Arithmetic Combinatorics

Vincent Tran

April 4, 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 $\mathbb{Z}, \mathbb{Z}^d, \mathbb{R}^d, \mathbb{Z}_p \coloneqq \mathbb{Z}/p\mathbb{Z}, \mathbb{Z}_2^n$. 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,

$$nA \coloneqq A + \cdots + A$$

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 (?). □

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

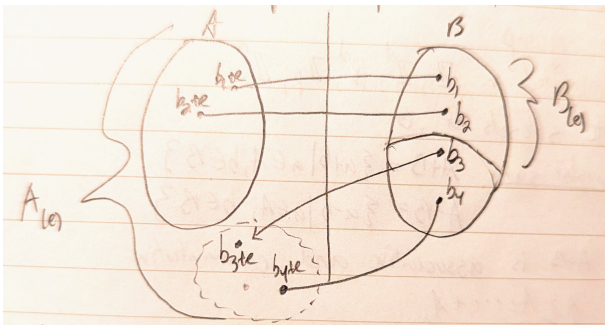

Figure 1: The e-transform

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 $e' - e$. □

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. □

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 $\partial\mathcal{F} \coloneqq \{G \in \binom{[n]}{k} | \exists F \in \mathcal{F}, |F \setminus G| = 1\}$. 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.

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

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

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 $G \cup \ell \in S_{ij}(\mathcal{F}) \implies G \cup \ell \cup j \setminus i \in F$. □

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 $e \in G$. □

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 $\to$ 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.

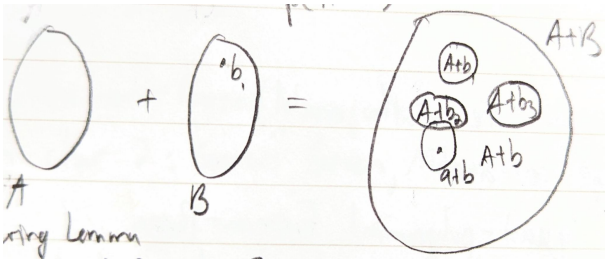

Figure 2: Rusza Covering Lemma

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. $b \in A - A + X$. □

5 3/28/24

Thus far we have been looking to cover A with a GAP, and now we are covering a GAP with $2A - 2A$.

First we prove Freiman:

Proof. Let $A = P$ and $B = 2A-2A$ in the Lemma 15 $\to X$ s.t. $|X| \leq \frac{|P+2A-2A|}{||P|}$. Because $P \subseteq 2A-2A$,

$$|X| \leq \frac{|P+2A-2A|}{|P|} \leq \frac{|4A-4A|}{|P|} \leq \frac{|4A-4A|}{|A|} \exp(k^{O(1)}.$$

Then $2A-2A \subseteq P-P+X$. WLOG, we can assume $0 \in A$ (shift). Hence $A \subseteq 2A-2A \subseteq P-P+X$.

So now all we need to do is to bound $\frac{|4A-4A|}{|A|}$. In the non-commutative case, this can be very large. In the torsion case, this can't be bounded, by letting $P = \mathbb{Z}_p$, which leads to $P - P$ being a gap, but may not be proper. To fix this, we introduce a new tool: □

5.1 Properization

Theorem 16. For any gap P of rank d, there exists a proper gap of rank d s.t. $P \subseteq Q$ and $|Q| \leq |P| \cdot d^{O(d^3)}$.

Inuitively, $\text{rank}(P) \leq K^{O(1)}$, roughly K.

5.2 Plünecke-Rusza Inequalities

Theorem 17. $A, B \subseteq G$ s.t. $|A+B| = K|A|$. Then $|\pm B \pm B \pm B \pm \ldots \pm B|$ (h times) $\leq K^h|A|$.

Corollary 2. Suppose $B = A$. Then $k = \delta[A]$. The inequality then becomes

$$|kA - \ell A| \leq K^{k+\ell}|A|.$$

The above Corollary then gives an upperbound on $\frac{|4A-4A|}{|A|}$, proving Freidman's Theorem.

Now let $\sigma[A] = \frac{|A-A|}{|A|}$.

Corollary 3. Then with $k = l = 1$, $\sigma[A] \leq \delta[A]^2$.

Now this result is going to be very useful, especially in its generalized form for Gower's Theorem.

Lemma 18 (Rusza Triangle Inequality)**.** Let G be an ablian group.

