SET IMAGES AND CONVEXITY PROPERTIES OF CONVOLUTIONS FOR SUM SETS AND DIFFERENCE SETS

A Dissertation
Presented to
The Academic Faculty

By

Chi-Nuo Lee

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy in the
School of Mathematics
College of Sciences

Georgia Institute of Technology

August 2023

SET IMAGES AND CONVEXITY PROPERTIES OF CONVOLUTIONS FOR SUM SETS AND DIFFERENCE SETS

Thesis committee:

Dr. Ernie Croot, Advisor
School of Mathematics
Georgia Institute of Technology

Dr. Anton Leykin
School of Mathematics
Georgia Institute of Technology

Dr. Michael Lacey
School of Mathematics
Georgia Institute of Technology

Dr. Will Perkins
School of Computer Science
Georgia Institute of Technology

Dr. Josephine Yu
School of Mathematics
Georgia Institute of Technology

Date approved: June 23, 2023

ACKNOWLEDGMENTS

I have the deepest gratitude for my advisor, Ernie Croot. His brilliance and kindness has helped me immensely. My family and friends have been supportive and caring along the way; without them I would not be able to do any of this. I would like to express my love for them. Thank you to the faculty and colleagues at Georgia Tech, I've learned so much in the past years.

Finally, special thanks to Terence Coelho, Emmanuel Yuan, and Kevin Chang.

TABLE OF CONTENTS

Acknowledgments iii

Chapter 1: Introduction 1

1.1 Preliminaries 1

1.2 Motivation - Connection to Roth's Theorem 6

1.3 Overview 9

Chapter 2: Set Images of Convolutions at Independent Sets 11

2.1 Set Image of Independent Sets 15

2.1.1 Set Image for Difference Sets 16

2.1.2 Set Image for Sum Sets 22

Chapter 3: Set Images of Convolutions at Arithmetic Progressions 31

3.1 A Recurrence Relation for Distribution of Convolution at Arithmetic Progressions 31

3.1.1 A Recurrence Relation for Sum Sets 31

3.1.2 A Recurrence Relation for Difference Sets 37

3.2 Convexity Sum Sets in 2d 42

Chapter 4: A Smoothness Property of Convolution 64

4.1 Preliminaries 64

4.1.1 Fourier Analysis Preliminaries 65

4.2 A Smoothness Property of 4-fold Convolution 67

4.3 Construction on the Bounds of the Smoothness Property 73

4.3.1 Intersections of many faces of a Cross-polytope 77

Appendices 84

Appendix A: Notation 85

Appendix B: Comparison of C_0^1 and S_0^1 86

Appendix C: Subsets and $1_A * 1_{-A}(0, 1, 2)$ 90

References 91

SUMMARY

Many recent breakthroughs in additive combinatorics, such as results relating to Roth's theorem or inverse sum set theorems, utilize a combination of Fourier analytical and physical methods. Physical methods refer to results relating to the physical space, such as almost-periodicity results regarding convolutions. This thesis will focus on the properties of convolutions.

Given an abelian group G and sets $A \subseteq G$, we study the properties of the convolution for sum sets and difference sets, $1_A * 1_A$ and $1_A * 1_{-A}$. Given $\boldsymbol{x} \in G^n$, we consider its corresponding *set image* of the sum set, the image of $f(A) := 1_A * 1_A(\boldsymbol{x})$, and the similarly defined set image of the difference set. We break down the study of set images into two cases, when $\boldsymbol{x}$ is independent, and when $\boldsymbol{x}$ is an arithmetic progression. In both cases, we provide some convexity result for the set image of both the sum set and difference set. For the case of the arithmetic progression, we prove convexity by first showing a recurrence relation for the distribution of the convolution.

Finally, we prove a smoothness property regarding 4-fold convolutions $1_A * 1_A * 1_A * 1_A$. We then construct different examples to better understand possible bounds for the smoothness property in the case of 2-fold convolutions $1_A * 1_A$.

CHAPTER 1
INTRODUCTION

1.1 Preliminaries

Given subsets of a group G, additive combinatorics is interested in understanding the "additive structure" of a set. This thesis will study the additive structure of sets through the notion of convolutions. To understand this idea, we must first define the fundamental concept of sum sets and difference sets [26].

Definition 1.1 (Sum Set and Difference Set)**.** Let G be Abelian group. Let $A, B \subseteq G$. Define the sum set

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

and difference set

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

G is referred to as the ambient group. For this thesis, all ambient groups G referenced are abelian. The difference set is not to be confused with set difference, which is denoted as $A \setminus B := \{a \in A : a \notin B\}$. For an element $a \in G$, we denote

$$a + B := \{a\} + B = \{a + b : b \in B\}$$

as the translation of B by the element a.

It is often useful to identify a set A with its corresponding characteristic function. This will allow us to view the sum set with the lens of convolutions, and utilize Fourier analysis techniques.

Definition 1.2 (Characteristic Function)**.** For a set $A \subseteq G$, the corresponding characteristic

function is defined as

$$1_A(x) := \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A. \end{cases}$$

In literature, $1_A(x)$ is sometimes notated as $A(x)$.

For finite abelian groups G, we may define the convolution of two functions as the following:

Definition 1.3 (Convolution)**.** Given functions $f, g : G \to \mathbb{C}$, we define the convolution of the two functions as

$$f * g(x) := \sum_{y \in G} f(y)g(x-y).$$

Let $\boldsymbol{x} \in G^n$ be a sequence. For convenience, all the following will denote the same thing:

$$1_A * 1_B(\boldsymbol{x}) = 1_A * 1_B(x_1, x_2, ..., x_n) = (1_A * 1_B(x_1), 1_A * 1_B(x_2), ..., 1_A * 1_B(x_n)).$$

The significance of convolutions to additive combinatorics is the following [25]: Given subsets A, B, the convolution of characteristic functions is

$$1_A * 1_B(x) = \sum_{y \in G} 1_A(y)1_B(x-y) = |\{(a,b) \in A \times B : a + b = x\}|. \tag{1.1}$$

The convolution of characteristic functions is the *representations* of x, the number of $a \in A, b \in B$ such that $a + b = x$. Therefore, the support of $1_A * 1_B(x)$ is exactly the sum set $A + B$, and the support of $1_A * 1_{-B}(x)$ is exactly the difference set $A - B$. These two functions will be our main object of study.

Given the function $1_A * 1_A(\cdot)$ and a fix $\boldsymbol{x} \in G^n$, we may view $1_A * 1_A(\boldsymbol{x})$ as a function of A. In this case, we are interested in understanding its corresponding *set image*.

Definition 1.4 (Set Image of $1_A * 1_A(\boldsymbol{x})$ and $1_A * 1_{-A}(\boldsymbol{x})$)**.** Given $\boldsymbol{x} \in G^n$, let $f_1, f_2 : \mathcal{P}(G) \to \mathbb{Z}^n$ be defined as

$$f_1(A) := 1_A * 1_A(\boldsymbol{x}), f_2(A) := 1_A * 1_{-A}(\boldsymbol{x}).$$

We call the image of f_1 the *set image* of $1_A * 1_A(\boldsymbol{x})$, and the image of f_2 the *set image* of $1_A * 1_{-A}(\boldsymbol{x})$.

An alternative way to view the set image is by viewing $1_A * 1_A(\boldsymbol{x})$ as a random variable. Given $\boldsymbol{x} \in G^n$, let A be a randomly chosen subset of G, let $1_A * 1_A(\boldsymbol{x})$ and $1_A * 1_{-A}(\boldsymbol{x})$ be random variables. The *set image* of $1_A * 1_A(\boldsymbol{x})$ and $1_A * 1_{-A}(\boldsymbol{x})$ is then the support of its density function.

An important tool that we will use is the Freiman homomorphism, which allows us to map sets to different ambient groups while maintaining their additive structure.

Definition 1.5 (Freiman Homomorphisms)**.** Let $A \subseteq G_1, B \subseteq G_2$ be subsets of abelian groups G_1, G_2. A *Freiman homomorphism of order k* is a mapping $\phi : A \to B$ such that

$$a_1 + ... + a_k = a'_1 + ... + a'_k \Longrightarrow \phi(a_1) + ... + \phi(a_k) = \phi(a'_1) + ... + \phi(a'_k)$$

for all $a_1, ..., a_k, a'_1, ..., a'_k \in A$. If there exists an inverse map $\phi^{-1} : B \to A$, which is also a Freiman homomorphism of order k, then ϕ is called a Freiman isomomorphism of order k, and A, B is Freiman isomomorphic of order k.

A Freiman homomorphism of order k is also conveniently refered to as a Freiman k-homomorphism. Note that a Freiman k-homomorphism is also a Freiman homomorphism of any order less than k. This is because if ϕ is a Frieman k-homomorphism, for any $a_1, ..., a_k, a'_1, ..., a'_k$ such that

$$a_1 + ... + a_{k-1} = a'_1 + ... + a'_{k-1},$$

then

$$a_1 + ... + a_{k_1} + 0 = a'_1 + ... + a'_{k-1} + 0$$

implies

$$\phi(a_1) + ... + \phi(a_{k-1}) + \phi(0) = \phi(a'_1) + ... + \phi(a'_{k-1}) + \phi(0)$$

$$\phi(a_1) + ... + \phi(a_{k-1}) = \phi(a'_1) + ... + \phi(a'_{k-1}).$$

Thus ϕ is a Frieman $(k-1)$-homomorphism. Note that group homomorphisms, linear transformations, or a translation by a element are all Frieman homomorphisms of arbitrary order.

Freiman isomorphisms preserve the additive structure, thus preserve the convolution and its set image in the following way:

Proposition 1.6 (Freiman Isomorphisms Preserve Convolution)**.** Let $\phi : S_1 \to S_2$ be a Freiman k-isomophism, then for all $x_1, ..., x_k \in S_1, A_1, A_2, ..., A_k \subseteq S_1$

$$1_{A_1} * 1_{A_2} \dots 1_{A_{k-1}} * 1_{A_k}(x_1 + ... + x_k)$$

$$= 1_{\phi(A_1)} * 1_{\phi(A_2)} \dots 1_{\phi(A_{k-1})} * 1_{\phi(A_k)}(\phi(x_1) + ... + \phi(x_k)).$$

Proof. By Eq. (1.1),

$$1_{A_1} * 1_{A_2} \dots 1_{A_{k-1}} * 1_{A_k}(x_1 + ... + x_k)$$

$$= |\{(a_1, ..., a_k) : \forall 1 \leq i \leq k, a_i \in A_i, a_1 + ... + a_k = x_1 + ... + x_k\}|$$

$$= |\{(\phi(a_1), ..., \phi(a_k)) : \forall 1 \leq i \leq k, \phi(a_i) \in \phi(A_i), \phi(a_1)+...+\phi(a_k) = \phi(x_1)+...+\phi(x_k)\}|$$

$$= 1_{\phi(A_1)} * 1_{\phi(A_2)} \dots 1_{\phi(A_{k-1})} * 1_{\phi(A_k)}(\phi(x_1) + ... + \phi(x_k)).$$

□

Proposition 1.7 (Freiman Isomorphisms Preserve Set Image)**.** Let $\phi : G \to G$ be a Freiman 2-isomorphism that maps a group to itself. For any $\boldsymbol{x} + \boldsymbol{y} = \boldsymbol{z} \in G^n$, the set image of

$1_A * 1_A(\boldsymbol{z})$ is the same as the set image of $1_A * 1_A(\phi(\boldsymbol{x}) + \phi(\boldsymbol{y}))$. If $\phi(-g) = -\phi(g)$ for all $g \in G$, then the set image of $1_A * 1_{-A}(\boldsymbol{z})$ is the same as the set image of $1_A * 1_{-A}(\phi(\boldsymbol{x}) + \phi(\boldsymbol{y}))$.

Proof. Let $\phi : G \to G$ be a Freiman 2-isomorphism. Then, by Proposition 1.6,

$$1_A * 1_A(\boldsymbol{z}) = 1_{\phi(A)} * 1_{\phi(A)}(\phi(\boldsymbol{x}) + \phi(\boldsymbol{y})).$$

Since ϕ is a bijection on G, the image of

$$f(A) := 1_{\phi(A)} * 1_{\phi(A)}(\phi(\boldsymbol{x}) + \phi(\boldsymbol{y}))$$

is equivalent to the image of

$$g(A) := 1_A * 1_A(\phi(\boldsymbol{x}) + \phi(\boldsymbol{y})).$$

Thus, the set images $1_A * 1_A(\boldsymbol{z})$ are equal to the set image of $1_A * 1_A(\phi(\boldsymbol{x}) + \phi(\boldsymbol{y}))$. If $\phi(-g) = -\phi(g)$ for all $g \in G$, then $\phi(-A) = -\phi(A)$, so

$$1_A * 1_A(\boldsymbol{z}) = 1_{\phi(A)} * 1_{\phi(-A)}(\phi(\boldsymbol{x}) + \phi(\boldsymbol{y})) = 1_{\phi(A)} * 1_{-\phi(A)}(\phi(\boldsymbol{x}) + \phi(\boldsymbol{y})).$$

As before, ϕ is a bijection on G so the set images $1_A * 1_{-A}(\boldsymbol{z})$ is equal to the set image of $1_A * 1_{-A}(\phi(\boldsymbol{x}) + \phi(\boldsymbol{y}))$. □

Lastly, this thesis will utilize big O notations.

Definition 1.8 (Big O Notation)**.** Let f, g be real valued function. We write $f(x) = O(g(x))$ if there exists M, x_0 such that $|f| \leq Mg(x)$ for all $x \geq x_o$. We write $f(x) = o(g(x))$ if there exists x_0 such that for all $\epsilon > 0$, $|f| \leq \epsilon g(x)$ for all $x \geq x_o$. We write $f \sim g$ if $f(x) = O(g(x))$ and $g(x) = O(f(x))$.

In this section, we've provided a very abridged version of these concepts, taking only the portions that are relevant to us. Those interested in a more comprehensive exposition may refer to the prologue, chapter 4, and chapter 5 of [26], on which many of the notations here are based.

1.2 Motivation - Connection to Roth's Theorem

This thesis will focus on the properties of $1_A * 1_A$ and $1_A * 1_{-A}$. These studies of convolutions are motivated by the utility of physical methods in combination with Fourier analytic methods in different additive combinatorics problems. Physical methods refer to ones that do not use Fourier transforms, and instead look at the convolution or sum sets. One such important topic is Roth's theorem on three-term arithmetic progressions in the integers.

Theorem 1.9 (Roth's Theorem [18])**.** Let $r_3(N)$ denote the size of the largest subset of $[0, N] \subseteq \mathbb{Z}$ that does not contain three-term arithmetic progressions, then

$$r_3(N) = o(N).$$

There has been considerable effort in trying to improve the upper bound of $r_3(N)$. Roth's original proof showed that

$$r_3(N) = O(N/\log\log N).$$

Heath-Brown [14] showed that there exists a constant c such that the upper bound is

$$r_3(N) = O(N/(\log N)^c).$$

Bourgain [6] then obtained

$$r_3(N) = O(N(\log\log N/\log N)^{1/2}).$$

The proofs above mainly utilize some adaptation of Fourier-analytic and Hardy-Littlewood circle methods.

The first proof to show that $r_3(N) = N/(\log N)^{1-o(1)}$ is by Sanders [20]. The proof utilizes the almost-periodicity result for convolutions, which was introduced by Croot and Sisask [8]. Bloom and Sisask [2] [4], and later Schoen [23] all have bounds of the form $N/(\log N)^{1-o(1)}$, with different improvements on the $o(1)$. The first bound that beats the logarithmic density is given by Bloom and Sisask [3], which gives

$$r_3(N) = O(N/(\log N)^{1+c}) \tag{1.2}$$

for some constant c. The current best known bounds is given by Kelley and Meka [15] [5], which gives

$$r_3(N) \leq N/e^{c(\log N)^{1/11}}$$

for some constant c.

All recent bound improvements utilize almost-periodicity results. Thus, we see the importance of combining Fourier-analytic with physical methods in these proofs. Here we provide one of the almost-periodicity type result utilized in [15], which comes from [24].

Theorem 1.10 (Almost-periodicity)**.** If $A_1, A_2, S \subseteq \mathbb{F}_q^n$ are such that A_1 and A_2 both have density at least α, then there is a subspace V of codimension

$$\operatorname{codim}(V) \ll_\epsilon (\log(2/\alpha))^4$$

such that

$$|\langle \mu_V * \mu_{A_1} * \mu_{A_2}, 1_S \rangle - \langle \mu_{A_1} * \mu_{A_2}, 1_S \rangle| \leq \epsilon.$$

Here $\mu_A := |A|^{-1} 1_A$ is the normalised characteristic function. Almost periodicity has also seen utility in Sander's work in inverse sumset theorems [21, 22].

In terms of the lower bound of $r_3(N)$, there has been construction of large sets without

three-term arithmetic progressions. One of such sets is the famous construction of Behrend [1]. The construction utilizes the geometric observation that spheres contain no three points that are collinear, and thus have no three-term arithmetic progressions. One can map a sphere in $\mathbb{Z}^n$ to $\mathbb{Z}$ with the appropriate Freiman 2-isomorphism to get the bounds of

$$r_3(N) \gg \frac{1}{\log^{1/4} N} \cdot \frac{N}{2^{2\sqrt{2}\sqrt{\log_2 N}}}.$$

Elkin [9] was able to improve the bound to

$$r_3(N) \gg \log^{1/4} N \cdot \frac{N}{2^{2\sqrt{2}\sqrt{\log_2 N}}}.$$

Here $\log_2$ denotes $\log$ base 2. The bounds here are calculated in [13]. Note that in both cases, the bounds are of the form $N/e^{c(\log N)^{1/2}}$ for some constant c. Behrend's original construction was in 1946; the lack of improvement over 70 years suggests that this may be close to the actual asymptotic behavior of $r_3(N)$. Indeed, Eq. (1.2) shows that the upper bound has a $1/11$ as the exponent compared to the lower bounds $1/2$.

Many of the upper bound proofs first solve analogous problems in finite fields $\mathbb{F}_p^n$ before relating it back to $\mathbb{Z}$. Thus, there is interest in the bounds for $r_3(\mathbb{F}_p^n)$, the size of the largest set in $\mathbb{F}_p^n$ that does not contain three-term arithmetic progressions. In the case of $p = 3$, this is referred to as the cap set problem. The current best upper bound for $r_3(\mathbb{F}_3^n)$ is $O(2.756^n)$, proved by Ellenberg and Gijswijt in [10, 27], and utilized the polynomial method developed by Croot, Lev, and Pach in [7]. Though these polynomial methods are the best methods in the finite field setting, they do not translate well into $\mathbb{Z}$. Thus the best bounds for $r_3(N)$ still use Fourier-analytic and almost-periodicity ideas. The current best lower bound is $O(2.218^n)$ given by Tyrell [28].

The examples above demonstrate convolutions as one of the key objects in solving these problems. Now we give a brief discussion on $1_A * 1_A$ to provide some intuition. Let $\boldsymbol{x} \in G^n$ be fixed. Given a random set A, perhaps of some density δ, what does the probability

distribution for the random variable $1_A * 1_A(\boldsymbol{x})$ look like? Here are some intuition for the case $G = \mathbb{Z}_N$, when the x_i's are random and "independent" from each other: For N odd, $\frac{x_i}{2}$ exists. For each $1_A * 1_A(x_i)$, if both $\frac{x_i}{2} \pm g$ is in A for some $g \in G$, that contributes 2 to $1_A * 1_A(x_i)$. The contribution of each g is a Bernoulli random variable. Thus, the random variable is $1_A * 1_A(x_i) = 2B(\frac{n-1}{2}, \delta^2) + B(1, \delta)$, where B is the binomial random variable. Here the term $B(1, \delta)$ is contributed by $g = 0$.

For N even, if x_i is even, we also consider $\frac{x_i}{2} \pm g$. Thus the random variable is $1_A * 1_A(x_i) = 2B(\frac{n}{2}-1, \delta^2)+B(2, \delta)$. Here the term $B(2, \delta))$ is contributed by $g = 0, \frac{n}{2}$. If x_i is odd, we consider $\frac{x_i+1}{2} + g, \frac{x_i-1}{2} - g$. Thus, the random variable is $1_A * 1_A(x_i) = 2B(\frac{n}{2}, \delta^2)$.

In each dimension, the random variable is approximately binomial. Thus if each x_i is "independent" from each other, we expect $1_A * 1_A(\boldsymbol{x})$ to approximate a normal distribution, with small "fluctuations" due to parity. However, these type of heuristics do not tell us what the convolution is like at extreme points, such as sets where certain convolutions are unusually large or unusually small. We will devote most of the thesis in trying to understand such extreme points, as boundaries of the set image.

1.3 Overview

Now we give a quick overview of the structure of the thesis. Chapter 2 is focused on understanding the set images of convolutions when evaluated at an "independent" set. We will first prove that the set image for the difference set is approximately a convex polytope, and that each coordinate of the convolution is independent from each other. We then prove that the exact same thing is true for sum set. We then map the result from general abelian groups to $\mathbb{Z}$ and finite fields.

Chapter 3 will first establish a recurrence relation for the distribution of convolution in the interval $(0, 1, ..., n)$. We will use this recurrence relation to prove that for the 2 dimensional case, the set image for the sum set is nearly a convex polytope. We will then prove that for the 3 dimensional case, the set image for the difference is nearly a convex polytope.

Chapter 4 will deviate from the previous studies of set images, and consider a smoothness property of 4-fold convolutions. This 4-fold convolutions result is reminiscent of some of the results relating Roth's theorem and inverse sum set theorems. We will then construct some examples to better understand the bounds on these smoothness properties.

CHAPTER 2

SET IMAGES OF CONVOLUTIONS AT INDEPENDENT SETS

In this chapter, for an additive group G, we are interested in understanding the set image of the random variable $1_A * 1_A(\boldsymbol{x})$ and $1_A * 1_{-A}(\boldsymbol{x})$. We look at two particular cases. On one extreme, $\boldsymbol{x}$ is an "independent" set. Here, as we are concerned with general finite abelian groups, "independent" does not refer to linear independence, but is tangentially related. We will rigorously define independence later. We show that for $\boldsymbol{x}$ that is "independent," each dimension of the set image is also independent from one another. On the other extreme, $\boldsymbol{x}$ is an arithmetic progression. In this case, the dimensions of $\boldsymbol{x}$ is no longer independent from each other. This case will be handled in the next chapter.

We will first describe a lemma that allows us to map sets from a cyclic group to $\mathbb{Z}$, or a larger cyclic group, while preserving its density and relative size of convolution. By taking sets from a smaller cyclic group and tiling $\mathbb{Z}$ or a bigger cyclic group, we get a new set where the density and convolutions are roughly preserved.

Lemma 2.1 (Tiling for Sum Sets)**.** Let $N_1 \leq N_2$. For any $A, B \subseteq \mathbb{Z}_{N_1}$, there exists a mapping $\phi_{tile} : \mathcal{P}(\mathbb{Z}_{N_1}) \times \mathcal{P}(\mathbb{Z}_{N_1}) \to \mathcal{P}([-\lfloor N_2/2 \rfloor, \lfloor N_2/2 \rfloor))$ such that

$$|\phi_{tile}(A, B)| = \frac{N_2}{2N_1}(|A| + |B|) + O(N_1),$$

$$1_{\phi_{tile}(A,B)} * 1_{\phi_{tile}(A,B)}(0, ..., N_1 - 1) \in \frac{N_2}{N_1} 1_A * 1_B(0, ..., N_1 - 1) + O(N_1)[0, 1]^{N_1}.$$

The same is true if you replace $[-\lfloor N_2/2 \rfloor, \lfloor N_2/2 \rfloor)$ with $\mathbb{Z}_{N_2}$.

