COMPRESSIONS IN EXTREMAL SET THEORY AND ADDITIVE NUMBER THEORY

by

DAVID GEORGE

(Under the Direction of Giorgis Petridis)

ABSTRACT

This thesis examines the use of compressions, the act of algorithmically replacing a set with a more structured set of the same size, in topics from extremal set theory and additive number theory.

INDEX WORDS: Compressions, Local LYM inequality, Freiman's theorem, Green-Tao

COMPRESSIONS IN EXTREMAL SET THEORY AND ADDITIVE NUMBER THEORY

by

DAVID GEORGE

B.S., Georgia State University, 2018

A Thesis Submitted to the Graduate Faculty of The University of Georgia in Partial Fulfillment of the Requirements for the Degree

MASTER OF ARTS

ATHENS, GEORGIA

2020

COMPRESSIONS IN EXTREMAL SET THEORY AND ADDITIVE NUMBER THEORY

by

DAVID GEORGE

Major Professor:	Giorgis Petridis
Committee:	Akos Magyar
	Paul Pollack

Electronic Version Approved:

Ron Walcott
Interim Dean of the Graduate School
The University of Georgia
August 2020

Table of Contents

1 Introduction

In combinatorics, one is often interested in properties of arbitrary sets (like the size of the shadow or of the sumset). Often the minimizers are thought to be structured sets. Proving such sets are extremal is not always easy, so this is where we can apply compressions. We will use these to investigate problems in two different fields: extremal set theory and additive number theory.

One of the problems is the Local LYM Inequality where take a set and compare the density of the set with its shadow. The other problem consists of a version of Freiman's theorem where we cover a set by translates of a generalized arithmetic progression that is dependant on its doubling constant, which is the ratio between the sizes of the sumset and of the set itself.

The goal of compressions is to take sets (of subsets of {1, ..., n} or of multi-dimensional sets consisting of non-negative integers) and replace them with more structured sets while maintaining the same number of elements. Structure for set systems is, roughly speaking, measured using the colex order and in subsets of integers by how close a set is to an arithmetic progression. The key property compressions have is that they do not increase the quantity under study. In this thesis, these quantities are specifically the size of the shadow and the size of the sumset.

In extremal graph theory, we will see that the size of shadows can be decreased by having more structured sets. Using compressions will help us in creating a bound from below for the size of the shadow. Classifying extremal sets is sometimes straightforward like with showing that a sumset $|A + A|$ is equal to $2|A| - 1$ iff A is an arithmetic progression), but classifying near extremal examples is usually more difficult. Compressions assist us with such a task in the number theory question of describing sets of small doubling.

2 Compressions

2.1 Defining Shadows

The material in this Section is based on Chapter 5 of [**Bol**] and discusses the shadows of hypergraphs. Given the edges of a hypergraph, or a family of sets, a lower shadow is defined to be all the subsets with 1 less element of each set in our family.

Definition 2.1 (Shadow)**.** *Let $\mathcal{A}$ be a hypergraph. Then the shadow of $\mathcal{A}$,*

$$\partial\mathcal{A} := \{A\backslash\{x\} : A \in \mathcal{A}, x \in A\}.$$

Unless stated otherwise, we will refer to a lower shadow as just a shadow. Let us call our ground set X, our family of sets $\mathcal{A}$, and the sets in $\mathcal{A}$ come from X, so we can just say $\mathcal{A}$ is a subset of the power set of X, or $\mathcal{A} \subseteq P(X)$.

Example 2.2

As an example, let $X = \{1, 2, 3, 4, 5\}$ and $\mathcal{A} = \{\{1, 2, 3\}, \{2, 3, 5\}, \{1, 2, 3, 4\}\}$. Removing one element from each set of $\mathcal{A}$ gives us:

$\{1, 2, 3\} \supseteq \{1, 2\}, \{1, 3\}, \{2, 3\}$

$\{2, 3, 5\} \supseteq \{2, 3\}, \{2, 5\}, \{3, 5\}$

$\{1, 2, 3, 4\} \supseteq \{1, 2, 3\}, \{1, 2, 4\}, \{1, 3, 4\}, \{2, 3, 4\}.$

The elements of the shadow $\partial\mathcal{A}$, are then all of these subsets. Note there are 10 listed subsets above, but $\{2, 3\}$ is part of two of our original sets, so $|\partial\mathcal{A}| = 9$.

2.2 Partioning Shadows

Let us partition $\mathcal{A}$ by the size of its elements. If $A \in \mathcal{A}$ such that $|A| = r$, we would say $A \in X^{(r)}$ where $X^{(r)}$ is the collection of the r-elements sets within X. It should be clear when $0 < r \leqslant |X|$

$$\partial X^{(r)} = X^{(r-1)}$$

and that the two families $X^{(r-1)}, X^{(r)}$ are completely disjoint. If we look at Example 2.2, the only case where we had a duplicate subset is when our original sets were the same size and shared some common elements. This allows us to define a shadow of $\mathcal{A} \subseteq X^{(r)}$ as

$$\partial\mathcal{A} = \{B \in X^{(r-1)} : B \subseteq A \text{ for some } A \in \mathcal{A}\}.$$

So given our original $\mathcal{A}$ that could contain many different sizes of sets, we would break up these sets by

$$\mathcal{A} = \bigcup_{i=0}^{n} \mathcal{A} \cap X^{(i)}$$

and as the $X^{(i)}$ are disjoint, this gives us

$$|\partial\mathcal{A}| = \sum_{i=0}^{n} |\partial(\mathcal{A} \cap X^{(i)})|.$$

2.3 Isoperimetric Problem

Now our question becomes how small can our shadow be? Given $\mathcal{A} \subseteq X^{(r)}$, its shadow $\partial\mathcal{A} \subseteq X^{(r-1)}$, so it is obvious that the upper bound would then be

$$|X^{(r-1)}| = \binom{|X|}{r-1}.$$

This idea of finding a bound for $|\partial\mathcal{A}|$ is an isoperimetric problem. The isoperimetric problem is to determine a plane figure of the largest possible area whose boundary has a

specified length. The closely related Dido's problem asks for a region of the maximal area bounded by a straight line and a curvilinear arc whose endpoints belong to that line.

Example 2.3

In $\mathbb{R}^2$, we can see that a circle should have a greater area than any polygon of equal perimeter. More generally, given a fixed perimeter, a circle has a greater area than any shape with the same perimeter. We can also look at this in another direction: given any region of fixed area, the disk will produce the smallest boundary. Notice how we go from a 2-dimensional structure (area), down to a 1-dimensional structure (perimeter). We can actually correlate area, like the disk, as our $\mathcal{A}$ and perimeter, like the circle, as $\partial\mathcal{A}$. The isoperimetric inequality associates the relation between the perimeter and area as follows:

$$L^2 \geqslant 4\pi A$$

where L is the perimeter and A is the area.

2.4 Lubell–Yamamoto–Meshalkin Inequality

The local LYM inequality [**Mes**, **Lub**, **Yam**] gives us a lower bound on our shadow with respect to the size of our initial family. This inequality also tells us that our family is at most as dense as its shadow.

Theorem 2.4 (Local LYM Inequality)**.** *Let* $|X| = n,\ 0 < r \leqslant n,$ *and* $\mathcal{A} \subseteq X^{(r)}$*. Then*

$$|\partial\mathcal{A}| \Big/ \binom{n}{r-1} \geqslant |\mathcal{A}| \Big/ \binom{n}{r} \tag{1}$$

where equality holds iff $\mathcal{A} = \varnothing$ *or* $\mathcal{A} = X^{(r)}$*.*

Proof. Let us create the ordered pair (A, B) where $A \in \mathcal{A}$ and $B \in \partial\mathcal{A}$ such that $B \subseteq A$. Given any $A \in \mathcal{A}$, as $\mathcal{A} \subseteq X^{(r)}, |A| = r$ and $\partial\mathcal{A} \subseteq X^{(r-1)}$. Removing one of the r elements

of A will then create a B that can pair with A. Actually, every B that pairs with A must be deduced from this operation. Thus we have

$$|\mathcal{A}|r = |\{(A, B) \in \mathcal{A} \times \partial\mathcal{A} : B \subseteq A\}|.$$

Now for any $B \in \partial\mathcal{A}$, we can add any element that B doesn't already contain to create a set in $X^{(r)} \supseteq \mathcal{A}$ which is $(n - (r-1))$ elements for each B. Now we have the inequality:

$$|\mathcal{A}|r = |\{(A, B) \in \mathcal{A} \times \partial\mathcal{A} : B \subseteq A\}| \leqslant |\partial\mathcal{A}|(n - r + 1). \tag{2}$$

So

$$\begin{aligned} |\partial\mathcal{A}|(n - r + 1) &\geqslant |\mathcal{A}|r \\ |\partial\mathcal{A}| \geqslant |\mathcal{A}| \cdot \frac{r}{n - r + 1} &= |\mathcal{A}| \cdot \frac{\binom{n}{r-1}}{\binom{n}{r}} \\ |\partial\mathcal{A}| \Big/ \binom{n}{r-1} &\geqslant |\mathcal{A}| \Big/ \binom{n}{r} \end{aligned}$$

which completes (1).

For equality, it is clear that if $\mathcal{A} = \varnothing$ or $A = X^{(r)}$ then we will have equality (0=0 or 1=1 respectively). For the converse, assume $\mathcal{A}$ is nonempty and equality holds. Let $A \in \mathcal{A}$ and $A' \in X^{(r)}$. We can create a path from A to A' by removing then adding one element at a time. Removing the first element will clearly be in $\partial\mathcal{A}$ by how we defined it, so let us call this set B_0. Using (2) and the fact that the equality now holds, all $(n - r + 1)$ sets in $X^{(r)}$ that contain $B \in \partial\mathcal{A}$ must also be in $\mathcal{A}$, thus adding one element to B_0 will create a set that is in $\mathcal{A}$. Following this path leads us to the conclusion that A' must be in $\mathcal{A}$, and thus $\mathcal{A} = X^{(r)}$. □

Now for $\mathcal{A} \subseteq P(X)$ (not just $X^{(r)}$), we partition $\mathcal{A}$ by $\mathcal{A}_i = \mathcal{A} \cap X^{(i)}$ and then have

$$|\partial\mathcal{A}| = \sum_{i=1}^{n} |\partial\mathcal{A}_i| \geqslant \sum_{i=1}^{n} \frac{i}{n - i + 1} |\mathcal{A}_i|.$$

Thus, our inequality becomes:

$$\sum_{i=1}^{n} |\partial \mathcal{A}_i| \Big/ \binom{n}{i-1} \geqslant \sum_{i=1}^{n} |\mathcal{A}_i| \Big/ \binom{n}{i}.$$

2.5 Colexicographical order

To improve the bound that the local LYM inequality gave us, we will need some order in our family. Fixing r now, let us dive into some ways of ordering $X^{(r)}$. The two most natural methods of ordering our set is lexicographical and colexicographical order, or lex and colex order respectively. For lex order, if we are given two different sequences of the same length, $a = a_1a_2...a_k$ and $b = b_1b_2...b_k$, then $a < b$ if $a_i < b_i$ for some i and $a_j = b_j$ for all $j < i$. Colex order works similarly; if we are given two different sequences of the same length, $a = a_1a_2...a_k$ and $b = b_1b_2...b_k$, then $a < b$ if $a_i < b_i$ for some i and $a_j = b_j$ for all $j > i$. A very subtle difference between the two, but this produces two very different orders. Each order has its uses; lex order is more intuitive in the sense that we use it for ordering words in a dictionary or just listing r-digit numbers in order. We will actually focus on colex order here as it is very useful in ordering regardless of the size of X.

For simplicity, for $X = \{1, 2, ..., n\}$, our r-element sets will be written as be r-digit numbers (so $\{2, 3, 8, 9\}$ will be denoted 2389).

