# Topics in Additive Combinatorics Summary

Immanuel Whang

## §0.1 Introduction

A very natural object of study in combinatorics in the study of sets, and more specifically, the study of set partitions. Indeed, we have already explored partitions in this class.

One observation one can make about partitions is that the actual elements of the sets we are partitioning do not matter, as long as they distinct. We only are interested in the number of elements in the initial set.

Additive combinatorics is what happens when we study specific sets, not only in isolation, but also in interaction with other sets. Typically, the sets that we will be studying will be subsets of $\mathbb{Z}, \mathbb{N}, \mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/N\mathbb{Z}, [n]$.

We will begin by defining some basic notions.

**Definition 0.1.** For finite subsets $A, B$ of an abelian group, the sumset $A + B$ is defined as

$$\{a + b : (a, b) \in A \times B\}.$$

**Definition 0.2.** Similarly, the difference set $A - B$ is defined to be

$$\{a - b : (a, b) \in A \times B\}.$$

**Definition 0.3.** The $k$-fold sumset of $A$ with itself, written as $kA$, is defined to be

$$\{a_1 + \cdots + a_k : (a_1, \cdots, a_k) \in A^k\}.$$

The doubling constant of $A$ is defined to be

$$K = \frac{|A + A|}{|A|}.$$

With these definitions in place, you can probably get a good idea of the questions in which additive combinatorics is interested in studying. When is $|A + B|$ small in relation to $|A|$ and $|B|$? Can we derive any information about $A$ and $B$ given that $|A + B|$ is small? Can we bound $|A + B|$ given limited information about $A$ and $B$? Those are the types of the problems that additive combinatorics is concerned with.

## §0.2 Foundational Results

**Theorem**

For nonempty sets $A, B \subset \mathbb{Z}$,

$$|A+B| \geq |A| + |B| - 1.$$

*Proof.* Assign the variable names $a_1, \ldots, a_{|A|}$ to elements in $A$ such that if $1 \leq i < j \leq |A|$, $a_i < a_j$. Do the same for $B$. Then, note that $a_1 + b_1 < a_1 + b_2 < \ldots < a_1 + b_{|B|}$, and $a_1 + b_{|B|} < a_2 + b_{|B|} < \ldots < a_{|A|} + b_{|B|}$, so we can combine these chains of inequalities to get one big inequality chain with $|A| + |B| - 1$ elements:

$$a_1 + b_1 < a_1 + b_2 < \ldots < a_1 + b_{|B|} < a_2 + b_{|B|} < \ldots < a_{|A|} + b_{|B|}.$$

Therefore, $|A + B|$ must have at least $|A| + |B| - 1$ distinct elements. To see that this is the best bound we can get without further imposing conditions on $A$ and $B$, consider $A = \{1\}$, $B = \{1\}$, which gives us $|A + B| = |A| + |B| - 1$. □

Next, we can see if we can improve our bound when we look at some other different types of subsets.

### §0.2.1 Cauchy-Davenport Theorem

**Theorem**

For prime $p$ and nonempty sets $A, B \subset \mathbb{Z}/p\mathbb{Z}$,

$$|A+B| \geq \min(p, |A| + |B| - 1).$$

*Proof.* Our inequality looks very similar to our previous one, but unfortunately, our proof does not hold in this case because we have "wraparounds," preventing us from using notions of size.

We will proceed with induction on the size of $B$.

**Base Case:** Note that if $|B| = 1$, $|A + B| = |A| = |A| + |B| - 1$, so $|A + B| \geq \min(p, |A| + |B| - 1)$ in this case.

**Inductive Hypothesis:** Suppose that there exists some $k$ such that if $|B| = k$, then $|A + B| \geq \min(p, |A| + |B| - 1)$. We wish to show the same holds for all $|B| = k + 1$.

