FREIMAN'S THEOREM

WANG FANGYU

XIAMEN UNIVERSITY MALAYSIA

2026

XIAMEN UNIVERSITY MALAYSIA
厦門大學馬來西亞分校

FINAL YEAR PROJECT REPORT

FREIMAN'S THEOREM

NAME OF STUDENT	:	WANG FANGYU
STUDENT ID	:	MAT2309449
SCHOOL/FACULTY	:	DEPARTMENT OF MATHEMATICS
PROGRAMME	:	MATHEMATICS AND APPLIED MATHEMATICS
INTAKE	:	2023/09
SUPERVISOR	:	PROF. JAN DOBROWOLSKI

JANUARY 2026

DECLARATION

I hereby declare that this thesis is based on my original work except for citations and quotations which have been duly acknowledged. I also declare that it has not been previously and concurrently submitted for any other degree or award at Xiamen University Malaysia or other institutions.

Signature	:	王方宇
Name	:	Wang Fangyu
ID No.	:	MAT2309449
Date	:	July 5, 2026

APPROVAL FOR SUBMISSION

I certify that this project/thesis, entitled “Freiman’s Theorem", and prepared by WANG FANGYU, has met the required standard for submission in partial fulfilment of the requirements for the award of Bachelor of Science in Mathematics and Applied Mathematics (Honours) at Xiamen University Malaysia.

Approved by,

Signature	:	Jan Dobrowolski
Supervisor	:	Prof. Jan Dobrowolski
Date	:	July 5, 2026

ACKNOWLEDGEMENTS

First and foremost, I would like to express my sincere gratitude to my supervisor, Professor Jan Dobrowolski. Over the past year, he has guided me into the fascinating world of additive combinatorics. It was through him that I saw, for the very first time, what a pure and genuine love for mathematics truly looks like. Furthermore, his perspective that pure mathematics is not reserved only for a few “geniuses”, but is accessible to anyone with genuine interest and perseverance, has been particularly encouraging to me.

Yet, beyond the mathematics, my most profound gratitude belongs to my mother. It is her unwavering devotion that granted me the freedom to choose the university I desired. She has been the silent engine behind every theorem and every lemma. Naturally, this thesis belongs to her as much as it does to me.

On a practical note, I must thank Oolong tea, which has selflessly dedicated its caffeine through this journey. Furthermore, the precise temperature control and the exact timing required to brew it provided me with a few rare moments of respite within the chaotic process of LaTeX compilation.

Three years of university have gone by in a flash. Looking back, it has been nine years since I first left home to pursue my studies. What I miss the most from these nine years are those leisurely afternoons, riding my bicycle home after school. Yet, I know those days are now far behind me. Years of living away from home have made me weary of this drifting life, but standing at this milestone, I remain grateful for the path that has led me here. I do not know how much further this path will lead me, but I have come this far. The journey continues.

後之視今亦由今之視昔故列敘時人錄其所述雖世殊事異所以興懷其致一也後之方宇亦將有感於斯文

— Adapted from *Lantingji Xu* (353 AD)

ABSTRACT

This thesis explores the structural properties of finite sets with small doubling. We provide a detailed proof of a fundamental result in additive combinatorics, Freiman's theorem, which states that any finite subset of integers with a small doubling constant must be contained within a generalized arithmetic progression (GAP). To achieve that, the thesis presents detailed proofs of several critical tools that are used in the classic proof, including the Plünnecke-Ruzsa inequality, Bogolyubov's lemma, and the Ruzsa Modeling Lemma. Throughout the thesis, we explore the transition mapping from the integer group $\mathbb{Z}$ to the finite cyclic group $\mathbb{Z}/N\mathbb{Z}$ and how it maps back to $\mathbb{Z}$. Using this connection, we ultimately show that a set A with doubling constant K must be contained in a generalized arithmetic progression of dimension at most $e^{K^{O(1)}}$ and volume at most $e^{e^{K^{O(1)}}}|A|$.

Keywords: Additive combinatorics, Freiman's theorem, small doubling, generalized arithmetic progression, Ruzsa modeling lemma.

CONTENTS

LIST OF FIGURES

LIST OF SYMBOLS / ABBREVIATIONS

GAP	:	Generalized Arithmetic Progression
$\mathbb{Z}$	:	The set of integers
$\mathbb{Z}/N\mathbb{Z}$	:	The cyclic group of integers modulo N
$\mathbb{F}_p^n$	:	The n-dimensional vector space over the finite field $\mathbb{F}_p$
$\lvert A\rvert$	:	The cardinality (number of elements) of a finite set A
$A+B$	:	The sumset of sets A and B, defined as $\{a+b : a \in A, b \in B\}$
$A-B$	:	The difference set of sets A and B
kA	:	The k-fold iterated sumset $A+\cdots+A$ (k times)
$\lambda \cdot A$	:	The dilation of set A by a scalar λ
$\mathrm{Bohr}(R,\varepsilon)$	:	The Bohr set with dimension $\lvert R\rvert$ and width ε
$f * g$	:	The convolution of functions f and g
$\widehat{f}(r)$	:	The Fourier transform of f
$\mathbb{E}_{x\in X} f(x)$	:	The average (expectation) of $f(x)$ over the set X
$\lVert x\rVert_{\mathbb{R}/\mathbb{Z}}$	:	The distance from a real number x to the nearest integer
Λ	:	A full-rank lattice in $\mathbb{R}^d$
$\det \Lambda$	:	The determinant of the lattice Λ
$\mathrm{vol}(K)$	:	The volume of a set K
λ_i	:	The i-th successive minimum of a convex body
$O(\cdot)$	:	Big O notation, denoting an asymptotic upper bound
$O(1)$	:	An absolute constant, or a quantity bounded by a constant

CHAPTER 1

INTRODUCTION

1.1 Background and Motivation

Additive combinatorics is a relatively new and active branch in the field of combinatorics. The name of this field mainly comes from the 2006 book Additive Combinatorics by Terence Tao and Van H. Vu [TV06]. Interestingly, although this field mainly studies the additive structure of sets, tools from seemingly unrelated mathematical fields often prove very useful for our research on the additive structure, such as harmonic analysis, convex geometry, graph theory, and probability theory. This is also one of the reasons why the field is so active today. Furthermore, it is truly fascinating when we can combine these seemingly different mathematical tools to successfully solve an additive structure problem. One very important question in additive combinatorics is the connection between the structure of a set A itself and the size of its sumset $A + A$. The forward version of this question is actually quite easy to understand. For example, if A is highly structured, like an arithmetic progression, the size of its sumset is roughly twice its original size. On the other hand, if A lacks such structured properties, like a Sidon set, the size of its sumset will expand to about $|A|^2/2$. These two different examples show us that if a set has some degree of structure, its sumset will not expand very fast; in other words, it is somewhat easier to control. This leads to the inverse problem: if we know the expansion rate of the sumset of A, what can we say about the structure of A? Freiman's theorem tells us that: if the expansion rate of a set A can be bounded by a constant K, then A is contained in a generalized arithmetic progression of size bounded in terms of K and $|A|$. As the name suggests, the original version of Freiman's theorem was published by Gregory Freiman in 1966 [Fre73]. However, the bounds in his proof were very large, and the proof process was quite complicated. The proof framework widely used in modern textbooks is the one introduced by the Hungarian mathematician Imre Ruzsa in 1994. By introducing the modeling lemma and tools from the geometry of numbers, Ruzsa greatly simplified the proof and improved the quantitative bounds.

1.2 Thesis Objectives

Graph Theory and Additive Combinatorics is a graduate-level introductory textbook written by MIT professor Yufei Zhao [Zha23], focusing on connecting graph theory and additive combinatorics. Chapter 7 of this book gives us a complete presentation of the "Structure of Set Addition" problem mentioned above. It provides us with powerful tools for studying additive sets, such as Plünnecke's inequality and the Ruzsa covering lemma. In addition, it introduces the core modules used in Ruzsa's proof, such as Freiman homomorphisms, the modeling lemma, and the geometry of numbers, and shows us how to use this toolkit to prove Freiman's theorem. Furthermore, this chapter introduces the Polynomial Freiman-Ruzsa conjecture. However, since this book was published earlier, this conjecture has already been proved in 2023 by four mathematicians: W. T. Gowers, Ben Green, Freddie Manners, and Terence Tao. Although the book provides a complete and well-organized proof, many proofs are rather concise in order to preserve the flow of the overall exposition. Some key intermediate steps are treated only briefly, often within a single sentence, making the whole book very difficult for beginners to read. For example, a single sentence in the book—"[Note $\det(\Lambda) = 1/N$ since there are exactly N points of Λ within each translate of the unit cube.]" [Zha23, p. 259]—takes us three pages to fully and clearly express in Chapter 5. Addressing these pain points above, this thesis will follow the Ruzsa proof path of Freiman's theorem, providing detailed proofs and filling in the mathematical and logical details omitted in Yufei Zhao's book. At the same time, we will also introduce some definitions and lemmas from Tao and Vu's Additive Combinatorics [Zha23] to help us better understand some concepts. The main focus of this thesis is to provide a detailed explanation and proof of the classical Freiman's theorem over the integers based on Zhao's book, presenting an undergraduate-level introduction to additive combinatorics in a relatively relaxed way. (Note: This thesis will not cover the Polynomial Freiman-Ruzsa theorem. Interested readers can read the paper On a conjecture of Marton written by W. T. Gowers, Ben Green, Freddie Manners, and Terence Tao [GGMT25].)

1.3 Structure of the Thesis

The structure and chapter arrangement of this thesis are as follows: In Chapter 2, we will give some basic definitions in additive combinatorics, discuss the sumset properties of a few sets with known structures, and present our final goal: Freiman's theorem. Chapter 3 will introduce some very practical and powerful additive combinatorics tools, such as the Ruzsa triangle inequality, Plünnecke's inequality, and the Ruzsa covering lemma. We will also show how to use these existing tools to prove a version of Freiman's theorem over finite field. In Chapter 4, we will introduce the concept of Freiman homomorphisms. In order to deepen the understanding of this concept, we will discuss several problems related to Freiman homomorphisms and provide a proposition. Next, we will show how applying Freiman homomorphisms helps us prove a powerful tool: the Ruzsa modeling lemma. Interestingly, in this chapter, we will see how probability theory provides strong support when we study additive combinatorics. Chapter 5 shows the highly cross-disciplinary feature of additive combinatorics. We will first introduce tools from harmonic analysis to help us prove how sumsets necessarily contain subspaces or approximate subspaces, such as Bohr sets. After that we will introduce some definitions from the geometry of numbers, as well as an important result in this area, Minkowski's theorem, which is also a powerful tool in additive combinatorics. Finally, in Chapter 6, we will complete our final "puzzle". We will use the combinatorial tools collected in the previous chapters to solve our initial problem and complete the proof of Freiman's theorem.