Example 2.5

As an example, the lex and colex order on the 4-element sets with $n = 5$ are:

Lex: 1234, 1235, 1245, 1345, 2345.

Colex: 1234, 1235, 1245, 1345, 2345.

(There is no difference for this specific family.)

For 4-element sets with $n = 6$:

Lex: 1234, 1235, 1236, 1245, 1246, 1256, 1345, 1346, 1356, 1456, 2345, 2346, 2356, 2456, 3456.

Colex: 1234, 1235, 1245, 1345, 2345, 1236, 1246, 1346, 2346, 1256, 1356, 1456, 2356, 2456, 3456.

For the colex order, notice how the first 5 sets, or the initial segment of length 5, for both n are exactly the same. Also notice for sets that contain the same final x digits (i.e. 1235, 1245, 1345, 2345 all end in 5), if we remove those digits, the newly-formed sets are in colex order (i.e. from sets that end in 5, removing 5 gives us 123, 124, 134, 234), the initial segment to be exact.

Example 2.6

Let $n = 9$ and $r = 3$. The initial segment of length 4 (in colex order) is: $\{123, 124, 134, 234\}$. The shadow of this family is $\{1, 2, 3, 4\}^{(2)}$, so its size is $\binom{4}{2} = 6$. Now let $B = \{123, 456, 789\}$. Its shadow has a size of $3 \cdot |\{1, 2, 3\}^{(2)}| = 3 \cdot \binom{3}{2} = 9$ Notice that even though $|B|$ is smaller, its shadow is much larger. This is no coincedence, our goal in this chapter is to show that $|\partial\mathcal{A}|$ is minimized if $\mathcal{A}$ is an initial segment in colex order.

2.6 Compressions

Based off of our previous example, it should be clear that the smaller the range of numbers being used within our family of sets, the smaller the shadow this will form. Compressions can be used to tackle this.

Definition 2.7 (Compression)**.** *Given a set $A \subseteq X$ and $i \neq j \in X$ a compression*

$$C_{ij}(A) := \begin{cases} (A \backslash \{j\}) \cup \{i\} & \text{if } i \notin A, j \in A \\ A & \text{otherwise} \end{cases}$$

This replaces the element j with i if i is not within the set, else the set will remain unchanged. It should be clear that $|C_{ij}(A)| = |A|$ and if $i < j$, then $C_{ij}(A) \leqslant A$ in the colex order.

Example 2.8

Let $\mathcal{A} = \{123, 236, 156, 346\}$. We see that

$C_{16}(123) = 123$ since we replace 6 with 1 and not the other way around

$C_{16}(236) = 123$

$C_{16}(156) = 156$ as 1 is already present within this set

$C_{16}(346) = 134$.

So far these compressions only work on single sets. We would like to extend this to a family of sets, which is where the notion of the compression operator comes into affect.

2.7 Compression Operator

The compression operator $\tilde{C}_{ij}$ is a map that sends a family of sets to another family of sets.

Definition 2.9 (Compression Operator)**.** *For $\mathcal{A} \subseteq P(X)$, we define the compression operator*

$$\tilde{C}_{ij}(\mathcal{A}) := \{C_{ij}(A) : A \in \mathcal{A}\} \cup \{A \in \mathcal{A} : C_{ij}(A) \in \mathcal{A}\}$$

This operator takes every set A in $\mathcal{A}$ and if $C_{ij}(A)$ is not in $\mathcal{A}$, then it replaces A with $C_{ij}(A)$, else A will stay as is. Similar to compressions, it is clear that $|\tilde{C}_{ij}(\mathcal{A})| = |\mathcal{A}|$ and the size of the sets in $\tilde{C}_{ij}(\mathcal{A})$ do not change, so if $\mathcal{A} \subseteq X^{(r)}$, then $\tilde{C}_{ij}(\mathcal{A}) \subseteq X^{(r)}$.

Example 2.10

Let $\mathcal{A} = \{123, 236, 156, 346\}$. (The same as the last example.) Then $\tilde{C}_{16}(\mathcal{A}) = \{123, 134, 236, 156\}$. Notice how even though $C_{16}(236) = 123$, 236 does not get replaced in $\tilde{C}_{16}(\mathcal{A})$ as 123 was already present within $\mathcal{A}$.

Let us also observe the shadows of A and $\tilde{C}_{ij}(\mathcal{A})$:

$$\begin{aligned} \partial\mathcal{A} &= \{12, 13, 23, 34, 15, 16, 26, 36, 46, 56\} \\ \partial\tilde{C}_{16}(\mathcal{A}) &= \{12, 13, 23, 34, 15, 16, 26, 36, 56\}. \end{aligned}$$

Notice how the compression actually lowered the size of our shadow. Given 4 elements within our family, it should be clear that the shadow of $\tilde{C}_{16}(\mathcal{A})$ is not minimized as our initial segment of length 4 ($\mathcal{F} = \{123, 124, 134, 234\}$) would be a much better choice. We could actually reach this initial segment with more compressions on this set system ($\mathcal{F} = \tilde{C}_{25}(\tilde{C}_{46}(\tilde{C}_{16}(\mathcal{A})))$).

2.8 Compressed Families

It is not always the case that we can compress any family into an initial segment (of colex order). We will define a set system $\mathcal{A} \subseteq X^{(r)}$ to be left compressed:

$$\mathcal{A} = \tilde{C}_{ij}(\mathcal{A}) \text{ for all } 1 \leqslant i < j \leqslant n$$

We refer to left compressed as compressed when there is no confusion. As i, j are both bounded by being integers between 1 and n, given any family $\mathcal{A}$, there is a compressed set $\mathcal{A}'$ which comes from applying $\tilde{C}_{ij}(\mathcal{A})$ a finite amount of times. This will be shown more formally in a later theorem, but it is worth noting this compressed set A' is not unique and these compressions are not commutative.

Clearly, all initial segments of colex order are compressed. What is a bit more interesting is that all initial segments of lex order are also compressed.

Example 2.11

Let $\mathcal{A} = \{123, 247, 256\}$. Then

$$\tilde{C}_{47}(\tilde{C}_{14}(\tilde{C}_{46}(\tilde{C}_{14}(\mathcal{A})))) = \{123, 124, 125\} = A'.$$

This is initial segment of length 3 in lex order (when $n \geqslant 5$). (Notice how we applied $\tilde{C}_{14}$ twice.) We cannot compress this any further: the 2 in the 125 would need to be replaced with a 3 (or 4) to create 134, but $\tilde{C}_{32}(\mathcal{A})$ would imply $i > j$ which we cannot do, so A' is compressed.

However, we if we apply a different set of compressions

$$\tilde{C}_{46}(\tilde{C}_{35}(\tilde{C}_{12}(\tilde{C}_{17}(\mathcal{A})))) = \{123, 124, 134\} = A''.$$

Now we have the inital segment of colex order. This shows us that A'' is compressed, but $A'' \neq A'$.

2.9 Compression Lemma

As hinted at with Example 2.10 and the idea of attempting to compress sets to colex order, $\mathcal{A}$ being compressed should decrease (not necessarily strictly) the size of our shadow. This lemma provides us with exactly that.

Lemma 2.12. *Let $\mathcal{A} \subseteq X^{(r)}$ and $1 \leqslant i < j \leqslant n$. Then*

$$|\partial\mathcal{A}| \geqslant |\partial\tilde{C}_{ij}(\mathcal{A})|. \tag{3}$$

Also, given $\mathcal{A} \subseteq X^{(r)}$, there is a compressed set system $\mathcal{A}' \subseteq X^{(r)}$ such that

$$|\mathcal{A}| = |\mathcal{A}'| \text{ and } |\partial\mathcal{A}| \geqslant |\partial\mathcal{A}'|. \tag{4}$$

Proof. For (3), we can start by just showing that

$$|\partial\mathcal{A}\backslash\partial\tilde{C}_{ij}(\mathcal{A})| \geqslant |\partial\tilde{C}_{ij}(\mathcal{A})\backslash\partial\mathcal{A}|.$$

As we can add the intersection of the two sets on both sides to obtain the original claim. Now, let $B \in \partial\tilde{C}_{ij}(\mathcal{A})\backslash\partial\mathcal{A}$. If we can create an injective map to $\partial\mathcal{A}\backslash\partial\tilde{C}_{ij}(\mathcal{A})$, then we are done. As $B \notin \partial\mathcal{A}$, $i \in B$ and $j \notin B$, thus if we apply $C_{ji}(B)$, then $j \in B$, so $C_{ji}(B) \notin \partial\tilde{C}_{ij}(\mathcal{A})$. As this operation essentially reversed what $\tilde{C}_{ij}(\mathcal{A})$ does, then B must be in $\partial\mathcal{A}$. For similar reasons, for a different $B' \in \partial\tilde{C}_{ij}(\mathcal{A})\backslash\partial\mathcal{A}$, applying the compression will also remove i and add j, so the outputs must be different. Thus we have

$$|\partial\mathcal{A}\backslash\partial\tilde{C}_{ij}(\mathcal{A})| \geqslant |\partial\tilde{C}_{ij}(\mathcal{A})\backslash\partial\mathcal{A}|$$

and by extension

$$|\partial\mathcal{A}| \geqslant |\partial\tilde{C}_{ij}(\mathcal{A})|.$$

For (4), we first will denote $\mathcal{A}$ as $\mathcal{A}_0$. Now, we will pick an operator $\tilde{C}_{ij}, 1 \leqslant i < j \leqslant n$ such that $\tilde{C}_{ij}(\mathcal{A}_0) \neq \mathcal{A}_0$ (this should exist or else $\mathcal{A}_0$ is compressed). We will denote $\mathcal{A}_1 = \tilde{C}_{ij}(\mathcal{A}_0)$ and continue this process until we end up at a compressed system $\mathcal{A}_k$. Now we need to show that k must be finite. To do this let us define the weight of a family of sets $\mathcal{F} \subseteq P(X)$ (for $X = \{1, ..., n\}$) as

$$w(\mathcal{F}) = \sum_{A\in\mathcal{F}} \sum_{x\in\mathcal{A}} x.$$

As $i < j$, it should be clear then that $w(\mathcal{A}_0) > w(\mathcal{A}_1) > \cdots > 0$ where $w(\mathcal{A}_0)$ is finite. That means there should be less than $w(\mathcal{A}_0)$ steps, so $k < w(\mathcal{A}_0)$. Thus, by how our compression operator is defined and by (3), we can see that $|\mathcal{A} = \mathcal{A}_0| = |\mathcal{A}_1| = |\mathcal{A}_2| = \cdots = |\mathcal{A}_k = A'|$ and $|\partial\mathcal{A}_0| \geqslant |\partial\mathcal{A}_1| \geqslant \cdots \geqslant |\partial\mathcal{A}_k|$. □

2.10 Initial Segments

We may finally approach the question of whether the initial segment of length k will produce the smallest shadow and prove a result of Kruskal [**Kru**], which was rediscovered by Katona [**Kat**]. The proof using compressions we present is due to Frankl [**Fra**].

Theorem 2.13 (Eberhard-Green-Manners)**.** *Given $\mathcal{A} \subseteq X^{(r)}$ such that $|\mathcal{A}| = \binom{m}{r}$, then $|\partial\mathcal{A}| \geqslant \binom{m}{r-1}$*

Proof. We will use induction on $m + r$. For $m = r = 1$, our assumption clearly holds. Now assume our assumption holds for $m+r < k$. We may start by assuming that $\mathcal{A}$ is compressed as this would only decrease our shadow by Lemma 2.12. Now let

$\mathcal{A}_1 = \{A \in \mathcal{A} : 1 \in A\}$

$\mathcal{B}_1 = \{A\backslash\{1\} : A \in \mathcal{A}_1\}$

$\mathcal{A}_2 = \mathcal{A}\backslash\mathcal{A}_1 \ \ (= \{A \in \mathcal{A} : 1 \notin A\})$.

