TOPICS IN ADDITIVE COMBINATORICS

OM LALA

Abstract

The essence of this paper deals with core structures in Additive Combinatorics, namely the sumset and the structures of the sets that produce the sumset. We construct tools that measure expansion and symmetry of the sumset. We walk through some of the most interesting ideas in early Additive Combinatorics.

1. Preliminaries

Unless stated otherwise, all sets considered will be finite subsets of the integers.

Definition 1.1 (Sumsets)**.** Let $A, B \subset \mathbb{Z}$ be finite sets. The sumset $A + B$ is defined by

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

The difference set is defined similarly by

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

The size of a sumset provides a basic measure of the additive behavior of the sets involved.

Definition 1.2 (Doubling Constant)**.** For a finite set $A \subset \mathbb{Z}$, the doubling constant of A is

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

A set A is said to have small doubling when $K(A)$ is bounded by an absolute constant, in which case A typically exhibits notable additive structure.

Definition 1.3 (Additive Translates and Dilates)**.** For $x \in \mathbb{Z}$ and $t \in \mathbb{Z}_{\geq 1}$, define

$$A + x = \{a + x : a \in A\}, \qquad tA = \{ta : a \in A\}.$$

These operations preserve many additive properties. For example, $|(A+x)+(A+x)| = |A+A|$ for any integer x.

Definition 1.4 (Iterated Sumsets)**.** For an integer $k \geq 1$, the k-fold sumset is

$$kA = \underbrace{A + A + \cdots + A}_{k \text{ times}}.$$

Iterated sumsets quantify how a set expands under repeated addition.

Date: December 7, 2025.

Definition 1.5 (Additive Energy)**.** For a finite set $A \subset \mathbb{Z}$, the additive energy of A is

$$E(A) = |\{(a,b,c,d) \in A^4 : a+b = c+d\}|.$$

Larger values of $E(A)$ indicate the presence of many additive coincidences and therefore increased additive structure. Energy is related to the size of the sumset through the inequality

$$|A+A| \le \frac{|A|^4}{E(A)}.$$

Definition 1.6 (Ruzsa Distance)**.** For finite, nonempty sets $A, B \subset \mathbb{Z}$, the Ruzsa distance between A and B is defined as

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

This quantity behaves analogously to a metric up to the triangle inequality.

Theorem 1.7 (Ruzsa Triangle Inequality)**.** *For finite sets $A, B, C \subset \mathbb{Z}$,*

$$|A-C| \le \frac{|A-B|\,|B-C|}{|B|}.$$

Definition 1.8 (Graph-Theoretic Representation)**.** Let $A, B \subset \mathbb{Z}$. Consider the directed bipartite graph $G(A,B)$ whose edges encode the additive relations

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

This representation is used in the proof of Plünnecke's inequality to control additive expansion through magnification ratios.

Definition 1.9 (Generalized Arithmetic Progressions)**.** A d-dimensional generalized arithmetic progression (GAP) is a set of the form

$$P = \{x_0 + k_1 x_1 + \cdots + k_d x_d : 0 \le k_i < L_i\}.$$

GAPs model structured subsets of the integers. Freiman's theorem states that sets of small doubling are always contained in a bounded-rank GAP.

Remark 1.10. The notions introduced above will be used throughout the remainder of this paper. They form the basis for the study of sumset growth (Section 2), Ruzsa-type inequalities (Section 3), Plünnecke's inequality (Section 4), Freiman's structural theorem (Section 5), and additive energy (Section 6).

2. Sumset Growth

We now examine in detail the behavior of the sumset $A+B$ and the difference set $A-B$ for two additive sets A, B contained in a common ambient group Z, as in Definition 0.1. We will also consider the iterated sumsets nA. It is important to note that the iterated sumset nA is generally distinct from the dilate $n \cdot A := \{na : a \in A\}$, although the inclusion

$$n \cdot A \subseteq nA$$

always holds. Likewise, the difference set $A-B$ should not be confused with the set-theoretic difference

$$A \setminus B = \{x \in A : x \notin B\}.$$

We continue to write $A + x = A + \{x\}$ for the translate of A by an element $x \in Z$.