Proof. Let $N_2 = n \cdot N_1 + r$ for some $n, 0 \leq r < N_1 \in \mathbb{Z}$. Let $m = \lfloor n/2 \rfloor - 2$. If $m \leq 1$, then all convolutions and set sizes are at most $N_2 = O(N_1)$, and thus the statement is trivially true. Therefore, we may assume $m \geq 2$. Let ϕ_p be the canonical injection mapping from

$\mathbb{Z}_{N_1}$ to $[0, ...N_1) \subseteq \mathbb{Z}$. For any $A \subseteq Z_{N_1}$, consider the mapping

$$\phi_{tile}(A, B) := \Big(\phi_p(A) + N_1 \cdot [1, m-1]\Big) \cup \Big(\phi_p(B) + N_1 \cdot [-m, -1]\Big).$$

Let $A'_i := \phi_p(A) + N_1 \cdot i$ for all $i \in [1, m-1]$, and $B'_i := \phi_p(B) + N_1 \cdot i$ for all $i \in [-m, -1]$. Let $a', b' \in \phi_{tile}(A, B)$ be such that

$$a' + b' = x \text{ for some } x \in [0, N_1).$$

Note that one of a' or b' is positive and the other is negative. Assume without loss of generality that a is positive, then $a' \in A'_i \subseteq [iN_1, (i+1)N_1)$ for some $i \in [1, m)$. Therefore

$$b' = x - a' \in ((-i-1)N_1, (-i+1)N_1),$$

so $b' \in B'_{-i-1}$ or B'_{-i}. Therefore

$$\begin{aligned} &1_{\phi_{tile}(A,B)} * 1_{\phi_{tile}(A,B)}(0, ..., N_1 - 1) \\ &= 2\Bigg(\sum_{i=1}^{m-1} 1_{A'_i} * 1_{B'_{-i}}(0, ..., N_1 - 1) + 1_{A'_i} * 1_{B'_{-i-1}}(0, ..., N_1 - 1)\Bigg). \end{aligned} \tag{2.1}$$

For any $i \in [1, m-1]$,

$$\{(a', b') \in A'_i \times B'_{-i} : a' + b' = x\}$$

$$= \{(a, b) \in A \times B : \phi_p(a) + \phi_p(b) = x\},$$

$$\{(a', b') \in A'_i \times B'_{-i-1} : a' + b' = x\}$$

$$= \{(a, b) \in A \times B : \phi_p(a) + \phi_p(b) = x + N_1\},$$

Combining the two, we have

$$\{(a', b') \in A'_i \times (B'_i \cup B'_{-i-1}) : a' + b' = x\}$$

$$= \{(a, b) \in A \times B : \phi_p(a) + \phi_p(b) = x, x + N_1\}.$$

$$= \{(a, b) \in A \times B : a + b = x\},$$

Thus we have

$$1_{A'_i} * 1_{B'_{-i}}(0, ..., N_1 - 1) + 1_{A'_i} * 1_{B'_{-i-1}}(0, ..., N_1 - 1) = 1_A * 1_B(0, ..., N_1 - 1). \quad (2.2)$$

Since $m = n/2 + O(1) = N_1/(2N_2) + O(1)$, combining Eq. (2.1) and Eq. (2.2) gives our desired equality. For the case of $\mathbb{Z}_{N_2}$, one may map $\phi_{tile}(A, B) \in \mathbb{Z}$ to $\mathbb{Z}_{N_2}$ with the canonical quotient map. Note that

$$\phi_{tile}(A, B) \subseteq [-mN_1, mN_1) \subseteq [-N_2/2 + 2N_1, N_2/2 - N_1] \subseteq \mathbb{R},$$

so for any $a', b' \in \phi_{tile}(A, B), a' + b' \notin [0, N_1) \pm N_2$. Thus, the convolutions are the same. □

We may prove a similar version for difference sets. We will abuse notation and continue to use ϕ_{tile} for the case of difference set. Although the two ϕ_{tile}'s are technically different, they serve the exact same purpose and share similar properties.

Lemma 2.2 (Tiling for Difference Sets)**.** Let $N_1 \leq N_2$. For any $A \subseteq \mathbb{Z}_{N_1}$, there exists a mapping $\phi_{tile} : \mathcal{P}(\mathbb{Z}_{N_1}) \to \mathcal{P}([0, N_2))$ such that

$$|\phi_{tile}(A)| = \frac{N_2}{N_1}|A| + O(N_1),$$

$$1_{\phi_{tile}(A)} * 1_{-\phi_{tile}(A)}(0, ..., N_1 - 1) = \frac{N_2}{N_1} 1_A * 1_{-A}(0, ..., N_1 - 1) + O(N_1)[0, 1]^{N_1}.$$

The same is true if you replace $[0, N_2)$ with $\mathbb{Z}_{N_2}$.

Since the convolution of difference sets are translation invariant, we may replace $[0, N_2)$ with $[c, n + N_2)$ for any $c \in \mathbb{Z}$.

Proof. Let $N_2 = n \cdot N_1 + r$ for some $n, 0 \leq r < N_1 \in \mathbb{Z}$. Let $m = 0$. If $m \leq 1$, then all convolutions and set sizes are at most $N_2 = O(N_1)$, and thus the statement is trivially true. Therefore, we may assume $m \geq 1$. Let ϕ_p be the canonical projection mapping from $\mathbb{Z}_{N_1}$ to $\mathbb{Z}$. For any $A \subseteq Z_{N_1}$, consider the mapping

$$\phi_{tile}(A) := \Big(\phi_p(A) + N_1 \cdot [0, m-1]\Big).$$

Let $A'_i := \phi_p(A) + N_1 \cdot i$, for all $i \in [0, m-1]$. For all $a', b' \in \phi_{tile}(A)$ such that

$$a' - b' = x \text{ for some } x \in [0, N_1).$$

If $a' \in A'_i \subseteq [iN_1, (i+1)N_1)$ for some $i \in [1, m)$, then

$$b' = a' - x \in ((i-1)N_1, (i+1)N_1),$$

so $b' \in A'_i$ or A'_{i-1}. Therefore

$$\begin{aligned} &1_{\phi_{tile}(A)} * 1_{-\phi_{tile}(A)}(0, ..., N_1 - 1) \\ &= \sum_{i=1}^{m-1} 1_{A'_i} * 1_{-A'_i}(0, ..., N_1 - 1) + 1_{A'_i} * 1_{-A'_{i-1}}(0, ..., N_1 - 1). \end{aligned} \tag{2.3}$$

For any $i \in [1, m-1]$,

$$\{(a', b') \in A'_i \times A'_i : a' - b' = x\}$$

$$= \{(a, b) \in A \times A : \phi_p(a) - \phi_p(b) = x\},$$

$$\{(a', b') \in A'_i \times A'_{i-1} : a' - b' = x\}$$

$$= \{(a,b) \in A \times A : \phi_p(a) + \phi_p(b) = x + N_1\}.$$

Combining the two, we have

$$\{(a',b') \in A_i' \times (A_i' \cup A_{i-1}') : a' - b' = x\}$$

$$= \{(a,b) \in A \times A : \phi_p(a) - \phi_p(b) = x, x + N_1\},$$

$$= \{(a,b) \in A \times B : a - b = x\}.$$

Thus we have

$$1_{A_i'} * 1_{-A_{-i}'}(0,...,N_1-1) + 1_{A_i'} * 1_{-A_{i-1}'}(0,...,N_1-1) = 1_A * 1_{-A}(0,...,N_1-1). \quad (2.4)$$

Since $m = n - 1 = N_1/N_2 + O(1)$, combining Eq. (2.3) and Eq. (2.4) gives our desired equality. For the case of $\mathbb{Z}_{N_2}$, one may map $\phi_{tile}(A) \in \mathbb{Z}$ to $\mathbb{Z}_{N_2}$ with the canonical quotient map. Note that

$$\phi_{tile}(A) \subseteq [0, mN_1) \subseteq [0, N_2 - N_1) \subseteq \mathbb{Z},$$

so for any $a', b' \in \phi_{tile}(A)$, $a' - b' \notin [0, N_1) - N_2$. Thus the convolutions are the same. $\square$

2.1 Set Image of Independent Sets

We will consider the set image of convolutions at the "basis" of finite abelian groups G. This allows us to extend the results to independent vectors in $\mathbb{F}_p^n$, and analogous "independent" points of $\mathbb{Z}_N$.

Definition 2.3. Let $G = \mathbb{Z}_{N_1} \times ... \times \mathbb{Z}_{N_d}$. For all $1 \leq i \leq d$, let $e_i \in G$ be the element that is 1 in the ith coordinate, and 0 everywhere else.

For the following theorems, we will utilize a slight abuse of notation. For some subgroup $G' = \mathbb{Z}_{N_1} \times ... \times \mathbb{Z}_{N_j}$, where $j \leq i$, we may also define $e_i \in G'$, the element that

is 1 in the ith coordinate, and 0 everywhere else. Thus, e_i may refer to a element of G, or a element of the subgroup; the distinction should be clear through the context given in the proof. Let $CH(\cdot)$ denote the convex hull of a set, and let $a^\frown b$ denote the concatenation of vectors a and b.

2.1.1 Set Image for Difference Sets

We first look at the set image for difference sets. The set image of the convolution can be defined below:

Theorem 2.4 (Set Image of Standard Basis for Difference Sets)**.** Let $G = \mathbb{Z}_{N_1} \times ... \times \mathbb{Z}_{N_d}$ be a finite abelian group. Let $E = |G|/\min_i N_i$. Given $\delta \in [0,1]$, and $\alpha_1, ..., \alpha_d \in [\max(0, 2\delta - 1), \delta]$, there exists a set $A \subseteq G$ such that $|A| = \delta|G| + O(E)$, and for all $1 \leq i \leq d$

$$1_A * 1_{-A}(e_i) = \alpha_i|G| + O(E).$$

Moreover, let S be the set image of the random variable $1_A * 1_{-A}(e_1, ..., e_d)$ and let $C \subseteq \mathbb{R}^d$ be

$$C := |G| \cdot CH(\{[0, 1/2]^d, (1, 1, ..., 1)\}),$$

then

$$S \subseteq C \subseteq S + [0, 1]^d \cdot O(E).$$

Proof. We may express C as

$$C = \bigcup_{\delta \in [0,1]} |G| \cdot [\max(0, 2\delta - 1), \delta]^d.$$

We will first show the first half of the theorem, that there exists a set A such that for all $1 \leq i \leq d$, $1_A * 1_{-A}(e_i) = \alpha_i|G| + O(E)$, which implies $C \subseteq S + [0, 1]^d \cdot O(E)$.

Without loss of generality, by swapping the Cartesian products we may assume that α_1

is less than or equal to all α_i's. We will construct A by iterating on each $\mathbb{Z}_{N_i}$. Let

$$t_1 := \alpha_1 N_1 + O(1), t_2 := (2\delta - \alpha_1)N_1 + O(1)$$

be $\alpha_1 N_1$ and $(2\delta - \alpha_1)N_1$ rounded to the nearest integer, respectively. Construct $A_1 \in \mathbb{Z}_{N_1}$ in the following way:

$$A_1 := [0, t_1] \cup \{x \in [t_1, t_2] : 2|x\}.$$

This construction is valid as $t_1 \leq t_2 \leq N$, given by $\alpha_1 \leq 2\delta - \alpha_1 \leq 1$.

The size of A_1 is

$$|A_1| = t_1 + \frac{t_2 - t_1}{2} + O(1) = \alpha_1 N_1/2 + \delta N_1 - \alpha_1 N_1/2 + O(1) = \delta N_1 + O(1).$$

Since any two element within $\{x \in [t_1, t_2] : 2|x\}$ is at least two apart, all contribution to the convolution $1_{A_1} * 1_{-A_1}(1)$ is given by $[0, t_1]$. The contributions at the boundaries of the two set is $O(1)$, thus

$$1_{A_1} * 1_{A_1}(1) = \alpha_1 N_1 + O(1).$$

Denote $P_i = \prod_{k=1}^{i} N_k$, and $m_i = \min_{1 \leq k \leq i} N_k$. Let $A_i \subseteq \mathbb{Z}_{N_1} \times ... \times \subseteq \mathbb{Z}_{N_i}$, be a set such that

$$|A_i| = \delta P_i + O(P_i/m_i), \text{ and } 1_{A_i} * 1_{-A_i}(e_j) = \alpha_j P_i + O(P_i/m_i)$$

for all $1 \leq j \leq i$. We construct A_{i+1} in the following way: Let

$$t := \frac{\alpha_{i+1} - \alpha_1}{\delta - \alpha_1} N_{i+1} \text{ rounded to the nearest integer}$$

and

$$A_{i+1} := (A_i \times [0, t]) \cup \{(a + se_1)^\frown s : a \in A_i, s \in [t+1, N_{i+1} - 1]\}.$$

This construction is valid as $\alpha_1 \leq \alpha_{i+1} \leq \delta$, so $0 \leq t \leq 1$.

By our construction, A_{i+1} is N_{i+1} disjoint shifted copies of A_i,

$$|A_{i+1}| = |A_i|N_{i+1} = \big(\delta P_i + O(P_i/m_i)\big)N_{i+1} = \delta P_{i+1} + O(P_{i+1}/m_i)$$

and

$$1_{A_{i+1}} * 1_{-A_{i+1}}(e_j) = 1_{A_i} * 1_{-A_i}(e_j)N_{i+1} = \big(\alpha_j P_i + O(P_i/m_i)\big)N_{i+1}$$

$$= \alpha_j P_{i+1} + O(P_{i+1}/m_i) = \alpha_j P_{i+1} + O(P_{i+1}/m_i)$$

for all $1 \leq j \leq i$.

Now we consider $1_{A_{i+1}} * 1_{-A_{i+1}}(e_{i+1})$. $A_i \times [0,t]$ is $t+1$ copies of A_i. Thus, the contribution within the set to $1_{A_{i+1}} * 1_{-A_{i+1}}(e_{i+1})$ is

$$t|A_i| = t\big(\delta P_i + O(P_i/m_i)\big) = t\delta P_i + O(P_{i+1}/m_i). \tag{2.5}$$

For $\{(a + se_1)^\frown s : a \in A_i, s \in [t+1, N_{i+1} - 1]\}$, all contributions to the convolution of e_{i+1} are of the form $(a + se_1)^\frown s, (a + se_1)^\frown (s+1)$. We have

$$(a + se_1)^\frown (s+1) = (a - e_1 + (s+1)e_1)^\frown (s+1),$$

thus for each $s \in [t+1, N_{i+1} - 2]$, a contributes to $1_{A_{i+1}} * 1_{-A_{i+1}}(e_{i+1})$ if $a, a - e_1 \in A_i$. As mentioned, all A_i's are shifted copies of A_{i-1}, and thus shifted copies of A_1. We may express

$$A_i = \bigcup_{b \in B} (A_1 + s_b) \times b,$$

where $B \subseteq \mathbb{Z}_{N_2} \times ... \times \mathbb{Z}_{N_i}$, and s_b is some shifting constant for each $b \in B$. For each b, there are $1_{A_1} * 1_{A_1}(1) = \alpha_1 N_1 + O(1)$ such $a, a - e_1 \in (A_1 + s_b) \times b$. From our construction, we have $|B| = P_i/N_1$. Thus the contribution for each $s \in [t, N_{i+1} - 2]$ to

$1_{A_{i+1}} * 1_{-A_{i+1}}(e_{i+1})$ is

$$(\alpha_1 N_1 + O(1)) \cdot |B| = \alpha_1 P_i + O(P_i/m_i).$$

The contribution for the interval $[t, N_{i+1} - 2]$ is then

$$\begin{aligned}(N_{i+1} - t - 1)(\alpha_1 P_i + O(P_i/m_i)) &= \alpha_1 P_{i+1} - t\alpha_1 P_i - \alpha_1 P_i + O(P_{i+1}/m_i) \\ &= \alpha_1 P_{i+1} - t\alpha_1 P_i + O(P_{i+1}/m_{i+1}).\end{aligned} \tag{2.6}$$

The contribution given by where the two sets meet, $s = N - 1$ and $A_i \times \{t - 1\}$, is $O(|A_i|) = O(P_i)$ which is $O(P_{i+1}/m_{i+1})$. Thus, the total contribution of the two sets given by Eq. (2.6) and Eq. (2.5) is

$$1_{A_{i+1}} * 1_{-A_{i+1}}(e_{i+1}) = \delta t P_i + \alpha_1 P_{i+1} - t\alpha_1 P_i + O(P_{i+1}/m_{i+1})$$

$$= \left(\frac{\alpha_{i+1} - \alpha_1}{\delta - \alpha_1}\delta + \alpha_1 - \frac{\alpha_{i+1} - \alpha_1}{\delta - \alpha_1}\alpha_1 \right) P_{i+1} + O(P_{i+1}/m_{i+1}) = \alpha_{i+1} P_{i+1} + O(P_{i+1}/m_{i+1}),$$

our desired size for the convolution. Setting $A := A_d$ completes our construction.

Since for all $\delta \in [0, 1], \alpha_1, ..., \alpha_d \in [\max(0, 2\delta - 1), \delta]$ there exists a set A such that $1_A * 1_{-A}(e_i) = \alpha_i |G| + O(E)$ for all $1 \leq i \leq d$, we have

$$C \subseteq S + [0, 1]^d \cdot O(E).$$

Now we show the second part of the theorem, $S \subseteq C$. We show that for all $A \subseteq G$, if $|A| = \delta |G|$, then for all $1 \leq i \leq d$, $1_A * 1_{-A}(e_i) = \alpha_i |G|$ for some $\alpha_1, ..., \alpha_d \in [\max(0, 2\delta - 1), \delta]$.

First consider the one dimensional case. Let $A \subseteq \mathbb{Z}_N$, and let $\delta := |A|/N$. We would like to consider the upper and lower bound of $\alpha := 1_A * 1_{-A}(1)/N$. For any $a \in A$ to contribute to the convolution, we need $a - 1$ or $a + 1 \in A$. Therefore, for A to maximize

α, A needs to be a continuous interval. Thus

$$1_A * 1_{-A}(1) = \delta N - 1, \text{ if } 0 < \delta < 1.$$

If A is the empty set or the whole set, then we have

$$1_A * 1_{-A}(1) = \delta N, \text{ if } \delta = 0, 1.$$

Now we consider the minimum of α. For any set A, consider the following process: Start with the whole group $\mathbb{Z}_N$, then remove each element in A^C one by one. For each $x \in A^C$ removed, if both $x-1, x+1$ have not been removed, the convolution decreases by 2. If one has been removed, then the convolution decreases by 1. If both have been removed, the convolution does not change. Thus, each step the convolution decreases by at most 2, and we have

$$1_A * 1_{-A}(1) \geq N - 2|A^c| = N - 2(1-\delta)N = 2\delta N - N.$$

Therefore, we've shown in the 1 dimensional case that

$$\max(0, 2\delta - 1)N \leq 1_A * 1_{-A}(1) \leq \delta N,$$

so

$$\max(0, 2\delta - 1) \leq \alpha \leq \delta. \tag{2.7}$$

Now we consider the general d dimension case. Given $A \subseteq G$, let

$$\delta := |A|/|G|, \alpha_i := 1_A * 1_{-A}(e_i)/|G| \text{ for all } 1 \leq i \leq n.$$

For any α_i, we may swap the first and ith coordinate and look at α_1 instead. Thus without

loss of generality, we consider α_1. For all $x \in \mathbb{Z}_{N_2} \times ... \times \mathbb{Z}_{N_d}$, define

$$A^x := \{a \in Z_{N_1} : a^\frown x \in A\}.$$

Define

$$\alpha_1^x := 1_{A^x} * 1_{-A^x}(a)/N_1, \delta^x := |A^x|/N_1.$$

Since each $A^x \subseteq Z_{N_1}$, by the bounds in one dimension Eq. (2.7), we have for all $x \in \mathbb{Z}_{N_2} \times ... \times \mathbb{Z}_{N_d}$

$$\max(0, 2\delta^x - 1) \leq \alpha_1^x \leq \delta^x. \tag{2.8}$$

Note that A^x corresponds to a partition of A, so

$$\sum_{x \in \mathbb{Z}_{N_2} \times ... \times \mathbb{Z}_{N_d}} |A^x| = \sum_{x \in \mathbb{Z}_{N_2} \times ... \times \mathbb{Z}_{N_d}} |\{a \in Z_{N_1} : a^\frown x \in A\}| = |A|,$$

dividing everything by $|G|$ gives

$$\sum_{x \in \mathbb{Z}_{N_2} \times ... \times \mathbb{Z}_{N_d}} \delta^x N_1/|G| = \delta \tag{2.9}$$

Note that for any $a^\frown x, (a+1)^\frown x \in A$ that contribute to the convolution at e_1, $a, a+1 \in A^x$. Thus, to calculate α_1, we simply have to sum the contribution to the convolution for each A^x.

$$1_A * 1_{-A}(e_1) = \sum_{x \in \mathbb{Z}_{N_2} \times ... \times \mathbb{Z}_{N_d}} 1_{A^x} * 1_{-A^x}(1)$$

$$\alpha_1 = \sum_{x \in \mathbb{Z}_{N_2} \times ... \times \mathbb{Z}_{N_d}} \alpha_1^x N_1/|G|$$

and by Eq. (2.8) and Eq. (2.9),

$$\max(0, 2\delta - 1) = \max\left(0, \left(\sum_{x \in \mathbb{Z}_{N_2} \times ... \times \mathbb{Z}_{N_d}} 2\delta^x N_1/|G|\right) - 1\right)$$

$$= \max\left(0, \sum_{x\in\mathbb{Z}_{N_2}\times\ldots\times\mathbb{Z}_{N_d}} 2\delta^x N_1/|G| - N_1/|G|\right)$$

$$= N_1/|G| \max\left(0, \sum_{x\in\mathbb{Z}_{N_2}\times\ldots\times\mathbb{Z}_{N_d}} 2\delta^x - 1\right)$$

$$\leq N_1/|G| \sum_{x\in\mathbb{Z}_{N_2}\times\ldots\times\mathbb{Z}_{N_d}} \max(0, 2\delta^x - 1) \leq N_1/|G| \sum_{x\in\mathbb{Z}_{N_2}\times\ldots\times\mathbb{Z}_{N_d}} \alpha_1^x = \alpha_1$$

and

$$\alpha_1 = \sum_{x\in\mathbb{Z}_{N_2}\times\ldots\times\mathbb{Z}_{N_d}} \alpha_1^x N_1/|G| \leq \sum_{x\in\mathbb{Z}_{N_2}\times\ldots\times\mathbb{Z}_{N_d}} \delta^x N_1/|G| = \delta.$$

Therefore for all α_i, we have $\alpha_i \in [\max(0, 2\delta - 1), \delta]$, and $S \subseteq C$. □

Remark. Note that by our construction, we actually have $|A| = \delta|G| + O(|G|/N_m)$, where $m = \arg\min_i(\alpha_i)$.

2.1.2 Set Image for Sum Sets

The same statements made about the set image of difference sets can be said about sum sets. The construction for sum sets is similar to the construction in difference sets but with some "mirroring". There are also technical differences in the inductive step that one needs to be careful of.

Theorem 2.5 (Set Image of Standard Basis for Sum Sets)**.** Theorem 2.4 is also true if you replace $1_A * 1_{-A}$ with $1_A * 1_A$.

Proof. We will follow a similar structure for the proof of Theorem 2.4, with adjustment to the construction of A_i and the inductive step. Without loss of generality, by swapping the Cartesian products we may assume that $\alpha_1 \leq \alpha_2 \leq \ldots \leq \alpha_n$. Let

$$t_1 := \alpha_1 N_1/2 + O(1), t_2 := (\delta - \alpha_1/2)N_1 + O(1)$$

be $\alpha_1 N_1/2$ and $(\delta - \alpha_1/2)N_1$ rounded to the nearest integer, respectively. Construct $A_1 \in$

$\mathbb{Z}_{N_1}$ to be the interval $A_1 := [-t_1, t_2]$. This construction is valid as $t_1, t_2 \leq N/2$, given by $\alpha_1, 2\delta - \alpha_1 \leq 1$.