Essentially, $\mathcal{A}_1$ are all the sets in $\mathcal{A}$ that contain 1. $\mathcal{B}$ is taking $\mathcal{A}_1$ and removing all 1's, so $|\mathcal{A}_1| = |\mathcal{B}_1|$. Furthermore, $\mathcal{A}_1$ is nonempty (as $\mathcal{A}$ is nonempty) since if $A \in \mathcal{A}$ did not contain 1, we may take some $j \in A$ and apply $\tilde{C}_{1j}(\mathcal{A})$, and since $\mathcal{A}$ is compressed, $C_{1j}(A) \in \mathcal{A}$.

Another thing to note is that $\partial\mathcal{A}_1 = \mathcal{B}_1 \cup (\partial\mathcal{B}_1 \cup \{1\})$ and since $1 \notin B$ for all $B \in \mathcal{B}_1$,

$$|\partial\mathcal{A}_1| = |\mathcal{B}_1| + |\partial\mathcal{B}_1|. \tag{5}$$

Now as $\mathcal{A}$ is compressed, for any set $A \in \mathcal{A}_2$, $C_{1j}(A) \in \mathcal{A}$ for all $j \in A$ and thus $C_{1j}(A) \in \mathcal{A}_1$ (for all $j \in A$). This tells us that

$$\partial\mathcal{A}_2 \subseteq \mathcal{B}_1 \tag{6}$$

Claim: $|\mathcal{A}_1| = |\mathcal{B}_1| \geqslant \binom{m-1}{r-1}$

Assume $|\mathcal{A}_1| = |\mathcal{B}_1| < \binom{m-1}{r-1}$. Then

$$|\mathcal{A}_2| = |\mathcal{A}\backslash\mathcal{A}_1| = |\mathcal{A}| - |\mathcal{A}_1| > \binom{m}{r-1} - \binom{m-1}{r-1} = \binom{m-1}{r}$$

Pick a subset $\mathcal{A}_2'$ of $\mathcal{A}_2$ such that $|\mathcal{A}_2'| = \binom{m-1}{r}$. As $(m-1) + r = k$, we can now apply our induction hypothesis (and also using (6)):

$$|\mathcal{B}_1| \geqslant |\partial\mathcal{A}_2| \geqslant |\partial\mathcal{A}_2'| \geqslant \binom{m-1}{r-1}$$

But $|\mathcal{B}_1| < \binom{m-1}{r-1}$ by our assumption, so we have reached a contradiction.

Thus, we have $|\mathcal{A}_1| = |\mathcal{B}_1| \geqslant \binom{m-1}{r-1}$. Pick a subset $\mathcal{A}_1'$ of $\mathcal{A}_1$ such that $|\mathcal{A}_1'| = |\mathcal{B}_1'| = \binom{m-1}{r-1}$. Then by (5) and our induction hypothesis:

$$|\partial\mathcal{A}| \geqslant |\partial\mathcal{A}_1'| = |\mathcal{B}_1'| + |\partial\mathcal{B}_1'| \geqslant \binom{m-1}{r-1} + \binom{m-1}{r-2} = \binom{m}{r-1}.$$

□

Note we have only shown that the set of the first k elements of $X^{(r)}$ in the colex order will produce the smallest shadow when $k = \binom{m}{r}$. We can extend this to any positive integer k by writing k as the sum of decreasing binomial coefficients.

Lemma 2.14. *For all positive $k \in \mathbb{Z}, \exists!$ natural numbers $m_s, m_{s+1}, ..., m_r$ such that $s \leqslant m_s < m_{s+1} < ... < m_r$ and:*

$$k = \sum_{j=s}^{r} \binom{m_j}{j}$$

We will not go over the proof of this lemma, but will we using this information, we can now extend this initial segment of colex order to any length k.

Theorem 2.15. *Given $\mathcal{A} \subseteq X^{(r)}$, we have $|\partial\mathcal{A}| \geqslant \partial^{(r)}|\mathcal{A}|$ where $\partial^{(r)}|\mathcal{A}|$ denotes the shadow of the first $|\mathcal{A}|$ sets in the colex order.*

Proof. This proof is similar to Theorem 2.13, so it will be exempted in this text. □

2.11 Upper Shadows

This new information can also be applied to upper shadows. Upper shadows are defined to be all the supersets with 1 more element of each set in our family. When discussing both upper and lower shadows, we will denote the upper shadow of a family of sets $\mathcal{A}$ as $\partial_u\mathcal{A}$ and keep lower shadows as $\partial\mathcal{A}$.

Complementary to lower shadows, the last k elements of $X^{(r)}$ in the colex order can form the smallest shadow.

Theorem 2.16. *Let $1 \leqslant r \leqslant n-1, \mathcal{A} \subseteq X^{(r)}$ and let $\mathcal{F}$ be the set of the last $|\mathcal{A}|$ elements of $X^{(r)}$ in colex order. Then*

$$|\partial_u\mathcal{A}| \geqslant |\partial_u\mathcal{F}|.$$

Proof. Denote $\mathcal{A}^c := \{X \backslash A : A \in \mathcal{A}\}$ as the family of complements of sets in $\mathcal{A}$. Notice that $(\partial_u \mathcal{A})^c = \partial(\mathcal{A}^c)$, and that $|\mathcal{A}^c| = |\mathcal{A}|$, so:

$$|\partial_u \mathcal{A}| = |(\partial_u \mathcal{A})^c| = |\partial(\mathcal{A}^c)|$$

Now observe that $\mathcal{F}^c$ is precisely the first $|A|$ elements of $X^{(n-r)}$ (in colex order) and $\mathcal{A}^c \subseteq X^{(n-r)}$, thus

$$|\partial_u \mathcal{A}| = |\partial(\mathcal{A}^c)| \geqslant |\partial \mathcal{F}^c| = |(\partial_u \mathcal{F})^c| = |\partial_u \mathcal{F}|.$$

□

3 Freiman's Theorem

3.1 Defining Sumsets

Let us turn our attention to the notion of sumsets. Given two sets $A, B \subseteq \mathbb{Z}$, the elements of the sumset takes an integer from A and an integer from B then takes the sum of those two. We can generalize this notation to an abelian (commutative) group G whose operation will be denoted through addition and $A, B \subseteq G$ (subgroups are not necessary).

Definition 3.1 (Sumset)**.** *Let $A, B \subseteq G$ be subsets of an abelian group G. The sumset $A+B$ is a set which is computed*

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

Example 3.2

Let $A = \{-1, 2\}$ and $B = \{10, 11\}$. Then

$$\begin{aligned} A + B &= \{-1 + 10, -1 + 11, 2 + 10, 2 + 11\} \\ &= \{9, 10, 12, 13\}. \end{aligned}$$

Notice here how $|A + B| = |A| + |B|$. This is definitely not always the case: let $C = \{0, 1, 2\}$. Then $C + C = \{0, 1, 2, 3, 4\}$, so $|C + C| \neq |C| + |C|$.

3.2 Doubling Bounds

We are more interested in examining the sumsets of the same set $A + A$ which we will call doubling. We will simply state these, but it is not too hard to show if we shift or dilate A, the size of its doubling remains the same:

$$t \cdot A = \{ta : a \in A \subseteq \mathbb{Z}, t \in \mathbb{Z} \backslash \{0\}\}$$

$$x + A = \{x + a : a \in A \subseteq \mathbb{Z}, t \in \mathbb{Z}\}$$

$$|A + A| = |(t \cdot A) + (t \cdot A)| = |(x + A) + (x + A)|.$$

Please note in this text that we will use the $\cdot$ symbol whenever we are dilating the set.

We can show that there must be a lower bound to the cardinality of these types of sumsets.

Theorem 3.3. *Let A be a finite set of integers. Then $|A + A| \geqslant 2|A| - 1$, and equality holds if and only if A is an arithmetic progression*

Proof. The first part of the proof is quite simple. As $|A|$ is finite (and a set of integers), we can order our set

$$A = \{a_1, a_2, ..., a_n\} \text{ where } a_1 < ... < a_n \text{ (and } |A| = n).$$

Then as each a_i is distinct,

$$a_1 + a_1 < a_1 + a_2 < ... < a_1 + a_n.$$

Similarly,

$$a_n + a_1 < a_n + a_2 < ... < a_n + a_n$$

so we have

$$a_1 + a_1 < a_1 + a_2 < ... < a_1 + a_n < a_2 + a_n < a_3 + a_n < ... < a_n + a_n$$

which produces precisely $2n - 1$ elements. Thus $|A + A| \geqslant 2|A| - 1$.

For equality, we will use induction on n and assume A (is ordered) and a_i is defined the same way as before. For $n = 2$, $A + A$ only has $2n - 1$ elements and any two numbers form an arithmetic progression.

Now assume this holds true for $k = n - 1$. Let us assume $|A + A| = 2n - 1$ (so we need to show A is an arithmetic progression and the converse). We know

$$a_1 + a_1 < a_1 + a_2 < ... < a_1 + a_{n-1} < a_2 + a_{n-1} < ... < a_{n-1} + a_{n-1} < a_{n-1} + a_n < a_n + a_n$$

is precisely $2n - 1$ elements, so these are our only distinct elements. Now let

$$A' = \{a_1, ..., a_{n-1}\}$$

Then $(A' + A') \subsetneq (A + A)$ and

$$(A + A) \backslash (A' + A') \subseteq \{a_1 + a_n, a_2 + a_n, ..., a_{n-1} + a_n, a_n + a_n\}. \tag{7}$$

As we determined our distinct elements in $A + A$ and

$$a_m + a_{n-1} < a_m + a_n < a_{n-1} + a_n \tag{8}$$

for all $m < n - 1$, there exists i, j such that $m < i \leqslant j < n$ and

$$a_i + a_j = a_m + a_n. \tag{9}$$

As $i \leqslant j \leqslant n - 1,\ a_m + a_n = a_i + a_j \in A' + A'$, so from (7)

$$(A + A) \backslash (A' + A') = \{a_{n-1} + a_n, a_n + a_n\},$$

and thus $|A' + A'| = 2n - 1 - 2 = 2(n - 1) - 1$. This allows us to apply our induction

hypothesis and confirm that A' must be an arithmetic progression. Now using (8) when $m = n - 2$, we have

$$a_{n-2} + a_{n-1} < a_{n-2} + a_n < a_{n-1} + a_n$$

then by (9)

$$a_{n-2} + a_n = a_{n-1} + a_{n-1},$$

so

$$a_n = a_{n-1} + (a_{n-1} - a_{n-2})$$

which precisely continues our arithmetic progression from A'. Thus A is an arithmetic progression.

For the converse, if A is an arithmetic progression, then

$$a_i + a_j = a_{i-d} + a_{j+d}$$

for all $1 \leqslant i - d \leqslant i \leqslant j \leqslant j + d \leqslant n$. Thus by letting $d = i - 1$ or $d = n - j$, our only distinct elements are

$$a_1 + a_1, a_1 + a_2, ..., a_1 + a_n, a_2 + a_n, ..., a_n + a_n,$$

so we can conclude that $|A + A| = 2n - 1$. □

Since we have found that these sumsets have a lower bound, the next natural step is to find an upper bound. As long as A is part of a abelian group, $A + A \leqslant \binom{|A|+1}{2}$ and this bound can be seen in $\mathbb{Z}$ by using any geometric sequence whose ratio is greater than 2 (i.e. $A = \{10, 100, ..., 10^{|A|}\}$).

We know that an arithmetic progression will produce a small doubling. Are there any other types of sets that will produce a small sumset? Freiman's Theorem is the motivation behind this proposition.

