Arithmetic Combinatorics

Vincent Tran

March 27, 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 **??**

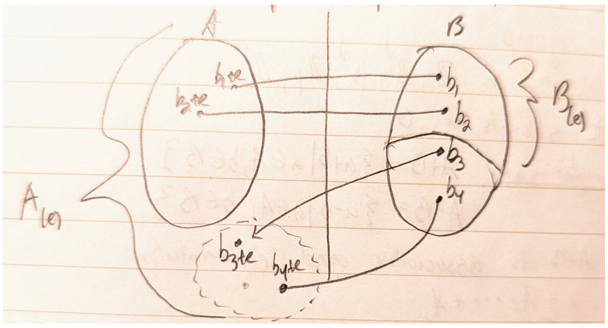

Figure 1: The e-transform

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 $e'-e$. $\square$

2 3/21/24

Let $A \subseteq G$ be non-empty and finite.

Definition 4. $\mathrm{Sym}_1(A) \coloneqq \{x | x + A = A\}$. This is clearly a subgroup of G.

Theorem 6 (Kneser (53))**.** Let $A, B \subseteq G, G = \mathrm{Sym}_1(A+B)$. Then $|A+B| \geq |A+H| + |B+H| - |H|$.

Proof. Proof 1: Induction on 4 parameters.

Proof 2: For $\mathbb{Z}$, $|H| = 1$ because H has to be 0 by ordering A. Then the statement is $|A+B| \geq |A|+|B|-1$, done by Cauchy-Davenport.

For $\mathbb{Z}_p$, $H = 0$ or $\mathbb{Z}_p$ as the only subgroups of $\mathbb{Z}_p$. This is trivial. $\square$

At this point, we know a lot about when $|A| = n, |A+A| = 2n-1$ (by Vosper's), and now we can get information about $|A+A| = 2n-1+b, b \leq n-1$:

Theorem 7 (Freiman's $3k-3$)**.** For $A \subseteq \mathbb{Z}$ and $|A+A| = 2n-1+b$ for $b \leq n-1$, then A is a subset of an $n+b$ term arithmetic progression.

Example 2. We can generate examples by letting $A = \{0, \ldots, n-2, n-1+b\} \subset \{0, 1, \ldots, n+b\}$. Notice that $|A+A| = 2n+b-1$ because of three cases:

$$\begin{cases} [0, n-2] + [0, n-2] = [0, 2n-2] \\ [0, n-2] + \{n-1+b\} = [2n-2, 2n-2+b] \\ \{n-1+b\} + \{n-1+b\} = \{2n-2+2b\} \end{cases}.$$

This is $2n-1+b$ elements.

2.1 Digression into Some Combinatorics

This is a treasured result in combinatorics, and will use a similar technique as the e-transform.

Definition 5. $[n] \coloneqq \{1, \ldots, n\}$.

Definition 6. $\Delta \subseteq \mathcal{P}([n])$ is an **ideal** if $\forall F \in \Delta, G \subseteq F \implies G \in \Delta$.

Definition 7.

$$\binom{[n]}{k} \coloneqq \{F \subseteq [n] | |F| = k\}.$$

Definition 8. The **shadow** of $\mathcal{F} = \Delta \cap \binom{[n]}{k}$ to be $\partial\mathcal{F} := \{G \in \binom{[n]}{k} | \exists F \in \mathcal{F}, |F \setminus G| = 1\}$. Intuitively, the shadow compacts sets, much like the e-transform.

Theorem 8 (Kruskal-Katoma). Let $|\mathcal{F}| = m$ and find x s.t. $m = \binom{x}{k}$. Then

$$|\partial\mathcal{F}| \geq \binom{x}{k-1}.$$

An equivalent statement is that given $\{i_1 < i_2 < \cdots < i_k\} \in \binom{[n]}{k}$, we can view it as the string $[i_k, \ldots, i_1]$ and order the $\binom{[n]}{k}$ lexicographically. Then let $\mathcal{R}(m,k)$ be the m smallest elements in this ordering. The equivalent statement is that $|\partial(\mathcal{F})| \geq |\partial(\mathcal{R}(m,k))|$.

Definition 9.

$$S_{ij} : \mathcal{P}([n]) \longrightarrow \mathcal{P}([n])$$
$$S_{ij}(A) = \begin{cases} A \setminus \{j\} \cup \{i\} & \text{if } j \in A \text{ and } i \notin A \\ A & \text{else} \end{cases}.$$

$$S_{ij} : \mathcal{P}(\mathcal{P}([n])) \longrightarrow \mathcal{P}(\mathcal{P}([n]))$$
$$S_{ij}(\mathcal{H}) := \{S_{ij}(H), \forall i, j\}.$$

Intuitively, this is trying to get G through the "wall" using S_{ij}. This is analogous to the e-transform from before.