The size of A_1 is

$$|A_1| = t_1 + t_2 + O(1) = (\alpha_1/2 + \delta - \alpha_1/2)N_1 + O(1) = \delta N_1 + O(1).$$

Now we consider the set of elements in A_1 that sum to $-1, 0, 1$. Since

$$(\delta - \alpha_1/2)N_1 \geq \delta N_1/2 \geq \alpha_1 N_1/2,$$

we have $t_2 \geq t_1$ and $[-t_1, t_1] \subseteq A$. For -1, all elements of $[-t_1, t_1 - 1]$, contribute to $1_{A_1} * 1_{A_1}(-1)$. For 0, all elements of $[-t_1, t_1]$, contribute to $1_{A_1} * 1_{A_1}(0)$. For 1, all elements of $[-t_1, t_1 + 1]$, contribute to $1_{A_1} * 1_{A_1}(1)$. Thus we have

$$1_{A_1} * 1_{A_1}(-1), 1_{A_1} * 1_{A_1}(0), 1_{A_1} * 1_{A_1}(1) = 2t_1 + O(1) = \alpha_1 N_1 + O(1).$$

Denote $P_i = \prod_{k=1}^{i} N_k$, and $m_i = \min_{1 \leq k \leq i} N_k$. Let $A_i \subseteq \mathbb{Z}_{N_1} \times ... \times \subseteq \mathbb{Z}_{N_i}$ be a set such that

$$|A_i| = \delta P_i + O(P_i/m_i)$$

and

$$1_{A_i} * 1_{A_i}(-e_j), 1_{A_i} * 1_{A_i}(e_j) = \alpha_j P_i + O(P_i/m_i)$$

$$1_{A_i} * 1_{A_i}(0) = \alpha_i P_i + O(P_i/m_i)$$

for all $1 \leq j \leq i$. We will construct A_{i+1} in the following way: Let

$$t := \frac{\alpha_{i+1} - \alpha_i}{\delta - \alpha_i} N_{i+1} \text{ rounded to the nearest even number}$$

$$A_{i+1} := (-A_i \times [-t/2 + 1, 0]) \cup (A_i \times [1, N_{i+1} - t/2]).$$

This construction is valid since $\alpha_i \le \alpha_{i+1} \le \delta$, so $0 \le t \le 1$.

As A_{i+1} is N_{i+1} copies of $-A_i$ and A_i,

$$|A_{i+1}| = |A_i|N_{i+1} = \big(\delta P_i + O(P_i/m_i)\big)N_{i+1} = \delta P_{i+1} + O(P_{i+1}/m_{i+1}).$$

For $-A_i$,

$$\begin{aligned} 1_{-A_i} * 1_{-A_i}(e_j) &= 1_{A_i} * 1_{A_i}(-e_j) = \alpha_j P_i + O(P_i/m_i) \\ 1_{-A_i} * 1_{-A_i}(-e_j) &= 1_{A_i} * 1_{A_i}(e_j) = \alpha_j P_i + O(P_i/m_i) \end{aligned} \tag{2.10}$$

so all copies of $-A_i, A_i$ contributes Eq. (2.10) to $1_{A_{i+1}} * 1_{A_{i+1}}(\pm e_j)$. Therefore, for all $1 \le j \le i$,

$$1_{A_{i+1}} * 1_{A_{i+1}}(e_j) = 1_{A_i} * 1_{A_i}(e_j)N_{i+1}$$

$$= \big(\alpha_j P_i + O(P_i/m_i)\big)N_{i+1} = \alpha_j P_{i+1} + O(P_{i+1}/m_i).$$

and

$$1_{A_{i+1}} * 1_{A_{i+1}}(-e_j) = 1_{A_i} * 1_{A_i}(-e_j)N_{i+1} = \alpha_j P_{i+1} + O(P_{i+1}/m_i).$$

Let $\epsilon \in \{-1, 0, 1\}$. Now we consider $1_{A_{i+1}} * 1_{A_{i+1}}(\epsilon e_{i+1})$. All contributions to the convolution are of the form $a^\frown s, -a^\frown(-s+\epsilon) \in A_{i+1}$. If $s \in [1, t/2]$ then $-s+\epsilon \in [-t/2+\epsilon, -1+\epsilon]$, and vice versa. Thus, we need $-a \in -A_i$, which is true for all $a \in A_i$. For all

$$s \in [-t/2+\epsilon, -1+\epsilon] \cup [1, t/2], a \in A_i,$$

we have $a^\frown s, -a^\frown(-s+\epsilon) \in A_{i+1}$. Thus all elements within this interval contributes to the convolution. The contribution for the interval $[-t/2+\epsilon, -1+\epsilon] \cup [1, t/2]$ is

$$|A_i| \cdot |[-t/2+\epsilon, -1+\epsilon] \cup [1, t/2]| = t|A_i| = t\big(\delta P_i + O(P_i/m_i)\big) = t\delta P_i + O(P_{i+1}/m_i). \tag{2.11}$$

Now we consider the interval $[t/2+1, N_{i+1}-t/2-1+\epsilon]$. For any $s \in [t/2+1, N_{i+1}-t/2-1+\epsilon]$, $-s+\epsilon$ is also in $[t/2+1, N_{i+1}-t/2-1+\epsilon]$. Therefore, any $a^\frown s, -a^\frown(-s+\epsilon)$ that contribute to the convolution must have $a \in A_i, -a \in A_i$. The number of such a is exactly $1_{A_i} * 1_{A_i}(0)$. Thus, the contribution within this interval is

$$\begin{aligned}|[t/2+1, N_{i+1}-t/2-1+\epsilon]| \cdot 1_{A_i} * 1_{A_i}(0) &= (N_{i+1}-t-1+\epsilon)(\alpha_i P_i + O(P_i/m_i)) \\ &= \alpha_i P_{i+1} - t\alpha_i P_i + O(P_{i+1}/m_i).\end{aligned} \tag{2.12}$$

Since $[-t/2+\epsilon, -1+\epsilon] \cup [1, t/2]$ and $[t/2+1, N_{i+1}-t/2-1+\epsilon]$ covers all but $O(1)$ of $\mathbb{Z}_{N_{i+1}}$, combining Eq. (2.11) and Eq. (2.12), gives the total contribution up to $O(P_i)$. Therefore

$$\begin{aligned}1_{A_{i+1}} * 1_{A_{i+1}}(\epsilon e_{i+1}) &= t\delta P_i + \alpha_i P_{i+1} - t\alpha_i P_i + O(P_{i+1}/m_i). \\ = \left(\frac{\alpha_{i+1}-\alpha_i}{\delta-\alpha_i}\delta + \alpha_i - \frac{\alpha_{i+1}-\alpha_i}{\delta-\alpha_i}\alpha_i\right) P_{i+1} + O(P_{i+1}/m_i) &= \alpha_{i+1}P_{i+1} + O(P_{i+1}/m_i).\end{aligned} \tag{2.13}$$

Thus, for all ϵ, the convolution is equal to Eq. (2.13). We have

$$1_{A_{i+1}} * 1_{A_{i+1}}(-e_{i+1}), 1_{A_{i+1}} * 1_{A_{i+1}}(0), 1_{A_{i+1}} * 1_{A_{i+1}}(e_{i+1}) = \alpha_{i+1}P_{i+1} + O(P_{i+1}/m_i)$$

All convolutions match our desired values. Setting $A := A_d$ completes our construction.

Since for all $\delta \in [0,1], \alpha_1, ..., \alpha_d \in [\max(0, 2\delta-1), \delta]$ there exists a set A such that $1_A * 1_A(e_i) = \alpha_i|G| + O(E)$ for all $1 \le i \le d$, we have

$$C \subseteq S + [0,1]^d \cdot O(E).$$

Now we show the second part of the theorem: $S \subseteq C$. We show that for all $A \subseteq G$, if $|A| = \delta|G|$, then for all $1 \le i \le d$, $1_A * 1_A(e_i) = \alpha_i|G|$ for some $\alpha_1, ..., \alpha_d \in [\max(0, 2\delta-$

$1), \delta]$.

First consider the one dimensional case. Let $A \subseteq \mathbb{Z}_N$, and let $\delta := |A|/N$. We would like to consider the upper and lower bound of $\alpha := 1_A * 1_A(1)/N$. For each $a \in A$, a contributes to the convolution if $-a+1 \in A$. We may partition A into the sets of the form $\{a, -a+1\}$. If N is even, each of the subset has 2 elements. If N is odd, all but one of the subset has 2 elements. That one subset is the case $a = 1/2$, which has one element since $a = -a+1$. To maximize α, all but at most one element of A should be in a pair. We have

$$1_A * 1_A(1) = \delta N \text{ or } \delta N - 1.$$

Now we consider what the minimum of α can be. For any set A, consider the following process: start with the whole group $\mathbb{Z}_N$, then remove each element in A^C one by one. For each $x \neq 1/2 \in A^C$ removed, if $-x+1$ has not been removed, the convolution decreases by 2; otherwise, the convolution does not change. If $1/2$ is removed, the convolution decreases by 1. At each step, the convolution decreases by at most 2, so

$$1_A * 1_{-A}(1) \geq N - 2|A^c| = N - 2(1-\delta)N = 2\delta N - N.$$

We've shown in the 1 dimensional case that

$$\max(0, 2\delta - 1)N \leq 1_A * 1_{-A}(1) \leq \delta N,$$

so

$$\max(0, 2\delta - 1) \leq \alpha \leq \delta. \tag{2.14}$$

Now we consider the general d dimension case. Given $A \subseteq G$, let

$$\delta := |A|/|G|, \alpha_i := 1_A * 1_{-A}(e_i)/|G| \text{ for all } 1 \leq i \leq n.$$

For any α_i, we may swap the first and ith coordinate and look at α_1 instead. Thus without loss of generality, we consider α_1. For all $x \in \mathbb{Z}_{N_2} \times ... \times \mathbb{Z}_{N_d}$, define

$$A^x := \{a \in Z_{N_1} : a^\frown x \in A\}.$$

Define

$$\alpha_1^x := 1_{A^x} * 1_{A^x}(a)/N_1, \delta^x := |A^x|/N_1.$$

Since each $A^x \subseteq Z_{N_1}$, by the bounds in one dimension Eq. (2.14), we have for all $x \in \mathbb{Z}_{N_2} \times ... \times \mathbb{Z}_{N_d}$

$$\max(0, 2\delta^x - 1) \leq \alpha_1^x \leq \delta^x. \tag{2.15}$$

Note that A^x corresponds to a partition of A, so

$$\sum_{x \in \mathbb{Z}_{N_2} \times ... \times \mathbb{Z}_{N_d}} |A^x| = \sum_{x \in \mathbb{Z}_{N_2} \times ... \times \mathbb{Z}_{N_d}} |\{a \in Z_{N_1} : a^\frown x \in A\}| = |A|,$$

dividing everything by $|G|$ gives

$$\sum_{x \in \mathbb{Z}_{N_2} \times ... \times \mathbb{Z}_{N_d}} \delta^x N_1/|G| = \delta \tag{2.16}$$

Note that for any $a^\frown x, (-a+1)^\frown x \in A$ that contribute to the convolution at e_1, $a, a+1 \in A^x$. Thus, to calculate α_1, we simply have to sum the contribution to the convolution for each A^x.

$$1_A * 1_{-A}(e_1) = \sum_{x \in \mathbb{Z}_{N_2} \times ... \times \mathbb{Z}_{N_d}} 1_{A^x} * 1_{-A^x}(1)$$

$$\alpha_1 = \sum_{x \in \mathbb{Z}_{N_2} \times ... \times \mathbb{Z}_{N_d}} \alpha_1^x N_1/|G|$$

and by Eq. (2.15) and Eq. (2.16),

$$\max(0, 2\delta - 1) = \max\left(0, \left(\sum_{x \in \mathbb{Z}_{N_2} \times ... \times \mathbb{Z}_{N_d}} 2\delta^x N_1/|G|\right) - 1\right)$$

$$= \max\left(0, \sum_{x \in \mathbb{Z}_{N_2} \times ... \times \mathbb{Z}_{N_d}} 2\delta^x N_1/|G| - N_1/|G|\right)$$

$$= N_1/|G| \max\left(0, \sum_{x \in \mathbb{Z}_{N_2} \times ... \times \mathbb{Z}_{N_d}} 2\delta^x - 1\right)$$

$$\leq N_1/|G| \sum_{x \in \mathbb{Z}_{N_2} \times ... \times \mathbb{Z}_{N_d}} \max(0, 2\delta^x - 1) \leq N_1/|G| \sum_{x \in \mathbb{Z}_{N_2} \times ... \times \mathbb{Z}_{N_d}} \alpha_1^x = \alpha_1$$

and

$$\alpha_1 = \sum_{x \in \mathbb{Z}_{N_2} \times ... \times \mathbb{Z}_{N_d}} \alpha_1^x N_1/|G| \leq \sum_{x \in \mathbb{Z}_{N_2} \times ... \times \mathbb{Z}_{N_d}} \delta^x N_1/|G| = \delta.$$

Therefore for all α_i, we have $\alpha_i \in [\max(0, 2\delta - 1), \delta]$, and $S \subseteq C$. □

If G is a vector field, then we may generalize $e_1, ..e_d$ to any basis by linear transformations.

Corollary 2.6 (Set Image of General Basis in Finite Fields)**.** Let p be a prime. Let $v_1, ...v_d \in \mathbb{F}_p^d$ be a basis. Given $\delta \in [0, 1]$, and $\alpha_1, ..., \alpha_d \in [\max(0, 2\delta - 1), \delta]$, there exists a set $A \subseteq \mathbb{F}_p^d$ such that $|A| = \delta|p^d| + O(p^{d-1})$, and for all $1 \leq i \leq d$

$$1_A * 1_A(v_i) = \alpha_i p^d + O(p^{d-1}).$$

Moreover, let S be the set image of the random variable $1_A * 1_{-A}(v_1, ..., v_d)$ and let $C \subseteq \mathbb{R}^d$ be

$$C := |G| \cdot CH(\{[0, 1/2]^d, (1, 1, ..., 1)\})$$

then

$$S \subseteq C \subseteq S + [0, 1]^d \cdot O(p^{d-1}).$$

The same statement is true if you replace $1_A * 1_A$ with $1_A * 1_{-A}$.

Proof. The case for the standard basis $e_1, ..., e_d$, is given by Theorem 2.4 and Theorem 2.5. For general basis $v_1, ..., v_d$, a linear transformation that maps $e_1, ..., e_d$ to $v_1, ..., v_d$ is a Frieman 2-isomorphism that maps 0 to 0. Thus, by Proposition 1.6, the set image is preserved. □

If each $N_1, ..., N_d \in \mathbb{Z}$ is coprime, and $G := \mathbb{Z}_{N_1} \times ... \times \mathbb{Z}_{N_d}$. Let ϕ_1 be some group automorphism of G. Let $\phi_2 : G \to \mathbb{Z}_N$ be a group isomorphism given by the Chinese Remainder theorem. Let $\phi_3 : \mathbb{Z}_N \to [0, N)$ be the inverse of the cannonical quotient homomophism from $\mathbb{Z}$ to $\mathbb{Z}_N$. The composition of these three mappings

$$\phi_z := \phi_3 \circ \phi_2 \circ \phi_1 \tag{2.17}$$

gives a mapping for the previous theorems from G to $\mathbb{Z}$.

Corollary 2.7. Let each $N_1, ..., N_d \in \mathbb{Z}$ be coprime, and $G := \mathbb{Z}_{N_1} \times ... \times \mathbb{Z}_{N_d}$. Let ϕ_z be a mapping in the form in Eq. (2.17), and let $x_i := \phi_z(e_i)$ for all $1 \leq i \leq d$. Given $N \geq |G|, \delta \in [0, 1]$, and $\alpha_1, ..., \alpha_d \in [\max(0, 2\delta - 1), \delta]$, there exists a set $A \in [-\lfloor N/2 \rfloor, \lfloor N/2 \rfloor]$ such that

$$|A| = \delta N + O(N/(\min_i N_i) + |G|)$$

$$1_A * 1_A(x_i) = \alpha_i N + O(N/(\min_i N_i) + |G|)$$

The same statement is true if you replace $1_A * 1_A$ with $1_A * 1_{-A}$, or if $[-\lfloor N/2 \rfloor, \lfloor N/2 \rfloor]$ is replaced with $\mathbb{Z}_N$

Proof. Let $A' \subseteq G$ be the set such that $|A'| = \delta|G| + O(E)$ and for all $1 \leq i \leq d$

$$1_{A'} * 1_{A'}(e_i) = \alpha_i|G| + O(E),$$

as described in Theorem 2.5. Since ϕ_1, ϕ_2 are group isomorphisms, by Proposition 1.6,

$\phi_2 \circ \phi_1(A')$ has the same size as A', and

$$1_{A'} * 1_{A'}(e_i) = 1_{\phi_2 \circ \phi_1(A')} * 1_{\phi_2 \circ \phi_1(A')}(\phi_2 \circ \phi_1(e_i)).$$

Then by Lemma 2.1, let $A := \phi_{tile}\big(\phi_2 \circ \phi_1(A'), \phi_2 \circ \phi_1(A')\big)$. Then

$$|A| = \frac{N}{|G|}|A'| + O(|G|) = \frac{N}{|G|}(\delta|G| + O(E)) + O(|G|) = \delta N + O(N/(\min_i N_i) + |G|)$$

$$1_A * 1_A(x_i) = \frac{N}{|G|} 1_{A'} * 1_{A'}(e_i) + O(|G|)$$

$$= \frac{N}{|G|}(\alpha_i|G| + O(E)) + O(|G|) = \alpha_i N + O(N/(\min_i N_i) + |G|).$$

For the $1_A * 1_{-A}$ case, let $A' \subseteq G$ be the set such that $|A'| = \delta|G| + O(E)$ and for all $1 \leq i \leq d$

$$1_{A'} * 1_{A'}(e_i) = \alpha_i|G| + O(E),$$

as described in Theorem 2.4. By Lemma 2.2, let $A := \phi_{tile} \circ \phi_2 \circ \phi_1(A')$. By the same calculation as the sum set case, we have our result.

For the $\mathbb{Z}_N$, case, one may map A to $\mathbb{Z}_N$ through the canonical quotient map. As described in Lemma 2.1 and Lemma 2.2, the size of the set and convolution is unchanged.

□

CHAPTER 3

SET IMAGES OF CONVOLUTIONS AT ARITHMETIC PROGRESSIONS

In this chapter, we will look at convolution at arithmetic progressions. Unlike the previous case of "independent" sets, there are now complicated influences between the values. We will prove a recurrence relation, and utilize it to understand the set image in lower dimensions.

3.1 A Recurrence Relation for Distribution of Convolution at Arithmetic Progressions

Here we will consider the group $\mathbb{Z}_N$, and $\mathbb{Z}$. Many of our arguments in this section will work for both groups by simple projection mappings. Therefore, we will use a slight abuse of notation, by identifying intervals $[-i, i]$ as either a subset of $\mathbb{Z}_N$, or $\mathbb{Z}$, depending on the context. Under the context that we are talking about $\mathbb{Z}_N$, we have $[-\lfloor N/2 \rfloor, \lfloor N/2 \rfloor] = \mathbb{Z}_N$.

3.1.1 A Recurrence Relation for Sum Sets

Let $b \in \mathcal{B} = \{0,1\}^n$ be a set of binary vectors. For any b, define $b' \in \{0,1\}^{n-1}$ as the sub-vertex of b with the last coordinate removed. Define

$$\mathcal{A}^i := \mathcal{P}([-i, i])$$

as the power set of $[-i, i] \subseteq \mathbb{Z}_N$ or $\mathbb{Z}$. For any $A \in \mathcal{A}^i$, we may identify A as a $2i+1$ dimensional binary vector v_A, where the first coordinate corresponds to $-i$, and the last coordinate corresponds to i. The jth coordinate is 1 if $-i-1+j \in A$. Consider the projection mapping $\psi : \mathcal{A}^i \to \mathcal{B}$, where $A \in \mathcal{A}^i$ is mapped to the vector that is the first n

coordinate of v_A. Define

$$\mathcal{A}_b^i := \{A \in \mathcal{A}^i : \psi(A) = b\}.$$

Definition 3.1. For all $\boldsymbol{y} \in [0, N]^{n+1}, b \in \mathcal{B}$, define

$$c^i(\boldsymbol{y}, b) := |\{A \in \mathcal{A}_b^i : 1_A * 1_A(0, 1, ..., n) = \boldsymbol{y}\}|.$$

Again, we may understand this definition through projections. For each $A \in \mathcal{A}_b^i$, we map it to $1_A * 1_A$, viewed as a vector in $\mathbb{Z}^N$. Mapping $1_A * 1_A$ to $1_A * 1_A(0, 1, ..., n)$ is then a projection to $\mathbb{Z}^n$. Therefore, $c^i(\boldsymbol{y}, b)$ is the number of $A \in \mathcal{A}_b^i$ such that

$$A \to 1_A * 1_A \to 1_A * 1_A(0, 1, ..., n)$$

is mapped to $\boldsymbol{y}$.

The function is of interest because for a random subset $A \subseteq \mathbb{Z}_N$,

$$c^i(\boldsymbol{y}, b)/|\mathcal{A}_b^i| = \mathbb{P}(1_A * 1_A(0, 1, ..., n) = \boldsymbol{y} | A \in \mathcal{A}_b^i).$$

Note that if we are working with $\mathbb{Z}_N$, $[-\lfloor \frac{N}{2} \rfloor, \lfloor \frac{N}{2} \rfloor] = \mathbb{Z}_N$, is the whole group, so

$$\sum_{b \in B} c^{\lfloor \frac{N}{2} \rfloor}(\boldsymbol{y}, b)/2^N = \mathbb{P}(1_A * 1_A(0, 1, ..., n) = \boldsymbol{y}).$$

Thus, calculating $c^i(y, b)$ gives the distribution for $1_A * 1_A(0, 1, ..., n)$.

Remark. Let $\boldsymbol{x} = (x_1, x_1 + r, ..., x_1 + nr)$ be a arithmetic progression where r is coprime to N and $2|x_1$ (or $2r$ is coprime to N). Note that $|\{A \in \mathbb{Z}_N : 1_A * 1_A(\boldsymbol{x}) = \boldsymbol{y}\}|$ is not actually dependent on $\boldsymbol{x}$. By Proposition 1.6, the case of arithmetic progressions are equivalent to the case $\boldsymbol{x} = (0, 1, ..., n)$, due to the following Freiman isomorphism:

$$\phi(x) := \frac{2x - x_1}{2r}. \tag{3.1}$$

For all $0 \leq i \leq n, x_i = x_i + 0$, so

$$\phi(x_i) + \phi(0) = \frac{2x_i - x_1}{2r} - \frac{x_1}{2r} = \frac{2x_1 + 2ir - x_1}{2r} - \frac{x_1}{2r} = i.$$

Thus

$$1_A * 1_A(\boldsymbol{x}) = 1_{\phi(A)} * 1_{\phi(A)}(\phi(\boldsymbol{x}) + \phi(0)) = 1_{\phi(A)} * 1_{\phi(A)}(0, 1, ..., n)$$

Since ϕ is an bijection,

$$|\{A \in \mathbb{Z}_N : 1_A * 1_A(\boldsymbol{x}) = \boldsymbol{y}\}| = |\{A \in \mathbb{Z}_N : 1_{\phi(A)} * 1_{\phi(A)}(0, 1, ..., n) = \boldsymbol{y}\}|$$

$$= |\{A \in \mathbb{Z}_N : 1_A * 1_A(0, 1, ..., n) = \boldsymbol{y}\}|$$

Therefore, although our recurrence relation only considers the convolution at $(0, 1, ..., n)$, it is equivalent to the general case $\boldsymbol{x} = (x_1, x_1 + r, ..., x_1 + nr)$.

We can generate the following recurrence relation for c^i on i.