3.3 Multidimensional Arithmetic Progressions

Let us expand our notion of sumsets. As long as we have a finite abelian group G, the sumsets $(A + B) + C$ and $A + (B + C)$ should be identical if we picture this element-wise, so we may simply state this as $A + B + C$.

Definition 3.4 (General Arithmetic Progression)**.** *A general or multidimensional arithmetic progression is in the form*

$$A = A_1 + A_2 + A_3 + \cdots + A_d$$

where A_i for each i is an arithmetic progression. We define d as the dimension of A.

Most progressions in this section will be arithmetic, so unless specified otherwise, all progressions are assumed to be arithmetic, and so we may refer to a d-dimensional arithmetic progression as just a general progression.

Example 3.5

Let $B = \{3, 4, 5\} + \{10, 20\}$. Then $B = \{13, 14, 15, 23, 24, 25\}$ and is a 2-dimensional progression.

Now let $A = \{0, 1, 2, ..., 9\} + \{0, 10, 20, ..., 90\} + \{0, 100, 200, ..., 900\}$. Then we can call A a 3-dimensional progression. However, A is precisely $\{0, 1, 2, ..., 998, 999\}$ which is a basic 1-dimensional progression. Notice here that $|A| = |A_1||A_2||A_3|$.

We could also define $A = \{0, 1, 2, ..., 19\} + \{0, 10, 20, ..., 80\} + \{0, 100, 200, ..., 900\}$, so there is no unique way of writing A, and the dimension of the progression is entirely dependent on the way we choose to define it. Also note that this time we have $|A| < |A_1||A_2||A_3|$. This is because each sum of the sumset is not unique: $11 + 50 + 700 = 1 + 60 + 700$.

Now with how large these general progressions can get, the upper bound on these sets also would seem to grow very large, but there is still some control that we have on them. Let us first observe what happens when each sum (in our sumset) is unique.

Theorem 3.6. *Let $P = P_1 + P_2 + \cdots + P_d$ be a d-dimensional arithmetic progression such that $|P| = |P_1||P_2|\cdots|P_d|$. Then $|P + P| \leqslant 2^d|P|$.*

Proof. As we are dealing with an abelian (commutative) group, and these sumsets are associative, we have:

$$\begin{aligned}
|P + P| &= |(P_1 + P_2 + \cdots + P_d) + (P_1 + P_2 + \cdots + P_d)| \\
&= |P_1 + P_2 + \cdots + P_d + P_1 + P_2 + \cdots + P_d| \\
&= |P_1 + P_1 + P_2 + P_2 + \cdots + P_d + P_d| \\
&= |(P_1 + P_1) + (P_2 + P_2) + \cdots + (P_d + P_d)| \\
&\leqslant |P_1 + P_1||P_2 + P_2|\cdots|P_d + P_d|
\end{aligned}$$

Now applying the lower bound for 1-dimensional progressions from Theorem 3.3,

$$\begin{aligned}
|P + P| &\leqslant |P_1 + P_1||P_2 + P_2|\cdots|P_d + P_d| \\
&\leqslant (2|P_1| - 1)(2|P_2| - 1)\cdots(2|P_d| - 1) \\
&\leqslant (2|P_1|)(2|P_2|)\cdots(2|P_d|) \\
&= 2^d|P_1||P_2|\cdots|P_d| = 2^d|P|
\end{aligned}$$

□

When our sums are not unique, we can view these general progressions in a different way.

Theorem 3.7. *Let P be a d-dimensional arithmetic progression. Then $|P + P| \leqslant 2^d|P|$.*

Proof. Let P_i be the i-th dimension of P. Now let us define $(n_1, n_2, ..., n_d) := n_1+n_2+\cdots+n_d$, so we can write

$$P = \{(p_{1,j_1}, p_{2,j_2}, ..., p_{d,j_d}) : p_{i,j_i} \text{ is the } j_i\text{-th term in } P_i\}.$$

Let us simplify our notation and just define $(p_{1,j_1}, p_{2,j_2}, ..., p_{d,j_d})$ as $(j_1, j_2, ..., j_d)$ where j_i denotes the j_i-th term in P_i (we're assuming P is ordered such that $p_{i,j_i} < p_{i,j_i+1}$ in P_i). For example, $(1, 1, ..., 1)$ is the sum of each of the first terms of P_i and $(|P_1|, |P_2|, ..., |P_d|)$ is the sum of the last. As the sums are not unique, we may have different points equal each other in P, but the closed hyperrectangle in Z^d formed by the diagonal from $(1, 1, ..., 1)$ to $(|P_1|, |P_2|, ..., |P_d|)$ still forms P.

Now consider $P + P$. We can use vector addition to form our new space

$$P + P := \{(m_1 + n_1, m_2 + n_2, ..., m_d + n_d)_+ : (m_1, ..., m_d), (n_1, ..., n_d) \in P\}.$$

This is well-defined precisely because each P_i is an arithmetic progression. We have denoted this space with the subscript $+$ to prevent confusion between P and $P + P$ (the points $(2, 2, ..., 2)$ and $(2, 2, ..., 2)_+$ are not necessarily the same) as we will still use the former space in this proof.

Due to the range of each value ($j_i \in \{1, 2, ..., |P_i|\}$ for each P_i), this makes:

$$P + P = \Big\{(j_1, j_2, ..., j_d)_+ : j_i \in \{2, 3, ..., |P_i| + |P_i|\}\Big\}.$$

Let us define O' to be the shift that sends $(|P_1| + 1, |P_2| + 1, ..., |P_d| + 1)_+$ to the origin or

$$(|P_1| + 1, |P_2| + 1, ..., |P_d| + 1)_+ \mapsto (0, 0, ..., 0)'_+.$$

Thus, $(1, 1, ..., 1) + P$ in O' is in the closed orthant where all terms are nonpositive. To be exact, every orthant in O' is partitioned by looking at the sumset $(j_1, j_2, ..., j_d) + P$ where each $j_i = 1$ or $|P_i|$. These sumsets will also form all of our terms in $P + P$, so $|P + P|$ is no more than product of the the number of orthants in our space and P, or $|P + P| \leqslant 2^d |P|$. $\square$

3.4 Large Subsets of Multidimensional Progressions

hese multidimensional progressions having relatively small doubling actually imply any subset of this progression of having small doubling. When dealing with general subsets in $\mathbb{Z}$ then, we should then find a good bound for our doubling by observing the smallest multidimensional progression we can fit it into. Let us look at a few examples that illustrate this.

Example 3.8

Let A be any subset of $\{1, 2, ..., 2n\}$ such that $|A| = n$. We can see that $A+A \subseteq \{2, 3, ..., 4n\}$, so $|A + A| \leqslant 4n = 4|A|$. Generally, if we look at any set A of size n to be a subset of $\{1, 2, ..., cn\}$, then the size of doubling is at most $2c|A|$.

Now consider the geometric sequence

$$M = \{10, 100, 1000, ..., 10^n\}.$$

Given the size of M, the doubling of this set is the largest it could be, $\binom{n+1}{2}$. So what is the smallest type of progression that M fits inside? We could try $\{1, 2, ..., 10^n\}$, or $\{10, 20, 30, ..., 10^n\}$, but the size of this is very large: 10^{n-1}. The next best we could try is an n-dimensional progression

$$\{0, 10\} + \{0, 100\} + \cdots + \{0, 10^n\}.$$

The size of this is much smaller: 2^n. We actually cannot do much better than this; the $(n-1)$-dimensional progression

$$\{10, 100\} + \{0, 1000 - 10\} + \{0, 10^4 - 10\} + \cdots + \{0, 10^n - 10\}$$

is twice as smaller (the size now being 2^{n-1}) than our previous approach.

The same goes if we let $M = \mathbb{Z}^n$ (the group is formed using vector addition). The smallest progression that would contain M would be a $(n-1)$-dimensional progression using the standard unit vectors: $\{e_1, e_2\} + \{0, e_3 - e_1\} + \{0, e_4 - e_1\} + \cdots + \{0, e_n - e_1\}$.

3.5 Freiman's Theorem

Now we are ready to discuss Freiman's Theorem [**Fre2**]. Before we start, we will define "size" a bit more rigorously. Let P is a d-dimensional arithmetic progression such that $P = P_1 + \cdots + P_d$, then the size of P is defined by

$$||P|| := \prod_{i=1}^{d} |P_i|$$

Notice how we have used the term size a few times already, this is because $|P| = ||P||$ when P is proper, which means that all sums are distinct (or if $d = 1$). We can now finally state Freiman's Theorem [**Fre2**].

Theorem 3.9 (Freiman)**.** *Let $A \subseteq \mathbb{Z}$. If $|A + A| \leqslant K|A|$, then there exists functions $d(K) : \mathbb{R} \to \mathbb{Z}^+$ and $C(K) : \mathbb{R} \to \mathbb{Z}^+$ such that $P \supseteq A$ is an d-dimensional progression such that $d \leqslant d(K)$ and $||P|| \leqslant C(K)|A|$.*

We will not go over the proof, but we will look over some examples (some should be very familiar).

Example 3.10

Given $A = \{10, 100, 1000, ..., 10^k\}$. Then $|A| = k$ and $|A + A| = \frac{k+1}{2}|A|$. We can let $d(K) = n - 1$ and $C(K) = \frac{2^{k-1}}{k}$. The same can be said for $A = \mathbb{Z}^d$.

For a more general example, let $|A + A| \leqslant 2|A|$. We know if $|A + A| \leqslant 2|A| - 1$, we must have an arithmetic progression. When $|A + A| = 2|A|$, the only case where we have this is when we skip one (middle) term in an arithmetic progression (i.e. $\{3, 6, 9, 15\}$). Thus, we may still look at a 1-dimensional progression where its size is 1 more than $|A|$. Thus if

$A \subseteq \mathbb{Z}$, for $K = 2,\ d = 1$ and $C = 1 + \epsilon$ where $\epsilon = \frac{1}{|A|}$. Alternatively, we could also state if $K = 2 - \epsilon$ where $\epsilon = \frac{1}{|A|}$ and $A \subseteq \mathbb{Z}$, then $d = C = 1$ as A must be an arithmetic progression, so we can let $P = A$.

Our geometric example actually shows us our maximum d and C in $\mathbb{Z}$. For any abelian group, our best bounds are $d < K$ and $C < e^{K^{O(1)}}$ though it is not easy to show the latter nor is known to be sharp.

3.6 Case when $K < 3$

There are some very interesting results when the size of the doubling is close to 3 times less than the size of the set. The proof of this theorem (the so-called Freiman $3k - 4$ theorem [**Fre1**]) will be excluded, but we will discuss the results.

Theorem 3.11 (Freiman)**.** *Let A be a finite set of integers and $|A| = k \geqslant 2$. Then if $|A + A| \leqslant 3k - 4$, then A is a subset of an arithmetic progression $|P|$ of at most size $2k - 3$.*

To show our $2k - 3$ bound is tight, let

$$A = \{1, 2, ..., k - 1\} \cup \{2k - 3\}.$$

Then

$$A + A = \{2, 3, ..., 2k - 2, ..., 3k - 4\} \cup \{4k - 6\},$$

so $|A| = k,\ |A + A| = 3k - 4$ and the smallest progression A fits inside is $\{1, 2, ..., 2k - 3\}$ whose size is $2k - 3$. To show that we cannot lower the bound $3k - 4$, consider

$$B = \{1, 2, ..., k - 1\} \cup \{k^2 + 2k - 3\}.$$

Then

$$B + B = \{2, 3, ..., 2k - 2\} \cup \{k^2 + 2k - 2, k^2 + 2k - 1, ..., k^2 + 3k - 4\},$$

so $|B| = k$ and $|B + B| = 3k - 3$, but the smallest progression B fits inside must have a size of $k^2 + 3k - 4$ which gets much larger than $2k - 3$ the bigger the value k gets.