Combinatorial Form:

$$|A - C| \leq \frac{|A - B| \cdot |B - C|}{|B|}.$$

Proof. We WTS that $|B| \cdot |A - C| \leq |A - B| \cdot |B - C|$. We prove it by finding an injective function $B \times (A - C) \rightarrowtail (A - B) \times (B - C)$

$\forall x \in A - C$ (arbitrary but fixed), represent it as $x = a_x - c_x, a_x \in A, c_x \in C$. Then map

$$(b, x) \mapsto (a_x - b, b - c_x).$$

Then say you're given $(a_x - b, b - c_x)$. Then you can recover a unique $x = a_x - b + b - c_x$ and from there recover a_x, c_x. This then gives b. □

Lemma 19 (Alternative Statement Rusza Triangle Inequality)**.**

$$\frac{|A - C|}{|A|^{\frac{1}{2}}|C|^{\frac{1}{2}}} \leq \frac{|A - B|}{|A|^{\frac{1}{2}}|B|^{\frac{1}{2}}} \cdot \frac{|B - C|}{|B|^{\frac{1}{2}}|C|^{\frac{1}{2}}}.$$

Definition 12 (Rusza's Distance)**.**

$$\boldsymbol{d(A, C)} = \ln \frac{|A - C|}{|A|^{\frac{1}{2}}|C|^{\frac{1}{2}}}.$$

We can check that it is almost a metric (semimetric). Since $|A - C| \geq \max(|A|, |C|)$, the fraction in the RHS is at least 1, showing that the RHS is non-negative. Clearly it is symmetric. By the Rusza Triangle Inequality, we have $d(A, C) \leq d(A, B) + d(B, C)$. But it violates positive definitiness (take A, C part of the same subgroup).

From this we have that $d(A, -A) = \ln \delta[A]$ and that $d(A, A) = \ln \sigma[A]$. Hence $\ln \sigma = d(A, A) \leq d(A, -A) + d(A, -A) = 2 \ln \delta[A]$

Now we return to the Plünecke-Rusza Inequalities **??**.

Theorem 20. With $K = \frac{|A+B|}{|A|}, |\pm B \pm B \pm \cdots \pm B| \leq K^h|A|$.

Big Names: Petridis, Julia Walls, Jim Gowers

It began as a very complicated proof in 2016, but it was seriously streamlined.

Proof. (Petridis')

Consider a simple case: We prove that if $|A + B| \leq K|A|$, then $|hB| \leq K^h|A|$.

If we decrease the RHS, then this inequality becomes stricter. So we can let A be the smallest such set. Note that we have B fixed the entire time.

WLOG, $\forall A' \subset A, |A' + B| \geq K|A'|$.

Lemma 21. Under all these assumptions, $|A + B + C| \leq K|A + C|$ for an arbitrary C.

This implies this case because $|hB| \leq |A + hB| \leq K|A + (h - 1)B| \leq K^2|A + (h - 2)B| \leq \cdots$ (let $C = (h - 1)B$ in the lemma). This leads to $|hB| \leq K^{h-1}|A + B| \leq K^h|A|$ (definition of K).

Proof. (Lemma)

We do induction on C. Suppose it is true up to $|C|$ and we have $C' = C \cup \{x\}$. Then $|A + B + C| \leq K|A + C|$. We want $|A + B + C'| \leq K|A + C'|$.

We have $A+B+C' \subseteq (A+B+C) \cup (A+B+\{x\}), A+C' \subseteq (A+C) \cup (A+x)$ by definition. Suppose for a second that this (RHS) was a disjoint unions. Then because $|A+B+C| \leq K|A+C|, |A+B+x| \leq |A+x|$, completing the proof.

By PIE (principle of inclusion exclusion), we have a W s.t.

$$W + x = (A + C) \cap (A + x).$$

This is a proper subset, because otherwise we are done (nothing else is added on both sides, i.e. $A+C' = (A+C)\cup(A+x) = A+x = A+C \implies |A+B+C'| \leq |A+B+C|+|A+B+x| \leq K|A+C| \leq K|A+C'|$). So $W = (A+C-x)\cap A$.

Next $(A+B+C)\cap(A+B+x) \supseteq W+x+B$ (we are supposing the LHS is small). By more PIE, we have that all we need to prove is that $|W+x+B| \geq K|W+x|$ and that $|W+B| \geq K|W|, W \subsetneq A$.

Then double induction on A and then top down. □

□

We are still focused on Lemma 14, i.e. that $\exists P \subseteq 2A-2A$ s.t. $|P| \geq |A|\exp(-K^{O(1)})$.