Theorem 3.2 (Recurrence Relation for Convolution of Intervals for Sum Sets)**.** Let $G = \mathbb{Z}_N$ or $\mathbb{Z}$, and let c^i be defined as above. Let $\mathcal{B} = \{0, 1\}^n$, then for all $\boldsymbol{y} \in [0, N]^{n+1}, b \in \mathcal{B}, n/2 < i < \frac{N-n}{2}$,

$$c^i(\boldsymbol{y}, b) = c^{i-1}(\boldsymbol{y}, b'^\frown 0) + c^{i-1}(\boldsymbol{y}, b'^\frown 1) + c^{i-1}(\boldsymbol{y} - 2 \cdot b^\frown 0, b'^\frown 0) + c^{i-1}(\boldsymbol{y} - 2 \cdot b^\frown 1, b'^\frown 1).$$

Remark. The argumentation is the same for $G = \mathbb{Z}_N$ or $\mathbb{Z}$. For convenience, throughout the theorem and lemmas, we will treat the ambient group as $\mathbb{Z}_N$. However, any intervals $[-i, i] \subseteq \mathbb{Z}_N$ can be mapped directly to $[-i, i] \in \mathbb{Z}$ without influencing the proof. Moreover, the upper bound $\frac{N-n}{2}$ only exists due to the "wrap-around" of $\mathbb{Z}_N$. For $\mathbb{Z}$, the only constraint on i is $n/2 < i$.

To prove Theorem 3.2, as well as the convexity property of the set image, we first prove the following lemma:

Lemma 3.3. Let $G = \mathbb{Z}_N$ or Z_N be the ambient group, and $n/2 < i < \frac{N-n}{2}$. Given $T \subseteq \{-i, i\}$, define the mapping $\phi_T(A) := A \cup T$. For all $A \in \mathcal{A}^{i-1}$, if $T = \emptyset$ or $\{-i\}$, then

$$1_A * 1_A(0, 1, ..., n) = 1_{\phi_T(A)} * 1_{\phi_T(A)}(0, 1, ..., n).$$

If $T = \{i\}$, for all $b \in B, A \in \mathcal{A}_b^{i-1}$,

$$1_A * 1_A(0, 1, ..., n) + 2 \cdot (0^\frown b) = 1_{\phi_T(A)} * 1_{\phi_T(A)}(0, 1, ..., n).$$

If $T = \{i, -i\}$, for all $b \in B, A \in \mathcal{A}_b^{i-1}$,

$$1_A * 1_A(0, 1, ..., n) + 2 \cdot (1^\frown b) = 1_{\phi_T(A)} * 1_{\phi_T(A)}(0, 1, ..., n).$$

Proof. Since A and T are disjoint, we have

$$1_{\phi_T(A)} * 1_{\phi_T(A)}(0, 1, ..., n) = 1_{A \cup T} * 1_{A \cup T}(0, 1, ..., n)$$

$$= 1_A * 1_A(0, 1, ..., n) + 2 \cdot 1_A * 1_T(0, 1, ..., n) + 1_T * 1_T(0, 1, ..., n)$$

First, consider the case $T = \emptyset$ or $\{-i\}$. For $T = \emptyset, \phi_T$ is the identity mapping so the convolution is trivially equal. If $T = \{-i\}$, assume

$$1_A * 1_T(0, 1, ..., n) \neq 0,$$

then there must exist some $a \in A$ such that $a - i \in [0, n]$, so $a \in [i, i + n]$. However $A \subseteq [-i + 1, i - 1]$, and

$$[-i, i - 1] \cap [i + 1, i + n] = \emptyset,$$

as $i + n < N - i$ by the bounds on i. Thus, no such a exists. We also have $1_T *$

$1_T(0, 1, ..., n) = 0$, as the bounds have $-2i > n - N$, so $-2i \notin [0, n]$. Thus, the convolution is equal in both cases.

Now, consider the case $T = \{i\}$ or $\{i, -i\}$. We've shown in the previous case $T = \{-i\}$ that $-i$ alone does not contribute to the convolution. Therefore,

$$1_A * 1_T(0, 1, ..., n) \neq 0$$

if and only if there exists $a \in A$ such that $a + i \in [0, n]$. For all $a \in A \cap [-i + 1, -i + n]$, we have $b_{i+a} = 1$ by definition of b. Thus a, i contributes to the $i + a$ coordinate of $1_A * 1_T(0, 1, ..., n)$. Thus

$$1_A * 1_T(0, 1, ..., n) = 0^\frown b.$$

For $T = \{i\}$,

$$1_T * 1_T(0, 1, ..., n) = 0,$$

as $2i > n$, so $2i \notin [0, n]$.

For $T = \{-i, i\}$, $i - i, -i + i = 0$ contributes 2 to $1_T * 1_T(0)$, the first entry. Thus

$$1_T * 1_T(0, 1, ..., n) = 2 \cdot e_1,$$

and

$$2 \cdot 1_A * 1_T(0, 1, ..., n) + 1_T * 1_T(0, 1, ..., n) = 2 \cdot (1^\frown b).$$

ϕ_T increases the convolution as described. □

Now we prove Theorem 3.2 using the mapping ϕ_T.

Proof of Theorem 3.2. For any subset $T \subseteq \{-i, i\}$, let $\phi_T : \mathcal{A}^{i-1} \to \mathcal{A}^i$ be as described in Lemma 3.3. For any $A \in \mathcal{A}^{i-1}$, since $T \cap A = \emptyset$, each ϕ_T is one-to-one. For any set $A' \in \mathcal{A}^i$, if

$$T = A' \cap \{-i, i\}, A = A' \cap [-i + 1, i - 1],$$

then $\phi_T(A) = A'$. Moreover, each mapping ϕ_T has a disjoint image. Therefore, the four images of each ϕ_T give a partition of $\mathcal{A}^i$.

Define

$$\mathcal{S} := \{A \in \mathcal{A}_b^i : 1_A * 1_A(0, 1, ..., n) = \boldsymbol{y}\},$$

then

$$c^i(\boldsymbol{y}, b) = |\mathcal{S}| = \sum_{T \subseteq \{-i, i\}} |\phi_T^{-1}(\mathcal{S})|.$$

Thus to figure out $c^i(\boldsymbol{y}, b)$, we simply have to calculate the number of sets that map into $\mathcal{S}$ by all ϕ_T.

By the definition of b, for all $b, A \in \mathcal{A}_b^{i-1}$, if $T = \emptyset$ or $\{i\}$, then $\phi_T(A) \in \mathcal{A}_{0^\frown b'}^i$. If $T = \{-i\}$ or $\{i, -i\}$, then $\phi_T(A) \in \mathcal{A}_{1^\frown b'}^i$.

Now we calculate the size of $\mathcal{S}$ for some given $b, \boldsymbol{y}$. If $b_0 = 0$, by Lemma 3.3, we see that for all $A \in \mathcal{A}^{i-1}$, if $T = \emptyset$, then $\phi_T(A) \in \mathcal{S}$ if and only if

$$A \in \mathcal{A}_{b'^\frown 0}^i \cup \mathcal{A}_{b'^\frown 1}^i, 1_A * 1_A(0, 1, ..., n) = \boldsymbol{y}.$$

The number of such A is

$$|\phi_\emptyset^{-1}(\mathcal{S})| = c^{i-1}(\boldsymbol{y}, b'^\frown 0) + c^{i-1}(\boldsymbol{y}, b'^\frown 1), \tag{3.2}$$

If $T = \{i\}$, then $\phi_T(A) \in \mathcal{S}$ if and only if

$$A \in \mathcal{A}_{b'^\frown 0}^i, 1_A * 1_A(0, 1, ..., n) + 2 \cdot b^\frown 0 = \boldsymbol{y},$$

or

$$A \in \mathcal{A}_{b'^\frown 1}^i, 1_A * 1_A(0, 1, ..., n) + 2 \cdot b^\frown 1 = \boldsymbol{y}.$$

The number of such A is

$$|\phi_{\{i\}}^{-1}(\mathcal{S})| = c^{i-1}(\boldsymbol{y} - 2 \cdot b^\frown 0, b'^\frown 0) + c^{i-1}(\boldsymbol{y} - 2 \cdot b^\frown 1, b'^\frown 1). \tag{3.3}$$

If $T = \{-i\}, \{-i, i\}$, then $\phi_T(A) \notin \mathcal{S}$, since $b_0 = 0$. Thus we have

$$|\phi_{\{-i\}}^{-1}(\mathcal{S})| = |\phi_{\{-i,i\}}^{-1}(\mathcal{S})| = 0. \tag{3.4}$$

The sum of Eq. (3.2), Eq. (3.3), Eq. (3.4) gives the desired recurrence relation.

If $b_0 = 1$, then the same argument also applies, except now with $\phi_\emptyset^{-1}, \phi_{\{-i\}}^{-1}$ swapped, and $\phi_{\{i\}}^{-1}, \phi_{\{-i,i\}}^{-1}$ swapped:

$$|\phi_{\{-i\}}^{-1}(\mathcal{S})| = c^{i-1}(\boldsymbol{y}, b'^\frown 0) + c^{i-1}(\boldsymbol{y}, b'^\frown 1),$$

$$|\phi_{\{-i,i\}}^{-1}(\mathcal{S})| = c^{i-1}(\boldsymbol{y} - 2 \cdot b^\frown 0, b'^\frown 0) + c^{i-1}(\boldsymbol{y} - 2 \cdot b^\frown 1, b'^\frown 1),$$

$$|\phi_\emptyset^{-1}(\mathcal{S})| = |\phi_{\{i\}}^{-1}(\mathcal{S})| = 0$$

The sum of above equations also gives the desired recurrence relation. □

3.1.2 A Recurrence Relation for Difference Sets

We may prove an analogous theorem for $1_A * 1_{-A}(0, 1, ...n)$.

Let $b \in B = \{0, 1\}^n$ be a set of binary vectors. For any b, define $b' \in \{0, 1\}^{n-1}$ as the sub-vertex of b with the first coordinate removed. Define the sets

$$\mathcal{D}^i := \mathcal{P}([0, i])$$

to be the power set of $[0, i]$. For any $A \in \mathcal{D}^i$, we may identify A as an $i + 1$ dimensional

binary vector v_A, where the first coordinate corresponds to whether $i \in A$, and the last coordinate corresponds to whether $0 \in A$. The jth coordinate is 1 if $i - j + 1 \in A$, and 0 otherwise.

Consider the projection mapping $\psi : \mathcal{D}^i \to B$, where $A \in \mathcal{D}^i$ is mapped to the vector that is the last n coordinate of v_A. Now we define

$$\mathcal{D}_b^i := \{A \in \mathcal{D}^i : \psi(A) = b\}.$$

For all $\boldsymbol{y} \in [0, N]^{n+1}, and b \in B$, define

$$d^i(\boldsymbol{y}, b) = |\{A \in \mathcal{D}_b^i : 1_A * 1_{-A}(0, 1, ..., n) = \boldsymbol{y}\}|$$

As in the sum set case, if we are working with $\mathbb{Z}_N$, $[0, N-1] = \mathbb{Z}_N$ is the whole group, so

$$\sum_{b \in B} d^{N-1}(\boldsymbol{y}, b)/2^N = \mathbb{P}(1_A * 1_{-A}(0, 1, ..., n) = \boldsymbol{y}).$$

Thus, calculating $d^i(y, b)$ gives the distribution for $1_A * 1_{-A}(0, 1, ..., n)$.

Remark. Let $\boldsymbol{x} = (0, r, ..., nr)$ be an arithmetic progression starting at 0, where r is coprime to N. As in the case of sum sets,$|\{A \in \mathbb{Z}_N : 1_A * 1_{-A}(\boldsymbol{x}) = \boldsymbol{y}\}|$ is not actually dependent on $\boldsymbol{x}$. Due to the Freiman isomorphism $\phi(x) := \frac{x}{r}$, $1/r$ exists, since r is coprime to N. Similar to the case of sum sets,

$$\phi(x_i) + \phi(0) = i + 0 = i.$$

Moreover, $\phi(-A) = -\phi(A)$. Thus,

$$1_A * 1_{-A}(\boldsymbol{x}) = 1_{\phi(A)} * 1_{\phi(-A)}(\phi(\boldsymbol{x}) + \phi(0)) = 1_{\phi(A)} * 1_{-\phi(A)}(0, 1, ..., n).$$

Since ϕ is an bijection,

$$|\{A \in \mathbb{Z}_N : 1_A * 1_{-A}(\boldsymbol{x}) = \boldsymbol{y}\}| = |\{A \in \mathbb{Z}_N : 1_{\phi(A)} * 1_{-\phi(A)}(0, 1, ..., n) = \boldsymbol{y}\}|$$

$$= |\{A \in \mathbb{Z}_N : 1_A * 1_{-A}(0, 1, ..., n) = \boldsymbol{y}\}|.$$

Therefore, although our recurrence relation only considers the convolution at $(0, 1, ..., n)$, it is equivalent to all $\boldsymbol{x}$.

We can generate the following recurrence relation for d^i on i.

Theorem 3.4 (Recurrence Relation for Convolution of Intervals for Difference Sets)**.** Let $G = \mathbb{Z}_N$, and let d^i be defined as above. Let $\mathcal{B} = \{0, 1\}^n$, then for all $\boldsymbol{y} \in [0, N]^{n+1}, b \in \mathcal{B}, n - 1 < i < N - n$,

$$d^i(\boldsymbol{y}, b) = d^{i-1}(\boldsymbol{y}, b'^\frown 0) + d^{i-1}(\boldsymbol{y}, b'^\frown 1) + d^{i-1}(\boldsymbol{y} - b^\frown 0, b'^\frown 0) + d^{i-1}(\boldsymbol{y} - b^\frown 1, b'^\frown 1).$$

Remark. As in the case of sum sets. The argumentation is the same for $G = \mathbb{Z}_N$ or $\mathbb{Z}$. As before, we will treat the ambient group as $\mathbb{Z}_N$. The upper bound $N - n$ only exists due to the "wrap-around" of $\mathbb{Z}_N$. For $\mathbb{Z}$ the only constraint on i is $n - 1 < i$.

To prove Theorem 3.2, as well as the convexity property of the set image, we first prove the following lemma:

Lemma 3.5. Let $n-1 < i < N-n$. Given $T \subseteq \{i\}$, define the mapping $\phi_T(A) := A \cup T$. For all $A \in \mathcal{D}^{i-1}$, if $T = \emptyset$, then

$$1_A * 1_{-A}(0, 1, ..., n) = 1_{\phi_T(A)} * 1_{-\phi_T(A)}(0, 1, ..., n).$$

If $T = \{i\}$, for all $b \in B, A \in \mathcal{D}_b^{i-1}$,

$$1_A * 1_{-A}(0, 1, ..., n) + (1^\frown b) = 1_{\phi_T(A)} * 1_{-\phi_T(A)}(0, 1, ..., n).$$

Proof. Since A and T are disjoint, we have

$$1_{\phi_T(A)} * 1_{-\phi_T(A)}(0, 1, ..., n) = 1_{A \cup T} * 1_{-(A \cup T)}(0, 1, ..., n)$$

$$= 1_A * 1_{-A}(0, 1, ..., n) + 1_A * 1_{-T}(0, 1, ..., n) + 1_T * 1_{-A}(0, 1, ..., n) + 1_T * 1_{-T}(0, 1, ..., n)$$

For the case $T = \emptyset$, ϕ_T is the identity mapping so the convolution is trivially equal.

For the case $T = \{i\}$, assume that there exists $a \in A$, such that $a - i \in [0, n]$, so $a \in [i, i + n]$. However, $A \subseteq [0, i - 1]$, and

$$[0, i - 1] \cap [i, i + n] = \emptyset,$$

as $i + n < N$ by the bounds on i. Therefore, no such a exists and we have that

$$1_A * 1_{-T}(0, 1, ..., n) = 0.$$

Now,

$$1_T * 1_{-A}(0, 1, ..., n) \neq 0$$

if and only if there exists $a \in A$ such that $i - a \in [0, n]$. For all $a \in A \cap [i - n, -i]$, we have $b_{a-i+n+1} = 1$ by definition of b. Thus a, i contributes to the $a - i + n + 1$ coordinate of $1_T * 1_{-A}(0, 1, ..., n)$. Thus

$$1_T * 1_{-A}(0, 1, ..., n) = 0^\frown b.$$

Lastly, $i - i = 0$, contributes to $1_T * 1_{-T}(0)$, the first entry. Thus

$$1_T * 1_{-T}(0, 1, ..., n) = e_1,$$

and

$$1_T * 1_{-A}(0, 1, ..., n) + 1_T * 1_{-T}(0, 1, ..., n) = 1^\frown b.$$

ϕ_T increases the convolution as described. □

Now we prove Theorem 3.4 using the mapping ϕ_T.

Proof of Theorem 3.4. We follow the proof of Theorem 3.2. For any subset $T \subseteq \{i\}$, let $\phi_T : \mathcal{D}^{i-1} \to \mathcal{D}^i$ be as described in Lemma 3.3. For any $A \in \mathcal{D}^{i-1}$, since $T \cap A = \emptyset$, each ϕ_T is one-to-one. For any set $A' \in \mathcal{D}^i$, if

$$T = A' \cap \{i\}, A = A' \cap [0, i-1],$$

then $\phi_T(A) = A'$. Moreover, each mapping ϕ_T has a disjoint image. Therefore, the two images of each ϕ_T give a partition of $\mathcal{D}^i$.

Define

$$\mathcal{S} := \{A \in \mathcal{D}^i_b : 1_A * 1_A(0, 1, ..., n) = \boldsymbol{y}\},$$

then

$$d^i(\boldsymbol{y}, b) = |\mathcal{S}| = \sum_{T \subseteq \{i\}} |\phi_T^{-1}(\mathcal{S})|.$$

Thus to figure out $d^i(\boldsymbol{y}, b)$, we simply have to calculate the number of sets that map into $\mathcal{S}$ by all ϕ_T.

By the definition of b, for all $b, A \in \mathcal{D}^{i-1}_b$, if $T = \emptyset$, then $\phi_T(A) \in \mathcal{D}^i_{0^\frown b'}$. If $T = \{-i\}$, then $\phi_T(A) \in \mathcal{D}^i_{1^\frown b'}$.

Now we calculate the size of $\mathcal{S}$ for some given $b, \boldsymbol{y}$. By Lemma 3.5, we see that for all $A \in \mathcal{D}^{i-1}$, if $T = \emptyset$, then $\phi_T(A) \in \mathcal{S}$ if and only if

$$A \in \mathcal{D}^i_{b'^\frown 0} \cup \mathcal{D}^i_{b'^\frown 1}, 1_A * 1_A(0, 1, ..., n) = \boldsymbol{y}.$$

The number of such A is

$$|\phi_{\emptyset}^{-1}(\mathcal{S})| = c^{i-1}(\boldsymbol{y}, b'^\frown 0) + c^{i-1}(\boldsymbol{y}, b'^\frown 1), \tag{3.5}$$

If $T = \{i\}$, then $\phi_T(A) \in \mathcal{S}$ if and only if

$$A \in \mathcal{D}^i_{b'^\frown 0}, 1_A * 1_A(0, 1, ..., n) + b^\frown 0 = \boldsymbol{y},$$

or

$$A \in \mathcal{D}^i_{b'^\frown 1}, 1_A * 1_A(0, 1, ..., n) + b^\frown 1 = \boldsymbol{y}.$$

The number of such A is

$$|\phi_{\{i\}}^{-1}(\mathcal{S})| = d^{i-1}(\boldsymbol{y} - b^\frown 0, b'^\frown 0) + d^{i-1}(\boldsymbol{y} - b^\frown 1, b'^\frown 1). \tag{3.6}$$

If $T = \{-i\}, \{-i, i\}$, then $\phi_T(A) \notin \mathcal{S}$, since $b_0 = 0$. Thus we have

$$|\phi_{\{-i\}}^{-1}(\mathcal{S})| = |\phi_{\{-i,i\}}^{-1}(\mathcal{S})| = 0. \tag{3.7}$$

The sum of Eq. (3.5), Eq. (3.6), Eq. (3.7) gives the desired recurrence relation. □

3.2 Convexity Sum Sets in 2d

Now we can prove the convexity property of the set image of convolutions using the recurrence mapping of Lemma 3.3. Let $2\mathbb{Z}$ denote the even numbers. Then we have the following description of the set image:

Theorem 3.6 (Convexity of Sum Set for 2-d)**.** For $N \geq 3$, $x_1, x_2 \in \mathbb{Z}_N$, if $x_1 - x_2$ is coprime to N, then the set image S of $1_A * 1_A(x_1, x_2)$ is nearly convex in the following sense: Let

$$C = CH(\{(0, 0), (N/2, 0), (0, N/2), (N, N)\}).$$

If N is odd, then

$$S = C \cap \mathbb{Z}^2 \setminus \{(N-1, N-1)\}.$$

If N, x_1 is even, then

$$S = C \cap (\mathbb{Z} \times 2\mathbb{Z}) \setminus \{(0, N/2)\}.$$

If N is even and x_1 is odd, then

$$S = C \cap (2\mathbb{Z} \times \mathbb{Z}) \setminus \{(N/2, 0)\}.$$

Remark. It is probably possible to have a combinatorics proof that is simpler by considering sets that maximize or minimize the convolutions. However, this proof: 1. Provides a interesting connection between the recurrence relation of convolutions and translations of geometric objects. 2. Allows us to consider the three dimensions. Combinatorial arguments seem to become much more difficult to manage when considering three dimensions or more. These mappings to geometric objects allows us to talk about three dimensions.

Proof. By Proposition 1.7, we only need to show the case $1_A * 1_A(0, 1)$ due to the following Freiman isomorphism: Let N be odd, or x_1 be even. Given x_1, x_2, we have the Freiman 2-isomorphism

$$\phi_1(x) := \frac{2x - x_1}{2(x_2 - x_1)}.$$

$1/(x_2 - x_1)$ exists, since it is coprime to N. If N is odd, then $1/2$ exists. If x_1 is even, then $x_1/2$ exists. Therefore, this mapping is valid in both cases. Note that $x_1 = x_1 + 0, x_2 = x_2 + 0$,

$$\phi_1(x_1) + \phi_1(0) = \frac{2x_1 - x_1}{2(x_2 - x_1)} - \frac{x_1}{2(x_2 - x_1)} = 0.$$

$$\phi_1(x_2) + \phi_1(0) = \frac{2x_2 - x_1}{2(x_2 - x_1)} - \frac{x_1}{2(x_2 - x_1)} = 1.$$

If N is even and x_1 is odd, then x_2 is even since $x_1 - x_2$ is coprime to N. Then, we can swap x_1, x_2 to get the previous case. The set image is then equivalent to $1_A * 1_A(1, 0)$.

Thus, by Proposition 1.7, the set image of $1_A * 1_A(x_1, x_2)$ is the same as $1_A * 1_A(0,1)$ or $1_A * 1_A(1,0)$. We will look at the case $1_A * 1_A(0,1)$.

Let $S_b^i \subseteq [0,N]^n$ be the set image corresponding to $\mathcal{A}_b^i$, that is

$$S_b^i := \{\boldsymbol{y} \in [0,N]^2 : \exists A \in \mathcal{A}_b^i, 1_A * 1_A(0,1) = \boldsymbol{y}\}.$$

We first show a recurrence relation for S_b^i using ϕ_T as described in Lemma 3.3. For any $T \subseteq \{-i, i\}$, define the mapping

$$\chi_T(S_b^{i-1}) := \{\boldsymbol{y} \in [0,N]^2 : \exists A \in \mathcal{A}_b^i, 1_{\phi_T(A)} * 1_{\phi_T(A)}(0,1) = \boldsymbol{y}\}.$$

For any set $A' \in \mathcal{A}^i$, $A' = A \cup T$ for some unique $A \in \mathcal{A}^{i-1}, T \subseteq \{-i, i\}$. Therefore, the four images of each ϕ_T give a partition of $\mathcal{A}^i$. $\mathcal{A}_0^i$ is covered by the image of $\phi_\emptyset, \phi_{\{i\}}$. $\mathcal{A}_1^i$ is covered by the image of $\phi_{\{-i\}}, \phi_{\{-i,i\}}$. The set image S_0^i, S_1^i is then covered by the four χ_T. More specifically, we have

$$\begin{aligned} S_0^i &= \chi_\emptyset(S_0^{i-1}) \cup \chi_\emptyset(S_1^{i-1}) \cup \chi_{\{i\}}(S_0^{i-1}) \cup \chi_{\{i\}}(S_1^{i-1}) \\ S_1^i &= \chi_{\{-i\}}(S_0^{i-1}) \cup \chi_{\{-i\}}(S_1^{i-1}) \cup \chi_{\{-i,i\}}(S_0^{i-1}) \cup \chi_{\{-i,i\}}(S_1^{i-1}) \end{aligned} \tag{3.8}$$

Now we evaluate what each set gets mapped to by each χ_T. First consider the cases $T = \emptyset, \{-i\}$. By Lemma 3.3, for $1_A * 1_A(0,1) = 1_{\phi_T(A)} * 1_{\phi_T(A)}(0,1)$. Thus we have

$$\chi_\emptyset(S_0^{i-1}) = \chi_{\{-i\}}(S_0^{i-1}) = S_0^{i-1}, \chi_\emptyset(S_1^{i-1}) = \chi_{\{-i\}}(S_1^{i-1}) = S_1^{i-1}$$

since none of the convolutions changed.