To state this $3k - 4$ Theorem in terms of Freiman's Theorem is that (if $A \subseteq \mathbb{Z}$, and) if $K = 3 - 4\epsilon$, where $\epsilon = \frac{1}{|A|}$, and $|A + A| \leqslant K|A|$, then there exists an arithmetic progression $P \supseteq A$ such that ($d = 1$ and) $||P|| \leqslant C(K)|A|$ where $C = 2 - 3\epsilon$.

3.7 Case when $K < 4$

For $|A + A| < 4|A|$, we actually will not refer to sumsets, but rather difference sets

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

Where subtracting is adding by an element's inverse. There are some very basic observations about the doubling of difference sets for any nonempty set A:

- If $x \in A - A$, then $-x \in A - A$
- $0 \in A - A$
- $|A - A|$ is always odd
- If A is an arithmetic progression, then $|A - A| = 2|A| - 1$
- $A - A = (x + A) - (x + A)$

It is also true that the cardinality of sumsets versus difference sets are very similar, so due to the last observation above, it is sometimes easier to look at difference sets when we discuss doubling.

Now, when $K < 4$, we have the following strong result of Eberhard, Green, and Manners [**EGM**].

Theorem 3.12. *There exists an absolute constant $c > 0$ and a function $f : \mathbb{R}^+ \to \mathbb{R}^+$ such that for all $\epsilon > 0$ and finite set of integers A, if $|A - A| \leqslant (4 - \epsilon)|A|$, then there exists an arithmetic progression P such that $|P| \geqslant f(\epsilon)|A|$ and $|A \cap P|/|P| \geqslant 1/2 + c\epsilon$*

First, it is worth noting that $|A \cap P|/|P|$ is referred to as the density of P in A. The function f is not specified either, it is only necessary that it goes to zero quickly as ϵ goes to zero (i.e. we could let $f(\epsilon) = \epsilon^{1/\epsilon}$).

Example 3.13

Let $A = \{1, ..., k-1\} \cup \{k^2 + 2k - 3\}$. This was an example we used for $K < 3$ where $|A + A| = 3k - 3$. Now, $A - A = \Big(\{1, 2, ..., k-1\} - \{1, 2, ..., k-1\}\Big) \cup \Big(- (k^2 + 2k - 3) + A\Big) \cup \Big((k^2 + 2k - 3) - A\Big)$, so $|A - A| = 2(k-1) - 1 + k + k - 2 = 4(k-1) < 4k$. Here we can just let $P = \{1, 2, ..., k-1\}$, and we have the density of P in A being 1.

Let $A = X \cup Y$ such that X, Y are (distinct) arithmetic progressions with the same common difference and $|X| \geqslant |Y|$. Then $A - A = (X - X) \cup (X - Y) \cup (Y - X) \cup (Y - Y) \leqslant 2|X| - 1 + 2(|X| + |Y| - 1) + 2|Y| - 1 = 4(|X| + |Y| - 1) < 4|A|$. We just need to let $P = X$, and the density in A is 1 again.

One example that would show use a density being less than one is starting with $A \subseteq \{1, ..., k\}$, such that

$$|A| \geqslant (1/2 + c\epsilon)k$$

Now $(A - A) \subseteq \{-(k-1), ..., -1, 0, 1, ..., (k-1)\}$, so $|A - A| \leqslant 2k - 1$. When ϵ is small, $\epsilon^2 \leqslant \epsilon$ and $1 \geqslant k\epsilon/2 - 3ck\epsilon^2$, so we have

$$\begin{aligned}
|A - A| &\leqslant 2k - 1 \\
&\leqslant 2k - (k\epsilon/2 - 3ck\epsilon^2) \\
&= (2 - \epsilon/2 + 3c\epsilon^2)k \\
&= (2 - \epsilon/2 + 4c\epsilon^2 - c\epsilon^2)k \\
&\leqslant (2 - \epsilon/2 + 4c\epsilon - c\epsilon^2)k \\
&= (4 - \epsilon)(1/2 + c\epsilon)k \\
&\leqslant (4 - \epsilon)|A|
\end{aligned}$$

Now when $P = \{1, ..., k\}$, we clearly obtain $|A \cap P|/|P| \geqslant 1/2 + c\epsilon$.

To show the bound for this theorem is sharp (why we can't let $|A-A| = 4|A|$), let $\epsilon > 0$ and take $d = 3\lceil 1/f(\epsilon)\rceil$. Now let

$$A = \{0, 1, 2, ..., d\} + \{0, d^2, 2d^2, ..., d \cdot d^2\}.$$

Then

$$A - A = \{-d, ..., -1, 0, 1, ..., d\} + \{-d^3, ..., -d^2, 0, d^2, ..., d^3\},$$

so as d gets very big (which it should, given $f(\epsilon)$ goes to 0 quickly),

$$|A - A| = (2d+1)(2d+1) \approx 4(d+1)^2 = 4|A|,$$

but the best we can make P is be a subset of $\{-d, ..., -1, 0, 1, ..., d\}$, so

$$|P| \leqslant 2d + 1 \leqslant 3d^{-1} \cdot d^2 < 3d^{-1} \cdot (d+1)^2 \leqslant f(\epsilon)|A|.$$

3.8 Doubling of General Groups

When discussing groups, there are some similar properties when we are trying to find a subset with small doubling. Just like how arithmetic progressions are small in $\mathbb{Z}$, arithmetic progressions in an abelian group G are small as well.

$$A := \{x + d, x + 2d, ..., x + kd : x, d \in G, k \in \mathbb{Z}^+\}$$

Where for example $4d$ means $d+d+d+d$, so kd is adding d by itself k times. Our sumset then becomes

$$A + A = \{x + 2d, x + 3d, ..., x + (2k)d\},$$

so we end up with if $|A| = k$, then $|A + A| \leqslant 2k - 1$.

Arithmetic progressions in groups are not the only example that result in small doubling, we can also look at subgroups of G (a subgroup H is a subset in G such that H follows the properties of a group and is closed). As subgroups are closed, this immediately tells us that the doubling a subgroup is itself! Notice that the only subgroups of $\mathbb{Z}$ are $\{0\}$ and $\mathbb{Z}$ which is why there is no doubling smaller than $2k-1$.

Combining these progressions and subgroups together, if P is an arithmetic progression and H is a subgroup of G ($H \leqslant G$), then if $A = P + H$ (so $|A| \leqslant |P||H|$),

$$\begin{aligned}
|A + A| &= |(P + H) + (P + H)| \\
&= |P + P + H + H| \\
&= |P + P + H| \\
&\leqslant |P + P||H| \\
&\leqslant (2|P| - 1)|H| \\
&\leqslant 2|P||H| \\
&= 2|A|
\end{aligned}$$

Also note for any coset $g + H$, due to the commutativity of our group,

$$\begin{aligned}
P + (g + H) &= (g + P) + H \\
&= g + \left\{x + nd : n \in \{1, ..., |P|\} \text{ and } x, d \in G\right\} + H \\
&= \left\{(g + x) + nd : n \in \{1, ..., |P|\} \text{ and } (g + x), d \in G\right\} + H \\
&= P' + H \text{ where } P' \text{ is an arithmetic progression}
\end{aligned}$$

Thus we will call these types of sets coset progressions.

Example 3.14

Let $G = \mathbb{Z}/64\mathbb{Z} = \{0, 1, ..., 63\}$ (the set of equivalence classes of integers modulo 64). Every set in this example will be a subset of G. Let

$$H = \{0, 8, 16, ..., 56\},\ P = \{7, 8, 9\}.$$

Then

$$|P + H| = |\{7, 15, 23, ..., 63\} \cup \{8, 16, ..., 56, 0\} \cup \{9, 17, ..., 57, 1\}| = 24.$$

Now we have

$$\begin{aligned}(P + H) + (P + H) &= (P + P) + H \\ &= \{14, 15, 16, 17, 18\} + H \\ &= \{14, 22, ..., 62, 6\} \cup \{15, 23, ..., 63, 7\} \cup \cdots \cup \{18, 26, ..., 60, 4, 12\},\end{aligned}$$

and thus $|(P + H) + (P + H)| = 48 = 2|P + H|$.

3.9 Groups with Torsion

We would like to apply Freiman's theorem to some more generalized groups as well. We do actually have a version that suffices for a special class of groups, albeit it takes a slightly different form. Let us introduce a few concepts in group theory to observe this special class.

The order of an element g of a group G is the least positive integer n such that $ng = 0$. The exponent of a group, $\exp(G)$, is the least positive integer n such that $ng = 0$ for all $g \in G$. This may also be found by taking the least common multiple of the orders of all the elements of G. If G is finite, $\exp(G) \leqslant |G|$, but if G is infinite, it does not necessarily mean that there is not an exponent for G.

If there is no exponent of G, we may look at the elements of G that do have a finite order called the torsion of G. The torsion group, $\mathrm{Tor}(G)$, is a subgroup of G (if G is abelian), and it must always exist (as 0 always has a finite order of 1). If 0 is the only element of the torsion group, we say that G is torsion-free.

Example 3.15

- $G = \mathbb{Z}/64\mathbb{Z}$ has an exponent of 64. Essentially if G is a cyclic group, then $\exp(G) = |G|$.
- S_3 is the set of all bijections $f : \{1, 2, 3\} \to \{1, 2, 3\}$ where the group operation is composition. $|S_3| = 6$, but every bijection's order is at most 3.

- $\mathbb{Z}$ clearly has no exponent, and is torsion-free.
- $G = (\mathbb{Z}/2\mathbb{Z})^\infty$ can be thought of as an infinite sequence of 1's and 0's with $1 + 1 = 0$ when adding two sequences. This is an example of an infinite group, yet $\exp(G)$ is only 2.
- $G = \mathbb{Z}/k\mathbb{Z} \times \mathbb{Z}$ (where k is a positive integer) is an example of an infinite group with no exponent that is not torsion-free. $\mathrm{Tor}(G)=\{(x, 0) : x \in \mathbb{Z}/k\mathbb{Z}\}$

We can now state Freiman's theorem for groups with an exponent. The following version was proved by Ruzsa in [**Ruz3**].

Theorem 3.16 (Ruzsa)**.** *Let $A \subseteq G$ be a subset of an abelian group of exponent $r \geqslant 2$. If $|A + A| \leqslant K|A|$, then A is contained in a subgroup $H \leqslant G$ such that*

$$|H| \leqslant f(r, K)|A|$$

where $f(r, K) = K^2 r^{K^4}$.

As shown before, we knew that coset progressions produced small doubling, so A being part of this subgroup H is an example of this. $f(r, K)$ does grow very quickly, just like how our upper bound for Freiman's Theorem for integers was $c < e^{K^{O(1)}}$.

3.10 History

When we discuss additive combinatorics, we normally deal with finite sets. Addition of these sets is a natural step to take, and understanding the fundamentals of the doubling of a set can increase our knowledge in similar areas such as taking the sumset of two different sets. Freiman's Theorem follows clearly from investigating the doubling of a set, but there has been other work to find the dimension and the size of the superset bounds (d and c respectively) present in Freiman's Theorem. Freiman's argument was carried out in a way as to give quantitative bounds by Bilu [**Bil**]. Ruzsa was in fact the first to make some progress for

obtaining good estimates for d and c [**Ruz1**, **Ruz2**]. Chang had some great improvements to these estimates [**Cha**]. Her research implemented many of the ideas of Ruzsa while adding new substantial work such as Chang's Spectral Lemma and Chang's Covering Lemma. We would also like to give credit to Sanders who provided many contributions after Chang [**San**]. Schoen proved the near-optimal bounds with $d = K^{1+o(1)}$ and $c = e^{(1+o(1))K}$ [**Sch**].