**Inductive Step:** Take any element $b$ from $B$ with $k+1$ elements and then remove it. Then, take its sumset with $A$. Our inductive hypothesis tells us that $|A + Bnb| \geq |A| + |B| - 2$. Then, if $|A + B|$ contains any elements not in $|A + Bnb|$, we are done. Consider what happens if $|A + B| = |A + B\backslash b|$. Then, we must have that for all $a \in A$, there exists $a' \in A$ and $b' \in B\backslash b$ such that $a + b = a' + b'$.

We can rearrange to get $a + b - b' = a' \Rightarrow a + b - b' \in A$. Now, let $B^-$ be the set of all values taken on by $b - b'$ (not all possible values!), noting that $|B^-| \leq k$ since $b' \neq b$. We can see that $A + B^- = \{a + b - b' | a \in A, b - b' \in B^-\}$, so via our prior work, we have $A + B^- \subset A \Rightarrow |A + B^-| \leq |A|$. And since $|B^-| \leq k$, we can use our inductive hypothesis to get

$$|A| \geq |A + B^-| \geq \min(p, |A| + |B^-| - 1).$$

Now, we have two ways for this to be true. If $p \leq |A| + |B^-| - 1$, then $|A| \geq p \Rightarrow |A| = p$ and our inductive step holds since $|A + B| = p$. If $p > |A| + |B^-| - 1$, then $|A| \geq |A| + |B^-| - 1$, which forces $|B^-|$ to be 1 since it is nonempty.

This tells us that for some $b' \in B \backslash b$, $A + b - b' = A$. Hence, if $x \in A$, then so must $x + b - b'$. Since $b \neq b'$, $b - b' \neq 0$, and because we are working in $\mathbb{Z}_p$, if $x \in A$, $\{x + n(b - b') | n \in \mathbb{Z}_p\} = \mathbb{Z}_p$. We assumed that $A$ is nonempty, so $A = \mathbb{Z}_p$, so our inductive step holds in this case as well.

So because we have proven our inductive step holds true in all possible cases, our induction holds and the statement is proven. We can easily verify this is the best possible bound by taking $A, B = \{1\}$.

□

This theorem can be used to prove many other results.

**Corollary**

For prime $p$ and $a, b \in \mathbb{Z}/p\mathbb{Z}$, for any $x \in \mathbb{Z}/p\mathbb{Z}$, there exist $y, z \in \mathbb{Z}/p\mathbb{Z}$ such that $x = ay^2 + bz^2$.

*Proof.* To use Cauchy-Davenport, we need two subsets of $\mathbb{Z}/p\mathbb{Z}$. The expression $ay^2 + bz^2$ thus motivates the consideration of two very natural sets: $aQ$ and $bQ$, where $Q$ is the set of all quadratic residues in $\mathbb{Z}/p\mathbb{Z}$ (note that $aQ$ is the set obtained by multiplying every element of $Q$ by $a$).

Now, we will split into casework. If $p = 2$, then $|Q| = 2$, and so $|aQ| = |bQ| = 2$. By Cauchy-Davenport, $|aQ + bQ| \geq \min(2, |aQ| + |bQ| - 1) = 2$, so $|aQ + bQ| = 2$, giving us that $aQ + bQ = \mathbb{Z}/p\mathbb{Z}$, so every $x \in \mathbb{Z}/p\mathbb{Z}$ can be expressed as $ay^2 + bz^2$ for some $y, z$.

If $p \neq 2$, then $|Q| = |aQ| = |bQ| = \frac{p+1}{2}$, so again by Cauchy-Davenport, we get

$$|aQ + bQ| \geq \min(p, |aQ| + |bQ| - 1) = p.$$

Thus, we have that $aQ + bQ = \mathbb{Z}/p\mathbb{Z}$, so the claim holds in this case as well and we are done. □

A very natural question one might ask is when equality occurs in the inequality given by Cauchy-Davenport. That is, when does $|A + B| = |A| + |B| - 1$? This leads us to the following statement:

**Theorem**

For nonempty subsets of $\mathbb{R}$ $A$ and $B$, $|A + B| = |A| + |B| - 1$ iff one of the following statements holds true:

(a) $|A| = 1$

(b) $|B| = 1$

(c) $A$ and $B$ are arithmetic sequences with the same common difference.