CHAPTER 2

FUNDAMENTALS OF SET ADDITION AND THE INVERSE PROBLEM

In this Chapter, we will first provide some basic definitions in additive combinatorics in mathematical language to start our research. Then we will discuss several 'forward' questions; that is, if we know the structure of a set, what properties of its sumset are preserved. After that, we will present the 'inverse' problem: if we know the expansion properties of the sumsets, what structure must their corresponding sets preserve. The answer of this 'inverse' question is exactly our ultimate goal: Freiman's theorem, which we will state formally at the end of this Chapter.

2.1 Additive Combinatorics Vocabulary

To start our rigorous mathematical journey, let us first build up our Additive Combinatorics Vocabulary.

As intuition, a *sumset* is the 'sum' of sets, and its definition is:

Definition 2.1 (Sumset)**.** [Zha23, p. 237]
Let A and B be finite subsets of some ambient abelian group. We define their *sumset* to be

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

Following by the definition of *sumset* is the definition of *sumset notation*, with which we must be careful in additive combinatorics.

Definition 2.2 (Sumset notation)**.** [Zha23, p. 238]
Given a positive integer k, we define the iterated sumset

$$kA := A + \cdots + A \ \ (k \text{ times}).$$

This is different from dilating a set, which is denoted by

$$\lambda \cdot A := \{\lambda a : a \in A\}.$$

We also consider the difference set

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

The expansion rate of a set A, as mentioned in Chapter 1, is formally called the *doubling constant* in additive combinatorics. The following is its formal definition.

Definition 2.3 (Doubling constant)**.** [Zha23, p. 238]
The *doubling constant* K of a finite subset A in an abelian group is the ratio

$$K = |A + A|/|A|.$$

Before the discussion of the forward questions, we need to introduce an important structured set. Its definition is as follows.

Definition 2.4 (GAP – generalized arithmetic progression)**.** [Zha23, p. 239]
A *generalized arithmetic progression (GAP)* in an abelian group Γ is defined to be an affine map

$$\phi : [L_1] \times \cdots \times [L_d] \to \Gamma.$$

That is, for some $a_0, \ldots, a_d \in \Gamma$,

$$\phi(x_1, \ldots, x_d) = a_0 + a_1 x_1 + \cdots + a_d x_d.$$

This GAP has *dimension* d and *volume* $L_1 \cdots L_d$. We say that this GAP is *proper* if ϕ is injective.

In practice, we frequently abuse notation and identify the GAP with its image set $\phi([L_1] \times \cdots \times [L_d]) \subseteq \Gamma$. Thus, when we say a set A is contained in a GAP, we mean that A is a subset of the image of this affine map.

2.2 The Forward Questions

To build our intuition about how a set's structure affects its *doubling constant*, let us examine a few concrete examples. We start with the simplest example, where the set is highly structured.

Example 2.5. Prove that if A is an arithmetic progression, then $|A + A| = 2|A| - 1$.

Solution. Let $a_0, a_1 \in \mathbb{R}$ be fixed coefficients, $l_1 \in \{0, 1, \ldots, N-1\}$, then define A as

$$A = \{a_0 + a_1 l_1\}.$$

Then A is an arithmetic progression, in the case where $a_1 = 0$, the cardinality of A, namely, $|A|$ is

$$|A| = 1,$$

and $A + A = A$ which implies that

$$|A + A| = 1 = |A + A| = 2|A| - 1.$$

In the case where $a_1 \neq 0$, the cardinality of A, namely, $|A|$ is equal to the number of possible values of l_1, that is,

$$|A| = N.$$

Notice that for $l_1, l_1{}' \in \{0, 1, \ldots, N-1\}$,

$$\begin{aligned} A + A &= a_0 + a_1 l_1 + a_0 + a_1 l_1{}' \\ &= 2a_0 + a_1 (l_1 + l_1{}'), \end{aligned}$$

and $l_1 + l_1{}' \in \{0, 1, \ldots, 2N-2\}$, then the cardinality of $A + A$, namely, $|A + A|$ is equal to the number of possible values of $l_1 + l_1{}'$, that is,

$$|A + A| = 2N - 1.$$

This implies that

$$|A + A| = 2|A| - 1.$$

□

Remark 2.6 (Easy bounds on sumset size)**.** [Zha23, p. 238] One can check that the *sumset* size above is actually the lower bound of the size of integer sumsets. More generally, the bound of the size of sumset of integer set A is:

$$2|A| - 1 \leqslant |A + A| \leqslant \binom{|A| + 1}{2}.$$

Proof. We start with the lower bound. Suppose that $|A| = N$, if we arrange the elements of A in increasing order as

$$a_1 < a_2 < \ldots < a_N.$$

We must have the following distinct elements in $A + A$:

$$\begin{aligned} a_1 + a_1, a_1 + a_2, \ldots, a_1 + a_N \\ a_2 + a_N \\ \vdots \\ a_N + a_N. \end{aligned}$$

It is trivial to verify there are $2N - 1$ elements above. Note that we omit the terms like $a_2 + a_4$ since it may have the same value as $a_1 + a_i$ for some $i > 4$. Therefore, we have the lower bound of $2|A| - 1$.

Now let us check the upper bound. Suppose that $|A| = N$ and that $A = \{a_1, a_2, \ldots, a_N\}$ satisfies for each $a_i + a_j$ and $a_m + a_n$ in $A + A$, if we have $(i, j) \notin \{(m, n), (n, m)\}$, then $a_i + a_j \neq a_m + a_n$. Such a set A maximizes its size of sumsets, and it suffices to check the number of unordered (a, b), where $a, b \in \{1, 2, \ldots, n\}$, to check the size of $|A + A|$.

1. For $a = b$, we have N options.
2. For $a \neq b$, for each fixed a, we have $N - 1$ options of b. Therefore, we have $N(N - 1)$ options of (a, b) and the number of unordered (a, b) is $\frac{N(N-1)}{2}$. This is because for each fixed a and each (a, b), there exist (b, a) when we fixed b to be our first component.

Therefore, the size of $|A + A|$ is $(N + \frac{N(N-1)}{2}) = \frac{N(N+1)}{2} = \binom{|A|+1}{2}$. □

The above shows that an arithmetic progression A has a *doubling constant* which is roughly 2, implying that the expansion of its *sumset* is easy to control. Intuitively, we are curious about whether there is a relationship between the *doubling constant* of a generalized arithmetic progression and this approximate *doubling constant* 2 of an arithmetic progression, is it supposed closely related with its *dimension* d and 2? It is true and we will prove that by the following example.

Example 2.7. Prove that if A is a d-dimensional generalized arithmetic progression, then $|A + A| \leqslant 2^d\,|A|$.

Solution. For each $i \in \{1, 2, \dots, d\}$, let $l_i \in \{1, 2, \dots, N_i\}$, $L_i \in \{2, 3, \dots, 2N_i\}$ and let $a_0, a_1, \dots, a_d \in \mathbb{R}$ be fixed coefficients, then define

$$A = \{a_0 + a_1 l_1 + a_2 l_2 + \cdots + a_d l_d\}. \tag{2.1}$$

Then A is a d-dimensional generalized arithmetic progression. Let $S_1 = \{(l_1, l_2, \dots, l_d)\}$, then we have

$$A = \{a_0 + (a_1, a_2, \dots, a_d)(l_1, l_2, \dots, l_d) \mid (l_1, l_2, \dots, l_d) \in S_1\}.$$

Let $S_2 = \{(L_1, L_2, \dots, L_d)\}$, then for $l_i, l_i' \in \{1, 2, \dots, N_i\}$ ($i \in 1, 2, \dots, d$), we have

$$\begin{aligned} A + A &= \{a_0 + (a_1, a_2, \dots, a_d)(l_1, l_2, \dots, l_d) + a_0 + (a_1, a_2, \dots, a_d)(l_1', l_2', \dots, l_d')\} \\ &= \{2a_0 + (a_1, a_2, \dots, a_d)(l_1 + l_1', l_2 + l_2', \dots, l_d + l_d')\} \\ &= \{2a_0 + (a_1, a_2, \dots, a_d)(L_1, L_2, \dots, L_d)\}. \end{aligned} \tag{2.2}$$

Let $E = \{0, 1\}^d$ and $n = (N_1, N_2, \dots, N_d)$, we observe that

$$S_2 = \bigcup_{e_i \in E} (S_1 + n \odot e_i),$$

where for $e_i = (e_{i1}, e_{i2}, \dots, e_{id}) \in E$, $n \odot e_i = (N_1 \cdot e_{i1}, N_2 \cdot e_{i2}, \dots, N_d \cdot e_{id})$.
Therefore

$$A + A = \left\{ 2a_0 + (a_1, a_2, \dots, a_d)(k_1, k_2, \dots, k_d) \mid (k_1, k_2, \dots, k_d) \in \bigcup_{e_i \in E} (S_1 + n \odot e_i) \right\}. \tag{2.3}$$