4 Green and Tao

4.1 Generalized Arithmetic Progressions

As a quick refresher, let us go over multidimensional arithmetic progressions. A progression P of dimension d is of the form $P = P_1 + P_2 + \cdots + P_d$ where each P_i is an arithmetic progression. Alternatively, we can write

$$P := x_0 + [L_1] \cdot x_1 + [L_2] \cdot x_2 + \cdots + [L_d] \cdot x_d$$

where each $x_i \in \mathbb{Z}$ and $[L_i] = \{0, 1, ..., L_i - 1\}$. The size of P is denoted $||P||$ and $||P|| = |P_1||P_2| \cdots |P_d| = L_1 \cdots L_d$. $|P| = ||P||$ if the sums in P are distinct, and we say P is proper when this happens.

More generally, for $t \in \mathbb{Z}^+$, we say that P is t-proper if all the sums in

$$tP := tx_0 + [tL_1] \cdot x_1 + \cdots + [tL_d] \cdot x_d$$

are distinct. Clearly, P is t-proper for all positive integers when P is a 1-dimensional progression. Another thing we can notice is that, for $t \geqslant 2$, t-proper implies $(t-1)$-proper.

Note tP can also be thought of as "adding" P (or more formally taking the sumset of P) by itself t times

$$tP = P + P + \cdots + P \ (t \text{ times}).$$

Whereas we will use the $\cdot$ symbol in between t and P if we are dilating the set

$$t \cdot P = \{tp : p \in P\}.$$

Example 4.1

$A = \{0, 1, 2, ..., 9\} + \{0, 10, 20, ..., 90\} + \{0, 100, 200, ..., 900\}$ is a 3-dimensional progression. $2A = \{0, 1, 2, ..., 18\} + \{0, 10, 20, ..., 180\} + \{0, 100, 200, ..., 1800\}$ does not have distinct sums, but A does, so A is proper/1-proper.

Let $B = \{3, 4, 5\} + \{10, 20\}$. Before we look at tB, we should note $B = 3 + \{0, 1, 2\} + 10 + \{0, 1\} \cdot 10 = 13 + \{0, 1, 2\} + \{0, 1\} \cdot 10$. Now $4B = 52 + \{0, 1, ..., 8\} + \{0, 1, 2, 3, 4\} \cdot 10$ is proper, so B is 4-proper.

4.2 Freiman Homomorphisms and Dimensions

Recalling from group theory, a group homomorphism $h : G \to G'$ satifies the property, $h(x + y) = h(x) + h(y)$ for all $x, y \in G$. When we are dealing with sumsets, A almost never contains $A + A$, so we need a better way of relating groups. Instead, we will define the Freiman homomorphism.

Definition 4.2 (Freiman Homomorphism)**.** *Given abelian groups G, G' and subsets $A \subseteq G$, $A' \subseteq G'$, the map $h : A \to A'$ is a Freiman homomorphism such that for $a, b, c, d \in A$, if $a + b = c + d$, then $h(a) + h(b) = h(c) + h(d)$.*

We also define h to be Freiman isomorphism if h is a Freiman homomorphism that has an inverse with the same property. With these isomorphisms, we are ready to talk about how we can associate a general arithmetic progression to a single dimension d.

Definition 4.3 (Freiman dimension)**.** *The Freiman dimension $d_F(A)$ of a set A is the largest dimension d for which A is Freiman isomorphic to a subset of $\mathbb{Z}^d$ not contained in a proper affine subspace.*

Example 4.4

A simple example of a Freiman homomorphism is taking any set and having the map z send all values to 0. We then have $z(a) + z(b) = z(c) + z(d) = 0$ for all a, b, c, d in our initial

set, so clearly z is a Freiman homomorphism. This map cannot be an Freiman isomorphism (when our initial set has at least 2 elements) as then z cannot have an inverse.

Let us start with the following sets

$$A = \{0, 1, 2, 30, 31, 32, 60, 61, 62\}$$
$$A' = \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2), (2,0), (2,1), (2,2)\}$$

and have $h : A' \to A$ be the map such that $h((x, y)) = 30x + y$. We can see here that h is a Freiman homomorphism: for example, $(1, 0) + (1, 2) = (2, 1) + (0, 1)$, and applying the transformation we can confirm that $30 + 32 = 61 + 1$.

As the map h is bijective, it does have an inverse, and we can also see that the inverse is a Freiman homomorphism. Thus, h is a Freiman isomorphism. It is also worth noting that $d_F(A) = 2$.

4.3 Freiman's Lemma

An interesting question that arises is whether there is a relationship between doubling and the Freiman dimension. We will see how Freiman's Lemma [**Fre2**] gives us a good bound in terms of our Freiman dimension.

Lemma 4.5 (Freiman's Lemma)**.** *Let $A \subseteq \mathbb{R}^d$ be a finite set such that $|A| = m$ and $d_F(A) = d$. Then*

$$|A + A| \geqslant (d + 1)m - \frac{d(d + 1)}{2}$$

Proof. We will use induction on m. When $m = 2$, it is clear that $d_F(A) = 1$, and $|A + A| = 3 \geqslant (d+1)m - d(d+1)/2$. Now assume that our assumption holds for $m \leqslant k$, and we will prove this for $k + 1$ (note when $|A| \leqslant m$, $d \leqslant m - 1$). Now we consider the convex hull of A and pick any $a_0 \in \mathcal{A}$. Consider $A' = A \backslash \{a_0\}$. Then $|A'| = m$, so the dimension of A' can be d or $d - 1$.

If the dimension is d, consider the $(d-1)$-dimensional supporting hyperplanes of the convex hull A'. Each hyperplane L intersects with with one of the sides of the convex hull where each side's vertices are elements of A', so $|A' \cap L| \geqslant d$. There must be an L specifically where L has a_0 on one side, and all other vertices on the other side or on L. Let's call this supporting hyperplane L_0. Then $a_0 + (A' \cap L_0)$ must disjoint from $A' + A'$. Thus, using the induction hypothesis (and the dimension of A' being d),

$$\begin{aligned}
|A + A| &= |(A' \cup \{a_0\}) + (A' \cup \{a_0\})| \\
&= |A' + A'| + |\{a_0\} + A'| + |\{a_0\} + \{a_0\}| \\
&\geqslant \left((d+1)m - \frac{d(d+1)}{2}\right) + |a_0 + (A' \cap L_0)| + 1 \\
&\geqslant (d+1)m - \frac{d(d+1)}{2} + d + 1 \\
&\geqslant (d+1)(m+1) - \frac{d(d+1)}{2}.
\end{aligned}$$

Now if the dimension is $d-1$, then clearly all of A' is part of a $(d-1)$-dimensional hyperplane, and a_0 is not part of it as $d_F(A) = d$. Hence

$$\begin{aligned}
|A + A| &= |(A' \cup \{a_0\}) + (A' \cup \{a_0\})| \\
&= |A' + A'| + |\{a_0\} + A'| + |\{a_0\} + \{a_0\}| \\
&\geqslant \left(dm - \frac{(d-1)d}{2}\right) + |A'| + 1 \\
&\geqslant dm - \frac{(d-1)d}{2} + m + 1 \\
&= (d+1)m - \frac{(d-1)d}{2} + 1 \\
&= (d+1)m - \frac{(d+1)d}{2} + d + 1 \\
&= (d+1)(m+1) - \frac{d(d+1)}{2}.
\end{aligned}$$

□

We can now relate the Freiman dimension to the doubling constant of a set with the following corollary.

Corollary 4.6. *Given a finite set $A \subseteq \mathbb{R}^d$, and $|A+A| \leqslant K|A|$ with $d_F(A) = d$, we have the inequality $d < 2K$.*

Proof. We have

$$(d+1)m - \frac{d(d+1)}{2} \leqslant |A+A| \ \leqslant K|A|$$

where $|A| = m$. We also know that $d \leqslant |A|$, so

$$\begin{aligned}(d+1)m - \frac{d(d+1)}{2} &\geqslant (d+1)|A| - \frac{|A|(d+1)}{2} \\ &= (d+1)(|A| - |A|/2) \\ &> d(|A|/2).\end{aligned}$$

Thus $d|A|/2 \leqslant |A+A| \leqslant K|A|$, so $d|A|/2 < K|A|$ or $d < 2K$ □

4.4 Discretized Brunn-Minkowski

We have just showed through Freiman's lemma that if it's Freiman's dimension is d with the general progression having size m, then it can be bounded below by $(d+1)m - (d+1)d/2$. We showed in the previous chapter that we could also fit the sumset into a translations of the general progressions, which would bound it above by $2^d m$ where d is just the dimension of the general progression. Both of these concepts will be used to prove a similar version of Freiman's lemma.

First, given sets $A, B \subseteq \mathbb{R}^d$, the sumset $A + B$ still adheres the same rules even when A or B contain an infinite amount of points. The Brunn-Minkowski inequality contains the volume of sumsets and this will be used to proved a discrete variant of Freiman's lemma.

Proposition 4.7 (Brunn-Minkowski inequality)**.** *Suppose that A and B are bounded open sets in $\mathbb{R}^d$. Then*

$$vol(A+B) \geqslant (vol(A)^{1/d} + vol(B)^{1/d})^d.$$

In particular, we have

$$vol(A+B) \geqslant 2^d \min\{vol(A), vol(B)\}.$$

Using this proposition will give us our variant of Freiman's lemma.

Lemma 4.8 (Discretized Brunn-Minkowski)**.** *Let $X, Y \subseteq \mathbb{R}^m$ be finite sets. Then for any $d \leqslant m$, we have*

$$|X+Y+\{0,1\}^d| \geqslant 2^d \min\{|X|, |Y|\},$$

where we embed $\mathbb{Z}^d$ inside $\mathbb{R}^m$ in the obvious manner.

Proof. We will start by assuming that $X, Y \subseteq \mathbb{Z}^d$. Let $A = X + (0,1)^d$ and $B = Y + (0,1)^d$. We see $A \cup B$ this forms at most $|X|+|Y|$ open cubes and equality when X, Y are completely disjoint. Now since X, Y are finite and $(0,1)^d$ is bounded, we may still use associativity when taking sumsets

$$A + B = X + (0,1)^d + Y + (0,1)^d = X + Y + (0,1)^d + (0,1)^d.$$

If we focus on the volume, we can see that

$$\mathrm{vol}((0,1)^d + (0,1)^d) = \mathrm{vol}((0,2)^d) = \mathrm{vol}(\{0,1\}^d + (0,1)^d)$$

and this will give us

$$\mathrm{vol}(A+B) = \mathrm{vol}(X + Y + \{0,1\}^d + (0,1)^d).$$

Using the Brunn-Minkowski inequality and the fact that $\mathrm{vol}(X + (0,1)^d) = |X|$ in $\mathbb{Z}^d$,

$$|X+Y+\{0,1\}^d| \geqslant 2^d \min\{|X|, |Y|\}.$$

Now we can let $X, Y \subseteq \mathbb{R}^d$. We then partition

$$X = X_1 \cup X_2 \cup \cdots \cup X_k \ , \quad Y = Y_1 \cup Y_2 \cup \cdots \cup Y_l$$

where $X_1, X_2, ..., X_k$ are disjoint cosets of $\mathbb{Z}^d$ (as X is finite, all of these are finite) and the same for $Y_1, ..., Y_l$. We can assume that $|X_1| \geqslant |X_i|, |Y_j|$ for all i, j by ordering the size of our disjoint cosets and swapping X, Y if necessary. We have shown that

$$|X_1 + Y_j + \{0,1\}^d| \geqslant 2^d \min\{|X_1|, |Y_j|\} = 2^d |Y_j|,$$

and as Y_j is disjoint for all j, we finally obtain

$$\begin{aligned} |X + Y + \{0,1\}^d| &\geqslant |X_1 + Y + \{0,1\}^d| \\ &= \sum_{j=1}^{l} |X_1 + Y_j + \{0,1\}^d| \\ &= \sum_{j=1}^{l} 2^d \min\{|X_1|, |Y_j|\} \\ &= \sum_{j=1}^{l} 2^d |Y_j| \\ &= 2^d |Y| \\ &= 2^d \min\{|X|, |Y|\}. \end{aligned}$$

□

To show this lemma is sharp, we can just let $X = Y = \{0,1\}^d$, or really any size box $[k]^d$. To create a bound for our sumset with the removal of $\{0,1\}^d$, we will be going back to compressions and a similar concept within a multidimensional space.