Now consider the cases $T = \{i\}, \{-i, i\}$. By Lemma 3.3,

$$1_A * 1_A(0,1) + 2 \cdot (0^\frown b) = 1_{\phi_{\{i\}}(A)} * 1_{\phi_{\{i\}}(A)}(0,1),$$

and

$$1_A * 1_A(0,1) + 2 \cdot (1^\frown b) = 1_{\phi_{\{-i,i\}}(A)} * 1_{\phi_{\{-i,i\}}(A)}(0,1).$$

Thus we have

$$\begin{aligned} \chi_{\{i\}}(S_0^{i-1}) &= S_0^{i-1} + 2 \cdot (0,0) = S_0^{i-1} \\ \chi_{\{i\}}(S_1^{i-1}) &= S_1^{i-1} + (0,2) \\ \chi_{\{-i,i\}}(S_0^{i-1}) &= S_0^{i-1} + (2,0) \\ \chi_{\{-i,i\}}(S_1^{i-1}) &= S_1^{i-1} + (2,2) \end{aligned} \tag{3.9}$$

Adding the points to the sets S_b^{i-1} denotes the translation by that point. Combining Eq. (3.9) with Eq. (3.8), we have that for all i,

$$\begin{aligned} S_0^i &= S_0^{i-1} \cup S_1^{i-1} \cup (S_1^{i-1} + (0,2)) \\ S_1^i &= S_0^{i-1} \cup S_1^{i-1} \cup (S_0^{i-1} + (2,0)) \cup (S_1^{i-1} + (2,2)). \end{aligned} \tag{3.10}$$

Now, using induction we will show that for $1 \leq i < (N-1)/2$,

$$S_1^i = C_1^i \cap (\mathbb{Z} \times 2\mathbb{Z}) \tag{3.11}$$

where

$$C_1^i := CH(\{(0,0), (i+1,0), (0, i-1/2), (2i+1, 2i)\}).$$

and

$$S_0^i = C_0^i \cap (\mathbb{Z} \times 2\mathbb{Z}), \tag{3.12}$$

where

$$C_0^i := C_1^{i-1} \cup (C_1^{i-1} + (0,2)),$$

For the base case $i = 1, 2$, we show in appendix Chapter B that Eq. (3.12) and Eq. (3.11) holds. Now assume by the induction hypothesis that Eq. (3.12), Eq. (3.11) holds for $i -$

$1, i-2$. Since all terms are intersecting $Z \times 2\mathbb{Z}$, including the translated terms which are translated by 2, we may rewrite Eq. (3.10) with the induction hypothesis as

$$\begin{aligned}
S_0^i &= \Big(C_0^{i-1} \cup C_1^{i-1} \cup (C_1^{i-1} + (0,2))\Big) \cap \Big(\mathbb{Z} \times 2\mathbb{Z}\Big) \\
&= \Big(C_1^{i-2} \cup (C_1^{i-2} + (0,2)) \cup C_1^{i-1} \cup (C_1^{i-1} + (0,2))\Big) \cap \Big(\mathbb{Z} \times 2\mathbb{Z}\Big) \\
&= \Big(C_1^{i-1} \cup (C_1^{i-1} + (0,2))\Big) \cap \Big(\mathbb{Z} \times 2\mathbb{Z}\Big) \\
S_1^i &= \Big(C_0^{i-1} \cup C_1^{i-1} \cup (C_0^{i-1} + (2,0)) \cup (C_1^{i-1} + (2,2))\Big) \cap \Big(\mathbb{Z} \times 2\mathbb{Z}\Big) \\
&= \Big(C_1^{i-2} \cup (C_1^{i-2} + (0,2)) \cup C_1^{i-1} \cup (C_1^{i-2} + (2,0)) \\
&\quad \cup (C_1^{i-2} + (2,2)) \cup (C_1^{i-1} + (2,2))\Big) \cap \Big(\mathbb{Z} \times 2\mathbb{Z}\Big) \\
&= \Big((C_1^{i-2} + (0,2)) \cup C_1^{i-1} \cup (C_1^{i-2} + (2,0)) \cup (C_1^{i-1} + (2,2))\Big) \cap \Big(\mathbb{Z} \times 2\mathbb{Z}\Big).
\end{aligned}$$

Thus to show Eq. (3.12) and Eq. (3.11), we only need to show

$$C_0^i = C_1^{i-1} \cup (C_1^{i-1} + (0,2)) \tag{3.13}$$

and

$$C_1^i = (C_1^{i-2} + (0,2)) \cup C_1^{i-1} \cup (C_1^{i-2} + (2,0)) \cup (C_1^{i-1} + (2,2)) \tag{3.14}$$

Eq. (3.13) is the definition of C_0^i, thus it is trivial. Now we look at Eq. (3.14). $C_1^{i-2} + (0,2), C_1^{i-1}, C_1^{i-2} + (2,0), C_1^{i-1} + (2,2)$ has vertices

$$\begin{aligned}
&\{(0,2), (i-1,2), (0, i-1/2), (2i-3, 2i-2)\} \\
&\{(0,0), (i,0), (0, i-3/2), (2i-1, 2i-2)\} \\
&\{(2,0), (i+1,0), (2, i-5/2), (2i-1, 2i-4)\} \\
&\{(2,2), (i+2,2), (2, i+1/2), (2i+1, 2i)\}.
\end{aligned} \tag{3.15}$$

We will first show that

$$C_1^i \supseteq (C_1^{i-2} + (0,2)) \cup C_1^{i-1} \cup (C_1^{i-2} + (2,0)) \cup (C_1^{i-1} + (2,2)) \tag{3.16}$$

by showing that C_1^i contains all of the vertices in Eq. (3.15). Since C_1^i contains the rectangle with vertices

$$\{(0,0), (i+1,0), (0,i-1/2), (i+1,i-1/2)\},$$

by convexity we have

$$\{(0,2), (i-1,2), (0,i-1/2), (0,0), (i,0),$$
$$(0,i-3/2), (2,0), (i+1,0), (2,i-5/2), (2,2)\} \subseteq C_1^i.$$

$(2i-3, 2i-2)$ and $(2, i+1/2)$ falls in L_1, the line from $(i+1,0)$ to $(2i+1,2i)$. $(2i-1, 2i-4)$ and $(i+2,2)$ falls in L_2, the line from $(i+1,0)$ to $(2i+1,2i)$. The slope of L_1 is $1/2$. The slope of the line from L_2 is 2. The slope of the line from $(2i-1,2i-2)$ to $(2i+1,2i)$ is 1. Thus, $(2i-1,2i-2)$ falls within the two lines and is in C^i. Therefore, C^i contains all vertices in Eq. (3.15). By convexity, we have Eq. (3.16).

Now we show

$$C_1^i \subseteq (C_1^{i-2} + (0,2)) \cup C_1^{i-1} \cup (C_1^{i-2} + (2,0)) \cup (C_1^{i-1} + (2,2)). \tag{3.17}$$

Note that the shapes above have symmetry across the line $x = y$ in $\mathbb{R}^2$, thus it is sufficient to show inclusion for $x \leq y$. Consider P, the closure of $C_1^i \setminus C_1^{i-2}$ with $x \leq y$.. We have

$$P = CH(\{(0,i-3/2), (0,i-1/2), (2i-1,2i-2), (2i+1,2i)\}).$$

Note that $C_1^{i-1} + (2, 2)$ covers

$$CH(\{(2, i + 1/2), (2, i - 1/2), (2i - 1, 2i - 2), (2i + 1, 2i)\})$$

and $C_1^{i-2} + (0, 2)$ covers

$$CH(\{((0, i - 3/2), (0, i - 1/2), (2, i + 1/2), (2, i - 1/2)\}).$$

Thus, P is completely covered, and we have Eq. (3.17). Combining with Eq. (3.16) shows Eq. (3.14).

Now let $i = \lfloor N/2 \rfloor$. Note that $S = S_0^i \cup S_1^i$. By Eq. (3.12), Eq. (3.11), we have

$$S_0^{i-1} = C_0^{i-1} \cap (\mathbb{Z} \times 2\mathbb{Z})$$

$$S_1^{i-1} = C_1^{i-1} \cap (\mathbb{Z} \times 2\mathbb{Z}).$$

However, our recurrence relation does not extend to $\lfloor N/2 \rfloor$, thus we have to calculate it explicitly.

First consider the case N, x_1 is even, $i = N/2 = -i$. Thus for the mapping χ_T, the only mapping is $T = \emptyset, \{i\}$. We have

$$S_0^i = \chi_\emptyset(S_0^{i-1}) \cup \chi_\emptyset(S_1^{i-1})$$
$$S_1^i = \chi_{\{i\}}(S_0^{i-1}) \cup \chi_{\{i\}}(S_1^{i-1})$$

For $T = \emptyset$, it is the identity mapping, so trivially we have

$$S_0^i = S_0^{i-1} \cup S_1^{i-1}.$$

For $T = \{i\}$, $i + i = 0$, thus it increases the convolution at 0 by 1. The sets in S_1^{i-1} contain $-(i - 1) = i + 1$, and $i + i + 1 = 1$, thus the convolution at 1 increases by 2. Thus we have

$$S_1^i = (S_0^{i-1} + (1,0)) \cup (S_1^{i-1} + (1,2)).$$

So

$$S = S_1^i \cup S_0^i$$

$$= \Big(C_1^{i-2} \cup (C_1^{i-2}+(0,2)) \cup C_1^{i-1} \cup (C_1^{i-2}+(1,0)) \cup (C_1^{i-2}+(1,2)) \cup (C_1^{i-1}+(1,2))\Big) \cap \Big(\mathbb{Z}\times 2\mathbb{Z}\Big)$$

$$= \Big((C_1^{i-2} + (0,2)) \cup C_1^{i-1} \cup (C_1^{i-2} + (1,0)) \cup (C_1^{i-1} + (1,2))\Big) \cap \Big(\mathbb{Z} \times 2\mathbb{Z}\Big). \quad (3.18)$$

Therefore, we need to show Eq. (3.18) is equal to $C \cap (\mathbb{Z} \times 2\mathbb{Z}) \setminus \{(0, N/2)\}$.

Now $C_1^{i-2} + (0,2), C_1^{i-1}, C_1^{i-2} + (1,0), C_1^{i-1} + (1,2)$ has vertices:

$$\begin{aligned} &\{(0,2), (i-1,2), (0, i-1/2), (2i-3, 2i-2)\} \\ &\{(0,0), (i,0), (0, i-3/2), (2i-1, 2i-2)\} \\ &\{(1,0), (i,0), (1, i-5/2), (2i-2, 2i-4)\} \\ &\{(1,2), (i+1,2), (1, i+1/2), (2i, 2i)\} \end{aligned} \quad (3.19)$$

We first show that C contains all vertices in Eq. (3.19). C contains the rectangle with vertices

$$\{(0,0), (i,0), (0,i), (2i,2i)\}.$$

By convexity we have

$$\{(0,2), (i-1,2), (0, i-1/2), (1,0), (i,0), (1, i-5/2), (0,0), (0, i-3/2), (1,2)\} \subseteq C_1^i.$$

The rest of the points fall between the line from $(i,0)$ to $(2i,2i)$ or the line from $(0,i)$ to $(2i,2i)$. Note that $(0,i)$ is not in Eq. (3.19), so $C \cap (\mathbb{Z} \times 2\mathbb{Z}) \setminus \{(0,N/2)\}$ contains Eq. (3.18). Now we show that Eq. (3.18) contains $C \cap (\mathbb{Z} \times 2\mathbb{Z}) \setminus \{(0,N/2)\}$. Q, the closure of $C \setminus C_1^{i-1}$ is

$$Q = CH(\{(0, i-3/2), (0, i), (2i-1, 2i-2), (2i, 2i)\}).$$

Note that $C_1^{i-1} + (1, 2)$ covers

$$CH(\{(1, i-1), (1, i+1/2), (2i-1, 2i-2), (2i, 2i)\})$$

and $C_1^{i-2} + (0, 2)$ covers

$$CH(\{(0, i-3/2), (0, i-1/2), (1, i-1), (1, i+1/2)\}).$$

The only point left is $(0, i)$. Thus Eq. (3.18) contains $C \cap (\mathbb{Z} \times 2\mathbb{Z}) \setminus \{(0, N/2)\}$, and that the two is equal.

Now we consider the case N is odd, $i = (N-1)/2$. We have Eq. (3.8) as before. Since $\chi_\emptyset, \chi_{\{i\}}$ is still the same mapping as in Eq. (3.9), S_0^i is the same as in Eq. (3.12). However, now adding $-i = 1/2$ increases the convolution at 1 by 1, so

$$\begin{aligned}
\chi_{\{-i\}}(S_0^{i-1}) &= S_0^{i-1} + (0, 1) \\
\chi_{\{-i\}}(S_1^{i-1}) &= S_1^{i-1} + (0, 1) \\
\chi_{\{-i,i\}}(S_0^{i-1}) &= S_0^{i-1} + (2, 1) \\
\chi_{\{-i,i\}}(S_1^{i-1}) &= S_1^{i-1} + (2, 3).
\end{aligned}$$

We then have

$$S_1^i = (S_0^{i-1} + (0, 1)) \cup (S_1^{i-1} + (0, 1)) \cup (S_0^{i-1} + (2, 1)) \cup (S_1^{i-1} + (2, 1)), \tag{3.20}$$

which is similar to the case $i < N/2 - 1$, except shifted by $(0, 1)$. Thus

$$S_1^i = \Big(C_1^i \cap (\mathbb{Z} \times 2\mathbb{Z})\Big) + (0, 1)$$

Thus we have

$$S = S_0^i \cup S_1^i = \Big(C_0^i \cap (\mathbb{Z} \times 2\mathbb{Z})\Big) \cup \bigg(\Big(C_1^i \cap (\mathbb{Z} \times 2\mathbb{Z})\Big) + (0,1)\bigg). \tag{3.21}$$

To show

$$S = C \cap \mathbb{Z}^2 \setminus \{(N-1, N-1)\},$$

we have to show

$$C_0^i \cap (\mathbb{Z} \times 2\mathbb{Z}) = C \cap (\mathbb{Z} \times 2\mathbb{Z}) \setminus \{(N-1, N-1)\}, \tag{3.22}$$

$$\Big(C_1^i \cap (\mathbb{Z} \times 2\mathbb{Z})\Big) + (0,1) = C \cap (\mathbb{Z} \times 2\mathbb{Z} + 1). \tag{3.23}$$

We first show Eq. (3.22). For any $(x, y) \in C \cap (\mathbb{Z} \times 2\mathbb{Z})$, the convext hull falls left of the line from $(i + 1/2, 0)$ to $(2i + 1, 2i + 1)$. Thus, $x \leq (y + 2i + 1)/2$. For y even, $(y + 2i + 1)/2$ is not a integer so $x \leq (y + 2i)/2$. Therefore we may shift the line by $(-1/2, 0)$ and now consider the line from $(i, 0)$ to $(2i + 1/2, 2i + 1)$. Since $2i + 1$ is odd, and we've removed $\{(N - 1, N - 1)\} = (2i, 2i)$ we may consider the line from $(i, 0)$ to $(2i - 1, 2i - 2)$. Similarly, consider the line from $(0, i)$ to $(2i + 1, 2i + 1)$, we may shift the line by $(0, 1/2)$ without including any additional points. Thus we consider the line from $(0, i + 1/2)$ to $(2i + 1, 2i + 3/2)$. Since $2i + 1$ is odd, the line from $(0, i + 1/2)$ to $(2i + 1, 2i + 3/2)$. becomes $(0, i + 1/2)$ to $(2i - 1, 2i)$. $C \cap (\mathbb{Z} \times 2\mathbb{Z}) \setminus \{(N - 1, N - 1)\}$ then have vertices at

$$\{(0, 0), (0, i), (i, 0), (2i - 1, 2i - 2), (2i - 1, 2i)\},$$

which is the same as $C_0^i \cap (\mathbb{Z} \times 2\mathbb{Z})$.

For Eq. (3.23), $\left(C_1^i \cap (\mathbb{Z} \times 2\mathbb{Z})\right) + (0,1)$ has vertices

$$\{(0,1),(i+1,1),(0,i+1/2),(2i+1,2i+1)\},$$

which is the same as C, except missing then line from $(0,0)$ to $(i,0)$, which is in $\mathbb{Z} \times 2\mathbb{Z}$ and not in $\mathbb{Z} \times 2\mathbb{Z} + 1$.

Thus Eq. (3.21) holds and we've shown the theorem in both the even and odd case. $\square$

Note that the 2 dimensional case of the difference set $1_A * 1_{-A}(0,1)$ is equivalent to the 1 dimensional case of Theorem 2.4. This is because $|A| = 1_A * 1_{-A}(0)$. By Theorem 2.4, the set image of $1_A * 1_{-A}(0,1)$ is approximately

$$CH(\{(0,0),(N/2,0),(N,N)\}).$$

Therefore, we will consider the 3 dimensional case for difference set. We will utilize a similar strategy of considering the change of the set images through out the recurrence relation. This will allow us to approximate the set image up to a small constant error term. We express this error term as $O(1)[0,1]^3$, which is the box $[0,1]^3$ dilated by some constant.

Theorem 3.7 (Convexity of Difference Set for 3-d)**.** For $N \geq 3$, $x \in \mathbb{Z}_N$, if x is coprime to N, then the set image S of $1_A * 1_{-A}(0,x,2x)$ is nearly convex in the following sense: Let

$$C = CH(\{(0,0,0),(N/3,0,0),(N/2,N/4,0),(N/2,0,N/2),(2N/3,N/3,N/3),(N,N,N)\}),$$

then

$$C \subseteq S + O(1)[0,1]^3 \subseteq C + O(1)[0,1]^3$$

Proof. By Proposition 1.7, we only need to show the case $1_A * 1_{-A}(0,1,2)$ due to the Freiman 2-isomorphism $\phi(t) = t/x$. x has a inverse, since it is coprime to N. Since

$\phi(-t) = -\phi(t)$,

$$1_A * 1_{-A}(0, x, 2x) = 1_{\phi(A)} * 1_{\phi(-A)}(\phi(0), \phi(x), \phi(2x)) = 1_{\phi(A)} * 1_{-\phi(A)}(0, 1, 2),$$

which has the same set image as $1_A * 1_{-A}(0, 1, 2)$, since ϕ is a bijection.

We will first show that $S \subseteq C + O(1)[0, 1]^3$. Let $S_b^i \subseteq [0, N]^n$ be the set image corresponding to $\mathcal{D}_b^i$, that is

$$S_b^i := \{\boldsymbol{y} \in [0, N]^3 : \exists A \in \mathcal{D}_b^i, 1_A * 1_{-A}(0, 1, 2) = \boldsymbol{y}\}.$$

Now we will establish the recurrence relation for all S_b^i, using ϕ_T as described in Lemma 3.5. For any $T \subseteq \{i\}$, define the mapping

$$\chi_T(S_b^{i-1}) := \{\boldsymbol{y} \in [0, N]^3 : \exists A \in \mathcal{D}_b^i, 1_{\phi_T(A)} * 1_{\phi_T(-A)}(0, 1, 2) = \boldsymbol{y}\}.$$

For any set $A' \in \mathcal{D}^i$, $A' = A \cup T$ for some unique $A \in \mathcal{D}^{i-1}, T \subseteq \{, i\}$. Therefore, the two images of each ϕ_T give a partition of $\mathcal{D}^i$. More specifically, we have

$$\begin{aligned} S_{00}^i &= \chi_\emptyset(S_{00}^{i-1}) \cup \chi_\emptyset(S_{01}^{i-1}) \\ S_{01}^i &= \chi_\emptyset(S_{10}^{i-1}) \cup \chi_\emptyset(S_{11}^{i-1}) \\ S_{10}^i &= \chi_{\{i\}}(S_{00}^{i-1}) \cup \chi_{\{i\}}(S_{01}^{i-1}) \\ S_{11}^i &= \chi_{\{i\}}(S_{10}^{i-1}) \cup \chi_{\{i\}}(S_{11}^{i-1}). \end{aligned} \tag{3.24}$$

Now we evaluate what each set gets mapped to by each χ_T. Let $A \in \mathcal{D}^{)-\infty}$.First consider the cases $T = \emptyset$. By Lemma 3.5, for $1_A * 1_{-A}(0, 1, 2) = 1_{\phi_T(A)} * 1_{-\phi_T(A)}(0, 1, 2)$. Thus we have that $\chi_\emptyset$ is the identity mapping.

Now consider the cases $T = \{i\}$. By Lemma 3.5,

$$1_A * 1_{-A}(0, 1, 2) + (1^\frown b) = 1_{\phi_{\{i\}}(A)} * 1_{-\phi_{\{i\}}(A)}(0, 1, 2).$$

Thus we have that

$$\begin{aligned}
\chi_{\{i\}}(S_{00}^{i-1}) &= S_{00}^{i-1} + (1,0,0) \\
\chi_{\{i\}}(S_{01}^{i-1}) &= S_{01}^{i-1} + (1,0,1) \\
\chi_{\{i\}}(S_{10}^{i-1}) &= S_{10}^{i-1} + (1,1,0) \\
\chi_{\{i\}}(S_{11}^{i-1}) &= S_{11}^{i-1} + (1,1,1)
\end{aligned} \tag{3.25}$$

Combining Eq. (3.25) with Eq. (3.24), we have

$$\begin{aligned}
S_{00}^{i} &= S_{00}^{i-1} \cup S_{01}^{i-1} \\
S_{01}^{i} &= S_{10}^{i-1} \cup S_{11}^{i-1} \\
S_{10}^{i} &= (S_{00}^{i-1} + (1,0,0)) \cup (S_{01}^{i-1} + (1,0,1)) \\
S_{11}^{i} &= (S_{10}^{i-1} + (1,1,0)) \cup (S_{11}^{i-1} + (1,1,1))
\end{aligned} \tag{3.26}$$

Now let

$$C^i := CH(\{(0,0,0),(i/3,0,0),(i/2,i/4,0),(i/2,0,i/2),(2i/3,i/3,i/3),(i,i,i)\}).$$

We will show using induction that for $3 \leq i < N-2$,

$$\begin{aligned}
S_{00}^{i} &\subseteq C^{i+1} \\
S_{01}^{i} &\subseteq C^{i+2} \\
S_{10}^{i} &\subseteq (C^{i} + (1,0,0)) \cup (C^{i+1} + (1,0,1)) \\
S_{11}^{i} &\subseteq (C^{i-1} + (2,1,0)) \cup (C^{i} + (2,1,1)).
\end{aligned} \tag{3.27}$$

First, consider the base case $i = 3$. The appendix Chapter C gives the 16 subset of $[0,3]$, which can be verified manually to exists in the convex hulls.