The reason this is better than what we have before is that we can prove this for

1. $A' \subseteq A$, $\frac{|A|}{|A'|\leq \exp(K^{O(1)})}$), Lemma 14 for $A' \implies$ BR lemma for A
2. BR Lemma is invariant under Freiman isomorphisms of order 8

Definition 13. Let G, H be abelian groups, $A \subseteq G, B \subseteq H$. A **Freiman Homomorphism** of order k is defined by

$$(G, A) \xrightarrow{\phi} (H, B)$$

s.t. $\phi : A \to B$ is a bijection between A, B s.t.

$$a_1 + \ldots a_k = a_1' + \ldots a_k' \implies \phi(a_1) + \ldots + \phi(a_k) = \phi(a_1') + \ldots + \phi(a_k').$$

An example is an injective homomorphism that maps $a_i \mapsto a_i'$. They are almost as good as homomorphisms, and they are indistinguishable up to k-tuples.

Definition 14. A **Freiman isomorphism** is a Freiman homorphism whose inverse is a Freiman homomorphism.

Proposition 22. If we have a Freiman isomorphism of order 8: $(G, A) \to (H, B)$, then BR lemma for A is equivalent to BR lemma for B.

Proof. Clearly we have a Freiman homomorphism $(G, 2A-2A) \to (H, 2B-2B)$ of order 2. We have injectivity is because ϕ is bijective and well-defined. Now suppose we have a proper gap $P \subseteq 2A-2A$. Then $\phi(P)$ is a proper gap or subgroup of H.

For $d = 2$, the gap is just a grid, and this grid is then translated into a wiggly grid. But we want it to be a full grid, and we have this by generating the right grid by the images of the terms on the LHS.

We have the relation that $a_1 + a_4 = a_2 + a_3 \to b_1 + b_4 = b_2 + b_3$. As another example, $a_1 + a_5 = 2a_2 \to b_1 + b_5 = 2b_2$. Simply repeat this.

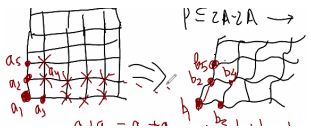

Figure 3: Grid with $d = 2$

We will complete this proof on Tuesday. □

Next we will use basic Fourier analysis to reduce BR Lemma in $\mathbb{Z}$ to BR Lemma in $\mathbb{Z}_N$ where $N > 16|8A-8A|$. By Chebyshev's theorem (?), we have $p \leq K^{O(1)}$ (also use Rusza Triangle inequality 17).

Proof. We have $k = 8$ and $(\mathbb{Z}, A) \xrightarrow{k} (\mathbb{Z}_N, B)$.

Lemma 23. $\exists A' \subseteq A$ with $|A'| \geq \frac{|A|}{k}$ and Freiman isomorphism between $(\mathbb{Z}, A') \xrightarrow{\phi} (\mathbb{Z}_N, B)$ where N has the same restriction.

Proof. Outline of proof: The isomorphism is constructed with a huge p. We will find one

$$(\mathbb{Z}, A') \xrightarrow{\phi} (\mathbb{Z}_p, L) \xrightarrow{\psi} (\mathbb{Z}_N, B).$$

THen ϕ is the quotient map, and ψ is the remainder function. It takes $a \in \mathbb{Z}_p^\times$, think about it as an integer, and $\psi(a) = a \pmod N$. □

□

6 4/2/24

The Freiman isomorphism definition is equivalent to

Definition 15. A **Freiman isomorphism** of order k is a map ϕ from $A \subseteq G$ to $B \subseteq H$ s.t.

$$\phi(a_1) + \phi(a_2) + \cdots + \phi(a_k) = \phi(a_1') + \phi(a_2') + \cdots + \phi(a_k') \iff a_1 + a_2 + \cdots + a_k = a_1' + a_2' + \cdots + a_k'$$

and $|A| = |B|$.

We flesh out the proof of the lemma from before:

Lemma 24. $\forall A \subseteq \mathbb{Z}$ and $N \geq 2k|kA - kA|, \exists A' \subseteq A$ s.t. $|A'| \geq |A|/k$ and Freiman isomorphism $(\mathbb{Z}, A') \to (\mathbb{Z}, B)$ of order k ($B \subseteq \mathbb{Z}_N$).

