned}$$

Fact 2:

$$\frac{|S||A|^{1/2}|B|^{1/2}}{2K} \leqslant \sum_{x\in S}\big|A\cap(x-B)\big| \leqslant |A||B|$$

Also

$$|A\overset{G}{+}B| \leqslant |S| \leqslant 2K|A|^{1/2}|B|^{1/2}$$

Then

$$|G| = \sum_{x\in S}\big|A\cap(x-B)\big| \geqslant \sum_{x\in S}\frac{\big|A\cap(x-B)\big|^2}{|A|^{1/2}|B|^{1/2}} \geqslant \frac{|A|^{3/2}|B|^{3/2}}{2K|A|^{1/2}|B|^{1/2}}.$$

□

Corollary 4.3 (BSG - Additive energy)**.** *The following are equivalent*

- $E(A,B) \geqslant K^{-C_1}|A|^{3/2}|B|^{3/2}$.
- *There exists* $G\subset A\times B$ *such that*

$$|G| \geqslant K^{-C_2}|A||B|$$
$$|A\overset{G}{+}B| \leqslant K^{C_2}|A|^{1/2}|B|^{1/2}$$

There are a lot of situations where $E(A,B)\approx |A||B|^2$.

4.1. **Assymetric BSG.**

Definition 4.4. *A set H is a K-approximate group if*

- $H = -H$.
- $H + H$ *contains* K *translations of* H.

Theorem 4.5 (Assymetric BSG)**.** *Let $A, B \subset Z$ such that*

$$E(A,B) \geqslant 2\alpha|A||B|^2 \quad (\alpha \in (0,1))$$
$$|A| \leqslant L|B|.$$

Then for every $\varepsilon > 0$ there exist:

- $O_\varepsilon(\alpha^{-O_\varepsilon(1)}L^\varepsilon)$*-approximate group H (small H)*
- $X \subset Z$ *such that* $|X| = O_\varepsilon\big(\alpha^{O_\varepsilon(1)}L^{-\varepsilon}\frac{|A|}{|H|}\big)$

such that

$$\big|A \cap (x+H)\big| = \Omega_\varepsilon\big(\alpha^{O_\varepsilon(1)}L^{-\varepsilon}|A|\big),$$

and for $x \in Z$

$$\big|B \cap (x+H)\big| = \Omega_\varepsilon\big(\alpha^{O_\varepsilon(1)}L^{\varepsilon}|B|\big).$$

5. Sixth meeting - Natalia Jurga

We will see some non-commutative analogues of what we've learned so far. Our setting will be a non-abelian group G with group operation $\cdot$, the inverse will be denoted as $x \mapsto x^{-1}$ and the identity will be 1. An example of this is $G = SL_2(\mathbb{Z})$.

Note that $x \cdot A \neq A \cdot x$ although $|A| = |A^{-1}| = |x \cdot A| = |A \cdot x|$. We have the trivial inequalities

$$\max\{|A|,|B|\} \leqslant |A \cdot B|, |B \cdot A| \leqslant |A||B|,$$

but in general $|B \cdot A| \neq |A \cdot B|$.

Example: Let $H \leqslant G$, $x \notin N(H)$, the normaliser of H, defined as $N(H) = \{x \in G : x \cdot H = H \cdot x\}$. Consider $A = H$, $B = x \cdot H$. Then

$$A \cdot B = H \cdot x \cdot H \qquad |A \cdot B| \approx |H|^2;$$
$$B \cdot A = x \cdot H \cdot H = x \cdot H \qquad |B \cdot A| = |H|.$$

Definition 5.1 (Rusza distance analog)**.** *Define the function*

$$d(A,B) = \log\left(\frac{|A \cdot B^{-1}|}{|A|^{1/2}|B|^{1/2}}\right).$$

This function satisfies the triangle inequality. To prove this it suffices to see

$$\frac{|A \cdot B^{-1}|}{|A|^{1/2}|B|^{1/2}} \leqslant \frac{|A \cdot C^{-1}|}{|A|^{1/2}|C|^{1/2}} \cdot \frac{|C \cdot B^{-1}|}{|C|^{1/2}|B|^{1/2}} = \frac{|A \cdot C^{-1}||CB^{-1}|}{|C|},$$

so we only have to show that

$$|C||A \cdot B^{-1}| \leqslant |A \cdot C^{-1}||C \cdot B^{-1}|,$$

and this is true because there are at most $|C|$ representations $ab = ac^{-1}cb$.