Note that since we have the recurrence relation Eq. (3.26), we may rewrite Eq. (3.27)

as

$$\begin{aligned} S_{00}^{i-1} \cup S_{01}^{i-1} &\subseteq C^{i+1} \\ S_{10}^{i-1} \cup S_{11}^{i-1} &\subseteq C^{i+2} \\ (S_{00}^{i-1} + (1,0,0)) \cup (S_{01}^{i-1} + (1,0,1)) &\subseteq (C^i + (1,0,0)) \cup (C^{i+1} + (1,0,1)) \\ (S_{10}^{i-1} + (1,1,0)) \cup (S_{11}^{i-1} + (1,1,1)) &\subseteq (C^{i-1} + (2,1,0)) \cup (C^i + (2,1,1)). \end{aligned} \tag{3.28}$$

Now as the inductive hypothesis, assume Eq. (3.27) holds for $i-1$. We first look at the first inclusion of Eq. (3.28). By the induction hypothesis, we have

$$S_{00}^{i-1} \cup S_{01}^{i-1} \subseteq C^i \cup C^{i+1} \subseteq C^{i+1}.$$

Now we look at the second inclusion of Eq. (3.28). By the induction hypothesis, we have

$$S_{10}^{i-1} \subseteq (C^{i-1} + (1,0,0)) \cup (C^i + (1,0,1)), S_{11}^{i-1} \subseteq (C^{i-2} + (2,1,0)) \cup (C^{i-1} + (2,1,1)).$$

Thus we need to show

$$\begin{aligned} (C^{i-1} + (1,0,0)) \cup (C^i + (1,0,1)) &\subseteq C^{i+2}, \\ (C^{i-2} + (2,1,0)) \cup (C^{i-1} + (2,1,1)) &\subseteq C^{i+2}. \end{aligned} \tag{3.29}$$

To show this, we will show that for all $k \geq 4$,

$$C^{k-2} + (1,0,1), C^{k-3} + (1,0,0), C^{k-3} + (2,1,1), C^{k-4} + (2,1,0) \subseteq C^k \tag{3.30}$$

We look at all four cases: for any $x \in C^{k-2} + (1,0,1)$, we may express

$$x = \frac{k-2}{k} y + (1,0,1)$$

for some $y \in C^k$. Note that $y, (k/2, 0, k/2) \in C^k$,

$$x = \frac{k-2}{k} y + \frac{2}{k}(k/2, 0, k/2), \frac{k-2}{k} + \frac{2}{k} = 1,$$

so $x \in C^k$ by convexity. Therefore, $C^{k-2} + (1, 0, 1) \subseteq C^k$.

For any $x \in C^{k-3} + (1, 0, 0)$, we may express

$$x = \frac{k-3}{k} y + (1, 0, 0)$$

for some $y \in C^k$. Note that $y, (k/3, 0, 0) \in C^k$,

$$x = \frac{k-3}{k} y + \frac{3}{k}(k/3, 0, 0), \frac{k-3}{k} + \frac{3}{k} = 1,$$

so $x \in C^k$ by convexity. Therefore, $C^{k-3} + (1, 0, 0) \subseteq C^k$.

For any $x \in C^{k-3} + (2, 1, 1)$, we may express

$$x = \frac{k-3}{k} y + (2, 1, 1)$$

for some $y \in C^k$. Note that $y, (2k/3, k/3, k/3) \in C^i$,

$$x = \frac{k-3}{k} y + \frac{3}{k}(2k/3, k/3, k/3), \frac{k-3}{k} + \frac{3}{k} = 1,$$

so $x \in C^k$ by convexity. Therefore, $C^{k-3} + (2, 1, 1) \subseteq C^k$.

For any $x \in C^{k-4} + (2, 1, 0)$, we may express

$$x = \frac{k-4}{k} y + (2, 1, 0)$$

for some $y \in C^k$. Note that $y, (k/2, k/4, 0) \in C^k$,

$$x = \frac{k-4}{k} y + \frac{4}{k}(k/2, k/4, 0), \frac{k-4}{k} + \frac{4}{k} = 1,$$

so $x \in C^k$ by convexity. Therefore, $C^{k-4} + (2,1,1) \subseteq C^k$. Therefore, we've shown Eq. (3.30), and Eq. (3.29) follows if we set $k = i + 2$.

Now we look at the third inclusion of Eq. (3.28). By the induction hypothesis, we have

$$S_{00}^{i-1} \subseteq C^i, S_{01}^{i-1} \subseteq C^{i+1}$$

thus

$$(S_{00}^{i-1} + (1,0,0)) \cup (S_{01}^{i-1} + (1,0,1)) \subseteq (C^i + (1,0,0)) \cup (C^{i+1} + (1,0,1))$$

immediately follows.

Now we look at the last inclusion of Eq. (3.28). We break the inclusion into two components,

$$S_{10}^{i-1} + (1,1,0) \subseteq (C^{i-1} + (2,1,0)) \cup (C^i + (2,1,1)) \tag{3.31}$$

and

$$(S_{11}^{i-1} + (1,1,1)) \subseteq (C^{i-1} + (2,1,0)) \cup (C^i + (2,1,1)). \tag{3.32}$$

Note that Eq. (3.31) is equivalent to the induction induction hypothesis

$$S_{10}^{i-1} \subseteq (C^{i-1} + (1,0,0)) \cup (C^i + (1,0,1)),$$

except everything is shifted by $(1,1,0)$. Thus Eq. (3.31) is true. Now we want to show Eq. (3.32). By the induction hypothesis we have

$$S_{11}^{i-1} \subseteq (C^{i-2} + (2,1,0)) \cup (C^{i-1} + (2,1,1)).$$

Shifting everything by $(1,1,1)$ gives

$$S_{11}^{i-1} + (1,1,1) \subseteq (C^{i-2} + (3,2,1)) \cup (C^{i-1} + (3,2,2)).$$

Thus to show Eq. (3.32), it is sufficient to show

$$(C^{i-2} + (3,2,1)) \cup (C^{i-1} + (3,2,2)) \subseteq (C^{i-1} + (2,1,0)) \cup (C^{i} + (2,1,1)). \quad (3.33)$$

To show Eq. (3.33), we will show that for all $k \geq 1$,

$$C^{k-1} + (1,1,1) \subseteq C^k \quad (3.34)$$

For any $x \in C^{k-1} + (1,1,1)$, we may express

$$x = \frac{k-1}{k} y + (1,1,1)$$

for some $y \in C^i$. Note that $y, (k,k,k) \in C^i$,

$$x = \frac{i-1}{k} y + \frac{1}{k}(k,k,k), \frac{k-1}{k} + \frac{1}{k} = 1,$$

so $x \in C^k$ by convexity. Therefore, $C^{k-1} + (1,1,1) \subseteq C^k$. Therefore we've shown Eq. (3.34). Eq. (3.33) follows as we can set $k = i$ or $i-1$ and apply shifts $(2,1,0)$ or $(2,1,1)$.

Thus we've shown Eq. (3.27). Note that $C^{i+2} \subseteq C^i + O(1)[0,1]^3$. Thus we have for all b,

$$S_b^{N-3} \subseteq C^N + O(1)[0,1]^3.$$

Now for any $A \in \mathbb{Z}_N, B \in \mathcal{D}^{N-3}$,

$$A \setminus B \subseteq \{N-1, N-2\}.$$

The contribution to any convolution given by $A \setminus B$ is therefore $O(1)$. Thus for all b,

$$S_b^N \subseteq C^N + O(1)[0,1]^3, S \subseteq C + O(1)[0,1]^3.$$

Now we want to show the second part

$$C \subseteq S + O(1)[0,1]^3.$$

For any point $y \in C$, we simply have to construct a set A such that

$$1_A * 1_{-A}(0,1,2) = y + O(1)[0,1]^3. \tag{3.35}$$

We first show Eq. (3.35) for the vertices of C. Consider the following sets. Let ϕ_{tile} be as described in Lemma 2.2. For $y = (0,0,0)$, we have $A = \emptyset$. For $y = (N,N,N)$, we have $A = \mathbb{Z}_N$.

For $y = (N/3, 0, 0)$, Let $A = \{0\} \subseteq \mathbb{Z}_3$, then

$$1_A * 1_{-A}(0,1,2) = (1,0,0),$$

$$1_{\phi_{tile}(A)} * 1_{-\phi_{tile}(A)}(0,1,2) = (N/3,0,0) + O(1)[0,1]^3.$$

For $y = (N/2, N/4, 0)$, Let $A = \{0,1\} \subseteq \mathbb{Z}_4$, then

$$1_A * 1_{-A}(0,1,2) = (2,1,0),$$

$$1_{\phi_{tile}(A)} * 1_{-\phi_{tile}(A)}(0,1,2) = (N/2,N/4,0) + O(1)[0,1]^3.$$

For $y = (N/2, 0, N/2)$, Let $A = \{0,2\} \subseteq \mathbb{Z}_4$, then

$$1_A * 1_{-A}(0,1,2) = (2,0,2),$$

$$1_{\phi_{tile}(A)} * 1_{-\phi_{tile}(A)}(0,1,2) = (N/2, 0, N/2) + O(1)[0,1]^3.$$

For $y = (2N/3, N/3, N/3)$, Let $A = \{0,1\} \subseteq \mathbb{Z}_3$, then

$$1_A * 1_{-A}(0,1,2) = (2,1,1),$$

$$1_{\phi_{tile}(A)} * 1_{-\phi_{tile}(A)}(0,1,2) = (2N/3, N/3, N/3) + O(1)[0,1]^3.$$

Now we consider the non-vertex points. Let $v_1, .., v_6$ be the 6 vertices. For any $y \in C$, by convexity there exists $\lambda_1, .., \lambda_6 \in [0,1]$, such that

$$y = \sum_{i=1}^{6} \lambda_i v_i$$

and

$$\sum_{i=1}^{6} \lambda_i = 1.$$

Let $A_1, ..., A_6 \subseteq \mathbb{Z}_N$ be sets constructed according to $v_1, ..., y_6$ respectively. Define $\lambda_0 := 0$. For $1 \leq i \leq 6$, define

$$A_i' := A_2 \cap \left[\sum_{k=0}^{i-1} \lambda_k N, \sum_{k=0}^{i} \lambda_k N \right).$$

Let $A := \bigcup_{i=1}^{6} A_i'$. Note that since each A_i is translation invariant by 3 or 4, we have

$$1_{A_i'} * 1_{-A_i'}(0,1,2) = \lambda_i 1_{A_i} * 1_{-A_i}(0,1,2) + O(1)[0,1]^3.$$

The convolution contribution between the three components is $O(1)$, so we have

$$1_A * 1_{-A}(0,1,2) = \sum_{i=1}^{6} \lambda_i 1_{A_i} * 1_{-A_i}(0,1,2) + O(1)[0,1]^3$$

$$= \sum_{i=1}^{6} \lambda_i v_i + O(1)[0,1]^3 = y + O(1)[0,1]^3.$$

Thus we have $C \subseteq S + O(1)[0,1]^3$. $\square$

Now we consider the sum set case. for the sum set case, we only include one direction of the inclusion. We show that the set image contains a convex polytope.

Theorem 3.8 (Convexity of Sum Set for 3-d)**.** For $N \geq 3$, $x \in \mathbb{Z}_N$, Let r be coprime to N and $2|x$, or let $2r$ be coprime to N. The set image S of $1_A * 1_A(x, x+r, x+2r)$ is nearly contains a convex polytope in the following sense: Let

$$C = CH\big(\{(0,0,0),(N/3,0,0),(0,0,N/3),(0,N/2,0),(N/2,N/4,0),$$
$$(0,N/4,N/2),(N/2,0,N/2),(2N/3,N/3,N/3),(N/3,N/3,2N/3),(N,N,N)\}\big)$$

then

$$C \subseteq S + O(1)[0,1]^3.$$

Proof. By the Freiman 2-isomorphism defined in Eq. (3.1), we only need to consider the case $(0,1,2)$. Moreover, $1_A * 1_A(2,1,0)$, also has the same set image, so the first and the third coordinate is symmetric. We may flip the first and third coordinate. If (a,b,c) is in the set imagine of $1_A * 1_A(x, x+r, x+2r)$, so is (c,b,a).

We first consider sets that correspond to the vertices. Let ϕ_{tile} be as described in Lemma 2.1. For $y = (0,0,0)$, we have $A = \emptyset$. For $y = (N,N,N)$, we have $A = \mathbb{Z}_N$. For $y = (N/3,0,0)$, Let $A, B = \{0\} \subseteq \mathbb{Z}_3$, then

$$1_A * 1_B(0,1,2) = (1,0,0),$$

$$1_{\phi_{tile}(A,B)} * 1_{-\phi_{tile}(A,B)}(0,1,2) = (N/3,0,0) + O(1)[0,1]^3.$$

For $y = (0,N/2,0)$, Let $A = \{0,2\}, B = \{1,3\} \subseteq \mathbb{Z}_4$, then

$$1_A * 1_B(0,1,2) = (0,2,0),$$

$$1_{\phi_{tile}(A,B)} * 1_{-\phi_{tile}(A,B)}(0,1,2) = (0, N/2, 0) + O(1)[0,1]^3.$$

For $y = (0, N/2, 0)$, Let $A = \{0,1\}, B = \{0,3\} \subseteq \mathbb{Z}_4$, then

$$1_A * 1_B(0,1,2) = (2,1,0),$$

$$1_{\phi_{tile}(A,B)} * 1_{-\phi_{tile}(A,B)}(0,1,2) = (N/2, N/4, 0) + O(1)[0,1]^3.$$

For $y = (N/2, 0, N/2)$, Let $A, B = \{0,2\} \subseteq \mathbb{Z}_4$, then

$$1_A * 1_B(0,1,2) = (2,0,2),$$

$$1_{\phi_{tile}(A,B)} * 1_{-\phi_{tile}(A,B)}(0,1,2) = (N/2, 0, N/2) + O(1)[0,1]^3.$$

For $y = (2N/3, N/3, N/3)$, Let $A, B = \{1,2\} \subseteq \mathbb{Z}_3$, then

$$1_A * 1_B(0,1,2) = (2,1,1),$$

$$1_{\phi_{tile}(A,B)} * 1_{-\phi_{tile}(A,B)}(0,1,2) = (2N/3, N/3, N/3) + O(1)[0,1]^3.$$

Now we consider the non-vertex points. Let $v_1, .., v_{10}$ be the 10 vertices. For any $y \in C$, by convexity there exists $\lambda_1, .., \lambda_1 0 \in [0,1]$, such that

$$y = \sum_{i=1}^{10} \lambda_i v_i$$

and

$$\sum_{i=1}^{10} \lambda_i = 1.$$

Let $A_1, ..., A_{10} \subseteq \mathbb{Z}_N$ be sets constructed according to $v_1, ..., y_{10}$ respectively. Define $\lambda_0 :=$

0. For $1 \leq i \leq 10$, define

$$A_i' := A_2 \cap \left[\sum_{k=0}^{i-1} \lambda_k N, \sum_{k=0}^{i} \lambda_k N \right).$$

Let $A := \bigcup_{i=1}^{10} A_i'$. Note that since each A_i is translation invariant by 3 or 4, we have

$$1_{A_i'} * 1_{A_i'}(0,1,2) = \lambda_i 1_{A_i} * 1_{A_i}(0,1,2) + O(1)[0,1]^3.$$

The convolution contribution between the three components is $O(1)$, so we have

$$1_A * 1_A(0,1,2) = \sum_{i=1}^{10} \lambda_i 1_{A_i} * 1_{A_i}(0,1,2) + O(1)[0,1]^3$$

$$= \sum_{i=1}^{10} \lambda_i v_i + O(1)[0,1]^3 = y + O(1)[0,1]^3.$$

Thus we have $C \subseteq S + O(1)[0,1]^3$. □

As we've seen in Chapter 2 and 3, the set images are convex polytopes in the cases we look at. This leads us to the conjecture that set images are always approximately convex polytopes:

Conjecture 3.9 (Shapes of Set images)**.** Let G be a finite abelian group, and $\boldsymbol{x} \in G^d$. Let S be the set image of $1_A * 1_A(\boldsymbol{x})$. There exists a convex polytope $C \subseteq \mathbb{R}^d$ with $O(f(d))$ many vertices such that

$$S \subseteq C \subseteq S + [0,1]^d \cdot O(d).$$

The same is true for $1_A * 1_{-A}(\boldsymbol{x})$

Here, it would be interesting to understand what $f(d)$ should be, and understand if the polytope C has some special structure.

CHAPTER 4

A SMOOTHNESS PROPERTY OF CONVOLUTION

In this chapter, we will prove a smoothness property for 4-fold convolutions $1_A * 1_A * 1_A * 1_A$ for sets A that are sufficiently dense. We will then make a conjecture on 3 and 2 fold convolutions. In the last section, we will construct different sets to see the potential bounds of these conjectures.

4.1 Preliminaries

Here are some concentration results in probability that we will utilize.

Theorem 4.1 (Markov's Inequality)**.** Let X be a non-negative random variable. For all $t > 0$,

$$\mathbb{P}(X \geq t) \leq \frac{\mathbb{E}(X)}{t}.$$

Theorem 4.2 (Bernstein's Inequality)**.** Let $X_1, ..., X_n$ be independent random variables. If $\mathbb{P}(|X_i| \leq M) = 1$ and $\mathbb{E}(X_i) = 0$, then for any $t > 0$

$$\mathbb{P}\left(\sum_{i=1}^{n} X_i \geq t\right) \leq \exp\left(-\frac{t^2}{2\sum_{i=1}^{n} \mathbb{E}(X_i^2) + 2Mt/3}\right).$$

For our purposes, we will often work with complex non-centered random variables. In this case we can restate Bernstein's Inequality as:

Proposition 4.3 (Bernstein's Inequality for Complex Random Variables.)**.** Let $X_1, ..., X_n$ be independent random variables. If $\mathbb{P}(|X_i - \mathbb{E}[X_i]| \leq M) = 1$, then for any $t > 0$

$$\mathbb{P}\left(\left|\sum_{i=1}^{n} X_i - \mathbb{E}[X_i]\right| \geq t\right) \leq 4\exp\left(-\frac{t^2}{4\sum_{i=1}^{n} \mathrm{Var}(|X_i|) + 4Mt/3}\right).$$

Proof. Denote $X := \sum_{i=1}^{n} X_i - \mathbb{E}[X_i]$. Since $|\Re(X)|^2 + |\Im(X)|^2 = |X|^2$, that

$$|X| \geq t \implies |\Re(X)| \geq \frac{t}{\sqrt{2}} \text{ or } |\Im(X)| \geq \frac{t}{\sqrt{2}}.$$

Thus

$$\mathbb{P}(|X| \geq t) \leq \mathbb{P}(|\Re(X)| \geq \frac{t}{\sqrt{2}}) + \mathbb{P}(|\Im(X)| \geq \frac{t}{\sqrt{2}}).$$

Both $\mathbb{P}(|\Re(X)| \geq \frac{t}{\sqrt{2}}), \mathbb{P}(|\Im(X)| \geq \frac{t}{\sqrt{2}})$ can be bounded by Bernstein's Inequality:

$$\mathbb{P}(\Re(X) \geq \frac{t}{\sqrt{2}}), \mathbb{P}(\Im(X) \geq \frac{t}{\sqrt{2}}) \leq \exp\left(-\frac{t^2}{4\sum_{i=1}^{n} \mathrm{Var}(|X_i|) + 4Mt/3}\right).$$

The same is true for $\mathbb{P}(-\Re(X) \geq \frac{t}{\sqrt{2}}), \mathbb{P}(-\Im(X) \geq \frac{t}{\sqrt{2}})$, thus by union bound

$$\mathbb{P}(|X| \geq t) \leq 4\exp\left(-\frac{t^2}{4\sum_{i=1}^{n} \mathrm{Var}(|X_i|) + 4Mt/3}\right).$$

□

Our proof will utilize the following approximation for binomial coefficients, which utilizes Stirling's formula [17, 16].

Lemma 4.4 (Stirling's Formula for binomial coefficients)**.** For all $\alpha \in (0, 1)$,

$$\binom{n}{\alpha n} \sim 2^{nH(\alpha)},$$

where $H(\alpha) := \alpha \log(1/\alpha) + (1-\alpha)\log(1/(1-\alpha))$ is the binary entropy function.

4.1.1 Fourier Analysis Preliminaries

In this section, we will define the Fourier analysis tools that we use, specifically in the finite abelian group setting. Let the ambient group G be a finite abelian group.

Definition 4.5 (Bilinear forms)**.** A *bilinear form* on a ambient group G is a mapping $(\xi, x) \to \xi \cdot x$ from $G \times G \to \mathbb{R}/\mathbb{Z}$, that is a homomorphism for both variables ξ, x separately. A bilinear form is degenerate if the mappings $x \to \xi \cdot x$, is identically zero for some non-zero ξ, or the mapping $\xi \to \xi \cdot x$ is identically zero for some non-zero x. A bilinear form is symmetric if $\xi \cdot x = x \cdot \xi$.

With a bilinear form, we can define the Fourier transform. Let $e(\theta) := \exp(2\pi i\theta)$, then we have the following:

Definition 4.6 (Fourier transform)**.** Given a function $f : G \to \mathbb{C}$ and bilinear form, define the Fourier transform $\hat{f} : G \to \mathbb{C}$ as

$$\hat{f}(\xi) = \sum_{x \in G} f(x)e(\xi \cdot x).$$

Note that in the view of Fourier analysis, all choices of bilinear form are equivalent. For our purpose, we will work with the specific standard choice of bilinear form. For an example, in the case of $G = \mathbb{Z}_N$, the bilinear form is $\xi \cdot x = \xi x/N$. The Fourier transform is then

$$\hat{f}(\xi) = \sum_{x \in G} f(x)e^{2\pi i \xi x/N}.$$

We will use the following important properties of Fourier transform [12]:

Proposition 4.7 (Properties of Fourier transform)**.** Let $f, g : G \to \mathbb{C}$ be two functions, then:

- $\hat{f}(0) = \sum_{x \in G} f(x)$.
- (Parseval identity) $\sum_{x \in G} |f(x)|^2 = |G|^{-1} \sum_{\xi \in G} |\hat{f}(\xi)|^2$.
- (Plancherel theorem) $\sum_{x \in G} f(x)g(x) = |G|^{-1} \sum_{\xi \in G} \hat{f}(\xi)\hat{g}(\xi)$.

- (Fourier inversion formula) $f(x) = |G|^{-1} \sum_{\xi \in G} \hat{f}(\xi)\overline{e(\xi \cdot x)}$.
- (Convolution) $\widehat{f * g} = \hat{f}\hat{g}$.

Definition 4.8 (Spectrum)**.** For any subset $A \subseteq G$, we define its α - spectrum to be

$$Spec_\alpha(A) = \{\xi \in G : |\hat{1}_A(\xi)| \geq \alpha|A|\}.$$

By Parseval's identity and Markov's inequality, we can give the following upper bound for the size of the spectrum:

Lemma 4.9 (Upper bound for size of spectrum)**.** Given $0 < \alpha \leq 1$ and $A \subseteq G$,

$$|Spec_\alpha(A)| \leq \alpha^{-2}|G||A|^{-1}.$$

Proof.

$$|Spec_\alpha(A)| = |G|\mathbb{P}(|\hat{1}_A(\xi)| \geq \alpha|A|) = |G|\mathbb{P}(|\hat{1}_A(\xi)|^2 \geq \alpha^2|A|^2) \leq |G|\mathbb{E}(|\hat{1}_A(\xi)|^2)\alpha^{-2}|A|^{-2}$$

$$= \left(\sum_{\xi \in G} |\hat{1}_A(\xi)|^2\right) \alpha^{-2}|A|^{-2} = |G| \left(\sum_{x \in G} |1_A(x)|^2\right) \alpha^{-2}|A|^{-2} = \alpha^{-2}|G||A|^{-1}$$

□

4.2 A Smoothness Property of 4-fold Convolution

In this section, we are interested in a smoothness property of convolution.

Given a set A large enough, for all sets S that is large enough where $1_A * 1_A(s_1 + s_2) \approx 0$, for all $s_1, s_2 \in S$, then there exists a $s \in S$ such that $1_A * 1_A(2s) \approx 0$. Similarly, if $1_A * 1_A(s_1 + s_2) \gg 0$, for all $s_1, s_2 \in S$, then there exists a $s \in S$ such that $1_A * 1_A(2s) \gg 0$.

Perhaps the conditions can be relaxed, where $1_A * 1_A(s_1 + s_2)$ doesn't have to be all large (or small.) The result can also be strengthened to say more or all $s \in S$ has $1_A * 1_A(s_1 + s_2)$ large (or small).

This is related to Roth's theorem, as $1_A * 1_A(2s) \neq 0$ corresponds to solutions to $x+y = 2s$, which is a 3-AP. If A is too small, this is not true, as Behrend's Type construction tells us that there are sets of size $\frac{n}{e^{c\sqrt{\log n}}}$ without any 3-AP's. Thus, we should maybe look at sets of size $|A| > \frac{n}{(\log n)^{10}}, |S| > (\log n)^{10}$.