Proof. We construct the maps

$$(\mathbb{Z}, A) \xrightarrow{\phi} (\mathbb{Z}_p, L) \to (\mathbb{Z}_n, B)$$

with p a sufficiently large prime. We find another ϕ_λ s.t. it is also a Freiman isomorphism. Pick $\lambda \in \mathbb{Z}_p^\times$ (it remains flexible; random in a sense). Then we can let $\phi_\lambda \coloneqq \lambda \circ \phi$ with ϕ being the quotient map $\mathbb{Z} \to \mathbb{Z}_p$.

Split up $\mathbb{Z}_p$ into k roughly equal intervals, where $\mathbb{Z}_p$ is represented by $\{0, 1, \ldots, p-1\}$. Pick the interval containing the most points in λA, call it $\lambda A'$. Then

$$b_1 + \cdots + b_k = b_1' + \cdots + b_k' \in \mathbb{Z},\ b_i, b_i' \in \lambda A'$$

iff

$$b_1 + \cdots + b_k \equiv b_1' + \cdots + b_k' \pmod p.$$

Then we can translate this by intervals to extend $\lambda A'$ to a set of size p with this property.

Next let $\iota : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ (exists because p is obscenely large). We WTS that

$$\iota(b_1) + \cdots + \iota(b_k) = \iota(b_1') + \iota(b_k') \pmod N \iff b_1 + \cdots + b_k \equiv b_1' + \cdots + b_k' \pmod N.$$

The only potential issue is if the LHS doesn't imply the RHS. Now consider the expression

$$b_1 + \cdots + b_k - b_1' - b_2' - \cdots - b_k' \pmod N.$$

This is in $[-kp, kp]$ because $b_i, b_i' \in L$. Notice that there are $2kp/N$ "bad" intervals that are 0 mod N and satisfy the iff in $\mathbb{Z}_p$.

Finally, define

$$\Delta \coloneqq \{a_1 + \cdots + a_k - a_1' - \cdots a_k' \neq 0 | a_i, a_i' \in A\}.$$

Clearly $\Delta \subseteq \mathbb{Z}_p$ and $|\Delta| = |kA - kA|$. Consider $\lambda\Delta$. The λ we picked from before was flexible, so we can use a probabilitic argument to pick a lambda retroactively that avoids all the bad points. The probability that Δ has a bad point is $|\Delta|/p \cdot 2kp/N = |\Delta| \cdots 2k/N$, which is less than 1 by hypothesis. □

6.1 Good Model (Dense)

Let $k = 8$. A good model gives us BR-Lemma in specific cases:

Our goal is to prove it true for $A \subseteq \mathbb{Z}_N$ ($\mathbb{Z}_2^N$) [1]. It's dense because

$$|kA - kA| < K^k|A|, \mu = \frac{|A'|}{|G|}.$$

Now we go on a tangent about the discrete Fourier transform.

[1] I don't know what this means, but it was in my notes

6.2 Discrete Fourier Analysis (on Abelian Groups)

6.2.1 Pontryagin Duality

Fix a locally compact abelian group (topological group whose closure of neighborhoods are compact), e.g. $\mathbb{Z}$ is a discrete one.

Definition 16.

$$\boldsymbol{T} = \mathbb{R}/\mathbb{Z} = \text{ the circle.}$$

Definition 17. For a group G,

$$\hat{\boldsymbol{G}} = \mathrm{Hom}(G, T) \text{ (continuous).}$$

Theorem 25 (Pontryagin Duality)**.**

$$\hat{\hat{G}} = G_i$$

where G_i is a separated component of G.

Example 3. $\hat{\mathbb{Z}} = T$.

Example 4. $\hat{T} = \mathbb{Z}$ because $\exp(i\theta) \to \exp(i\alpha\theta)$ are the morphisms, but not all α since exp has the periodic property. So we only want $\alpha = n \in \mathbb{Z}$.

Definition 18. Let G be an abelian finite group. The **characters** of G are elements of $\hat{G}$, which are all group homomorphisms because we are using the discrete topology.

For finite G, $\hat{G} = G$, but this isn't canonical (depends on basis). As such it isn't very useful.

To find $\hat{\mathbb{Z}_N}$, we send $1 \mapsto \xi_N$, and call this map $\chi(\xi)$. In the particular case of $\mathbb{Z}_2^N$, (fix standard basis of e_i), each $\chi_i : e_i \mapsto 1$ or -1. So here, $S = \{i | \chi(e_i) = -1\}$ implies that

$$\chi(S)(x_1, \ldots, x_n) = (-1)^{\sum_{i \in S} x_i} = (-1)^{\langle x, S \rangle}.$$

To focus on discrete fourier transform, take an arbitrary $f : G \to \mathbb{C}$.