4.5 Down-sets

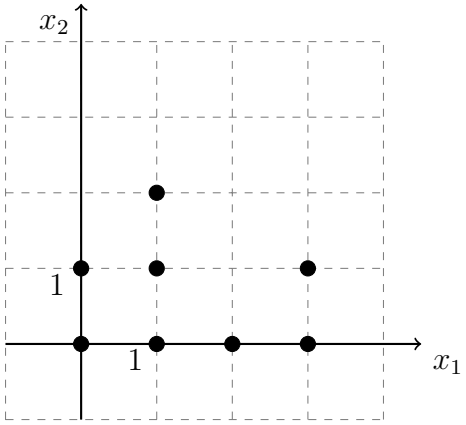
Given $\mathbb{Z}^d$, we will only focus on the closed first orthant for now (where all terms are non-negative) which we will denote $\mathbb{N}_0^d$.

Definition 4.9 (Down-set)**.** *Let $i \leqslant d$ be a positive integer , a set $B \subseteq \mathbb{N}_0^d$ is an i-down-set if $(b_1, ..., b_d) \in B$, then $(b_1, b_2, ..., b_{i-1}, x, b_{i+1}, ..., b_d) \in B$ for all $x \in [b_i]$. B is a down-set if it is an i-down-set for each i.*

Example 4.10

$\{0,1\}^d$, or more generally any cube $[k]^d$, or even more generally any hyperrectangle $[L_1] \times \cdots \times [L_d]$ is clearly a down-set. (Remember the axes must be included for these down-sets.)

Let A be the set of points in the following graph.



Then A is a 2-down-set, but not a 1-down-set (and thus, not a down-set). We would need to add the points $(2,1), (0,2)$ or remove/shift left the points $(1,2), (3,1)$ for A to become a down-set.

Let $B = A \cup \{(2,1), (0,2)\}$. Then this down-set consists of the union of two "filled-in" rectangles (one rectangle has the diagonal from $(0,0)$ to $(1,2)$ and the other from $(0,0)$ to $(3,1)$); both of these filled-in rectangles are clearly down-sets themselves.

One property that can be observed from down-sets is if B is a down-set,

$$(b_1, ..., b_d) \in B \implies \{(x_1, ..., x_d) : x_i \in [b_i],\ \forall i \in \{1, ..., d\}\} \subseteq B.$$

This essentially tells us that if we have a point in our down-set, the hyperrectangle formed with the diagonal from that point to the origin is part of the down-set. This property also shows us that if $A, B \subseteq \mathbb{N}_0^d$ are down-sets, then $A + B$ is a down-set.

Now, as down-sets must contain values on the axes, given a down-set A, shifting one unit "down" or by $-e_i$ for some i creates the same amount of points not in A as shifting one unit up. More generally,

$$|A + \{0, 1\}^d| = |A - \{0, 1\}^d| = \sum_{I \subsetneq \{1,...,d\}} |\pi_I(A)| \tag{10}$$

where $\pi_I(A)$ is the orthongonal projection

$$\pi_I(\sum_{i=1}^{d} a_i e_i) := \sum_{i \in I} a_i e_i.$$

Example 4.11

Letting B be the same set as our previous example. Then

$$\begin{aligned} |\ \big((0,1) + B\big) \backslash B\ | &= |\{(0,3), (1,3), (2,2), (3,2)\}| = 4 \\ |\ \big(B - (0,1)\big) \backslash B\ | &= |\{(0,-1), (1,-1), (2,-1), (3,-1)\}| = 4 \\ |\pi_{\{1\}}(B)| &= |\{(0,0), (1,0), (2,0), (3,0)\}| = 4. \end{aligned}$$

We can apply the same operations for the rest of the points in $\{0, 1\}^d$ and compare to obtain that $|B + \{0, 1\}^2| = |B - \{0, 1\}^2| = \sum_{I \subsetneq \{1,2\}} |\pi_I(B)|$.

Now if we combine (10) and our Discretized Brunn-Minkowski Lemma, we get the following corollary

Corollary 4.12. *Let $X, Y \subseteq \mathbb{N}_0^d$ be down-sets. Then*

$$|X + Y| \geqslant 2^d \min\{|X|, |Y|\} - \sum_{I \subsetneq \{1,\dots,d\}} |\pi_I(X + Y)|.$$

4.6 Compressions and the Down-Set Lemma

Going back full circle, we will use compressions to form a bound for subsets of down-sets. Let us familiar ourselves with compressions in this context.

Definition 4.13 (Compression)**.** *An i-compression $\mathcal{C}_i(A)$ of a set $A \subseteq \mathbb{N}_0^d$ is decreasing all the values of i-th coordinate of each element until this new set forms an i-down-set. Specifically,*

$$\mathcal{C}_i(A) := \Big\{(a_1, ..., a_{i-1}, x_{a_i}, a_{i+1}, ..., a_d) : (a_1, ..., a_d) \in A,$$
$$x_{a_i} \in \big\{0, 1, ..., -1 + \big|\{t : (a_1, ..., a_{i-1}, t, a_{i+1}, ..., a_d) \in A\}\big|\big\}\Big\}.$$

Example 4.14

Let A be our example from Example 4.10. Then as A is a 2-down-set, $\mathcal{C}_2(A) = A$. $\mathcal{C}_1(A) = A\backslash\{(1,2),(3,1)\} \cup \{(0,2),(2,1)\}$.

Let $B = \{(1,0),(0,1),(0,2)\}$. Then $\mathcal{C}_1(B) = \{(0,0),(0,1),(0,2)\}$ and $\mathcal{C}_2(B) = \{(1,0),(0,0),(0,1)\}$. However, both these i-compressions are down-sets, so $\mathcal{C}_2(\mathcal{C}_1(B)) \neq \mathcal{C}_1(\mathcal{C}_2(B))$. This shows us that compressions may not commmute.

We may now observe the following

Lemma 4.15. *Let $X, Y \subseteq \mathbb{N}_0^d$ be down-sets, and let $A \subseteq X$ and $B \subseteq Y$ be arbitrary subsets of these down-sets. Then*

$$|A + B| \geqslant 2^d \min\{|A|, |B|\} - \sum_{I \subsetneq \{1,\dots,d\}} |\pi_I(X + Y)|.$$

Proof. We will need to show one statement first before going about this proof.

Claim: *For every* $i \in \{1, ..., d\}$, $|\mathcal{C}_i(A) + \mathcal{C}_i(B)| \leqslant |A + B|$.

Pick $i \in \{1, ..., d\}$ and let $I = \{1, ..., d\}\backslash\{i\}$ then to prove this, we just need to prove the statement is true for every line in $\mathbb{N}_0^d$ parallel to the x_i-axis or for all $x \in \pi_I(\mathbb{N}_0^d)$,

$$|\big(\mathcal{C}_i(A) + \mathcal{C}_i(B)\big) \cap \pi_I^{-1}(x)| \leqslant |\big(A + B\big) \cap \pi_I^{-1}(x)|.$$

The right-hand side can be written as

$$\left| \bigcup_{y+z=x} \Big(A \cap \pi_I^{-1}(y)\Big) + \Big(B \cap \pi_I^{-1}(z)\Big) \right|$$

Now as our compression only changes the i-th coordinate, if $\alpha \in A, \beta \in B$ such that $(\alpha + \beta)$ in on the line, then applying $\mathcal{C}_i$ and taking the sum must be on the same line still. Taking note of this, we can write the left-hand side as

$$\max\Big\{ \sup_{y+z=x} \big\{|A \cap \pi_I^{-1}(y)| + |B \cap \pi_I^{-1}(z)| - 1\big\}, 0\Big\}.$$

Thus, our claim must be true as for any sets $C, D \subseteq \mathbb{Z}^d$, $|C + D| \geqslant \max\{|C| + |D| - 1, 0\}$.

Now by definition $\mathcal{C}_d...\mathcal{C}_2\mathcal{C}_1(A)$ must be a down-set and $|\mathcal{C}_i(A)| = |A|$, so we have

$$\begin{aligned}
&|A + B| \geqslant |\mathcal{C}_1(A) + \mathcal{C}_1(B)| \geqslant |\mathcal{C}_d...\mathcal{C}_1(A) + \mathcal{C}_d...\mathcal{C}_1(B)| \\
&\geqslant 2^d \min\{|\mathcal{C}_d...\mathcal{C}_1(A)|, |\mathcal{C}_d...\mathcal{C}_1(B)|\} - \sum_{I \subsetneq \{1,...,d\}} |\pi_I(\mathcal{C}_d...\mathcal{C}_1(A) + \mathcal{C}_d...\mathcal{C}_1(B))| \\
&= 2^d \min\{|A|, |B|\} - \sum_{I \subsetneq \{1,...,d\}} |\pi_I(\mathcal{C}_d...\mathcal{C}_1(A) + \mathcal{C}_d...\mathcal{C}_1(B))| \\
&\geqslant 2^d \min\{|A|, |B|\} - \sum_{I \subsetneq \{1,...,d\}} |\pi_I(X + Y)|.
\end{aligned}$$

The last inequality should follow as if $A \subseteq X$ where X is a down-set, then $\mathcal{C}_i(A) \subseteq X$. $\square$

Finally, using this lemma, we can prove this theorem of Green and Tao [**GT**]. Compressions were first used to bound sumsets by Bollobás and Leader [**BL**].

Theorem 4.16 (Green-Tao)**.** *Suppose that* $C \subseteq [L_1] \times \cdots \times [L_d]$*. Then*

$$|C + C| \geqslant 2^d |C| + \prod_{i=1}^{d} (2L_i - 1) - \prod_{i=1}^{d} 2L_i.$$

Proof. From Lemma 4.15, we let $A = B = X = Y = [L_1] \times \cdots \times [L_d] = C$. We have

$$|C + C| \geqslant 2^d |C| - \sum_{I \subsetneq \{1,\ldots,d\}} |\pi_I([2L_1 - 1] \times \cdots \times [2L_d - 1])|.$$

Simplifying the summation then produces our statement. □

We will be using a corollary to this statement however, as the bound follows more logically than the theorem.

Corollary 4.17. *Let* $d \geqslant 1$*, and* $L_1 \geqslant \cdots \geqslant L_d \geqslant 1$ *be integers and suppose* $A \subseteq [L_1] \times \cdots \times [L_d]$*. Then*

$$|A + A| \geqslant 2^d |A| - d2^d L_1 \cdots L_{d-1}.$$

Proof. Rearranging our last two terms in our previous theorem gives us

$$|A + A| \geqslant 2^d |A| - 2^d L_1 \cdots L_d \left(1 - (1 - \frac{1}{2L_1}) \cdots (1 - \frac{1}{2L_d})\right).$$

It is not hard to verify that for all $x \in (0, 1]$, $1 - \frac{x}{2} \geqslant e^{-x}$, so this gives us

$$(1 - \frac{1}{2L_1}) \cdots (1 - \frac{1}{2L_d}) \geqslant \exp\left(-\frac{1}{L_1} - \cdots - \frac{1}{L_d}\right) \geqslant \exp(-\frac{d}{L_d}) \geqslant 1 - \frac{d}{L_d}.$$

The final inequality comes from the fact that $e^x \geqslant 1 + x$.