For every $(k_1, k_2, \dots, k_d) \in (S_1 + n \odot e_i)$, $e_i \in E$ we have

$$(k_1, k_2, \dots, k_d) = (l_1, l_2, \dots, l_d) + n \odot e_i,$$

for some $(l_1, l_2, \dots, l_d) \in S_1$.
Thus for $\kappa \in A + A$ corresponding to $(k_1, k_2, \dots, k_d)$, we have

$$\begin{aligned} \kappa &= 2a_0 + (a_1, a_2, \dots, a_d)(k_1, k_2, \dots, k_d) \\ &= 2a_0 + (a_1, a_2, \dots, a_d) \cdot ((l_1, l_2, \dots, l_d) + (n \odot e_i)) \\ &= 2a_0 + (a_1, a_2, \dots, a_d) \cdot (l_1, l_2, \dots, l_d) + (a_1, a_2, \dots, a_d) \cdot (n \odot e_i) \\ &= a_0 + (a_1, a_2, \dots, a_d) \cdot (l_1, l_2, \dots, l_d) + a_0 + (a_1, a_2, \dots, a_d) \cdot (n \odot e_i). \end{aligned}$$

Observe that $\alpha = a_0 + (a_1, a_2, \ldots, a_d) \cdot (l_1, l_2, \ldots, l_d) \in A$ and $c_i := a_0 + (a_1, a_2, \ldots, a_d) \cdot (n \odot e_i)$ is a constant, and $\kappa = \alpha + c_i$.
Therefore, for any $S_{e_i} = (S_1 + n \odot e_i) \in \bigcup_{e_i \in E} (S_1 + n \odot e_i)$,

$$\begin{aligned} A_{e_i} &= \{2a_0 + (a_1, a_2, \ldots, a_d)(k_1, k_2, \ldots, k_d) \mid (k_1, k_2, \ldots, k_d) \in S_{e_i}\} \\ &= A + c_i \end{aligned}$$

is a translate of A.
Hence

$$|A_{e_i}| = |A|. \tag{2.4}$$

Notice that

$$\begin{aligned} A + A &= \left\{ 2a_0 + (a_1, a_2, \ldots, a_d)(k_1, k_2, \ldots, k_d) \mid (k_1, k_2, \ldots, k_d) \in \bigcup_{e_i \in E} (S_1 + n \odot e_i) \right\} \\ &= \bigcup_{e_i \in E} \{2a_0 + (a_1, a_2, \ldots, a_d)(k_1, k_2, \ldots, k_d) \mid (k_1, k_2, \ldots, k_d) \in S_{e_i}\} \\ &= \bigcup_{e_i \in E} A_{e_i}, \end{aligned}$$

and since for $e_i, e_j \in E$, $e_i \neq e_j$, the sets A_{e_i} and A_{e_j} are not necessarily disjoint, we have

$$\begin{aligned} |A + A| &= \left| \bigcup_{e_i \in E} A_{e_i} \right| \\ &\leqslant \sum_{e_i \in E} |A_{e_i}|. \end{aligned} \tag{2.5}$$

It is straightforward to verify that $|E| = 2^d$, and by combining (2.4), (2.5) we conclude that

$$|A + A| \leqslant 2^d |A|. \tag{2.6}$$

□

This example answer our intuitively curiosity as mentioned before, the *doubling constant* of a generalized arithmetic progression can be roughly presented by 2^d. This implies that the size of the *sumset* of a generalized arithmetic progression A is roughly 2^d times of the size of A. Motivated by that, let us now focus on the difference set $A - A$ and check whether it can be covered by 2^d- many translates of A.

Example 2.8. Assuming that A is a d-dimensional generalized arithmetic progression, prove that $A - A$ can be covered by $f(d)$- many translates of A for some constant $f(d)$ depending only on d.

Solution. For each $i \in \{1, 2, \ldots, d\}$, let $l_i \in \{1, 2, \ldots, N_i\}$, $L_i \in \{1 - N_i, 2 - N_i, \ldots, N_i - 1\}$ and let $a_0, a_1, \ldots, a_d \in \mathbb{R}$ be fixed coefficients, then define

$$A = \{a_0 + a_1 l_1 + a_2 l_2 + \cdots + a_d l_d\}. \tag{2.7}$$

Then A is a d-dimensional generalized arithmetic progression. Let $S_1 = \{(l_1, l_2, \ldots, l_d)\}$, then we have

$$A = \{a_0 + (a_1, a_2, \ldots, a_d)(l_1, l_2, \ldots, l_d) \mid (l_1, l_2, \ldots, l_d) \in S_1\}.$$

Let $S_2 = \{(L_1, L_2, \ldots, L_d)\}$, then for $l_i, l_i' \in \{1, 2, \ldots, N_i\}$ ($i \in 1, 2, \ldots, d$), we have

$$\begin{aligned} A - A &= \{a_0 + (a_1, a_2, \ldots, a_d)(l_1, l_2, \ldots, l_d) - a_0 - (a_1, a_2, \ldots, a_d)(l_1', l_2', \ldots, l_d')\} \\ &= \{(a_1, a_2, \ldots, a_d)(l_1 - l_1', l_2 - l_2', \ldots, l_d - l_d')\} \\ &= \{(a_1, a_2, \ldots, a_d)(L_1, L_2, \ldots, L_d)\}. \end{aligned} \tag{2.8}$$

Let $E = \{-1, 0\}^d$ and $n = (N_1, N_2, \ldots, N_d)$, we observe that

$$S_2 = \bigcup_{e_i \in E} (S_1 + n \odot e_i),$$

where for $e_i = (e_{i1}, e_{i2}, \ldots, e_{id}) \in E$, $n \odot e_i = (N_1 \cdot e_{i1}, N_2 \cdot e_{i2}, \ldots, N_d \cdot e_{id})$. Therefore

$$A - A = \left\{ (a_1, a_2, \ldots, a_d)(k_1, k_2, \ldots, k_d) \mid (k_1, k_2, \ldots, k_d) \in \bigcup_{e_i \in E} (S_1 + n \odot e_i) \right\}. \tag{2.9}$$

For every $(k_1, k_2, \ldots, k_d) \in (S_1 + n \odot e_i)$, $e_i \in E$ we have

$$(k_1, k_2, \ldots, k_d) = (l_1, l_2, \ldots, l_d) + n \odot e_i,$$

for some $(l_1, l_2, \ldots, l_d) \in S_1$.
Thus for $\kappa \in A - A$ corresponding to $(k_1, k_2, \ldots, k_d)$, we have

$$
\begin{aligned}
\kappa &= (a_1, a_2, \ldots, a_d)\,(k_1, k_2, \ldots, k_d) \\
&= (a_1, a_2, \ldots, a_d) \cdot ((l_1, l_2, \ldots, l_d) + (n \odot e_i)) \\
&= (a_1, a_2, \ldots, a_d) \cdot (l_1, l_2, \ldots, l_d) + (a_1, a_2, \ldots, a_d) \cdot (n \odot e_i) \\
&= a_0 + (a_1, a_2, \ldots, a_d) \cdot (l_1, l_2, \ldots, l_d) + (-a_0) + (a_1, a_2, \ldots, a_d) \cdot (n \odot e_i)\,.
\end{aligned}
$$

Observe that $\alpha = a_0 + (a_1, a_2, \ldots, a_d) \cdot (l_1, l_2, \ldots, l_d) \in A$ and $c_i := (-a_0) + (a_1, a_2, \ldots, a_d) \cdot (n \odot e_i)$ is a constant, and $\kappa = \alpha + c_i$.

Therefore, for any $S_{e_i} = (S_1 + n \odot e_i) \in \bigcup_{e_i \in E} (S_1 + n \odot e_i)$,

$$
\begin{aligned}
A_{e_i} &= \{(a_1, a_2, \ldots, a_d)\,(k_1, k_2, \ldots, k_d) \mid (k_1, k_2, \ldots, k_d) \in S_{e_i}\} && (2.10) \\
&= A + c_i && (2.11)
\end{aligned}
$$

is a translate of A.

Notice that

$$
\begin{aligned}
A - A &= \left\{(a_1, a_2, \ldots, a_d)\,(k_1, k_2, \ldots, k_d) \mid (k_1, k_2, \ldots, k_d) \in \bigcup_{e_i \in E} (S_1 + n \odot e_i)\right\} \\
&= \bigcup_{e_i \in E} \{(a_1, a_2, \ldots, a_d)\,(k_1, k_2, \ldots, k_d) \mid (k_1, k_2, \ldots, k_d) \in S_{e_i}\} \\
&= \bigcup_{e_i \in E} A_{e_i}. && (2.12)
\end{aligned}
$$

It is straightforward to verify that $|E| = 2^d$, hence we conclude that $A - A$ can be covered by 2^d translates of A. $\square$

The following is another clearly structured set A. However, it is geometrically structured instead of linearly structured, and we will show that its *doubling constant* is depends on its size instead of a constant.

Example 2.9. Fix $r \in \mathbb{Z}$, $r \geqslant 2$, prove that if $A = \left\{1, r, r^2, \ldots, r^{N-1}\right\}$, then the *doubling constant* of A, namely, $\frac{|A+A|}{|A|} = \frac{N+1}{2}$.

Solution. Observe that $A = \{r^a \mid a \in \{0, 1, \ldots, N-1\}\}$ so that $|A| = N$, and

$$A + A = \left\{r^a + r^b \mid a, b \in \{0, 1, \ldots, N-1\}\right\}.$$

For $a, b, a', b' \in \{0, 1, \ldots, N-1\}$, suppose that

$$r^a + r^b = r^{a'} + r^{b'}.$$

Without loss of generality, we may assume that $a \leqslant b$ and $a' \leqslant b'$. Hence we have

$$r^a \left(1 + r^{b-a}\right) = r^{a'} \left(1 + r^{b'-a'}\right).$$

If $a = a'$, then $r^b = r^{b'}$, which implies that $b = b'$.
If $a \neq a'$, then without loss of generality, we may assume that $a < a'$, then

$$\frac{1 + r^{b-a}}{r^{a'-a}} = 1 + r^{b'-a'}. \tag{2.13}$$

For the right-hand side of (2.13), since $a' \leqslant b'$, $1 + r^{b'-a'}$ is an integer and satisfies

$$1 + r^{b'-a'} \geqslant 1 + r^0 = 2.$$

For the right-hand side of (2.13), let $\alpha = a' - a$.
If $b = a$, then

$$\frac{1 + r^{b-a}}{r^{a'-a}} = \frac{1+1}{r^\alpha} = \frac{2}{r^\alpha}. \tag{2.14}$$