Definition 19.

$$\langle \boldsymbol{f}, \boldsymbol{g} \rangle = \mathbb{E}_{x \in_R G}[f(x)\overline{g}(x)].$$

with $\mathbb{E}$ the expectation.[2]

The conjugation is needed for it to be a Hermitian inner product.

Definition 20. The discrete Fourier transform is

$$\hat{f} : \hat{G} \to \mathbb{C}$$

s.t. $\hat{f}(\chi) = \langle f, \chi \rangle$.

Property 26. 1. $\langle \chi, \chi \rangle = 1$

2. Orthogenality property: for $\chi_1(x_0) \neq \chi_2(x_0$ for some x_0,

$$\langle \chi_1, \chi_2 \rangle = 0.$$

Proof. 1) Obvious

2) Note that conjugation of characters is inversion.

$$\mathbb{E}_x[\chi_1(x)\chi_2^{-1}(x)] = \mathbb{E}_x[\chi_1(x + x_0)\chi_2^{-1}(x + x_0)] = \chi_1(x_0)\chi_2(x_0)^{-1}\mathbb{E}[\chi_1(x)\chi_2^{-1}(x)].$$

Hence $\chi_1(x_0)\chi_2(x_0)^{-1} \neq 1 \implies \langle \chi_1, \chi_2 \rangle = 0$. □

[2] I don't know what the subscript in expectation means

Look at a $G \times \hat{G}$ matrix. It is unitary because of the above properties.

$$\begin{pmatrix} \chi_1 & \chi_2 & \cdots \end{pmatrix} \implies |\hat{G}| = |G|.$$

The Hadamard matrix is another name for matrix.

Then

$$f(x) = \sum_{\chi \in \hat{G}} \hat{f}(\chi)\chi(x).$$

Exercise 6.1. We might want conjugation.

When you translate back and forth, you lose a factor of $\frac{1}{N^{\frac{1}{2}}}$, but not here because we don't care and it's built into expectation.

Theorem 27 (Parseval's Identity)**.**

$$|f|^2 = \mathbb{E}_x[|f(x)|^2] = \sum_{\chi} |\hat{f}(\chi)|^2.$$

6.2.2 Convolution

Definition 21.

$$\boldsymbol{(f * g)(x)} \coloneqq \mathbb{E}_y[f(x-y)g(y)] = \mathbb{E}_{y_1,y_2}[f(y_1)g(y_2)|y_1 + y_2 = x].$$

f, g give probability distributions over G, and the convolution is basically interpolating them and making it nicer.

Proposition 28.

$$\hat{f * g} = \hat{f} \cdot \hat{g}.$$

Proof. We WTS that $\hat{f * g} = \hat{f}\hat{g}$. We only need to show that $\forall x \in \hat{G}$ we have $\langle f * g, x\rangle = \langle f, x\rangle \langle g, x\rangle$.

We have that

$$\langle f * g, x\rangle = \mathbb{E}_{x,y}[f(x-y)g(y)\chi^{-1}(x)].$$

Then letting $z = x - y$ gives

$$\mathbb{E}_{y,z}[f(z)g(y)\chi^{-1}(y+z)] = \mathbb{E}_{y,z}[f(z)g(y)\chi^{-1}(y)\chi(z)].$$

This then equals

$$\langle f, x\rangle \langle g, x\rangle .$$

□

We mostly care about [3]

Definition 22.

$$\mathbb{L}_{\boldsymbol{A}} = \begin{cases} 1 & x \in A \\ 0 & \text{else} \end{cases}.$$

[4]

Theorem 29.

$$|\mathbb{L}_A|^2 = \mu = \sum_{\chi} |\chi(\mathbb{L})|^2.$$

Lemma 30.

$$|\chi(\mathbb{L}_A)|^4 \geq \mu^4.$$

Proof. Consider $\mathbb{L}_A * \widehat{\mathbb{L}_A * \mathbb{L}_{-A}} * \mathbb{L}_{-A} = \hat{\mathbb{L}_A} * \hat{\mathbb{L}_A} * \hat{\mathbb{L}_{-A}} * \hat{\mathbb{L}_{-A}} = |\mathbb{L}_A|^4$. □

[3] the below may be wrong

[4] I can't tell what the symbol here is, I assume it's a bold font L