Theorem 4.10 (4-fold convolution)**.** Fix $0 < \epsilon < 1$, and Let $N > N_0(\epsilon)$. Let G be a finite abelian group such that $|G| = N$. Let $A, S \subseteq G$ be such that $|A| \geq N^{1-\epsilon}, |S| = N^{c\epsilon}$ for some c. If for every $s_1, s_2 \in S, s_1 \neq s_2$,

$$1_A * 1_A * 1_A * 1_A(s_1 + s_2) \ < \ |A|^3 N^{(2-3c/2)\epsilon}, \tag{4.1}$$

then, there exists $s' \in S$, such that

$$1_A * 1_A * 1_A * 1_A(2s') \ < \ |A|^3 N^{(3-c/2)\varepsilon}.$$

Note that if $c \leq 6$, the bound is $|A|^3$ trivial, so we may assume $c > 6$, where we are giving polynomial bounds. To prove the theorem, we first show the following lemma:

Lemma 4.11. Let $R, S \subseteq G$, be subsets of a finite abelian group, where $|G| = N > 64, |R| = k \geq 4, |S| = l$, and $l \geq 15k+3$. There exists a sequence of weights $(w_1, ..., w_l) \in \{-1, 0, 1\}^l$ not all zero, such that for all $r \in R$,

$$\left| \sum_{t=1}^{l} w_t \overline{e(s_t \cdot r)} \right| < \frac{l}{2^{l/(3k)}},$$

and for all $\xi \in G$,

$$\left| \sum_{t=1}^{l} w_t \overline{e(s_t \cdot \xi)} \right| < 6\sqrt{k} \log N.$$

Proof. Enumerate the elements of S as $\{s_1, ..., s_l\}$. Let $\delta_1, ..., \delta_l$ be Bernoulli random variables with $\mathbb{P}(\delta_i = 1) = \frac{k}{l}$ for all $1 \leq i \leq l$. For all $\xi \in G$, define the random variable

$$X_\xi = \sum_{t=1}^{l} \delta_t \overline{e(s_t \cdot \xi)}.$$

We have

$$|\delta_t \overline{e(s_t \cdot \xi)} - \mathbb{E}(\delta_t \overline{e(s_t \cdot \xi)})| \leq 1, \ \sum_{i=1}^{l} \mathrm{Var}(|\delta_t \overline{e(s_t \cdot \xi)}|) = l\frac{k}{l}(1 - \frac{k}{l}) \leq k.$$

Therefore, by Proposition 4.3, for any $\xi \in G$,

$$\begin{aligned} &\mathbb{P}(|X_\xi - \mathbb{E}(X_\xi)| \geq 3\sqrt{k}\log(N)) \leq 4\exp\left(-\frac{9k\log^2(N)}{4k + 4\sqrt{k}\log(N)}\right) \\ &\leq 4\exp\left(-\frac{9k\log^2(N)}{6k\log(N)}\right) = 4N^{-3/2} < \frac{1}{2N}. \end{aligned} \tag{4.2}$$

By the union bound

$$\begin{aligned} &\mathbb{P}(\forall \xi \in G, |X_\xi - \mathbb{E}(X_\xi)| \geq 3\sqrt{k}\log(N)) \\ &= 1 - \mathbb{P}(\exists \xi \in G, |X_\xi - \mathbb{E}(X_\xi)| \geq 3\sqrt{k}\log(N)) \\ &\leq 1 - N \cdot \mathbb{P}(|X_\xi - \mathbb{E}(X_\xi)| \geq 3\sqrt{k}\log(N)) < \frac{1}{2}. \end{aligned} \tag{4.3}$$

Let $\Delta \subseteq \{0,1\}^l$ denote the set of all sequence $(\delta_1, ..., \delta_l)$ such that, for all $\xi \in G$,

$$|\sum_{t=1}^{l} \delta_t \overline{e(s_t \cdot \xi)} - \mathbb{E}(X_\xi)| < 3\sqrt{k}\log(N) \tag{4.4}$$

By Eq. (4.3), $|\Delta| > 2^l(1 - 1/2) = 2^{l-1}$.

Now consider the set $\{x + iy \in \mathbb{C} : |x|, |y| \leq l\}^k$. Partition the set into translates of the cell

$$\{x + iy \in \mathbb{C} : 0 \leq |x|, |y| \leq l/2^{\lceil l/(3k)+1/2 \rceil}\}^k.$$

The number of translates in the partition is

$$(2 \cdot 2^{\lceil l/(3k)+1/2 \rceil})^{2k} \leq (2 \cdot 2^{l/(3k)+3/2})^{2k} = 2^{2l/3+5k}.$$

Since $l \geq 15k+3$, $|\Delta| > 2^{l-1} \geq 2^{2l/3+5k}$. Enumerate all the elements of $R = \{r_1, ..., r_k\}$. By the pigeonhole principle, there must exist $(\delta_1, ..., \delta_l), (\delta'_1, ..., \delta'_l) \in \Delta$ such that

$$\left(\sum_{t=1}^{l} \delta_t \overline{e(s_t \cdot r_1)}, ..., \sum_{t=1}^{l} \delta_t \overline{e(s_t \cdot r_k)} \right)$$

$$\left(\sum_{t=1}^{l} \delta'_t \overline{e(s_t \cdot r_1)}, ..., \sum_{t=1}^{l} \delta'_t \overline{e(s_t \cdot r_k)} \right)$$

belong to the same cell. Let $(w_1, ..., w_l) := (\delta_1, ..., \delta_l) - (\delta'_1, ..., \delta'_l)$. For such weights, we have for all $r \in R$

$$\left| \sum_{t=1}^{l} w_t \overline{e(s_t \cdot r)} \right|^2 = \left| \sum_{t=1}^{l} (\delta_t - \delta'_t) \overline{e(s_t \cdot r)} \right|^2$$

$$= \Re \left(\sum_{t=1}^{l} (\delta_t - \delta'_t) \overline{e(s_t \cdot r)} \right)^2 + \Im \left(\sum_{t=1}^{l} (\delta_t - \delta'_t) \overline{e(s_t \cdot r)} \right)^2$$

$$\leq 2 \left(l/2^{\lceil l/(3k)+1/2 \rceil} \right)^2 \leq 2 \left(l/2^{l/(3k)+1/2} \right)^2 = \left(l/2^{l/(3k)} \right)^2.$$

By Eq. (4.4) and the triangle inequality, for all $\xi \in G$,

$$\left| \sum_{t=1}^{l} w_t \overline{e(s_t \cdot \xi)} \right| = \left| \sum_{t=1}^{l} \delta_t \overline{e(s_t \cdot \xi)} - \sum_{t=1}^{l} \delta'_t \overline{e(s_t \cdot \xi)} \right|$$

$$\leq \left| \sum_{t=1}^{l} \delta_t \overline{e(s_t \cdot \xi)} - \mathbb{E}(X_\xi) \right| + \left| \sum_{t=1}^{l} \delta'_t \overline{e(s_t \cdot \xi)} - \mathbb{E}(X_\xi) \right| < 6\sqrt{k} \log(N).$$

Thus $(w_1, ..., w_l)$ is our desired weight.

□

Proof of Theorem 4.10. Enumerate the elements of S as $\{s_1, ..., s_l\}$. Let $\alpha = N^{(1-c/2)\epsilon}$,

and define the set $R := Spec_\alpha(A)$.

Let $(w_1, ..., w_l)$ be the weights as described in Lemma 4.11, according to S and R. Let j be an index such that $w_j = 1$; if no such weight exists, then simply multiply all weights by -1 so the bounds of Lemma 4.11 is still satisfied. Let $s' := s_j$. We define the following functions:

$$F(\xi) := N^{-1}\widehat{1_A}^4(\xi)\overline{e(s' \cdot \xi)}$$

$$W_1(\xi) := \sum_{t=1}^{l} w_t\overline{e(\xi \cdot s_t)}, W_2(\xi) := \sum_{\substack{t=1 \\ t\neq j}}^{l} w_t\overline{e(\xi \cdot s_t)}.$$

By Fourier inversion in Proposition 4.7, we have

$$1_A * 1_A * 1_A * 1_A(2s') = N^{-1}\sum_{\xi\in G}\widehat{1_A}^4(\xi)\overline{e(\xi \cdot 2s')}$$

$$= N^{-1}\sum_{\xi\in R}\widehat{1_A}^4(\xi)\overline{e(\xi \cdot 2s')} + N^{-1}\sum_{\xi\in R^c}\widehat{1_A}^4(\xi)\overline{e(\xi \cdot 2s')}$$

$$= N^{-1}\sum_{\xi\in R}\widehat{1_A}^4(\xi)\overline{e(\xi \cdot s')e(\xi \cdot s')} + N^{-1}\sum_{\xi\in R^c}\widehat{1_A}^4(\xi)\overline{e(\xi \cdot s')e(\xi \cdot s')}.$$

Since $\overline{e(\xi \cdot s')} = W_1(\xi) - W_2(\xi)$, we have

$$\begin{aligned} &= \sum_{\xi\in R} F(\xi)(W_1(\xi) - W_2(\xi)) + \sum_{\xi\in R^c} F(\xi)(W_1(\xi) - W_2(\xi)) \\ &= \sum_{\xi\in R} F(\xi)W_1(\xi) + \sum_{\xi\in R^c} F(\xi)W_1(\xi) - \sum_{\xi\in G} F(\xi)W_2(\xi). \end{aligned} \tag{4.5}$$

We will first look at the first sum. By Lemma 4.9, $|R| \leq \alpha^{-2}N|A|^{-1}$. For $\xi \in R$, by Lemma 4.11,

$$|W_1(\xi)| \leq \frac{|S|}{2^{|S|/(3|R|)}} \leq |S|2^{-\alpha^2 N^{-1}|S||A|/3} \leq N^{c\epsilon}2^{-N^{2\epsilon-c\epsilon-1+c\epsilon+1-\epsilon}/3}$$

$$= N^{c\epsilon} 2^{-N^\epsilon/3} \ll N^{(2-c/2)\epsilon},$$

and

$$|F(\xi)| \le N^{-1}|A|^2 |\widehat{1_A}(\xi)|^2.$$

Thus, the first sum is bounded by Parseval

$$\left| \sum_{\xi \in R} F(\xi) W_1(\xi) \right| \ll |A|^2 N^{-1} \sum_{\xi \in R} |\widehat{1_A}(\xi)|^2 N^{(2-c/2)\epsilon} \le |A|^3 N^{(2-c/2)\epsilon}. \tag{4.6}$$

For the second sum $\xi \in R^c$, we have $|\widehat{1_A}(\xi)| \le \alpha |A|$, and $W_1(\xi) < 3\sqrt{|R|}\log N$ by Lemma 4.11.

$$\left| \sum_{\xi \in R^c} F(\xi) W_1(\xi) \right| \le 6\sqrt{|R|}(\log N) N^{-1} \sum_{\xi \in R^c} |\widehat{1_A}(\xi)|^4 \le 6(\log N)\sqrt{|R|} N^{-1} \alpha^2 |A|^2 \sum_{\xi \in R^c} |\widehat{1_A}(\xi)|^2.$$

By Lemma 4.9, $\sqrt{|R|} \le \alpha^{-1} N^{1/2} |A|^{-1/2}$, so

$$\le 6(\log N) N^{1/2} |A|^{-1/2} \alpha |A|^2 N^{-1} \sum_{\xi \in R^c} |\widehat{1_A}(\xi)|^2 \le 6(\log N) N^{1/2} |A|^{-1/2} \alpha |A|^3$$

$$= 6(\log N) |A|^3 N^{(1-c/2)\epsilon + \epsilon/2} \ll |A|^3 N^{(2-c/2)\epsilon}. \tag{4.7}$$

For the third sum, we have

$$\sum_{\xi \in G} F(\xi) W_2(\xi) = \sum_{\xi \in G} N^{-1} \overline{e(\xi \cdot s')} \sum_{\substack{t=1 \\ t \ne j}}^{l} \widehat{1_A}^4(\xi) w_t \overline{e(\xi \cdot s_t)}$$

$$= N^{-1} \sum_{\xi \in G} \sum_{\substack{t=1 \\ t \ne j}}^{l} \widehat{1_A}^4(\xi) w_t \overline{e(\xi \cdot (s' + s_t))} = \sum_{\substack{t=1 \\ t \ne j}}^{l} w_t N^{-1} \sum_{\xi \in G} \widehat{1_A}^4(\xi) \overline{e(\xi \cdot (s' + s_t))}$$

by Fourier inversion

$$= \sum_{\substack{t=1 \\ t \neq j}}^{l} w_t 1_A * 1_A * 1_A * 1_A(s' + s_t).$$

By our assumption of convolution at sums of different elements,

$$\left| \sum_{\xi \in G} F(\xi) W_2(\xi) \right| < N^{c\epsilon} |A|^3 N^{(2-3c/2)\epsilon} = |A|^3 N^{(2-c/2)\epsilon}. \tag{4.8}$$

Putting Eq. (4.6), Eq. (4.7), and Eq. (4.8) together, we have our desired result. □

As shown in the proof, the 4-fold of the convolution is necessary for the Fourier coefficients to decay at a sufficient rate. Thus, to get a power-like bound, 4-fold convolution is perhaps necessary. However, there may be arguments utilizing almost-periodicity and Bohr neighborhood that allow us to get similar results. These arguments typically work with sets of size $n/e^{(\log n)^c}$ for some c. Here we have an conjecture for the smoothness of 2-fold convolution.

Conjecture 4.12. Let G be a finite abelian group such that $|G| = N$. Let $A, S \subseteq G$ be such that $|A| > N/e^{(\log N)^{1/6}}$, $|S| > e^{2(\log N)^{1/6}}$. For every $s_1, s_2 \in S, s_1 \neq s_2$,

$$1_A * 1_A(s_1 + s_2) \sim 0. \tag{4.9}$$

Then, there exists $s' \in S$, such that

$$1_A * 1_A(2s') \sim 0.$$

4.3 Construction on the Bounds of the Smoothness Property

In this section, we are interested in understanding the bounds one would expect for 2 convolution versions of Theorem 4.10. We want to construct A, S such that $|A|, |S|$, is large and $1_A * 1_A(2s)$ is large, but $1_A * 1_A(s_1 + s_2)$ is small for all $s, s_1, s_2 \in S$. We would like

to see how big the gap between $1_A * 1_A(2s), 1_A * 1_A(s_1 + s_2)$ can be, while keeping A, S as dense as possible.

These constructions are inspired by the construction of Behrend for the lower bound of Roth's Theorem [1]. They also share some similarities with the Niveau set construction of Ruzsa [19], or Gowers [11].

Let $M \in \mathbb{Z}$ be a boundary parameter. For all constructions in $\mathbb{Z}^d$, we are going to map it to $[-M, M]^d \subseteq \mathbb{Z}$ using the following Frieman 2-isomorphism $\upsilon : \mathbb{Z}^d \to [0, (4M+2)^d] \subseteq \mathbb{Z}$,

$$\upsilon(\boldsymbol{x}) := \sum_{k=1}^{d} (x_k + M + 1)(4M+2)^{k-1}. \tag{4.10}$$

We begin with a relatively simple construction of hyper cubes in $\mathbb{Z}^d$:

Proposition 4.13 (Hypercube Construction)**.** Given N, d, let $M = \lfloor N^{1/d}/4 - 1/2 \rfloor$. There exists sets $A, S \subseteq [0, N] \subseteq \mathbb{Z}$ such that $|S| = d, |A| \geq d(2M)^{d-1}$, and for all $s \in S$,

$$1_A * 1_A(2s) \geq (2M+1)^{d-1}.$$

For all $s_1 \neq s_2 \in S$,

$$1_A * 1_A(s_1 + s_2) \leq (2M+1)^{d-2}.$$

Proof. Let $e_i, 1 \leq i \leq d$ be the standard basis in $\mathbb{Z}^d$. Let $S = \{Me_i : 1 \leq i \leq d\}$ and

$$A := \{v \in \mathbb{Z}^d : \|v\|_\infty = M\}$$

is the hypercube formed by all hyperplanes normal to points in S. Then we have

$$|S| = d, |A| = (2M+1)^d - (2M)^d \geq d(2M)^{d-1}.$$

Given $s \in S$, if x is in the hyperplane normal to s, then $2s - x$ is also in the hyperplane.

Thus,

$$1_A * 1_A(2s) \geq (2M+1)^{d-1}.$$

Let $x + y = s_1 + s_2, x \in A_s y \in A_{s'}$. We have $x \cdot s = d, (s_1 + s_2 - x) \cdot s' = d$. This is equivalent to the system

$$[s, -s']^T x = [d, d + (s_1 + s_2) \cdot s']^T.$$

This is equivalent to the shifted null space of the matrix $[s, -s']^T$. Shifting the hyperplane to the origin only increase the number of points in the box, thus

$$1_A * 1_A(s_1 + s_2) \leq |\{v \in [-M, M]^d : [s, s']^T v = 0\}|$$

Since $s_1 \neq s_2, \|s_1 + s_2\|_2^2 < 2d$. If $s = s'$, then x, y lie in the same hyper plane and $\|x+y\|_2^2 \geq 2d$. Therefore $s \neq s'$ and $[s, s']^T$ has rank 2. Thus there exists two columns i, j that are pivot columns. Therefore, i, j coordinate of v must be 0 for $[s, s']^T v = 0$. Thus we have $(2M+1)^{d-2}$ choices for the other coordinates.

$$1_A * 1_A(s_1 + s_2) \leq (2M+1)^{d-2} \tag{4.11}$$

Now mapping A to $\mathbb{Z}$ with v in Eq. (4.10) gives our desired set. □

In a similar way, we may look at cross-polytopes instead of hyper cubes.

Proposition 4.14 (Cross-Polytope Construction)**.** Given N, d, where d is even, let $M = \lfloor N^{1/d}/4 - 1/2 \rfloor$. There exists sets $A, S \subseteq [0, N] \subseteq \mathbb{Z}$ such that

$$|S| = 2^{d-1}, |A| \geq 2^{d-1}(2M-1)^d/(Md - d + 1) - \binom{2^{d-1}}{2}(2M+1)^{d-2}$$

and for all $s \in S$,

$$1_A * 1_A(2s) \geq (2M-1)^d/(Md - d + 1).$$

For all $s_1 \neq s_2 \in S$,

$$1_A * 1_A(s_1 + s_2) \leq (2M+1)^{d-2}.$$

Proof. Let $S = \{s \in \{-1,1\}^d : s_1 = 1\}$ and let

$$A := \{v \in [-M, M]^d \subseteq \mathbb{Z}^d : \exists s \in S \text{ such that } v \cdot s = d\}.$$

is the cross-polytope formed by all hyperplanes normal to points in S. Fix $s \in S$, we would like to find a lower bound for the size of

$$A_s := \{v \in [-M, M]^d \subseteq \mathbb{Z}^d : v \cdot s = d\}.$$

Without loss of generality, we may assume $s = (1, 1, ..., 1)$. Note that if $v \cdot s = 0, v \in [-M+1, M-1]^d$, then $(v+s) \cdot s = d, (v+s) \in [-M, M]^d$. Therefore, We may instead consider

$$A_0 := \{v \in [-M+1, M-1]^d \subseteq \mathbb{Z}^d : v_1 + ... + v_d = 0\}.$$

Let

$$r_x = \{(v_1, ..., v_{d/2}) \in [-M+1, M-1]^{d/2} : v_1 + ... + v_{d/2} = x\}.$$

For any x, If

$$v_1 + ... + v_{d/2} = w_1 + ... + w_{d/2} = x,$$

then

$$v_1 + ... + v_{d/2} - w_1 + ... + w_{d/2} = 0.$$

Then we have $(v_1, ..., v_{d/2}, w_1, ..., w_{d/2}) \in A_0$. This is true for any pairs of vectors $v.w \in r_x$. r_x is none empty for $x \in [-Md/2 + d/2, Md/2 - d/2]$. By Cauchy–Schwarz, we have

$$|A_0| \geq \sum_{x \in \mathbb{Z}} |r_x|^2 \geq \left(\sum_{x \in \mathbb{Z}} |r_x| \right)^2 / \left| [-Md/2 + d/2, Md/2 - d/2] \right|$$

$$= \left(\sum_{x \in \mathbb{Z}} |r_x| \right)^2 / (Md - d + 1) = |[-M + 1M - 1]^{d/2}|^2 / (Md - d + 1)$$

$$= (2M - 1)^d / (Md - d + 1) \tag{4.12}$$

Now we give a upper bound for the intersection of two hyper planes. If $x \in A_s \cap A_{s'}$, then $[s, s']^T x = [d, d]^T$. The intersection is equivalent to the shifted null space of the matrix. $[s, s']^T$. Thus

$$|A_s \cap A_{s'}| \leq |\{v \in [-MM]^d : [s, s']^T v = 0\}|$$

All $s \neq s'$ are independent from each other, so $[s, s']^T$ has rank 2. By the same argument as Eq. (4.11),

$$|A_s \cap A_{s'}| \leq (2M + 1)^{d-2}$$

By inclusion exclusion, Eq. (4.12), and Eq. (4.11) we have

$$|S| = 2^{d-1}, |A| \geq 2^{d-1}(2M - 1)^d / (Md - d + 1) - \binom{2^{d-1}}{2} (2M + 1)^{d-2} \tag{4.13}$$

All $a \in A_s$ contribute to the convolution $1_A * 1_A(2s)$ so

$$1_A * 1_A(2s) \geq |A_0| \geq (2M - 1)^d / (Md - d + 1) \tag{4.14}$$

by Eq. (4.12). By the same argument as Eq. (4.11) again,

$$1_A * 1_A(s_1 + s_2) \leq (2M + 1)^{d-2}.$$

Now mapping A to $\mathbb{Z}$ with υ in Eq. (4.10) gives our desired set. □

4.3.1 Intersections of many faces of a Cross-polytope

Now we consider a more sophisticated construction.

Theorem 4.15. Given $d \geq d_0, N$, where $3|d$. Let $M := \lfloor N^{1/d}/4 - 1/2 \rfloor$, and k, k' be such

that $kk'^2 = 1.058^d$. There exist sets $A, S \subseteq [0, N] \subseteq \mathbb{Z}$ such that

$$|S| \geq k, |A| \geq kk'(2M-1)^d/(Md-d+1) - \binom{kk'}{2}(2M+1)^{d-2}$$

and for all $s \in S$,

$$1_A * 1_A(2s) \geq k'(2M-5)^d/(Md-3d+1) - \binom{k'}{2}(2M+1)^{d-2}.$$

For all $s_1 \neq s_2 \in S$,

$$1_A * 1_A(s_1+s_2) \leq (2M+1)^{d-2}.$$

Proof. Let $H_0 = \{-1, 1\}^d, S_0 = \{-3, 3\}^d$. We will pick a random k-subset $S := \{s_1, ..., s_k\} \subseteq S_0$.

Let $\mathcal{H} := \mathcal{H}(S)$ be the set of all sequences $H = (h_{11}, ..., h_{kk'})$, where each h_{ij} follows the following conditions:

1. For all $1 \leq i \leq k, 1 \leq j \leq k'$, we have $h_{ij} \cdot s_i = d$.
2. Each h_{ij} is distinct.
3. For all $1 \leq i \leq k, 1 \leq j \leq k'$ and $s_a, s_b \in S, s_a \neq s_b$, we have $h_{ij} \cdot \frac{s_a+s_b}{2} \neq d$.