The only situation that makes (2.14) an integer is when $r = 2$ and $\alpha = 1$, in which case (2.14) equals 1. This contradicts the fact that the right-hand side is greater than or equal to 2.
If $b \neq a$, let $\beta = b - a$, then

$$\begin{aligned} \frac{1 + r^{b-a}}{r^{a'-a}} &= \frac{1 + r^\beta}{r^\alpha} \\ &= \frac{1}{r^\alpha} + \frac{r^\beta}{r^\alpha}. \end{aligned} \tag{2.15}$$

Since $\alpha > 0$, if $\beta \geqslant \alpha$, (2.15) can not be an integer, if $\beta < \alpha$, then (2.15) can write in form of

$$\frac{1}{r^\alpha} + \frac{1}{r^\gamma},$$

where $\gamma = \alpha - \beta > 0$ and $\gamma < \alpha$.Thus

$$\frac{1}{r^\alpha} + \frac{1}{r^\gamma} < 2\frac{1}{r^\gamma} \leqslant \frac{2}{r} \leqslant 1.$$

Therefore we can conclude that the right-hand side can not be an integer.
Above shows that the only possible case in which $r^a + r^b = r^{a'} + r^{b'}$ holds is when $a = a'$ and $b = b'$.
It is trivial to show that for $a, b \in \{0, 1, \ldots, N-1\}$, there are $\binom{N+1}{2}$ unordered pairs of

(a, b), which implies that $|A+A| = \binom{N+1}{2}$.
Thus

$$\frac{|A+A|}{|A|} = \frac{\binom{N+1}{2}}{N} = \frac{N\,(N+1)\,/2}{N} = \frac{N+1}{2}. \tag{2.16}$$

□

This example shows that even though different sets may all be structured, their structures can nevertheless vary in quality. Here, quality refers to the difficulty of controlling the behavior of their *sumsets*.

2.3 Inverse Question

In the last section, we have discussed several behaviors of the *sumset* of different structured sets, namely, their *doubling constant*. Across mathematics, we are always curious about the Inverse Question, informally speaking, for instance, if we know an 'if' statement is 'true', we will be curious about whether the 'only if' statement is also true. Therefore, while we discuss the from structure to *doubling constant* question above, we will naturally curious about the Inverse Question of above Forward Question, that is, if we know the behavior of the *sumset* of some set, namely, its *doubling constant*, what we can say about its structure?

Gregory Freiman gave us the answer in 1966, which is widely known as Freiman's theorem [Fre73]. However, we will state the simplified and improved version of this theorem given by Hungarian mathematician Imre Ruzsa in 1994. His proof framework is now more frequently been used in modern textbooks-which includes our main reference-Graph Theory and Additive Combinatorics by Yufei Zhao [Zha23]. We shall prove this theorem follow by the proof framework in Zhao's book in Chapter 6 after we collected all the tools we need.

The following is the formal statement of Freiman's theorem:

Theorem 2.10 (Freiman's theorem)**.** [Fre73][Zha23, p. 260]
Let $A \subseteq \mathbb{Z}$ be a finite set satisfying $|A+A| \leqslant K|A|$. Then A is contained in a GAP of dimension at most $d(K)$ and volume at most $f(K)|A|$, where $d(K) \leqslant \exp(K^C)$ and $f(K) \leqslant \exp(\exp(K^C))$ for some absolute constant C.

CHAPTER 3

ADDITIVE TOOLKITS AND FREIMAN'S THEOREM WITH BOUNDED EXPONENT

In the previous Chapter, we have built some intuition in additive combinatorics and shown our ultimate goal. However, the statement is far from straightforward to prove from any perspective. In that case, we will start to build up our toolkits from this Chapter to help us solve it.

More specifically, in this Chapter, we will show some very practical and powerful tools in additive combinatorics and use them to prove a weaker version of Theorem 2.10, which is over finite fields.

3.1 Combinatorial Toolkits

3.1.1 Triangle inequalities

Here are some basic and useful inequalities relating the sizes of sumsets.

Theorem 3.1 (Ruzsa triangle inequality)**.** [Ruz89][Zha23, p. 240]
If A, B, C are finite subsets of an abelian group, then

$$|A|\,|B-C| \leqslant |A-B|\,|A-C|\,.$$

Proof. Let A, B, C be finite subsets of an abelian group. For any $d \in B-C$, we define $b(d) \in B$ and $c(d) \in C$ such that $d = b(d) - c(d)$. Define

$$\phi : A \times (B-C) \to (A-B) \times (A-C)$$
$$\phi((a,d)) = (a - b(d), a - c(d))\,.$$

For any $(a_1, d_1), (a_2, d_2) \in A \times (B-C)$, if

$$\phi((a_1, d_1)) = \phi((a_2, d_2))\,,$$

then

$$a_1 - b(d_1) = a_2 - b(d_2)$$
$$a_1 - c(d_1) = a_2 - c(d_2).$$

Subtracting these two equalities we get

$$b(d_1) - c(d_1) = b(d_2) - c(d_2),$$

which implies that $d_1 = d_2$ by definition of the functions b and c.
Hence $a_1 = a_2$, showing that ϕ is injective.
Therefore,

$$|A||B-C| = |A \times (B-C)| \leqslant |(A-B) \times (A-C)| = |A-B||A-C|.$$

$\square$

Remark 3.2. [Zha23, p. 241] Theorem 3.1 is named 'triangle' following the definition of:

Definition 3.3 (Ruzsa distance)**.** [Zha23, p. 241] If A, B are two subsets of an abelian group, then the *Ruzsa distance* is defined as:

$$\rho(A,B) := \log \frac{|A-B|}{\sqrt{|A||B|}}.$$

Theorem 3.1 can be rewritten as

$$\rho(B,C) \leqslant \rho(A,B) + \rho(A,C).$$

However, the function ρ is not a metric since $\rho(A,A) \neq 0$ in general.

Remark 3.4. [Zha23, p. 241] By replacing B with $-B$ and/or C with $-C$, Theorem 3.1 implies some additional sumset inequalities:

$$|A||B+C| \leqslant |A+B||A-C|;$$
$$|A||B+C| \leqslant |A-B||A+C|;$$
$$|A||B-C| \leqslant |A+B||A+C|.$$

However, the trick in Remark 3.4 cannot be used to prove the similarly looking inequality

$$|A||B+C| \leqslant |A+B||A+C|.$$

Therefore, we provide a separate proof (Theorem 3.6) of this inequality several pages later after showing Lemma 3.5, which plays a critical role in proving Theorem 3.6 and Theorem 3.7.

3.1.2 Expansion ratio bounds and another triangle inequality

Lemma 3.5 (Expansion ratio bounds (Petridis's lemma)). [Pet12][Zha23, p. 242] Let X and B be finite subsets of an abelian group, with $|X| > 0$. Suppose

$$\frac{|Y+B|}{|Y|} \geqslant \frac{|X+B|}{|X|}, \text{ for all nonempty } Y \subseteq X.$$

Then for any nonempty finite subset C of the abelian group,

$$\frac{|X+C+B|}{|X+C|} \leqslant \frac{|X+B|}{|X|}.$$

Proof. We use induction to prove this. For the base case $|C| = 1$, there is only one element in C, say, c_1. Since X and B are subsets of an abelian groups,

$$X + c_1 + B = X + B + c_1.$$

Thus

$$|X + c_1 + B| = |X + B + c_1|.$$

Since $X + B + c_1$ and $X + c_1$ are translates of $X + B$ and X, respectively,

$$|X + c_1 + B| = |X + B + c_1| = |X + B|$$
$$|X + c_1| = |X|.$$

Thus

$$\frac{|X+c_1+B|}{|X+c_1|} = \frac{|X+B|}{|X|}.$$

For the induction step, assume that for some set C, the following inequality holds:

$$\frac{|X+C+B|}{|X+C|} \leqslant \frac{|X+B|}{|X|}.$$

Now consider $C \cup \{c\}$ for some $c \notin C$, we wish to show that

$$\frac{|X+(C\cup\{c\})+B|}{|X+(C\cup\{c\})|} \leqslant \frac{|X+B|}{|X|}.$$

Let

$$Y = \{x \in X \mid (x + c + B) \subseteq (X + C + B)\} \subseteq X,$$

then we have

$$\frac{|Y+B|}{|Y|} \geqslant \frac{|X+B|}{|X|}.$$

So we have

$$\begin{aligned}
|Y+B| &\geqslant \frac{|X+B|}{|X|} \cdot |Y| \\
-|Y+B| &\leqslant -\frac{|X+B|}{|X|} \cdot |Y| \\
|X+B| - |Y+B| &\leqslant |X+B| - \frac{|X+B|}{|X|} \cdot |Y| \\
&= \frac{|X+B|}{|X|} \cdot |X| - \frac{|X+B|}{|X|} \cdot |Y| \\
&= \frac{|X+B|}{|X|} \left(|X| - |Y|\right). \qquad (3.1)
\end{aligned}$$

Notice that

$$|(X+c+B) \setminus (X+C+B)| = |X+c+B| - |(X+c+B) \cap (X+C+B)|. \qquad (3.2)$$

For all $x \in Y$, by the definition of Y, we have

$$x+c+B \subseteq (X+c+B) \cap (X+C+B),$$

which implies that

$$\begin{aligned}
Y+c+B &\subseteq (X+c+B) \cap (X+C+B) \\
|Y+c+B| &\leqslant |(X+c+B) \cap (X+C+B)|. \qquad (3.3)
\end{aligned}$$

Since $Y+c+B$ and $X+c+B$ are translates of $Y+B$ and $X+B$, respectively,

$$|Y+c+B| = |Y+B| \qquad (3.4)$$

$$|X+c+B| = |X+B|. \qquad (3.5)$$

Therefore, by combining (3.2), (3.3), (3.4), (3.5), we have

$$|(X+c+B) \setminus (X+C+B)| \leqslant |X+B| - |Y+B|. \qquad (3.6)$$

Notice that

$$|(X+c) \setminus (X+C)| = |X+c| - |(X+c) \cap (X+C)|. \qquad (3.7)$$

For every $x \in X$ satisfying $x + c \in (X + c) \cap (X + C)$,

$$x + c + B \subseteq X + C + B.$$

Thus

$$x \in Y$$
$$x + c \in Y + c,$$

which implies

$$(X + c) \cap (X + C) \subseteq Y + c \tag{3.8}$$
$$|(X + c) \cap (X + C)| \leqslant |Y + c| \,. \tag{3.9}$$