Also, d is not a distance. But more is true

$$d(A,B) = 0 \quad \iff \quad H \leqslant G,\ A = x \cdot H,\ B = y \cdot H.$$

($\Leftarrow$) Is not hard to prove:

$$\exp\big(d(A,B)\big) = \frac{|(x\cdot H)(y\cdot H)^{-1}|}{|x\cdot H|^{1/2}|y\cdot H|^{1/2}} = \frac{|x\cdot H\cdot y^{-1}|}{|H|} = 1.$$

($\Rightarrow$) we don't know how to prove.

5.1. **Rusza covering lemma. Question:** Can we find a more efficient way of covering $A\cdot B\subset A\cdot X$ for $X\subset B$?

Lemma 5.2. *Suppose $|A\cdot B|\leqslant K|A|$ then there exists $X\subset B$ with $|X|\leqslant K$ such that $B\subset A^{-1}\cdot A\cdot x$.*

Proof. Let $\mathcal{B}=\{X\subset B : \{A\cdot x\}\text{are disjoint } \forall x\in X\}$. Choose X maximal in $\mathcal{B}$. Then

$$|A\cdot X| = \sum_{x\in X}|A\cdot x| = |X||A| \implies |X| = \frac{|A\cdot X|}{|A|}\leqslant K.$$

Using the maximality of X we get the covering. □

5.2. **Plünnecke's inequality.** To get an analog of Plünnecke's inequality we'd want to bound a product like $|A^{\varepsilon_1}\cdots A^{\varepsilon_k}|$ where $\varepsilon_i=\pm 1$. We'd like to have something like $|A\cdot A|\leqslant K|A|$ implies $|A^n|\leqslant K^n|A|$.

But there is a problem with this. Let's look at the following example.

Example: If $H\leqslant G$, $A=H\cup\{x\}$ for some $x\notin N(H)$. Then

$$A\cdot A = H\cup(x\cdot H)\cup(H\cdot x)\cup\{x^2\}$$
$$|A\cdot A|\leqslant 3|H|+1\leqslant 3|A|-2.$$

And we would expect to have, for example for $n=3$, $|A\cdot A\cdot A|\leqslant K^3|A|$. However

$$A\cdot A\cdot A\supset H\cdot x\cdot H,$$

and this can be very large! Since

$$|H\times H| = |H|^2 = \big(|A|-1\big)^2 \gg |A|.$$

Proposition 5.3. *The following are equivalent.*

(1) $|A\cdot A\cdot A|\leqslant K^{c_1}|A|$.
(2) $|A^n|\leqslant K^{c_2}|A|$ for all $n\geqslant 1$ (there is an analogue of this with ε_is)
(3) There exists a K^{c_3}-approximate group $H\supset A$ where $|H|\leqslant K^{c_2}|A|$.

Where H is a K-approximate group if $\mathrm{Id}\in H$, $H=H^{-1}$, and if $|X|\leqslant K$ then

- $H\cdot H\subset X\cdot H\subset H\cdot X\cdot X$.
- $H\cdot H\subset H\cdot X\subset X\cdot X\cdot H$.

References

[TV06] Tao T, Vu VH. Additive Combinatorics. Cambridge University Press (2006).

A. E. de Orellana, University of St Andrews, Scotland
Email address: aedo1@st-andrews.ac.uk