Additive Combinatorics

Harry Armitage

January 23, 2021

Contents

1 Elementary Tools

Asymptotic notation: for functions f, g we will write $f = O(g)$ to mean there is a constant $c > 0$ such that, for large enough x, $|f(x)| \leq c|g(x)|$. Sometimes, we will write $f = O_h(g)$ if c depends on h. We will also sometimes write $f \ll g$ to mean $f = O(g)$ (or indeed $g \gg f$, or $f \ll_h g$). We will also write such things as $(x+h)^2 = x^2 + O_h(x)$. We will often write $\log X$ - it will typically be irrelevant which base, but it will be assumed that X is large.

All sets will be finite and nonempty unless otherwise specified. Usually, they will be subsets of some abelian group, denoted by G. If finite, we will write $N = |G|$, for instance $G = \mathbb{Z}/N\mathbb{Z}$ or $\mathbb{F}_p^n$ (where $N = p^n$). Much of what we do is valid for any abelian group, some of it only for finite groups, and some only for specific groups. Often, it can be generalised and sometimes not - e.g. $\mathbb{F}_p^n$ vs $\mathbb{Z}/N\mathbb{Z}$.

We will write $\mathbb{1}_A(x)$ for the indicator function on a subset $A \subseteq G$, i.e. $\mathbb{1}_A(x) = 1$ if $x \in A$, and 0 if not. We also define the convolution of functions $f, g : G \to G$ by

$$(f \star g)(x) = \sum_{y \in G} f(y)g(x-y) = \sum_{y+z=x} f(y)g(z)$$

We define the "difference convolution" by

$$(f \circ g)(x) = \sum_{z \in G} f(x+z)g(z) = \sum_{y-z=x} f(y)g(z)$$

We define an inner product on function $G \to \mathbb{C}$ by

$$\langle f, g \rangle = \sum_{x \in G} f(x)\overline{g(x)}$$

We have the trivial but useful adjoin property that

$$\langle f \star g, h \rangle = \langle f, h \circ \bar{g} \rangle$$

which follows from $x + y = z \iff x = z - y$.

2 Sum Sets

Given $A, B \subset G$ we define

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

Note that these are set operations, and don't necessarily follow any nice algebraic properties. For instance $(A + B) - B \neq A$, and in general is a much larger set.

We have trivial bounds $|A| \leq |A + B| \leq |A||B|$ - the first follows as, for fixed b, $\{a + b : a \in A\}$ is a set of size $|A|$ contained in $A + B$, and the second follows as $+$ is a surjection $A \times B \twoheadrightarrow A + B$.

When $A = B$, this surjection maps (a_1, a_2) and (a_2, a_1) to the same element, and hence $|A + A| \leq \frac{|A|(|A|+1)}{2} = \frac{1}{2}|A|^2 + O(|A|)$.

Are these trivial bounds sharp?

If A is a subgroup, then $|A + A| = |A|$ (or if A is a coset of a subgroup).

If $A = \{1, 2, 4, \ldots, 2^k\}$, then $|A + A| = \frac{|A|(|A|+1)}{2}$, as all pairwise sums are distinct. We can also have $A = \{1, 4, 16, \ldots, 2^{2k}\}$, $B = \{2, 8, \ldots, 2^{2k+1}\}$, and get $|A + B| = |A||B|$.

Lemma 2.1. $|A + A| \leq |A| \iff$ *A is a coset of a subgroup.*

Proof. Since both properties are invariant under translation, without loss of generality take $0 \in A$. So $A \subseteq A + A$, so since $|A + A| = |A|$, we must have $A = A + A$. Hence A is closed under addition. For any $a \in A$ there are $|A|$ many distinct translates $a + a'$ for $a' \in A$. By closure, these are all in A, and so one must be 0. Hence $a + a' = 0$, and we have inverses. □

In groups where there are many finite subgroups, we have many A such that $|A + A| = |A|$. What about in $\mathbb{Z}$? Here, there are no nontrivial finite subgroups, and so this result tells us that, if $|A| > 1$, then $|A + A| > |A|$.

Lemma 2.2. *If $A \subset \mathbb{Z}$ then $|A + A| \geq 2|A| - 1$. Equality holds if and only if A is an arithmetic progression (i.e. $|A + A| < 2|A| \implies$ A is an arithmetic progression).*

Proof. Suppose we order A like $\{a_1 < a_2 < \ldots a_n\}$. This induces an ordering on some elements of $A + A$:

$$2a_2 < a_1 + a_2 < a_1 + a_3 < \ldots < a_1 + a_n < a_2 + a_n < a_3 + a_n < \ldots < 2a_n$$

This gives $2n - 1$ distinct sums in $A + A$.

For the second part, it suffices to show that if equality holds then, for any $1 \leq i < n$ there is some $j > i$ with $a_j - a_i = a_2 - a_1$, as then $a_j = a_1 + (j - 1)(a_2 - a_1)$, and we have an arithmetic progression.

Consider for $2 \leq i < n$, the sum $a_2 + a_i \in A + A$. Since $|A + A| = 2n - 1$, the above ordered list is all of $A + A$, and so one of them is $a_2 + a_i$. Since $i < n$, $a_2 + a_i < a_j + a_n$ for all $2 \leq j \leq n$, and so $a_2 + a_i = a_1 + a_j$. □

What about if $A \subseteq \mathbb{F}_p$, for p a prime?