Since addition in Z is associative and commutative, the same is true for the addition of sets. However, set addition does not admit an inverse operation. For example, while $A+B-B$ always contains A, it is typically much larger than A. Similarly, when $n>m$, the set $nA-mA$ contains $(n-m)A$ but is usually strictly larger.

A fundamental problem in this area is to determine when the sumset $A+B$ is "small" and when it is "large." More precisely, we are interested in understanding the cardinality of $|A+B|$ in terms of $|A|$ and $|B|$. The following elementary bounds serve as a starting point.

Lemma 2.1 (Trivial sumset estimates)**.** *Let A, B be additive subsets of a common ambient group Z, and let $x \in Z$. Then:*

$$|A+x| = |A|, \qquad |A|, |B| \le |A+B|, \qquad |A-B| \le |A|\,|B|. \tag{2.1}$$

Moreover,

$$|A| \le |A+A| \le \frac{|A|(|A|+1)}{2}. \tag{2.2}$$

More generally, for each integer $n \ge 1$, we have $|(n+1)A| \ge |nA|$ and

$$|nA| \le \binom{|A|+n-1}{n} = \frac{|A|(|A|+1)\cdots(|A|+n-1)}{n!}. \tag{2.3}$$

We remark that the lower bound in 2.1 may be improved in certain special groups Z, or when the sets A and B possess additional structure or dimension.

Proof. We prove only 2.3, as the other inequalities follow easily or are straightforward. The proof proceeds by induction on $|A|$.

If $|A|=1$, then both sides of 2.3 are equal to 1. Now assume $|A|>1$. Write $A = B \cup \{x\}$, where B is a nonempty set of size $|B| = |A|-1$. Then

$$nA = \bigcup_{j=0}^{n} \left(jB + (n-j)\,x\right).$$

■

Now, We begin with two fundamental bounds for the size of a sumset. Let $A, B \subset \mathbb{Z}$ be finite sets.

Lemma 2.2 (Lower and upper bounds for sumsets)**.** *For any finite sets $A, B \subset \mathbb{Z}$, the following inequalities hold:*

$$|A|+|B|-1 \;\le\; |A+B| \;\le\; |A|\,|B|.$$

Proof. The upper bound follows immediately from the definition of $A+B$, since each of the $|A||B|$ ordered pairs $(a,b) \in A \times B$ produces at most one element of $A+B$.

For the lower bound, list the elements of A and B in increasing order:

$$A = \{a_1 < a_2 < \cdots < a_m\}, \qquad B = \{b_1 < b_2 < \cdots < b_n\}.$$

Then the sums

$$a_1+b_1 < a_1+b_2 < \cdots < a_1+b_n$$

are strictly increasing, as are the sums

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

In particular,

$$a_1 + b_1 \le a_i + b_j \le a_m + b_n$$

for all i, j, and there are at least $m + n - 1$ distinct integer values between these extremes. Hence $|A + B| \ge m + n - 1$. ■

The following classical result provides a sharp lower bound for sumsets in prime-order cyclic groups.

Theorem 2.3 (Cauchy–Davenport)**.** *Let p be a prime, and let $A, B \subset \mathbb{Z}/p\mathbb{Z}$ be nonempty subsets. Then*

$$|A + B| \ \ge\ \min\bigl(p,\ |A| + |B| - 1\bigr).$$

This inequality shows that in a torsion-free setting or in $\mathbb{Z}/p\mathbb{Z}$, the sumset cannot be substantially smaller than the sum of the sizes of the individual sets. A nice discussion can be found on [Nat96].

Exact Inverse Sumset Theorem. We now record a basic structural characterization of sets for which the sumset $A + B$ has the smallest possible size.