Lemma 9. For $\mathcal{F} \subseteq \binom{[n]}{k}$ and $\partial(S_{ij}(\mathcal{F})) \subseteq S_{ij}(\partial\mathcal{F})$, then $|\partial(S_{ij}\mathcal{F})| \leq |S_{ij}(\partial(\mathcal{F}))|$.

Proof. For $G \in \partial(S_{ij}(\mathcal{F}))$, we have that $G + \ell \in S_{ij}(\mathcal{F})$ for some ℓ. If this is true up to $k-1$, then when $G \cup i \setminus j \in \partial(\mathcal{F})$, then .we can just swap i, j and find that $G \in S_{ij}(\partial\mathcal{F})$. Let G' be a preimage of $G + \ell$.

Case one is that $G' + \ell \in \mathcal{F}$. The only case is $G \cup i \setminus j \notin \partial(\mathcal{F})$. If $i = \ell$, then $G' \cup \ell - j \in \partial(\mathcal{F})$, a contradiction.

If $i \neq \ell$: $G' \cup i \notin \mathcal{F}$ (otherwise $G' \in \partial\mathcal{F}$, completing the proof), which implies $G' \cup i \setminus j \setminus \ell \notin \mathcal{F}$ because otherwise $G' \cup i \setminus j \in \partial(\mathcal{F})$ which completes it with a swap. But $G' + \ell \in \mathcal{F} \implies$ we can shift and have $G \cup \ell = G' \setminus j \cup i \cup \ell \in S_{ij}(\mathcal{F})$. This then implies that $G \setminus j \cup i \in \partial(S_{ij}(F)) \implies G \in S_{ij}(\partial(S_{ij}(\mathcal{F})))$.

If $G' \cup \ell \notin \mathcal{F}$: Then $G \cup \ell \in S_{ij}(\mathcal{F}) \implies G \cup \ell \cup j \setminus i \in F$. $\square$

Proof. (Krushkal-Katoma) By the Lemma, we can assume no more shifts can be done. However, this doesn't trivialize the problem like the e-transform case: $\{\{1,2\},\{1,3\},\{1,4\}\}$ and $\{\{1,2\},\{2,3\},\{1,3\}\}$ are both extremal and we can't shift in.

Define $\mathcal{F}(1) = \{F | 1 \in F\}, F(0) = \{F | 1 \notin F\}$. Assume this is true for smaller sets. We just need to show that $|\partial(F(0))| \leq |F(1)|$.

Take $G \in \partial(F(0))$. Then S_{e_1} doesn't affect G by assumption, so $G \cup \{1\} \in F(1)$ for an arbitrary element $e \in G$. $\square$

3 Doubling Constant

Definition 10.

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

We have dealt with $\delta[A] \leq 2$, the $3k-3$ theorem gives us $\delta[A] \leq 3$. In general, we need generalized arithmetic progressions.

This is Freiman's Theorem and the Polynomial Freiman-Rusza conjecture, which was solved recently in characteristic 2 by Gowers, Green, Manners, Tao.

How to construct sets with small doubling constants?

For A an arithmetic progression, we are done. Define A, B as independent if $|A+B| = |A| \cdot |B|$. Then

$$\delta[A+B] = \frac{|A+B+A+B|}{|A+B|} = \frac{|(A+A)+(B+B)|}{|A| \cdot |B|} \leq \frac{|A+A|}{|A|} \cdot \frac{|B+B|}{|B|} \leq \delta[A] \cdot \delta[B].$$

4 3/26/24

Now we look to generalized arithmetic progressions (gap) of rank d: $A_1 + \cdots + A_d$ with A_i being ap.

Definition 11. A gap is **proper** if $|A_1 + \cdots + A_d| = |A_1| \cdot |A_2| \cdots |A_d|$

P is a proper ap $\implies \delta[P] \leq 2^d$ with $d = \text{rank}(P)$.
Now suppose $B \subseteq A$ and let $\mu = \frac{|B|}{|A|}$. Then $\delta[B] = \frac{|B+B|}{|B|} \leq \frac{|A+A|}{|B|} = \mu^{-1}\delta[A]$.
There are two cases for the group:

- Torsion Free (e.g. $\mathbb{Z}, \mathbb{Z}_p^d, \mathbb{R}^d$)
- Forsion (e.g. $\mathbb{Z}_2^n$)

Theorem 10 (Freiman (Torsion Free))**.** Fix an integer k. Then $\exists$ constants d, μ (depending on k only) s.t. $\forall A \subseteq \mathbb{Z}$ and $\delta[A] = k$, then there exists a propery gap P s.t. $\text{rank}(P) \leq d$, $A \subseteq P$, and $\frac{|P|}{|A|} \leq \mu^{-1}$.