Lemma 2.3 (Cauchy-Davenport)**.** *If $A, B \subset \mathbb{F}_p$, then $|A + B| \geq \min(|A| + |B| - 1, p)$.*

Proof. We fix $B \subset \mathbb{F}_p$, and then prove the inequality for all $A \subset \mathbb{F}_p$ by induction on $|B|$.

When $|B| = 1$, this is trivial, since $|A + B| = |A| = \min(|A|, p)$.

Suppose that $|B| \geq 2$, so we have $b_1 \neq b_2$ distinct elements of B, and let $z = b_1 - b_2 \neq 0$. If $A + z \subset A$ then, for any fixed $a \in A$, we have $a + z \in A$, so $a + kz \in A$ for all $k \in \mathbb{N}$ by induction on k. Hence $A = \mathbb{F}_p$, as $\mathbb{F}_p$ is cyclic, and so we are done as $|A + B| = p = \min(|A| + |B| - 1, p)$.

Otherwise, $A + z \nsubseteq A$, and so there exists $a \in A$ such that $a + z \notin A$. Let $x = a - b_1$. Then $B + x$ contains some element not in A, namely $a + z = b_2 + x$, and some element in A, namely $a = b_1 + x$.

So $1 \leq |A \cap (B + x)| < |B|$. Now note that:

$$A + B \supseteq ((A - x) \cup B) + (A \cap (B + x))$$

To verify this, if $a' + b' \in RHS$, then either:

1. $a' \in A - x$. Then since $b' \in B + x$, $a' + b' \in A + B - x + x = A + B$.
2. $a' \in B$. Then since $b' \in A$, $a' + b' \in A + B$.

Hence if $A' = (A - x) \cup B$, $B' = A \cap (B + x)$, then $1 \leq |B'| < |B|$, $|A' + B'| \leq |A + B|$. By induction, $|A + B| \geq \min(|A'| + |B'| - 1, p)$.

But $|A'| = |(A-x) \cup B| = |A-x| + |B| - |(A-x) \cap B| = |A| + |B| - |B'|$. Hence $|A| + |B| = |A'| + |B'|$. □

This trick, transforming from $(A, B) \to ((A - x) \cup B, A \cap (B + x))$, is sometimes called the ***Dyson e-transform***.

We can characterise the case of equality as APs: if $|A + B| = |A| + |B| - 1$ then, aside from edge cases, A and B must be APs of the same step seize ("Vosper's Theorem").

We say that A has ***small doubling*** if $|A + A| \leq K|A|$ where K is "small" (e.g. $O(1)$). We've seen two examples of sets with small doubling:

- Cosets of subgroups ($K = 1$).
- Arithmetic progressions ($K = 2 - \frac{1}{|A|} = 2 + O(1)$).

There are two ways to generate new sets with small doubling from old.

1. Pass to a large subset. If $|A + A| \leq K|A|$ and $X \subset A$, then $|X + X| \leq |A + A| \leq \left(K\frac{|A|}{|X|}\right)|X|$. If $|X| \geq K^{-O(1)}|A|$, then A has doubling K implies X has doubling at most $K^{O(1)}$.
2. Pass to a sumset. If $|A + A| \leq K|A|$ and $X = A + Y$, then $|X + X| \leq |A + A + Y + Y| \leq |Y|^2|A + A| \leq (K|Y|^2)|X|$. So if A has doubling K and $X = A + Y$ where $|Y| \leq K^{O(1)}$, then X has doubling $\leq K^{O(1)}$. In fact it suffices if $|Y + Y| \leq K^{O(1)}|Y|$ and $|X| \geq K^{-O(1)}|A||Y|$.

This accounts for all sets with small doubling. That is, if $|A + A| \leq 100|A|$, then A is obtained from a coset or AP via these two operations. We'll state this more precisely and prove it later on.

3 Sumset Calculus

How are the sizes of sumsets related to each other?

Lemma 3.1 (Ruzsa's Triangle Inequality)**.** *For any sets A, B, C, $|A + B| \leq \frac{|A+C||B-C|}{|C|}$.*

Proof. For each $x = A + B$, fix an arbitrary representation $x = a_x + b_x$. Consider the map $C \times (A + B) \to (A + C) \times (B - C)$ given by $(c, x) \mapsto (c + a_x, b_x - c)$. This is clearly well defined - to finish the proof we will show that it is injective.

Note that we can recover x from the image of (c, x) by noting $(c + a_x) + (b_x - c) = a_x + b_x = x$. Then we can also recover c by subtracting a_x from $c + a_x$, and hence this map is injective. □

What about iterated sumsets? We write kA for the k-fold sumset of A, i.e. the set of all sums $a_1 + \ldots + a_k$ where $a_i \in A$.

Note that $|A| \leq |kA| \leq |A|^k$. This does not mean A dilated by k!

If $|A$ is small, we might want to know whether $|A + A|$ being small implies that $|kA|$ are also relatively small? The answer turns out to be yes! This is known as Plünnecke's inequality, which says that if $|A+A| \leq K|A|$, then $|kA| \leq K^k|A|$. The original proof by Plünnecke is graph-theoretic - it can be found in Tao & Vu. More recently, Petridis has found an alternative proof which is presented here.