Arithmetic Combinatorics

Vincent Tran

March 20, 2024

1 3/19 - Elementary Methods

1.1 Inverse Theorems

We will look at sum sets, product sets, and a few times quotient sets.

The context for this will be G, an abelian group. We are interested in $\mathbb{Z}, \mathbb{Z}^d, \mathbb{R}^d, \mathbb{Z}_p := \mathbb{Z}/p\mathbb{Z}, \mathbb{Z}_2^n$. Let A, B, C be finite subsets of G. In addition, all sets will be non-empty.

Definition 1. Minkowski Sum

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

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

Clearly $A + B$ is associative and commutative.

Similarly,

$$nA := A + \cdots + A$$

n times.

Property 1. $nA - mA \neq (n - m)A$ in general, i.e. the Minkowski sum doesn't distribute.

Question 1. When is $A + A$ small?

Trivially, we have

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

We are looking for when $|A + A|$ is close to $|A|$.

Direct Problem: How small can $|A + A|$ be?

Inverse: For which A is $|A + A|$ small?

Example 1. Let $G = \mathbb{Z}$, $A = [0, n-1]$. Then $A + A = [0, 2n-2] \implies |A + A| = 2|A| - 1$.

By using affine transformations $\phi : \mathbb{Z} \to \mathbb{Z}$ defined by $\phi(x) = ax+b$, we have that $b, b+r, \ldots, b+(n-1)r$ is a value for $|A|$ s.t. $|A + A| = 2|A| - 1$.

Definition 2. Generalized Arithmetic Progressions: They are of the form $b + r_1x_1 + \cdots + r_dx_d$ where $x_i \in [0, n_i - 1]$, i.e. affinely transformed sums of A_i.

Theorem 2. $\forall A \subseteq \mathbb{Z} |A + A| \geq 2|A| - 1$.

Proof. Proof 1: Induction. Let $A = \{a_1 < a_2 < \cdots < a_n\}$ and define $A' = A \setminus \{a_n\}$. By the induction hypothesis, $|A' + A'| \geq 2|A'| - 1 = 2n - 3$. By noticing that $2a_n, a_n + a_{n-1}$ are elements not in $A' + A'$ but are in $A + A$, we have that $|A + A| \geq 2|A| - 1$.

Proof 2: Go bi. We can generalize this theorem to more variables: $|A + B| \geq |A| + |B| - 1$, in which case induction is ever simpler as only the largest element is needed.

Proof 3: Take two sets A, B, represent them as cicles with elements in descending order in them. Take $|B|$ picks in A and $|A|$ picks in B. Draw a bar connecting a pick in A to a pick in B. Do this for all picks in B. Then do this for all picks in A (above two steps). We then have found $|A| + |B| - 1$ distinct elements (?). $\square$

Theorem 3 (Cauchy-Davenport)**.** For $G = \mathbb{Z}_p$, $|A + B| \geq \min(|A| + |B| - 1, p)$.

Definition 3 (e-transform). Fix an element $e \in A - B$. Then

$$A_{(e)} ::= A \cup (B + e)$$
$$B_{(e)} ::= B \cap (A - e).$$

See **??**

Lemma 4. 1. $|A_{(e)}| + |B_{(e)}| = |A| + |B|$

2. $|A_{(e)} \geq |A|$

3. $A_{(e)} + B_{(e)} \subseteq A + B$

Proof. For a), clearly $A_{(e)}$ contains $|A|$ elements plus some. Then for any element $b \in B$, $b + e \in A$ or $\notin A$.

If $b + e \in A$, then $b \in A - e \implies b \in B_{(e)}$.

If $b + e \notin A$, then obviously $b + e \in A_{(e)}$ and not in A. Thus $|A_{(e)}| + |B_{(e)}| = |A| + |B|$.

b) is truly trivial.

c) If we take $a \in A_{(e)}$ and it falls in A, then we are done as $B_{(e)} \subseteq B$. So the only hard case is when $a \in B + e \setminus A$. By definition, $A_{(e)} + B_{(e)}$ consists of $a + b, b \in B_{(e)}$ and hence $b \in A \setminus e$. Thus $b = a' - e \implies a + b = a + a' - e = b' + a'$ for $b' \in B$ since $a \in B + e$. □

Proof: Cauchy-Davenport. If $|B| = 1$ then we are trivially done. We then use induction on the size of B and the e-transform to see that $B_{(e)} = B \forall e \in A \setminus B$. Hence $\forall e \in A - B$, $B + e \subseteq A \implies B + A - B \subseteq A$, i.e. $A + (B - B) \subseteq A$.