Since $Y + c$ and $X + c$ are translates of Y and X, respectively,

$$|Y + c| = |Y| \tag{3.10}$$
$$|X + c| = |X| \,. \tag{3.11}$$

Therefore, by combining (3.7), (3.9), (3.10), (3.11), we have

$$|(X + c) \setminus (X + C)| \geqslant |X| - |Y| \,. \tag{3.12}$$

By combining (3.1), (3.6), (3.12), we have

$$|(X + c + B) \setminus (X + C + B)| \leqslant \frac{|X + B|}{|X|} |(X + c) \setminus (X + C)| \,.$$

Let

$$\frac{|X + B|}{|X|} = K.$$

We have shown that

$$|(X + c + B) \setminus (X + C + B)| \leqslant K \, |(X + c) \setminus (X + C)|$$

and assumed that

$$|X + C + B| \leqslant K \, |X + C| \,.$$

Observe that

$$|X + (C \cup \{c\}) + B| = |X + C + B| + |(X + c + B) \setminus (X + C + B)|$$
$$|X + (C \cup \{c\})| = |X + C| + |(X + c) \setminus (X + C)|\,.$$

Therefore we have

$$\begin{aligned}
\frac{|X + (C \cup \{c\}) + B|}{|X + (C \cup \{c\})|} &= \frac{|X + C + B| + |(X + c + B) \setminus (X + C + B)|}{|X + C| + |(X + c) \setminus (X + C)|} \\
&\leqslant \frac{K\,|X + C| + K\,|(X + c) \setminus (X + C)|}{|X + C| + |(X + c) \setminus (X + C)|} \\
&= \frac{K\,(|X + C| + |(X + c) \setminus (X + C)|)}{|X + C| + |(X + c) \setminus (X + C)|} \\
&= K.
\end{aligned}$$

So we can conclude that

$$\frac{|X + (C \cup \{c\}) + B|}{|X + (C \cup \{c\})|} \leqslant \frac{|X + B|}{|X|}.$$

□

Now, let us use our newly acquired tool to solve our remaining problem as mentioned before.

Theorem 3.6 (Another triangle inequality)**.** [Zha23, p. 244]
Let A, B, C be finite subsets of an abelian group.
Then

$$|A|\,|B + C| \leqslant |A + B|\,|A + C|\,.$$

Proof. Choose a nonempty subset $X \subseteq A$ that minimizes the ratio $\frac{|X+B|}{|X|}$. Thus

$$\frac{|X + B|}{|X|} \leqslant \frac{|A + B|}{|A|}, \tag{3.13}$$

and for any nonempty $Y \subseteq X \subseteq A$,

$$\frac{|Y + B|}{|Y|} \geqslant \frac{|X + B|}{|X|}.$$

By Lemma 3.5,

$$|X + C + B| \leqslant |X + C|\,\frac{|X + B|}{|X|}. \tag{3.14}$$

Since X is a subset of A,

$$|X + C| \leqslant |A + C| . \tag{3.15}$$

By combining (3.13), (3.14) and (3.15),

$$|B + C| \leqslant |X + B + C| \leqslant |X + C| \frac{|X + B|}{|X|} \leqslant |A + C| \frac{|A + B|}{|A|}.$$

Hence we conclude that

$$|A| |B + C| \leqslant |A + B| |A + C| .$$

$\square$

3.1.3 Plünnecke's inequality

Plünnecke's inequality is a very useful tool in additive combinatorics, which allows us to bound the size of some difference set by its original size and its *doubling constant*. (The special case $A = B$ of the following statement)

Theorem 3.7 (Plünnecke's inequality)**.** [Plü70, Ruz89][Zha23, p. 242]
Let A and B be finite subsets of an abelian group satisfying

$$|A + B| \leqslant K |A| .$$

Then for all integers $m, n \geqslant 0$,

$$|mB - nB| \leqslant K^{m+n} |A| .$$

Proof (Petridis [Pet12]). Choose a nonempty subset $X \subseteq A$ that minimizes the ratio $\frac{|X+B|}{|X|}$. Thus

$$\frac{|X + B|}{|X|} \leqslant \frac{|A + B|}{|A|} \leqslant K,$$

and for any nonempty $Y \subseteq X \subseteq A$,

$$\frac{|Y + B|}{|Y|} \geqslant \frac{|X + B|}{|X|}.$$

By Lemma 3.5, for all integers $n \geqslant 0$, take $C = nB$, which is nonempty and finite,

$$\frac{|X + C + B|}{|X + C|} = \frac{|X + nB + B|}{|X + nB|} = \frac{|X + (n + 1) B|}{|X + nB|} \leqslant \frac{|X + B|}{|X|} \leqslant K.$$

Hence

$$|X + (n+1)\,B| \leqslant K\,|X + nB|\,.$$

Thus

$$K\,|X| \geqslant |X + B|\,, K^2\,|X| \geqslant K\,|X + B| \geqslant |X + 2B|\,, \ldots.$$

Therefore, by induction,

$$K^n\,|X| \geqslant |X + nB|\,, \text{for all integers } n \geqslant 0. \tag{3.16}$$

Since B is in an abelian group and by *Ruzsa triangle inequality*, for all integers $m, n \geqslant 0$,

$$\begin{aligned} |X|\,|mB - nB| &= |X|\,|nB - mB| = |X|\,|(-mB) - (-nB)| \\ &\leqslant |X - (-mB)|\,|X - (-nB)| = |X + mB|\,|X + nB|\,. \end{aligned} \tag{3.17}$$

By combining (3.16) and (3.17) we obtain

$$|mB - nB| \leqslant |X + mB|\,|X + nB|\,/\,|X| \leqslant K^m\,|X| \cdot K^n\,|X|\,/\,|X| = K^{m+n}\,|X|\,.$$

Since X is a subset of A, $K^{m+n}\,|X| \leqslant K^{m+n}\,|A|$.
Therefore

$$|mB - nB| \leqslant K^{m+n}\,|A|\,.$$

□

Remark 3.8 (History of Theorem 3.7)**.** [Zha23, p. 242] Theorem 3.7 is the more general statement of the historical Plünnecke's inequality, which is the special case $A = B$ of Theorem 3.7. The historical version was first proved by Helmut Plünnecke [Plü70]. Imre Ruzsa [Ruz89] gave a simpler version of Plünnecke's proof and also extended it from sums to differences. Therefore, the historical version is also known as Plünnecke-Ruzsa inequality. However, Ruzsa's proof was still quite long and complex. In a surprising breakthrough, Giorgis Petridis [Pet12] found a very short proof of the result by introducing his novel tool, Petridis's lemma (Lemma 3.5), which is the one we presented above.

3.1.4 Ruzsa covering lemma

Here is a simple and powerful tool in the study of sumsets.

Theorem 3.9 (Ruzsa covering lemma)**.** [Ruz99][Zha23, p. 244]
Let X and B be finite sets in some abelian group. If

$$|X + B| \leqslant K |B|,$$

then there exists a subset $T \subseteq X$ with $|T| \leqslant K$ such that

$$X \subseteq T + B - B.$$

Proof. Let $T \subseteq X$ be a maximal subset such that $t + B$ are disjoint for all $t \in X$. Here maximal means T cannot be enlarged while preserving this property, equivalently, if there exists $x \in X \setminus T$ such that for all $t \in T$, $(x + B) \cap (t + B) = \emptyset$, then $T \cup \{x\}$ is a superset of T and still satisfies the disjointness property, which contradicts the maximality of T. Hence, for every $x \in X \setminus T$, there must exist $t \in T$ such that $(x + B) \cap (t + B) \neq \emptyset$.
By disjointness,

$$|T| |B| = |T + B| \leqslant |X + B| \leqslant K |B|.$$

Thus

$$|T| \leqslant K.$$

By the definition of T, for all $x \in X$, there exists $t \in T$ such that $(x + B) \cap (t + B) \neq \emptyset$, thus there exist $b, b' \in B$ such that

$$x + b = t + b'$$
$$x = t + b' - b$$
$$x \in T + B - B, \text{for all } x \in X.$$

Therefore,

$$X \subseteq T + B - B.$$

□

3.2 Freiman's Theorem over Finite Fields

Before demonstrating what we can achieve using the toolkits we have built so far, we first introduce the following concept.

Definition 3.10 (Exponent of an abelian group)**.** [Zha23, p. 246] The *exponent* of an abelian group (written additively) is the smallest positive integer r such that $rx = 0$ for all elements x of the group. If no finite r exists, we say that its exponent is infinite (some conventions say that the exponent is zero).

We shall prove a more general result Theorem 3.12, to prove the following statement.

Theorem 3.11 (Freiman's theorem in $\mathbb{F}_2^n$)**.** [Ruz99][Zha23, p. 246]
If $A \subseteq \mathbb{F}_2^n$ has $|A + A| \leq K|A|$, then A is contained in a subspace of cardinality at most $f(K)|A|$, where $f(K)$ is a constant depending only on K.