Proposition 2.4 (Exact inverse sumset theorem)**.** *Suppose A, B are additive subsets of a common ambient group Z. The following statements are equivalent:*

(1) $|A + B| = |A|$;
(2) $|A - B| = |A|$;
(3) $|A + nB - mB| = |A|$ *for at least one pair of integers* $(n, m) \neq (0, 0)$;
(4) $|A + nB - mB| = |A|$ *for all integers* n, m;
(5) *there exists a finite subgroup $G \subseteq Z$ such that B is contained in a coset of G, and A is a union of cosets of G.*

Proof. We show that (1) implies (5). The remaining implications are similar or straightforward.

By translating B if necessary, we may assume that $0 \in B$. Since $A + B \supseteq A + \{0\} = A$ and $|A + B| = |A|$, we must have $A + B = A$. Thus $a + b \in A$ for all $a \in A$ and $b \in B$, which implies $A + b = A$ for every $b \in B$.

Define the *symmetry group* of A by

$$_1(A) := \{h \in Z : A + h = A\}.$$

From the previous paragraph we have $B \subseteq_1 (A)$.

It remains to verify that $_1(A)$ is a finite subgroup of Z, and that A is a union of cosets of $_1(A)$. These facts follow from routine arguments: if $h_1, h_2 \in_1 (A)$, then

$$A + (h_1 - h_2) = (A + h_1) - h_2 = A - h_2 = A,$$

so $_1(A)$ is a subgroup; finiteness follows from A being finite. Furthermore, if $a \in A$, then the entire coset $a +_1 (A)$ is contained in A because adding any element of $_1(A)$ does not change A.

Taking $G :=_1 (A)$ proves (5). ■

The group $_1(A)$, as well as its generalization $_\alpha(A)$, will be analyzed more systematically in later sections, where they play an important role in understanding extreme cases of sumset growth.

Doubling and Difference Constants. A standard way to quantify the additive structure present in a set A is through its doubling and difference constants.

Definition 2.5 (Doubling and difference constants)**.** For a finite additive set A, define the doubling constant

$$\sigma[A] := \frac{|A+A|}{|A|}.$$

Similarly, define the difference constant

$$\delta[A] := \frac{|A-A|}{|A|}.$$

From inequality (2.2) we obtain the bounds

$$1 \le \sigma[A] \le \frac{|A|+1}{2}, \qquad 1 \le \delta[A] \le \frac{|A|-1}{2} + \frac{1}{|A|}.$$

These constants measure how rapidly A expands under addition or subtraction. Small values of $\sigma[A]$ or $\delta[A]$ indicate strong internal structure, while large values correspond to sets with little additive organization.

The exact inverse sumset theorem shows that the only way the sumset $A+B$ can have the minimal possible size $|A|$ is if A is a union of cosets of a finite subgroup, and B is contained within a single coset of that subgroup. Thus *zero growth* in the sumset forces A and B to exhibit rigid algebraic structure.

The doubling constant $\sigma[A]$ provides a first quantitative measure of how far a set is from this ideal configuration. If $\sigma[A]$ is close to 1, then A behaves similarly to a coset progression and is highly structured. If $\sigma[A]$ is large—for instance, comparable to $|A|$—then A resembles a random set.

These ideas will appear in later sections.

3. Ruzsa's Triangle Inequality and Ruzsa Distance

Definition 3.1 (Ruzsa distance)**.** Let A and B be additive sets in a common ambient group Z. The Ruzsa distance between A and B is defined by

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

For example, $d(A,A) = \log \delta[A]$, where $\delta[A] = |A-A|/|A|$ is the difference constant.

We now justify the term "distance."

Lemma 3.2 (Ruzsa triangle inequality)**.** *The Ruzsa distance is non-negative, symmetric, and satisfies*

$$d(A,C) \le d(A,B) + d(B,C)$$

for all additive sets A, B, C in a common ambient group Z.