*Proof.* **If**: Clearly, if $|A| = 1$, then $|A + B| = |B|$, and the same holds if $|B| = 1$. If $A$ and $B$ are arithmetic sequences with the same common difference, let $d$ be the common difference, $a$ be the smallest element of $A$, and $b$ be the smallest element of $B$.

Then, the smallest element we can make is $a+b$, and the largest element is $a+b+d(|A|+|B|-2)$. Note that all elements in $|A+B|$ must be congruent to $a+b$ mod $d$, and note that we can make all numbers from $a+b$ to $a+b+d(|A|+|B|-2)$ that are congruent to $a+b$ mod $d$. Hence, we have $|A+B| = |A|+|B|-1$, so we have proved the if direction of the statement.

**Only If:** We want to show that if $|A + B| = |A| + |B| - 1$, then one of our three conditions must be satisfied. This is equivalent to proving that if $|A+B| = |A|+|B|-1$ and $|A|, |B| > 1$, then $A$ and $B$ are arithmetic sequences with the same common difference.

So let's assume that $|A|, |B| > 1$. Then, we can use the same strategy as earlier and let $A = \{a_1, a_2, \cdots, a_m\}$ and $B = \{b_1, b_2, \cdots, b_n\}$, where $a_i < a_j$ and $b_i < b_j$ if $i < j$. We know that

$$a_1 + b_1 < a_2 + b_1 < \cdots < a_m + b_1 < a_m + b_2 < \cdots < a_m + b_n.$$

Because this chain has $|A|+|B|-1$ elements, we know that all other elements of $|A+B|$ must be equal to some element in this chain.

We can generate a similar but different chain:

$$a_1 + b_1 < a_1 + b_2 < \cdots < a_m + b_2.$$

We can now match up this chain with the first part of our prior chain (this works because the subchain has the same number of elements and starts and end at the same number):

$$a_1 + b_1 < a_2 + b_1 < \cdots < a_m + b_2.$$

Therefore, we get $a_{i-1} + b_2 = a_i + b_1$ for all $2 \leq i \leq m$, so $a_i - a_{i-1} = b_2 - b_1$.

We can repeat this argument conversely to get that $b_i - b_{i-1} = a_2 - a_1$ for all $2 \leq i \leq n$, so both $A$ and $B$ are arithmetic sequences.

Finally, we know that these arithmetic sequences must have the same common difference because $a_2 + b_1 = a_1 + b_2$, so we are done. □

**Theorem**

For finite sets $A, B, C \subset G$, $|A||B - C| \leq |A - B||A - C|$.

*Proof.* We will define a mapping from $A \times B - C$ to $A - B \times B - C$ and show it is injective, hence proving the inequality. For each $x \in B - C$, fix a "representative" pair $(b, c) \in B \times C$ such that $b - c = x$. Then, define the mapping $f(a, x) = (a - b, a - c)$. If $f(a_1, x_1) = f(a_2, x_2)$, then $x_1 = x_2$ since the difference between the mapped-to coordinates is just $x_1$ and $x_2$. Then, $a_1 = a_2$ because if $x_1 = x_2$, then $b_1 = b_2$ and $c_1 = c_2$, meaning that $a_1 = a_2$. Therefore, this mapping is injective and the inequality holds. □

The astute reader may notice that this relationship looks very similar to the triangle inequality, and in fact, it can be used to define a notion of distance in relation to sets.

**Definition 0.4.** (Ruzsa Distance) For finite subsets of a group $A$ and $B$, the Ruzsa distance between the sets is

$$d(a,b) = \log \frac{|A-B|}{\sqrt{|A||B|}}.$$

This definition comes in handy in the proof of the final result in this handout.

**Theorem**

(Plünnecke-Ruzsa inequality) For finite subsets $A$ and $B$, let $K$ be any constant such that $|A+B| \leq K|A|$. Then, for al lnonnegative integers $m$ and $n$,

$$|mB - nB| \leq K^{m+n}|A|.$$