Theorem 3.12 (Freiman's theorem in groups with bounded exponent)**.** [Ruz99][Zha23, p. 246] Let A be a finite set in an abelian group with exponent $r < \infty$. If $|A + A| \leqslant K\,|A|$, then

$$|\langle A\rangle| \leqslant K^2 r^{K^4}\,|A|\,.$$

Proof. By Theorem 3.7,

$$|A + (2A - A)| = |3A - A| \leqslant K^4\,|A|\,.$$

By Theorem 3.9 (applied with $X = 2A - A$ and $B = A$), there exist $T \subseteq 2A - A$, $|T| \leqslant K^4$ such that

$$2A - A \subseteq T + A - A.$$

We will use induction to prove that for all integers $n \geqslant 1$,

$$(n + 1)\,A - A \subseteq nT + A - A. \tag{3.18}$$

The base case $n = 1$ holds. For the induction step, assume that for some $n \geqslant 1$, the following holds:

$$(n + 1)\,A - A \subseteq nT + A - A.$$

Adding A to both sides, we have

$$(n+2)\,A - A \subseteq nT + 2A - A.$$

Since $2A - A \subseteq T + A - A$,

$$(n+2)\,A - A \subseteq nT + T + A - A = (n+1)\,T + A - A.$$

Therefore, by induction, the statement holds for all integers $n \geqslant 1$.
For any $a \in \langle A \rangle$,

$$a = n_1 a_1 + n_2 a_2 + \cdots + n_{|A|} a_{|A|},$$

where $a_i \in A$ and $n_i \leqslant r$.
For any nA, $n \geqslant 1$, since $nA = A + A + \cdots + A$, for any $x \in nA$,

$$x = n_1 x_1 + n_2 x_2 + \cdots + n_{|A|} x_{|A|},$$

where $x_i \in A$ and $\sum_{i=1}^{|A|} n_i = n$.
This implies that for any $a \in \langle A \rangle$, there exists $n \geqslant 1$ such that $a \in nA$. Thus

$$\langle A \rangle \subseteq \bigcup_{n \geqslant 1} nA.$$

By adding $A - A$ to each set nA, we get

$$\langle A \rangle \subseteq \bigcup_{n \geqslant 1} (nA + A - A). \tag{3.19}$$

Since each element of nT is a sum of n elements from T, and $\langle T \rangle$ contains all integer linear combinations of elements of T, we have

$$nT \subseteq \langle T \rangle.$$

Hence, by the property of set addition,

$$nT + A - A \subseteq \langle T \rangle + A - A. \tag{3.20}$$

By combining (3.18), (3.19) and (3.20), we have

$$\langle A \rangle \subseteq \langle T \rangle + A - A. \tag{3.21}$$

Since for any $t \in \langle T \rangle$,

$$t = n_1 t_1 + n_2 t_2 + \cdots + n_{|T|} t_{|T|},$$

where $t_i \in T$ and $n_i \leqslant r - 1$, there are at most $r^{|T|}$ elements in $\langle T \rangle$. Thus

$$|\langle T \rangle| \leqslant r^{|T|} = r^{K^4}. \tag{3.22}$$

By Theorem 3.7

$$|A - A| \leqslant K^2 |A| . \tag{3.23}$$

By combining (3.21), (3.22) and (3.23), we have

$$|\langle A \rangle| \leqslant |\langle T \rangle + A - A| \leqslant |\langle T \rangle| \, |A - A| \leqslant K^2 r^{K^4} |A| .$$

□

Remark 3.13 (Remark of Theorem 3.11)**.** [Zha23, p. 246] Notice that Theorem 3.11 is a special case of Theorem 3.12 with *exponent* $r = 2$. Therefore the size of $\langle A \rangle$, which contains A, is at most $K^2 2^{K^4} |A|$, thus A is contained in a subspace of cardinality at most $f(K)|A|$, where $f(K) = K^2 2^{K^4}$ is a constant depending only on K.

CHAPTER 4

FREIMAN HOMOMORPHISMS AND MODELING LEMMA

In Chapter 3, we have proved a weaker version of Freiman's theorem. In fact, it is way more complicated to prove Theorem 2.10, which we state in Chapter 6. Therefore, a more powerful toolkit must be built. In this Chapter, we will prove a powerful tool: the Ruzsa modeling lemma. Interestingly, we will see how probability theory provides strong support when we study additive combinatorics. Furthermore, we will introduce an important concept in additive combinatorics, Freiman homomorphism, which is a strong bridge allows us to map a subset of $\mathbb{Z}$ into a finite field model, while preserving its additive structure. Also, we will provide the proof of Ruzsa modeling lemma, which relies on the Freiman homomorphism. In order to deepen the understanding of this concept, we will also discuss several examples related to Freiman homomorphisms and provide a proposition.

4.1 Freiman Homomorphisms

4.1.1 Freiman homomorphisms

Definition 4.1 (Freiman homomorphism)**.** [Zha23, p. 248]
Let A and B be subsets in two possibly different abelian groups. Let $s \geqslant 2$ be a positive integer. We say that $\phi : A \to B$ is a *Freiman s-homomorphism* (or *Freiman homomorphism of order s*), if

$$\phi(a_1) + \cdots + \phi(a_s) = \phi(a'_1) + \cdots + \phi(a'_s)$$

whenever $a_1, \ldots, a_s, a'_1, \ldots, a'_s \in A$ satisfy

$$a_1 + \cdots + a_s = a'_1 + \cdots + a'_s.$$

We say that ϕ is a *Freiman s-isomorphism* if ϕ is a bijection, and both ϕ and ϕ^{-1} are Freiman s-homomorphisms. We say that A and B are *Freiman s-isomorphic* if there exists a Freiman s-isomorphism between them.

Remark 4.2 (Why we need Freiman homomorphism)**.** As a preview of later chapters, many subsequent theorems will focus on $\mathbb{Z}/N\mathbb{Z}$ rather than $\mathbb{Z}$ itself. This is because directly studying $\mathbb{Z}$ would make many problems quite challenging, but the unique characteristics of

$\mathbb{Z}/N\mathbb{Z}$ offer a natural advantage in the derivation of many theorems. However, our target, Freiman's theorem, focuses on the set of integers. This is where Freiman homomorphisms play a crucial role. As mentioned in the introduction, Freiman homomorphisms allow us to map a subset of $\mathbb{Z}$ into a finite field model while preserving its additive structure. This implies that we can apply the tools from $\mathbb{Z}/N\mathbb{Z}$ to the set of integers. We will see this usefulness in the final proof in Chapter 6.

4.1.2 Examples over Freiman homomorphisms

In order to deepen the understanding of above concept, we provide some examples related to it. The following is to show that the Freiman s-homomorphisms or Freiman s-isomorphisms are preserved under composition.

Example 4.3. [Zha23, p. 248] Prove that if ϕ_1 and ϕ_2 are both Freiman s-homomorphisms, then their composition $\phi_1 \circ \phi_2$ is also a Freiman s-homomorphism and if ϕ_1 and ϕ_2 are both Freiman s-isomorphisms, then their composition $\phi_1 \circ \phi_2$ is a Freiman s-isomorphism.

Solution. Let A, B, C be subsets of possibly different abelian groups. Let $\phi_1 : A \to B$, $\phi_2 : B \to C$ be Freiman s-homomorphisms. Then for any $a_1, a_2, \ldots, a_s, a_1', a_2', \ldots, a_s' \in A$, satisfying

$$a_1 + a_2 + \cdots + a_s = a_1' + a_2' + \cdots + a_s'.$$

Since ϕ_1 is a Freiman s-homomorphism, we have $\phi_1(a_i), \phi_1(a_i') \in B$ for all $1 \leqslant i \leqslant s$, and

$$\phi_1(a_1) + \phi_1(a_2) + \cdots + \phi_1(a_s) = \phi_1(a_1') + \phi_1(a_2') + \cdots + \phi_1(a_s').$$

Since ϕ_2 is also Freiman s-homomorphisms

$$\begin{aligned}&\phi_2(\phi_1(a_1)) + \phi_2(\phi_1(a_2)) + \cdots + \phi_2(\phi_1(a_s))\\ =&\phi_2(\phi_1(a_1')) + \phi_2(\phi_1(a_2')) + \cdots + \phi_2(\phi_1(a_s')).\end{aligned}$$

This is exactly

$$\begin{aligned}&(\phi_2 \circ \phi_1)(a_1) + (\phi_2 \circ \phi_1)(a_2) + \cdots + (\phi_2 \circ \phi_1)(a_s)\\ =&(\phi_2 \circ \phi_1)(a_1') + (\phi_2 \circ \phi_1)(a_2') + \cdots + (\phi_2 \circ \phi_1)(a_s').\end{aligned}$$

Thus $\phi_2 \circ \phi_1$ is a Freiman s-homomorphism.
Assume that ϕ_1 and ϕ_2 above are both Freiman s-isomorphisms, then ϕ_1 and ϕ_2 are bijections. Hence $\phi_2 \circ \phi_1$ is a bijection. We have shown $\phi_2 \circ \phi_1$ is a Freiman s-homomorphism. To conclude that $\phi_2 \circ \phi_1$ is a Freiman s-isomorphism, it suffices to show that $(\phi_2 \circ \phi_1)^{-1}$ is a Freiman s-homomorphism.
Since ϕ_1 and ϕ_2 are Freiman s-isomorphisms, ϕ_1^{-1}, ϕ_2^{-1} are Freiman s-homomorphisms. We have shown that the composition of two Freiman s-homomorphisms is a Freiman s-homomorphism, hence we can conclude that $(\phi_2 \circ \phi_1)^{-1} = \phi_1^{-1} \circ \phi_2^{-1}$ is a Freiman s-homomorphism.

□

The Freiman s-homomorphisms and Freiman s-isomorphisms are also are also preserved under descending of order.

Example 4.4. [Zha23, p. 248] Prove that every Freiman $(s+1)$-homomorphism is automatically a Freiman s-homomorphism and every Freiman $(s+1)$-isomorphism is automatically a Freiman s-isomorphism.

Solution. Let A, B be subsets in two possibly different abelian groups. Let $\phi : A \to B$ be $(s+1)$-homomorphism. Set $a_{s+1}, a'_{s+1} \in A$ and $a_{s+1} = a'_{s+1}$. Hence $\phi(a_{s+1}) = \phi\left(a'_{s+1}\right)$. Then for any $a_1, a_2, \ldots, a_s, a'_1, a'_2, \ldots, a'_s \in A$, satisfying

$$a_1 + a_2 + \cdots + a_s = a'_1 + a'_2 + \cdots + a'_s.$$

We have

$$\begin{gathered} a_1 + a_2 + \cdots + a_s + a_{s+1} = a'_1 + a'_2 + \cdots + a'_s + a'_{s+1} \\ \phi(a_1) + \phi(a_2) + \cdots + \phi(a_s) + \phi(a_{s+1}) = \phi(a'_1) + \phi(a'_2) + \cdots + \phi(a'_s) + \phi\left(a'_{s+1}\right). \end{gathered}$$

Hence

$$\phi(a_1) + \phi(a_2) + \cdots + \phi(a_s) = \phi(a'_1) + \phi(a'_2) + \cdots + \phi(a'_s).$$

Therefore ϕ is a Freiman s-homomorphism.
Assume that ϕ above is a Freiman $(s+1)$-isomorphism. Hence ϕ is a bijection. We have shown that ϕ is a Freiman s-homomorphism. To conclude that ϕ is a Freiman s-isomorphism, it suffices to show that ϕ^{-1} is a Freiman s-homomorphism.