Corollary 1. $\delta[A] \leq \mu^{-1}2^d$

The point of this is that $\exists \mu^{-1}, d \leq k^{o(1)}$.
We really want d to be tight to k.
But we can always find a crazy set $|X| = k$ and $\delta[X] = k$ s.t. d has to be k.

Conjecture 11 (Polynomial Freiman-Rusza Conjecture)**.** For $A \subseteq P + X$ with $|X| \leq k^{O(1)}$, $\text{rank}(A) \leq O(\log K)$.

Theorem 12 (Gowers, Green, Manners, Tao (23))**.** $\forall A \subseteq \mathbb{Z}_2^n$ with $\delta[A] = k$, $\exists H \subseteq \mathbb{Z}_2^n$ s.t. $\exists X(|X| \leq k^{O(1)})$ s.t. $A \subseteq H + X$, then $|H| \leq k^{O(1)}|A|$.

Some History:

1. Freiman's Proof (didn't draw much attention)
2. Rusza's Proof which brought in analysis $\rightarrow$ more attention
3. Sanders proved quasi-polynomial Freiman Rusza
4. Recent GGMT polynomial FR conjection in characteristic 2 (promised in general as well)

In this class 1, 2, and 4 will be discussed.
Let $A \subseteq \mathbb{R}^d$ (under addition). Freiman's can still apply here.

Lemma 13 (Freiman Dimension Reduction Lemma)**.** Let $k = \delta[A], d = \text{rk}(\text{Span}(A))$. Then $|A + A| \geq (d+1)|A| - d(d+1)/2 \implies \delta[A] \geq d+1, d \leq k-1$.
This is obviously false in char $\neq 0$.

Proof. We do induction on $|A|$. This is easily true for $|A| = 1$.

Then for $|A| > 1$, take the convex hull of A. Take a point $a \in A$. So $A' = A \setminus \{a\} \implies |A' + A'| \geq (d'+1)|A'| - d'(d'+1)/2$ by induction hypothesis.

If $\text{rk}(A') = d$, then $a \in A$ has d neighbors, $a_1, \ldots, a_d$. The midpoints $\frac{a+a_1}{2}, \ldots, \frac{a+a_d}{2}$ are not in A' because otherwise $a \in A'$, a contradiction of the number of neighbors (?). Hence $a+a_1, \ldots, a+a_d \notin A'+A'$ (separate them by a hyperplane, Minkowski sum of a convex set is convex).

So $|A+A| \geq |A'+A'| + d + 1 \geq (d+1)(|A'|+1) - d(d+1)/2$, completing the induction in this case.

If $\text{rk}(A') = d-1$, then a is outside the $d-1$ dimensional hyperplane A' is in, which implies that $a + A', a + a \notin A' + A' \implies |A+A| = |A'+A'| + |A'| + 1$, which by induction once again completes the proof. □

We want $A \subseteq P$ s.t. A is dense in P. We can't find a gap in A, $A + A$, but strangely we can in $2A - 2A$.

Lemma 14 (Bogolubov)**.** $\forall A \subseteq \mathbb{Z}, \exists P \subseteq 2A - 2A$ s.t. P is a proper gap and dense in $2A - 2A$, i.e.

$$|P| \geq \frac{|2A - 2A|}{\exp(k^{O(1)})}.$$

Can apply for $k = |A|^{o(1)}$ as well.

Lemma 15 (Rusza Covering Lemma)**.** $\forall A, B \subseteq G$, $\exists X \subseteq B$ s.t.

1. $|X| \leq |A + B|/|A|$
2. So $B \subseteq A - A + X$.

See Figure 2.

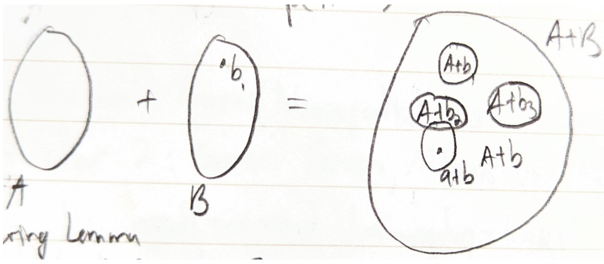

Figure 2: Rusza Covering Lemma

Proof. 1) is trivial. We are looking for the set $X = \{b_1, \ldots, b_a\}$ that has the maximal number of translates that are pairwise disjoint.

2) Fix an element $a + b \in A + B$. Then $A + b$ has to intersect an element $x \in X$ s.t. $A + x \cap A + b \neq \emptyset$. Hence there is $a_1 + b = a_2 + x \iff b = a_2 + x - a_1 \implies \forall b \in B, \exists x \in X$ s.t. $b \in A - A + X$. $\square$