Proof. Non-negativity follows directly from (2.1). Symmetry follows since $B-A = -(A-B)$. To prove the triangle inequality, it suffices to show

$$|A-C| \le \frac{|A-B|\,|B-C|}{|B|}.$$

Using the identity $a-c = (a-b)+(b-c)$, every element of $A-C$ has at least $|B|$ distinct representations of this form, from which the bound follows. ∎

The Ruzsa distance satisfies all axioms of a metric except that $d(A, A)$ need not vanish for all sets A; it does vanish when A is a union of cosets of a finite subgroup. This leads to the following exact characterization of when d is zero.

Proposition 3.3. *Suppose (A, Z) is an additive set. The following are equivalent:*

(1) $\sigma[A] = 1$ (that is, $|A + A| = |A|$);
(2) $\delta[A] = 1$ (that is, $|A - A| = |A|$, or $d(A, A) = 0$);
(3) $d(A, B) = 0$ *for at least one additive set* B;
(4) $|nA - mA| = |A|$ *for at least one pair of non-negative integers* n, m *with* $n + m \geq 2$;
(5) $|nA - mA| = |A|$ *for all non-negative integers* n, m;
(6) A *is a coset of a finite subgroup of* Z.

The Ruzsa distance provides a quantitative measure of additive similarity between sets, and the triangle inequality is the key tool that allows one to relate the sizes of various sumsets and difference sets. The preceding proposition shows that $d(A, B) = 0$ occurs only in the highly structured case when A is a finite subgroup coset. Thus the Ruzsa distance detects exactly when a set exhibits perfect additive symmetry, and later sections will show how this distance interacts with both Plünnecke theory and additive energy.

4. Plünnecke's Inequality

Plünnecke's inequality provides one of the strongest general principles relating small doubling to long-term additive behavior. The assumption $|A + B| \leq K|A|$ can be viewed as a first indication that A does not expand too rapidly when combined with B. Plünnecke's theory shows that this mild hypothesis already forces a precise and highly nontrivial form of controlled growth for all higher-order sumsets.

Theorem 4.1 (Plünnecke's inequality)**.** *Let A and B be additive sets in an ambient group Z and assume*

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

Then for every positive integer k there exists a subset $X \subseteq A$ such that

$$|X + kB| \leq K^k|X|.$$

In particular,

$$|kB| \leq K^k|A|.$$

This result shows that the phenomenon of small doubling does not disappear when we consider iterated sums. Instead, the same bound K propagates multiplicatively: once $A+B$ is known to grow slowly, every higher sumset involving B expands at most exponentially in k with base K. The existence of the subset X is essential: it reflects that a well-chosen portion of A captures the "least expanding" part of the $A + B$ interaction. This subset controls the growth of the entire additive structure generated by B.

A classical refinement combines Plünnecke's inequality with Ruzsa's triangle inequality to obtain universal bounds for more complicated additive expressions.

Corollary 4.2 (Plünnecke–Ruzsa estimates)**.** *Let A, B be additive sets with $|A+B| \leq K|A|$. Then for all integers $n, m \geq 1$,*

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

These estimates illustrate that small doubling is robust under repeated addition and subtraction. For instance, if $|A \pm A| \leq K|A|$, then

$$|nA - nA| \leq K^{2n}|A| \quad \text{for all } n \geq 1.$$

Thus sets that are approximately stable under a single additive operation remain approximately stable under every iterated one. This form of bounded expansion is a strong indicator of underlying structure; indeed, such behavior is characteristic of generalized arithmetic progressions and finite subgroup cosets. A useful discussion can be found on [TV06]

Acknowledgments

The author would like to thank Simon Rubenstein-Salzedo and the Euler Circle for hosting the Combinatorics class and providing useful feedback. The author would also like to thank his TA, Freya Edholm for providing very useful feedback and insightful discussions.

Bibliography

References

[Nat96] Melvyn B. Nathanson. *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, volume 165 of *Graduate Texts in Mathematics*. Springer, 1996.

[TV06] Terence Tao and Van Vu. *Additive Combinatorics*, volume 105 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, 2006.