Since ϕ is a Freiman $(s+1)$-isomorphism, ϕ^{-1} is a Freiman $(s+1)$-homomorphisms. We have shown that every Freiman $(s+1)$-homomorphism is automatically a Freiman s-homomorphism, hence we can conclude that ϕ^{-1} is a Freiman s-homomorphisms. $\square$

The following example shows that a Freiman homomorphism is a weaker version of group homomorphism.

Example 4.5. [Zha23, p. 248] Prove that every group homomorphism is a Freiman homomorphism of every order.

Solution. Let $(G, *), (H, \cdot)$ be two abelian groups. Let $\phi : G \to H$ be a homomorphism. Then for any $g_1, g_2 \in G$, we have

$$\phi(g_1 * g_2) = \phi(g_1) \cdot \phi(g_2).$$

For any $s \geqslant 2$, $g_1, g_2, \ldots, g_s, g_1', g_2', \ldots, g_s' \in G$ satisfying

$$g_1 * g_2 * \cdots * g_s = g_1' * g_2' * \cdots * g_s'.$$

We have

$$\begin{gathered}\phi(g_1 * g_2 * \cdots * g_s) = \phi(g_1) \cdot \phi(g_2 * \cdots * g_s) \\ = \phi(g_1) \cdot \phi(g_2) \cdot \phi(g_3 * \cdots * g_s) = \cdots = \phi(g_1) \cdot \phi(g_2) \cdots \phi(g_s) \\ = \phi(g_1' * g_2' * \cdots * g_s') = \phi(g_1') \cdot \phi(g_2' * \cdots * g_s') \\ = \phi(g_1') \cdot \phi(g_2') \cdot \phi(g_3' * \cdots * g_s') = \cdots = \phi(g_1') \cdot \phi(g_2') \cdots \phi(g_s').\end{gathered}$$

This shows that ϕ is a Freiman s-homomorphism. $\square$

A Freiman homomorphism is often easy to construct for certain special sets. For instance, a *Sidon set* S, which is defined as a set that has no nontrivial solutions to $a+b=c+d$, for $a, b, c, d \in S$.

Example 4.6. [Zha23, p. 248] Let S be a *Sidon set*, prove that every map from S to an abelian group is a Freiman 2-homomorphism.

Solution. Let G be an abelian group and $\phi : S \to G$, for any $s_1, s_2, s_1', s_2' \in S$ satisfying

$$s_1 + s_2 = s_1' + s_2'.$$

Without loss of generality, we may assume that

$$s_1 = s_2, s_1' = s_2'.$$

Then

$$\begin{aligned}\phi(s_1) &= \phi(s_1')\\ \phi(s_2) &= \phi(s_2').\end{aligned}$$

Thus

$$\phi(s_1) + \phi(s_2) = \phi(s_1') + \phi(s_2').$$

□

Although some mappings do preserve all the additive relations on the forward direction, it is not always true for their inverses.

Example 4.7. [Zha23, p. 248] The natural embedding $\phi : \{0,1\}^n \to (\mathbb{Z}/2\mathbb{Z})^n$ is the restriction of a group homomorphism from $\mathbb{Z}^n$, show that it is a Freiman homomorphism of every order and it is also a bijection. Show that the inverse of ϕ does not preserve all additive relations (e.g., $1+1=0+0 \pmod 2$) hence ϕ is not a Freiman 2-isomorphism).

Solution. Let $A := \{0,1\}^n$ be a subset of abelian group $(\mathbb{Z}^n, +)$ and $B := (\mathbb{Z}/2\mathbb{Z})^n$ be a subset of abelian group. Let $\phi : A \to B$ be the natural embedding. For any $s \geqslant 2$, $a_1, a_2, \ldots, a_s, a_1', a_2', \ldots, a_s' \in A$, satisfying

$$a_1 + a_2 + \cdots + a_s = a_1' + a_2' + \cdots + a_s'.$$

We have

$$\begin{aligned}&\phi(a_1) + \phi(a_2) + \cdots + \phi(a_s)\\ &= ([\pi_1(a_1 + a_2 + \cdots + a_s)], [\pi_2(a_1 + a_2 + \cdots + a_s)], \ldots, [\pi_n(a_1 + a_2 + \cdots + a_s)])\\ &= ([\pi_1(a_1' + a_2' + \cdots + a_s')], [\pi_2(a_1' + a_2' + \cdots + a_s')], \ldots, [\pi_n(a_1' + a_2' + \cdots + a_s')])\\ &= \phi(a_1') + \phi(a_2') + \cdots + \phi(a_s'),\end{aligned}$$

where π_i is the projection function and $[z]$ denotes the congruence class of z in $\mathbb{Z}/2\mathbb{Z}$. Therefore, ϕ is a Freiman s-homomorphism.

For any $a_1, a_2 \in A$, if $\phi(a_1) = \phi(a_2)$, then

$$([\pi_1(a_1)], [\pi_2(a_1)], \dots, [\pi_n(a_1)]) = ([\pi_1(a_2)], [\pi_2(a_2)], \dots, [\pi_n(a_2)])$$
$$\pi_i(a_1) = \pi_i(a_2), \text{for any } i \in \{1, 2, \dots, n\}$$
$$a_1 = a_2.$$

Thus ϕ is injective.
For any $b = ([b_1], [b_2], \dots, [b_n]) \in B$, there exist $(b_1, b_2, \dots, b_n) \in A$ such that

$$(b_1, b_2, \dots, b_n) = \phi^{-1}(b).$$

Thus ϕ is surjective and we can conclude that ϕ is a bijection.
Take $b_1 = ([1], [1], \dots, [1]), b_2 = ([0], [0], \dots, [0]) \in B$, then

$$b_1 + b_1 = b_2 + b_2,$$

and

$$\begin{aligned}
&\phi^{-1}(b_1) + \phi^{-1}(b_1) \\
&= (1, 1, \dots, 1) + (1, 1, \dots, 1) = (2, 2, \dots, 2) \\
&\neq \phi^{-1}(b_2) + \phi^{-1}(b_2) \\
&= (0, 0, \dots, 0) + (0, 0, \dots, 0) = (0, 0, \dots, 0).
\end{aligned}$$

Therefore, ϕ^{-1} is not a Freiman s-homomorphism, which implies ϕ is not a Freiman 2-isomorphism. $\square$

The next example further illustrates the slight distinction between Freiman homomorphisms and Freiman isomorphisms. It also shows that this distinction can disappear when we add some restrictions.

Example 4.8. [Zha23, p. 248] Show that for $N \geqslant 2$, the natural embedding $\phi : [N] \to \mathbb{Z}/N\mathbb{Z}$ is a Freiman homomorphism of every order, but it is not a Freiman 2-isomorphism. Moreover, show that when the domain is restricted to all integers less than N/s, the map ϕ becomes a Freiman s-isomorphism onto its image.

Solution. Let $A := [N]$ be a subset of abelian group $(\mathbb{Z}, +)$ and $B := \mathbb{Z}/N\mathbb{Z}$ be a subset of abelian group. Let $\phi : A \to B$ be the natural embedding.

For any $s \geqslant 2$, $a_1, a_2, \ldots, a_s, a_1', a_2', \ldots, a_s' \in A$, satisfying

$$a_1 + a_2 + \cdots + a_s = a_1' + a_2' + \cdots + a_s'.$$

We have

$$\begin{aligned}
&\phi(a_1) + \phi(a_2) + \cdots + \phi(a_s) \\
&= [a_1 + a_2 + \cdots + a_s] \\
&= [a_1' + a_2' + \cdots + a_s'] \\
&= \phi(a_1') + \phi(a_2') + \cdots + \phi(a_s').
\end{aligned}$$

where $[z]$ denotes the congruence class of z in $\mathbb{Z}/N\mathbb{Z}$.
Therefore, ϕ is a Freiman s-homomorphism.
Since $N \geqslant 2$, if N is even, take $b_1 = \left[\frac{N}{2}\right], b_2 = [0] \in B$, then

$$b_1 + b_1 = b_2 + b_2,$$

and

$$\begin{aligned}
&\phi^{-1}(b_1) + \phi^{-1}(b_1) \\
&= \frac{N}{2} + \frac{N}{2} = N \\
&\neq \phi^{-1}(b_2) + \phi^{-1}(b_2) \\
&= 0 + 0 = 0.
\end{aligned}$$

If N is odd, take $b_1 = \left[\frac{N-1}{2}\right], b_2 = \left[\frac{N+1}{2}\right], b_3 = [0] \in B$, then

$$b_1 + b_2 = b_3 + b_3,$$

and

$$\begin{aligned}
&\phi^{-1}(b_1) + \phi^{-1}(b_2) \\
&= \frac{N-1}{2} + \frac{N+1}{2} = N \\
&\neq \phi^{-1}(b_3) + \phi^{-1}(b_3) \\
&= 0 + 0 = 0.
\end{aligned}$$

Therefore, ϕ^{-1} is not a Freiman 2-homomorphism, which implies ϕ is not a Freiman 2-isomorphism.