We would like to show that there exists a set S with the conditions above, by showing $\mathbb{E}(|\mathcal{H}|) > 0$. Let $\mathcal{H}_1$ be the set of sequences that satisfies conditions 1, and $\mathcal{H}_2$ be the set of sequences that satisfies conditions 1 and 2. Note that for a given s_i, for $s_i \cdot h_{ij} = d, 2d/3$ of the entry has to match signs with h_{ij}, and $d/3$ of the entries has to have opposite signs, giving $\binom{d}{d/3}$ choices. Therefore we have $|\mathcal{H}_1| = \binom{d}{d/3}^{kk'}$ choices if we allow repetitions. To get distinct elements, as each h_{ij} is chosen, it has to be removed from the pool of potential choices. Then, we have

$$|\mathcal{H}_2| \geq \prod_{t=1}^{kk'} \left(\binom{d}{d/3} - t \right).$$

Now let $\mathcal{H}_{ijab} \subseteq \mathcal{H}_1$ be the set of sequences that satisfies conditions 1, but

$$h_{ij} \cdot \frac{s_a + s_b}{2} = d.$$

Assume $a \neq b$; this means $\mathcal{H}_{ijab}$ is the subset of $\mathcal{H}_1$ that fails condition 3 on the elements h_{ij}, s_a, s_b. Therefore, we have $\mathcal{H} = \mathcal{H}_2 \setminus (\bigcup_{i,j,a\neq b} \mathcal{H}_{ijab})$, the set of sequences that satify all 3 conditions. Note that $\mathcal{H}_{ijab} = \mathcal{H}_{ijba}$, so we simply have to account for the cases when $a < b$. Thus, by union bound we have

$$|\mathcal{H}| \geq |\mathcal{H}_2| - \sum_{i,j,a<b} |\mathcal{H}_{ijab}|.$$

Note that $\mathbb{E}(|\mathcal{H}_{ijab}|)$ is the same for all $i \neq a, b$, and the same for all $i = a$ or b. We will show that for all i, j, a, b,

$$\mathbb{E}(|\mathcal{H}_{ijab}|) \leq \binom{d}{d/3}^{kk'} 2^{-d} \binom{d}{d/3}.$$

First consider $i = a$ or b. For any $h \in H_0$ where $h \cdot s_a = d$, $h \cdot \frac{s_a+s}{2} = d$, if and only if $h \cdot s = d$. Let s_a be given, and $h \in H_0, s \in S_0$ be randomly chosen:

$$\mathbb{P}(h \cdot \frac{s_a + s}{2} = d | h \cdot s_a = d, s \neq s_a) = \mathbb{P}(h \cdot s = d | h \cdot s_a = d, s \neq s_a).$$

As discussed, there are $\binom{d}{d/3}, s \in S_0$ such that $h \cdot s = d$. Since $s \neq s_a$, we have $\binom{d}{d/3} - 1$ choices. Thus, given a h, let $s \in S_0 \setminus s_a$ be randomly selected.

$$\mathbb{P}(h \cdot s = d | h \cdot s_a = d, s \neq s_a) = \left(\binom{d}{d/3} - 1 \right) / (2^d - 1) \leq 2^{-d} \binom{d}{d/3}. \tag{4.15}$$

Thus for each $1 \leq a, b \leq k, 1 \leq j \leq k'$, we give the upper bound to the expectation:

$$\mathbb{E}(|\mathcal{H}_{ajab}|) = \mathbb{E}(|\mathcal{H}_{bjab}|) \leq \binom{d}{d/3}^{kk'} 2^{-d} \binom{d}{d/3}.$$

Now we consider $i \neq a, b$. Let $s_a \neq s_b$ be given. Let $s \in S_0$ be randomly selected, then $h \in H_0$ be randomly selected amongst vectors such that $h \cdot s = d$:

$$\mathbb{E}(|\mathcal{H}_{ijab}|) = \mathbb{E}(|\mathcal{H}_1|)\mathbb{P}(h \cdot \frac{s_a + s_b}{2} = d | h \cdot s = d, s \neq s_a, s_b).$$

To give a upper bound to the expectation, we separate the probability using conditional probability:

$$\begin{aligned} &\mathbb{P}(h \cdot \frac{s_a + s_b}{2} = d | h \cdot s = d, s \neq s_a, s_b) = \\ &\mathbb{P}(h \cdot \frac{s_a + s_b}{2} = d | h \cdot s = d)/\mathbb{P}(s \neq s_a, s_b) \\ -\mathbb{P}(h \cdot \frac{s_a + s_b}{2} = d | h \cdot s = d, s = s_a \text{ or } s_b)&\mathbb{P}(s = s_a \text{ or } s_b)/\mathbb{P}(s \neq s_a, s_b). \end{aligned} \tag{4.16}$$

We would like to give an upper bound to Eq. (4.16). We first calculate $\mathbb{P}(h \cdot \frac{s_a+s_b}{2} = d | h \cdot s = d)$, the probability that condition 3 is satisfied for h, s_a, s_b. Note that because s is selected independently from s_a, s_b, we have

$$\mathbb{P}(h \cdot \frac{s_a + s_b}{2} = d | h \cdot s = d) = \mathbb{P}(h \cdot \frac{s_a + s_b}{2} = d).$$

Let t be such that $\frac{s_a+s_b}{2}$ has $\frac{d}{3} + 2t$ entries that are non-zero. Since we are trying to get a upper bound, first assume that the probability is non-zero. This implies that $0 \leq t \leq d/3$ is an integer. Since the calculation is the same, assume without loss of generality that all non-zero entries are 3, and not -3. Note that if $t < 0$, then $h \cdot \frac{s_a+s_b}{2} < d$ for any $h \in H$; , the condition is not satisfied. If $t \geq 0$, then if h is -1 at t of the non-zero entries, and 1 at

all other non-zero entries,

$$h \cdot \frac{s_a + s_b}{2} = 3(\frac{d}{3} + t) - 3t = d.$$

Thus we have $\binom{\frac{d}{3}+2t}{t}$ choices for the non-zero entries. For the 0 entries, h can be anything, thus giving us $2^{\frac{2d}{3}-2t}$ choices. Thus, given a random $h \in H$, the probability is then:

$$\mathbb{P}(h \cdot \frac{s_a + s_b}{2} = d) = 2^{-d}\binom{\frac{d}{3} + 2t}{t} 2^{\frac{2}{3}d-2t}.$$

For any $0 \leq t \leq d/3$, we have that

$$\binom{\frac{d}{3} + 2t}{t} 2^{-2t} \Big/ \left[\binom{\frac{d}{3} + 2(t+1)}{(t+1)} 2^{-2(t+1)}\right] = \frac{4(t+1)(\frac{d}{3} + t + 1)}{(\frac{d}{3} + 2t + 1)(\frac{d}{3} + 2t + 2)} < 1$$

because $4(t+1) + (\frac{d}{3} + t + 1) \leq (\frac{d}{3} + 2t + 1) + (\frac{d}{3} + 2t + 1)$, thus

$$4(t+1)(\frac{d}{3} + t + 1) \leq (\frac{d}{3} + 2t + 1)^2 \leq (\frac{d}{3} + 2t + 1)(\frac{d}{3} + 2t + 2).$$

The probability monotonically increases as t increases, and is maximized for $t = \frac{d}{3}$, and

$$\mathbb{P}(h \cdot \frac{s_a + s_b}{2} = d) \leq 2^{-d}\binom{d}{d/3}.$$

Now we calculate $\mathbb{P}(h \cdot \frac{s_a+s_b}{2} = d | s = s_a \text{ or } s_b)$. Note that this is the same as the first case considered, when $i = a$ or b. Thus, this is equal to Eq. (4.15). We also have that

$$\mathbb{P}(s = s_a \text{ or } s_b) = 2^{1-d}, \mathbb{P}(s \neq s_a, s_b) = 1 - 2^{-d+1}.$$

Combining everything we have, Eq. (4.16) has the upper bound

$$\begin{aligned}\mathbb{P}(h\cdot\frac{s_a+s_b}{2}=d|h\cdot s=d, s\neq s_a,s_b)\leq\\ \left(2^{-d}\binom{d}{d/3}-2^{-d}\binom{d}{d/3}2^{1-d}\right)/(1-2^{1-d})=2^{-d}\binom{d}{d/3}.\end{aligned}\tag{4.17}$$

Thus for each $1\leq i,a,b\leq k, 1\leq j\leq k'$, we give the upper bound to the expectation:

$$\mathbb{E}(|\mathcal{H}_{ijab}|)\leq\binom{d}{d/3}^{kk'}2^{-d}\binom{d}{d/3}.$$

Thus we have

$$\begin{aligned}\mathbb{E}|\mathcal{H}|&\geq\mathbb{E}\left(|\mathcal{H}_1|\right)-\mathbb{E}\left(\sum_{i,j,a<b}|\mathcal{H}_{ijab}|\right)\\ &\geq\prod_{t=1}^{kk'}\left(\binom{d}{d/3}-t\right)-\sum_{i,j,a<b}\mathbb{E}|\mathcal{H}_{ajab}|\\ &\geq\prod_{t=1}^{kk'}\left(\binom{d}{d/3}-t\right)-k'k\binom{k}{2}\binom{d}{d/3}^{kk'+1}2^{-d}\\ &\geq\left(\binom{d}{d/3}-kk'\right)^{kk'}-k'k\binom{k}{2}\binom{d}{d/3}^{kk'+1}2^{-d}\\ &\geq\binom{d}{d/3}^{kk'}\left[\left(1-\frac{kk'}{\binom{d}{d/3}}\right)^{kk'}-k'k\binom{k}{2}\binom{d}{d/3}2^{-d}\right].\end{aligned}$$

By Lemma 4.4, $\left(\frac{27}{4}-\epsilon\right)^{d/3}<\binom{d}{d/3}<\left(\frac{27}{4}\right)^{d/3}$ for d large enough. Let $c=\frac{2\cdot2^{2/3}}{3}-\epsilon\approx 1.058, k'k^2=c^d$. Then we have that

$$k'k\binom{k}{2}\binom{d}{d/3}2^{-d}<c^d\left(\frac{27}{4}\right)^{d/3}2^{-d}=o(1).$$

Note that

$$\left(1-\frac{kk'}{\binom{d}{d/3}}\right)^{kk'}=\left(1-\frac{(kk')^2/\binom{d}{d/3}}{kk'}\right)^{kk'}$$

$(kk')^2=1.058^{2d}<\left(\frac{27}{4}-\epsilon\right)^{d/3}<\binom{d}{d/3}$. Thus as $d\to\infty$,

$$\left(1 - \frac{kk'}{\binom{d}{d/3}}\right)^{kk'} \to e^0 = 1.$$

Therefore $\mathbb{E}|\mathcal{H}| > 0$. There exists a $H = (h_{11}, ..., h_{kk'})$ such that all three conditions are satisfied.

Let S be a set such that $\mathcal{H}(S)$ is none empty, and let H be a element of such $\mathcal{H}(S)$. Define

$$A = \{a \in [-M, M]^d \subseteq \mathbb{Z}^d : \exists h \in H \text{ such that } a \cdot h = d\}.$$

The size of A is very similar to that of Eq. (4.13). Except now we have kk' hyperplanes instead of s^{d-1}. Therefore, we have

$$|S| = k, |A| \geq kk'(2M-1)^d/(Md - d + 1) - \binom{kk'}{2}(2M+1)^{d-2}.$$

$1_A * 1_A(2s)$ is similar to the case of Eq. (4.14). Except this time, S is vectors in $\{-3, 3\}^d$ instead of $\{-1, 1\}^d$. Thus everything needs to shift by 3 instead of 1 to the origin. We have the contribution of a single hyperplane to the convolution of $1_A * 1_A(2s)$ is

$$(2M-5)^d/(Md - 3d + 1)$$

There are k' hyperplanes through each s. By the same arguement, the intersection of each hyperplane is at most Eq. (4.11). Thus we have

$$1_A * 1_A(2s) \geq k'(2M-5)^d/(Md - 3d + 1) - \binom{k'}{2}(2M+1)^{d-2}.$$

By Eq. (4.11) again,

$$1_A * 1_A(s_1 + s_2) \leq (2M+1)^{d-2}.$$

□

Appendices

APPENDIX A

NOTATION

$A + B$	Sum set (Definition 1.1)
$A - B$	Difference set (Definition 1.1)
$a^\frown b$	Concatenation of vectors a and b (Section 2.1)
$c \cdot A$	Dilation of set A by element c
$x \cdot \xi$	Bilinear form (Definition 4.5)
$\exp(x)$	e^x, exponential of x
$e(x)$	$\exp(2\pi i x)$ (Section 4.1.1)
$\overline{x}$	Complex conjugate of x
$\lvert x \rvert$	Absolute value of x. If x is a complex number, then the 2-norm of x.
$\Re(x), \Im(x)$	The real and imaginary part of the complex number x.
$O(f(x)), f \sim g$	Big O notation (Definition 1.8)
A^c	Complement of set A
$\mathcal{P}(A)$	Power set of set A
$x \vert y$	x divides y
$\mathcal{B}$	$[0,1]^n$ the set of binary vectors of length n (Section 3.1.1)
$A \setminus B$	$\{a \in A : a \notin B\}$, the set difference

APPENDIX B

COMPARISON OF C_0^1 AND S_0^1

In this section we will verify that the base cases for Theorem 3.6 holds.

First, look at the base case $i = 1$.

$$C_0^1 = CH(\{(0,0),(0,-1/2),(1,0)\}) \cup CH(\{(0,2),(0,3/2),(1,2)\}),$$

so

$$C_0^1 \cap (\mathbb{Z} \times 2\mathbb{Z}) = \{(0,0),(1,0),(1,2)\}. \tag{B.1}$$

Now let's look at S_0^1. For the four possible sets $A \in \mathcal{A}_0^1$:

$$\begin{aligned} A = \emptyset &: 1_A * 1_A(0,1) = (0,0) \\ A = \{0\} &: 1_A * 1_A(0,1) = (1,0) \\ A = \{1\} &: 1_A * 1_A(0,1) = (0,0) \\ A = \{0,1\} &: 1_A * 1_A(0,1) = (1,2). \end{aligned} \tag{B.2}$$

We see that the points of Eq. (B.1) and Eq. (B.2) matches exactly.

C_1^1 has vertices

$$\{(0,0),(2,0),(0,1/2),(3,2)\},$$

thus it contains $(1,0),(2,1)$. Thus,

$$C_1^1 \cap (\mathbb{Z} \times 2\mathbb{Z}) = \{(0,0),(1,0),(2,0),(3,2)\}. \tag{B.3}$$

For the four possible subsets $A \in \mathcal{A}_1^1$:

$$\begin{aligned} A = \{-1\} &: 1_A * 1_A(0,1) = (0,0) \\ A = \{-1,0\} &: 1_A * 1_A(0,1) = (1,0) \\ A = \{-1,1\} &: 1_A * 1_A(0,1) = (2,0) \\ A = \{-1,0,1\} &: 1_A * 1_A(0,1) = (3,2). \end{aligned} \tag{B.4}$$

We see that the points of Eq. (B.3) and Eq. (B.4) matches exactly. Now we look at the case $i = 2$:

$$C_0^2 = CH(\{(0,0),(2,0),(0,1/2),(3,2)\}) \cup CH(\{(0,2),(2,2),(0,3/2),(3,4)\}),$$

so

$$C_0^1 \cap (\mathbb{Z} \times 2\mathbb{Z}) = \{(0,0),(1,0),(2,0),(1,2),(3,2),(0,2),(2,2),(3,4)\}). \tag{B.5}$$

Now let's look at S_0^1. For the 16 possible sets $A \in \mathcal{A}_0^2$, we list the 12 that are not listed in Eq. (B.1):

$$\begin{aligned} A = \{-1\} &: 1_A * 1_A(0,1) = (0,0) \\ A = \{-1,0\} &: 1_A * 1_A(0,1) = (1,0) \\ A = \{-1,1\} &: 1_A * 1_A(0,1) = (2,0) \\ A = \{-1,0,1\} &: 1_A * 1_A(0,1) = (3,2) \\ A = \{2\} &: 1_A * 1_A(0,1) = (0,0) \\ A = \{0,2\} &: 1_A * 1_A(0,1) = (1,0) \\ A = \{1,2\} &: 1_A * 1_A(0,1) = (0,0) \\ A = \{0,1,2\} &: 1_A * 1_A(0,1) = (1,2) \end{aligned}$$

$$A = \{-1, 2\} : 1_A * 1_A(0, 1) = (0, 2)$$
$$A = \{-1, 0, 2\} : 1_A * 1_A(0, 1) = (1, 2)$$
$$A = \{-1, 1, 2\} : 1_A * 1_A(0, 1) = (2, 2)$$
$$A = \{-1, 0, 1, 2\} : 1_A * 1_A(0, 1) = (3, 4). \tag{B.6}$$

We see that the points of Eq. (B.5) and Eq. (B.6) matches exactly.

C_1^2 has vertices

$$\{(0, 0), (3, 0), (0, 3/2), (5, 4)\},$$

thus,

$$C_1^1 \cap (\mathbb{Z} \times 2\mathbb{Z}) = \{(0, 0), (1, 0), (2, 0), (3, 0), (1, 2), (2, 2), (3, 2), (4, 2), (5, 4)\}. \tag{B.7}$$

Now let's look at S_0^1. For the eight possible sets $A \in \mathcal{A}_1^2$, we list the 12 that are not listed in Eq. (B.1):

$$A = \{-2, -1\} : 1_A * 1_A(0, 1) = (0, 0)$$
$$A = \{-2, -1, 0\} : 1_A * 1_A(0, 1) = (1, 0)$$
$$A = \{-2, -1, 1\} : 1_A * 1_A(0, 1) = (2, 0)$$
$$A = \{-2, -1, 0, 1\} : 1_A * 1_A(0, 1) = (3, 2)$$
$$A = \{-2, 2\} : 1_A * 1_A(0, 1) = (2, 0)$$
$$A = \{-2, 0, 2\} : 1_A * 1_A(0, 1) = (3, 0)$$
$$A = \{-2, 1, 2\} : 1_A * 1_A(0, 1) = (2, 0)$$
$$A = \{-2, 0, 1, 2\} : 1_A * 1_A(0, 1) = (3, 2)$$
$$A = \{-2, -1, 2\} : 1_A * 1_A(0, 1) = (2, 2)$$
$$A = \{-2, -1, 0, 2\} : 1_A * 1_A(0, 1) = (3, 2)$$

$$A = \{-2, -1, 1, 2\} : 1_A * 1_A(0, 1) = (4, 2)$$
$$A = \{-2, -1, 0, 1, 2\} : 1_A * 1_A(0, 1) = (5, 4). \tag{B.8}$$

We see that the points of Eq. (B.7) and Eq. (B.8) matches exactly. Thus, the set image is as described for the base case.

APPENDIX C

SUBSETS AND $1_A * 1_{-A}(0, 1, 2)$

In this section, we list the base cases for Theorem 3.7. We give all 16 subset of $[0, 3]$, and it's convolution $1_A * 1_{-A}(0, 1, 2)$. Subsets are expressed in its vector form v_A, so $A = \{0, 2, 3\}$ would be $v_A = [1, 0, 1, 1]$.

v_A	$1_A * 1_{-A}(0, 1, 2)$
$[0, 0, 0, 0]$	$(0, 0, 0)$
$[1, 0, 0, 0]$	$(1, 0, 0)$
$[0, 1, 0, 0]$	$(1, 0, 0)$
$[1, 1, 0, 0]$	$(2, 1, 0)$
$[0, 0, 1, 0]$	$(1, 0, 0)$
$[1, 0, 1, 0]$	$(2, 0, 1)$
$[0, 1, 1, 0]$	$(2, 1, 0)$
$[1, 1, 1, 0]$	$(3, 2, 1)$
$[0, 0, 0, 1]$	$(1, 0, 0)$
$[1, 0, 0, 1]$	$(2, 0, 0)$
$[0, 1, 0, 1]$	$(2, 0, 1)$
$[1, 1, 0, 1]$	$(3, 1, 1)$
$[0, 0, 1, 1]$	$(2, 1, 0)$
$[1, 0, 1, 1]$	$(3, 1, 1)$
$[0, 1, 1, 1]$	$(3, 2, 1)$
$[1, 1, 1, 1]$	$(4, 3, 2)$

REFERENCES

[1] F. A. Behrend, "On sets of integers which contain no three terms in arithmetical progression," *Proceedings of the National Academy of Sciences*, vol. 32, no. 12, pp. 331–332, 1946.

[2] T. F. Bloom, "A quantitative improvement for roth's theorem on arithmetic progressions," *Journal of the London Mathematical Society*, vol. 93, no. 3, pp. 643–663, 2016.

[3] T. F. Bloom and O. Sisask, "Breaking the logarithmic barrier in roth's theorem on arithmetic progressions," *arXiv preprint arXiv:2007.03528*, 2020.

[4] T. F. Bloom and O. Sisask, "Logarithmic bounds for roth's theorem via almost-periodicity," *arXiv preprint arXiv:1810.12791*, 2018.

[5] T. F. Bloom and O. Sisask, "The kelley–meka bounds for sets free of three-term arithmetic progressions," *arXiv preprint arXiv:2302.07211*, 2023.

[6] J. Bourgain, "On triples in arithmetic progression," *Geometric and Functional Analysis*, vol. 9, no. 5, pp. 968–984, 1999.

[7] E. Croot, V. Lev, and P. Pach, "Progression-free sets in zn 4 are exponentially small (2016)," *URL: https://arxiv. org/pdf/1605.01506. pdf*,

[8] E. Croot and O. Sisask, "A probabilistic technique for finding almost-periods of convolutions," *Geometric and functional analysis*, vol. 20, pp. 1367–1396, 2010.

[9] M. Elkin, "An improved construction of progression-free sets," in *Proceedings of the twenty-first annual ACM-SIAM symposium on Discrete Algorithms*, SIAM, 2010, pp. 886–905.

[10] J. Ellenberg and D. Gijswijt, "On large subsets of fn q with no three-term arithmetic progression. 2016," *URL: https://arxiv. org/pdf/1605.09223. pdf*,

[11] T. Gowers, *More on the cap-set problem*, Mar. 2011.

[12] B. Green, *Finite field models in additive combinatorics*, 2004. arXiv: math/0409420 [math.NT].

[13] B. Green and J. Wolf, "A note on elkin's improvement of behrend's construction," in *Additive number theory: Festschrift in honor of the sixtieth birthday of Melvyn B. Nathanson*, Springer, 2010, pp. 141–144.

[14] D. R. Heath-Brown, "Integer sets containing no arithmetic progressions," *Journal of the London Mathematical Society*, vol. 2, no. 3, pp. 385–394, 1987.

[15] Z. Kelley and R. Meka, "Strong bounds for 3-progressions," *arXiv preprint arXiv:2302.05537*, 2023.

[16] D. J. MacKay, *Information theory, inference and learning algorithms*. Cambridge university press, 2003.

[17] H. Robbins, "A remark on stirling's formula," *The American Mathematical Monthly*, vol. 62, no. 1, pp. 26–29, 1955.

[18] K. F. Roth, "On certain sets of integers," *J. London Math. Soc*, vol. 28, no. 1, pp. 104–109, 1953.

[19] I. Z. Ruzsa, "Essential components," *Proceedings of the London Mathematical Society*, vol. 3, no. 1, pp. 38–56, 1987.

[20] T. Sanders, "On roth's theorem on progressions," *Annals of Mathematics*, pp. 619–636, 2011.

[21] T. Sanders, "On the bogolyubov–ruzsa lemma," *Analysis & PDE*, vol. 5, no. 3, pp. 627–655, 2012.

[22] T. Sanders, "The structure theory of set addition revisited," *Bulletin of the American Mathematical Society*, vol. 50, no. 1, pp. 93–127, 2013.

[23] T. Schoen, "Improved bound in roth's theorem on arithmetic progressions," *Advances in Mathematics*, vol. 386, p. 107 801, 2021.

[24] T. Schoen and O. Sisask, "Roth's theorem for four variables and additive structures in sums of sparse sets," in *Forum of Mathematics, Sigma*, Cambridge University Press, vol. 4, 2016, e5.

[25] O. Sisask, "Discrete fourier analysis-structures in sumsets," Ph.D. dissertation, Fourier analysis of groups in combinatorics, 2013.

[26] T. Tao and V. Vu, *Additive Combinatorics* (Cambridge Studies in Advanced Mathematics). Cambridge University Press, 2006, ISBN: 9781139458344.

[27] T. Tao, *A symmetric formulation of the croot-lev-pach-ellenberg-gijswijt capset bound*, Jun. 2016.

[28] F. Tyrrell, "New lower bounds for cap sets," *arXiv preprint arXiv:2209.10045*, 2022.