As $|B| \geq 2$, we can let $d = b_1 - b_2$ and see that $A + d = A + (B - B) = A$ and the same is true for all multiples of d (equality is true since $|A| \leq |A + (B - B)|$). Since $A = \mathbb{Z}_p$ and we are done (this is the min). □

Theorem 5 (Vosper)**.** For $A, B \subseteq \mathbb{Z}$ and $|A + B| = |A| + |B| - 1$, then A, B are a.p. (arithmetic progressions) with the same step.

Proof. (Proof from Tao, not class)

First we handle three cases:

A or B are arithmetic progressions: WLOG say A is. Then $A = \{a, a + v, \ldots, a + nv\}$. So then $|B| + n = |A| + |B| - 1 = |A + B|$ by hypothesis.

WLOG let $A = \{a, a + v, \ldots, a + (n - 1)v\} + \{0, v\}$ with v positive. So $|A + B| = |\{a, \ldots, a + (n - 1)v\} + B + \{0, v\}| \geq n - 1 + |B + \{0, v\}|$ by Cauchy-Davenport. By Cauchy-Davenport again, we have that $|B + \{0, v\}| \geq |B| + 1$ and from above ($|B| + n \geq n - 1 + |B + \{0, v\}|$) we have that $|B| + 1 = |B + \{0, v\}|$.

The largest element of B (say b_n) plus v isn't in B, so this is the only element of $B + \{0, v\}$ that isn't in B, giving us that $B \setminus \{b_n\} + v \subseteq B$. Hence B is an arithmetic progression.

If $|A + B|$ is an arithmetic progression, then let $C = -(\mathbb{Z}_p \setminus (A + B))$. Notice that $|C| = p - |A + B| = p + 1 - |A| - |B|$. It follows that C is an arithmetic progression with the same step because the step is an additive generator in $\mathbb{Z}_p$. As such if we continue out the progression and reversed it (by negating), we would get the later half that isn't in $-(A + B)$.

Next we can see that $C + B \subseteq (\mathbb{Z}_p \setminus A)$ because if $C + B$ intersected $-A$ at say $-a = c + b$, then $-(a + b)$ would be in $-(A + B)$ but also C, a contradiction. Hence $p - |A| \geq |C + B| \geq |C| + |B| - 1 = p - |A|$ by Cauchy-Davenport. So $|C + B| = p - |A| = |C| + |B| - 1$. By the work before, this gives us that B is an arithmetic progression of the same step as C. Similarly for A.

Now to prove this for when none of them are arithmetic progressions. We use induction. For $|B| = 2$, we have that B is an arithmetic progression and we are done.

$|B| > 2$: We have two cases:

$1 < |B_{(e)}| < |B|$ for some $e \in A - B$: By the lemma and starting hypothesis, $|A_{(e)} + B_{(e)}| = |A_{(e)}| + |B_{(e)}| - 1$ and by the inductive hypothesis $B_{(e)}$ and $A_{(e)}$ are arithmetic progressions with the same step. Hence $A + B = A_{(e)} + B_{(e)}$ is an arithmetic progression, reducing us back into the previous case.

$|B_{(e)}| = |B|$ or $1 \, \forall e \in A - B$. Let $E \subseteq A - B$ be the set of e s.t. $|B_{(e)}| = |B|$. Then $B + E \subseteq A$ and by Cauchy-Davenport, we have that $|B| + |E| - 1 \leq |A| \iff |E| \leq |A| - |B| + 1$. Since $|A - B| \geq |A| + |B| - 1$

by Cauchy-Davenport, by pidgeonhole principle there are at least $2|B|-2$ values of e. By pidgeonhole again, we have e, e' s.t. $B_{(e)} = B_{(e')} = \{b\}$.

Since $|A+B| = |A| + |B| - 1$, $A + B = A_{(e)} + b = A_{(e')} + b$ and thus $A \cup (B+e) = A \cup (B+e')$. As $|B_{(e)}| = 1$, $A \cap B + e = b + e$ and similarly for e', $B + e$ and $B + e'$ differ by at most one element (use the fact that $A \cup (B+e) = A \cup (B+e')$). Hence B is an arithmetic sequence of $e' - e$. $\square$