Thus, we have

$$\begin{aligned}
|A+A| &\geqslant 2^d|A| - \prod_{i=1}^{d}(2L_i-1) - \prod_{i=1}^{d} 2L_i \\
&= 2^d|A| - 2^d L_1 \cdots L_d \left(1 - (1-\frac{1}{2L_1}) \cdots (1-\frac{1}{2L_d})\right) \\
&\geqslant 2^d|A| - 2^d L_1 \cdots L_d \left(1 - (1-\frac{d}{L_d})\right) \\
&\geqslant 2^d|A| - d2^d L_1 \cdots L_{d-1}.
\end{aligned}$$

□

Do note the order of $L_1, ..., L_{d-1}$ does not affect the corollary itself, so we really only need that L_d is the no bigger than any of the other integers $L_1, ..., L_{d-1}$.

4.7 Introduction to the Green-Tao Result

We are going to work through a few more examples and theorems to introduce us to the Green-Tao theorem.

First, our goal is to discuss Freiman's Theorem, and the estimates surrounding it, so let us re-state it here.

Theorem 3.5 (Freiman)**.** *Let $A \subseteq \mathbb{Z}$. If $|A+A| \leqslant K|A|$, then there exists functions $d(K) : \mathbb{R} \to \mathbb{Z}^+$ and $c(K) : \mathbb{R} \to \mathbb{Z}^+$ such that $P \supseteq A$ is an n-dimensional progression such that $n \leqslant d(K)$ and $||P|| \leqslant c(K)|A|$.*

Example 4.18

Let n be a positive integer, $P = \{1, \ldots, n\}$, and G a geometric progression of size n and a common ratio of n^2. Then let

$$A = P + G.$$

We then have

$$|A| = |P||G| = n^2$$

and

$$|A+A| = |P+P+G+G| \leqslant |P+P||G+G| \leqslant 2n \cdot n^2 = 2n|A|.$$

Now we will let $K = 2n$.

If we want to contain A in a generalised arithmetic progression (that is not huge relative to the size to A) we need to first put G in a generalised arithmetic progression. The best way this can be done is not that different to containing G in a proper generalised arithmetic progression Q of dimension n and size 2^n similar to Example 3.8. Then

$$A \subseteq P + Q.$$

$P + Q$ is a generalised arithmetic progression of dimension $1 + n \geqslant \frac{K}{2}$ and size $n \cdot 2^n = 2^{(1+o(1))K}|A|$.

Schoen has proved the values of d and c for these arbitrary sets that are very similar to those above [**Sch**].

Theorem 4.19 (Schoen)**.** *Each set $A \subseteq \mathbb{Z}$ satisfying $|A+A| \leqslant K|A|$ is contained in a generalized arithmetic progression of dimension at most $d(K)$ and size at most $C(K)|A|$ with*

$$d(K) = K^{1+o(1)} \text{ and } C(K) = \exp((1+o(1))K).$$

Using this theorem along with the work of Bilu and Chang we can ensure that the progression in t-proper and that $d(K) \leqslant 2K$, at a relatively small cost in the bound of $C(K)$. This was noted in the paper of Green and Tao. In fact $d(K)$ is bounded above by the Freiman dimension $d_F(A)$ of the size A. In Section 4.2 Freiman dimension is introduced and it is shown in Corollary 4.6 that it is at most $2K$.

Theorem 4.20 (Schoen)**.** *There exists an absolute constant c with the following property: For every integer $t \geqslant 1$, each set $A \subseteq \mathbb{Z}$ satisfying $|A+A| \leqslant K|A|$ is contained in a t-proper*

generalized arithmetic progression of dimension at most $d(K)$ and size at most $C(K)|A|$ with

$$d(K) = 2K \text{ and } C(K) = \exp(c\log(K)K) = K^{cK}.$$

This is not always an efficient way to contain A, as Example 4.18 shows. A question that has been studied is if we can create a more efficient covering of A by using more than one generalised arithmetic progression. The following variation of Example 4.18 is indicative.

Example 4.21

Let n be a positive integer, $\ell = \lfloor \log_2(n) \rfloor$, P be a proper generalized arithmetic progression of dimension ℓ and size n, and G be a geometric progression of size n and common ratio of (range $P)^2$. Set

$$A = P + G.$$

We have

$$|A| = |P||G| = n^2$$

and

$$|A + A| = |P + P + G + G| \leqslant |P + P||G + G| \leqslant 2^\ell n \cdot n^2 = n^2|A|.$$

So we may take $K = n^2$.

Then we have

$$A = \bigcup_{g \in G} g + P$$

being covered by $n = \sqrt{K}$ arithmetic progressions of dimension $\ell = \lfloor \log_2(K) \rfloor / 2$.

Green and Tao proved a result for general sets with similar dependencies on the dimension of generalised arithmetic progressions needed to cover A but worse dependency on the number of progressions [**GT**]. A crucial step in their argument uses compressions, relating Freiman's theorem to the material in Chapter 3.

Theorem 4.22 (Green-Tao)**.** *There exists an absolute constant c with the following property: Each set $A \subseteq \mathbb{Z}$ satisfying $|A + A| \leqslant K|A|$ is contained in at most $e^{c\log(K)K^2}$ generalized arithmetic progressions of dimension at most $\log_2(K)$.*

An example in [**LR**] shows that for general sets at least $K^{\log\log(K)}$ progressions of dimension $\log(K)$ are necessary and not a polynomial in K number, as Example 4.21 may suggest. Green and Tao's paper has weaker bounds because they use a theorem of Chang [**Cha**] instead of Schoen's stronger result that was published later. It should be clear to require the progression to have size at most $|A|$.

4.8 Proof of the Green-Tao Result

Sketch of proof of Theorem 4.22 from Theorem 4.16. In this sketch we do not make use of Freiman isomorphisms and so identify boxes $[L_1] \times \cdots \times [L_d]$ with generalized arithmetic progressions $P_1 + \cdots + P_d$ (where $|P_i| = L_i$).

By Theorem 4.20 for $t = 2$ we have

$$A \subseteq P_1 + \cdots + P_d$$

with $d = 2K$, $|P_1| \ldots |P_d| \leqslant |A|e^{c\log(K)K}$, and $P_1 + \cdots + P_d$ is 2-proper. We further assume that $|P_1| \geqslant \cdots \geqslant |P_d|$ and set $L_i = |P_i|$. We also let $\ell = \lfloor \log_2(K) \rfloor$.

For each $x \in P_{\ell+2} + \cdots + P_d$ define

$$A_x = A \cap (P_1 + \cdots + P_{\ell+1} + x).$$

Note that

$$A = \bigcup_x A_x,$$

that

$$A + A \supseteq \bigcup_x (A_x + A_x)$$

and that the $A_x + A_x$ are distinct (because the progression is 2-proper). Hence

$$|A + A| \geqslant \sum_x |A_x + A_x|.$$

By Corollary 4.17 we have that for each x

$$|A_x + A_x| \geqslant 2^{\ell+1}|A_x| - (\ell+1)2^{\ell+1}L_1 \dots L_\ell.$$

Summing over all $x \in P_{\ell+2} + \dots + P_d$ gives

$$\begin{aligned} |A + A| &\geqslant 2^{\ell+1}\sum_x |A_x| - (\ell+1)2^{\ell+1}L_1 \dots L_\ell L_{\ell+2} \dots L_d \\ &\geqslant 2K|A| - (\ell+1)2^{\ell+1}L_1 \dots L_\ell L_{\ell+2} \dots L_d. \end{aligned}$$

Since $|A + A| \leqslant K|A|$ we get

$$K|A| \leqslant (\ell+1)2^{\ell+1}\frac{L_1 \dots L_d}{L_{\ell+1}} \leqslant 4\frac{\log(K)Ke^{c\log(K)K}}{L_{\ell+1}}|A|.$$

Therefore, for some new c,

$$L_{\ell+1} \leqslant e^{c\log(K)K}.$$

By monotonicity of the L_i we get, for some new c,

$$L_{\ell+1} \dots L_d \leqslant e^{c\log(K)K^2}.$$

Thus $|P_{\ell+1} + \dots P_d| \leqslant e^{c\log(K)K^2}$ and therefore A can be covered by $e^{c\log(K)K^2}$ translates of $P_1 + \dots + P_\ell$, a generalized arithmetic progression of dimension $\lfloor \log_2(K) \rfloor$. □

References

[Bil] Y. Bilu, Structure of sets with small sumset. Structure theory of set addition. Astérisque No. 258 (1999), xi, 77–108.

[Bol] B. Bollobás, Combinatorics. Set systems, hypergraphs, families of vectors and combinatorial probability. Cambridge University Press, Cambridge, 1986.

[BL] B. Bollobás and I. Leader, Sums in the grid. Discrete Math. 162 (1996), no. 1-3, 31–48.

[Cha] M.-C. Chang, A polynomial bound in Freiman's theorem. (English summary) Duke Math. J. 113 (2002), no. 3, 399–419.

[EGM] S. Eberhard, and B. Green, and F. Manners, Sets of integers with no large sum-free subset. Ann. of Math. (2) 180 (2014), no. 2, 621–652.

[Fra] P. Frankl, A new short proof for the Kruskal-Katona theorem. Discrete Math. 48 (1984), no. 2-3, 327–329.

[Fre1] G. A. Freiman, The addition of finite sets. I. (Russian) Izv. Vysš. Učebn. Zaved. Matematika 1959 1959 no. 6 (13), 202–213.

[Fre2] G. A. Freiman, Foundations of a structural theory of set addition. Translated from the Russian. Translations of Mathematical Monographs, Vol 37. American Mathematical Society, Providence, R. I., 1973.

[GT] B. Green and T. Tao, Compressions, convex geometry and the Freiman-Bilu theorem. Q. J. Math. 57 (2006), no. 4, 495–504.

[Kat] G. Katona, A theorem of finite sets. Theory of graphs (Proc. Colloq., Tihany, 1966), pp. 187–207. Academic Press, New York, 1968.

[Kru] J. B. Kruskal, The number of simplices in a complex. 1963 Mathematical optimization techniques pp. 251–278 Univ. of California Press, Berkeley, Calif.

[LR] S. Lovett and O. Regev, A counterexample to a strong variant of the polynomial Freiman-Ruzsa conjecture in Euclidean space. Discrete Anal. 2017, Paper No. 8, 6 pp.

[Lub] D. Lubell, A short proof of Sperner's lemma. J. Combinatorial Theory 1 (1966), 299.

[Mes] L. D. Mešalkin, A generalization of Sperner's theorem on the number of subsets of a finite set. Teor. Verojatnost. i Primenen 8 1963 219–220.

[Ruz1] I. Z. Ruzsa, Arithmetical progressions and the number of sums. Period. Math. Hungar. 25 (1992), no. 1, 105–111.

[Ruz2] I. Z. Ruzsa, Generalized arithmetical progressions and sumsets. Acta Math. Hungar. 65 (1994), no. 4, 379–388.

[Ruz3] I. Z. Ruzsa, Sumsets and structure. Combinatorial number theory and additive group theory, 87–210, Adv. Courses Math. CRM Barcelona, Birkhäuser Verlag, Basel, 2009.

[San] T. Sanders, Appendix to: "Roth's theorem on progressions revisited" [J. Anal. Math. 104 (2008), 155–192; MR2403433] by J. Bourgain. J. Anal. Math. 104 (2008), 193–206.

[Sch] T. Schoen, Near optimal bounds in Freiman's theorem. Duke Math. J. 158 (2011), no. 1, 1–12.

[Yam] K. Yamamoto, Logarithmic order of free distributive lattice. J. Math. Soc. Japan 6 (1954), 343–353.