Let A' be the restricted domain to all integers less than N/s, namely, $A' = \{0, 1, \ldots, \lceil N/s \rceil - 1\}$. Let B' be the image of A' under the map ϕ, namely, $B' = \{[0], [1], \ldots, [\lceil N/s \rceil - 1]\}$ For any $a_1, a_2 \in A'$, if $\phi(a_1) = \phi(a_2)$, then

$$[a_1] = [a_2]$$
$$a_1 = a_2.$$

Thus $\phi|_{A'}$ is injective.
For any $[b] \in B'$, we have $b \in A'$ such that

$$b = \phi|_{A'}{}^{-1}([b]).$$

Thus $\phi|_{A'}$ is surjective and we can conclude that $\phi|_{A'}$ is a bijection.
Since A' and B' are the subsets of A and B, respectively, the 'Freiman s-homomorphism' property holds for $\phi|_{A'}$. To conclude that $\phi|_{A'}$ is a Freiman s-isomorphism, it suffices to show that $\phi|_{A'}{}^{-1}$ is a Freiman s-homomorphism.
For any $b_i, b\prime_i \in \{0, 1, \ldots, \lceil N/s \rceil - 1\}$ $(i = 1, \ldots, s)$, let $[b_1], [b_2], \ldots, [b_s], [b'_1], [b'_2], \ldots, [b'_s] \in B'$. Suppose that:

$$[b_1] + [b_2] + \cdots + [b_s] = [b'_1] + [b'_2] + \cdots + [b'_s].$$

We have

$$b_1 + b_2 + \cdots + b_s - (b'_1 + b'_2 + \cdots + b'_s) = nN \text{ , for some } n \in \mathbb{Z}.$$

Since $\operatorname{diam} A' = \sup_{a_i, a_j \in A'} |a_i - a_j| = \lceil N/s \rceil - 1$, and for the corresponding preimages $b_1, b_2, \ldots, b_s, b'_1, b'_2, \ldots, b'_s \in A'$,

$$\begin{aligned}
&|(b_1 + b_2 + \cdots + b_s) - (b'_1 + b'_2 + \cdots + b'_s)| \\
&= |b_1 - b'_1 + b_2 - b'_2 + \cdots + b_s - b'_s| \\
&\leqslant \sum_{i=1}^{s} |b_i - b'_i| \\
&\leqslant s \cdot (\lceil N/s \rceil - 1) \\
&< s \cdot (N/s + 1 - 1) = N,
\end{aligned}$$

hence

$$n = 0.$$

Therefore, we must have

$$\sum_{i=1}^{s} \phi^{-1}([b_i]) = \sum_{i=1}^{s} b_i = \sum_{i=1}^{s} \phi^{-1}([b_i']) = \sum_{i=1}^{s} b_i',$$

hence, $\phi|_{A'}{}^{-1}$ is a Freiman s-homomorphism. $\square$

Remark 4.9 (Diameter)**.** [Zha23, p. 248] Example 4.8 has the following easy generalization(Proposition 4.10), which we shall use later. The diameter of a set A is defined to be

$$\operatorname{diam} A = \sup_{a,b \in A} |a - b|.$$

Proposition 4.10 (Small diameter sets)**.** [Zha23, p. 248]
If $A \subseteq \mathbb{Z}$ has diameter $\operatorname{diam} A < N/s$, then A is Freiman s-isomorphic to its image mod N.

Proof. Let $A \subseteq \mathbb{Z}$ with $\operatorname{diam} A = \sup_{a_i, a_j \in A} |a_i - a_j| < N/s$. Let $\phi : A \to \mathbb{Z}/N\mathbb{Z}$ be the natural embedding given by

$$\phi(a) = [a],$$

with image $\phi(A) \subseteq \mathbb{Z}/N\mathbb{Z}$.
For any $a_i, a_j \in A$, if $\phi(a_i) = \phi(a_j)$, then

$$[a_i] = [a_j]$$
$$a_i - a_j = nN, \text{ for some n } \in \mathbb{Z}.$$

Since $\operatorname{diam} A < N/s$, $|a_i - a_j| < N/s < N$, thus we must have

$$n = 0$$
$$a_i = a_j.$$

Thus ϕ is injective, hence ϕ is a bijection onto its image.
For any $a_i, a_i' \in A$ $(i = 1, \ldots, s)$, let $[a_i], [a_i'] \in \phi(A)$. Suppose that:

$$a_1 + a_2 + \cdots + a_s = a_1' + a_2' + \cdots + a_s'.$$

We have

$$\begin{aligned}\sum_{i=1}^{s} \phi(a_i) &= \sum_{i=1}^{s} [a_i] = \left[\sum_{i=1}^{s} a_i\right] \\ &= \sum_{i=1}^{s} \phi(a_i') = \sum_{i=1}^{s} [a_i'] = \left[\sum_{i=1}^{s} a_i'\right].\end{aligned}$$

Thus, ϕ is a Freiman s-homomorphism.
For any $[a_1], [a_2], \ldots, [a_s], [a_1'], [a_2'], \ldots, [a_s'] \in \phi(A)$, satisfying

$$[a_1] + [a_2] + \cdots + [a_s] = [a_1'] + [a_2'] + \cdots + [a_s'].$$

We have

$$a_1 + a_2 + \cdots + a_s - (a_1' + a_2' + \cdots + a_s') = nN \text{ , for some n } \in \mathbb{Z}.$$

Since $\operatorname{diam} A = \sup\limits_{a_i, a_j \in A} |a_i - a_j| < N/s$, and for the corresponding preimages $a_1, a_2, \ldots, a_s, a_1', a_2', \ldots, a_s' \in A$,

$$\begin{aligned}&|(a_1 + a_2 + \cdots + a_s) - (a_1' + a_2' + \cdots + a_s')| \\ &= |a_1 - a_1' + a_2 - a_2' + \cdots + a_s - a_s'| \\ &\leqslant \sum_{i=1}^{s} |a_i - a_i'| \\ &< s \cdot (N/s) = N.\end{aligned}$$

hence

$$n = 0.$$

Therefore, we must have

$$\sum_{i=1}^{s} \phi^{-1}([a_i]) = \sum_{i=1}^{s} a_i = \sum_{i=1}^{s} a_i' = \sum_{i=1}^{s} \phi^{-1}([a_i']),$$

hence, ϕ^{-1} is a Freiman s-homomorphism.
Therefore we conclude that ϕ is a Freiman s-isomorphism, A is Freiman s-isomorphic to its image mod N. $\square$

4.2 Ruzsa Modeling Lemma

The Ruzsa modeling lemma is a powerful tool in additive combinatorics as it allows us to find a 'not too small' subset A' of $A \subseteq \mathbb{Z}$, which can be mapped to a subset of $\mathbb{Z}/N\mathbb{Z}$ while preserving all its additive relations. However, its proof is a bit complicated, so as a warm-up, let us first prove an easier result in the finite field model. Although it is an easier version, the proof of Modeling lemma over finite fields also requires some tools from probability theory just as the proof over integer sets. Let us first examine what exactly we have 'borrowed' from probability theory.

4.2.1 Tools from probability theory

Lemma 4.11 (Boole's Inequality)**.** For any countable sequence of events $A_1, A_2, \ldots$ in a probability space, the probability that at least one of the events occurs is bounded by the sum of the probabilities of the individual events:

$$\mathbb{P}\left(\bigcup_i A_i\right) \leq \sum_i \mathbb{P}(A_i).$$

Lemma 4.12 (Pigeonhole Principle)**.** Let n, m be positive integers with $n > m$. If n items are put into m containers, then at least one container must contain more than one item. In terms of mappings, if $f : X \to Y$ is a function between finite sets and $|X| > |Y|$, then there exist distinct elements $x, x' \in X$ such that $f(x) = f(x')$.

4.2.2 Modeling lemma over finite field

Now with the help of probability theory, here is the warm-up.

Proposition 4.13 (Modeling lemma in finite field model)**.** [Ruz99][Zha23, p. 249]
Let $A \subseteq \mathbb{F}_2^n$. Suppose $|sA - sA| \leqslant 2^m$ for some positive integer m. Then A is Freiman s-isomorphic to some subset of $\mathbb{F}_2^m$.

Proof. Let $B \in \mathbb{F}_2^{m\times n}$ be a matrix chosen uniformly at random. We will construct a linear map $\phi : A \to \mathbb{F}_2^m$ defined by $\phi(a) = Ba$ and show that it is a Freiman s-isomorphism.

For any $d = \begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_n \end{pmatrix} \in (sA - sA) \setminus \{0\}$, let $Bd = \begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_m \end{pmatrix}$. Let $B_i = \begin{pmatrix} b_{i_1} \\ b_{i_2} \\ \vdots \\ b_{i_n} \end{pmatrix}$ denote the i-th row of the matrix B. For any index i,

$$z_i = B_i \cdot d.$$

Since there exists at least one i such that $d_i \neq 0$, suppose that $d_k = 1 \neq 0$. Then

$$z_i = B_i \cdot d = \sum_{j=1}^{n} b_{i_j} d_j = b_{i_k} d_k + \sum_{j \neq k} b_{i_j} d_j = b_{i_k} + \sum_{j \neq k} b_{i_j} d_j.$$

Since $d \in (sA - sA) \setminus \{0\}$ and $B \in \mathbb{F}_2^{m \times n}$, $d_i \in \{0, 1\}$ and $b_i \in \{0, 1\}$. Thus the possible values of $S = \sum_{j \neq k} b_{i_j} d_j \pmod 2$ and b_{i_k} are 1 or 0.
Then if $b_{i_k} = 0$,

$$b_{i_k} + \sum_{j \neq k} b_{i_j} d_j = 0 + S,$$

if $b_{i_k} = 1$,

$$b_{i_k} + \sum_{j \neq k} b_{i_j} d_j = 1 + S.$$

Notice that the value of S is independent of b_{i_k}, this implies that the value of $z_i = b_{i_k} + \sum_{j \neq k} b_{i_j} d_j$ only depends on b_{i_k}.
Since B is chosen uniformly at random, b_{i_k} takes the values 0 or 1 each with probability $\frac{1}{2}$, thus the probability $P_i(z_i = b_{i_k} + \sum_{j \neq k} b_{i_j} d_j = 0) = P_i(z_i = b_{i_k} + \sum_{j \neq k} b_{i_j} d_j = 1) = \frac{1}{2}$.
Since B_i is independent of $B_j, j \neq i$, the value of z_i is independent of $z_j, j \neq i$, thus the probability that $B_i d = 0$ is

$$P_1 = \prod_{i=1}^{m} P_i(z_i = 0) = \frac{1}{2^m}.$$

Since $|sA - sA| \leqslant 2^m$, $|(sA - sA) \setminus \{0\}| < 2^m$. Lemma 4.11 gives us the probability P_2 that there exists $d \in sA - sA \setminus \{0\}$ such that $B_i d = 0$ is

$$P_2 \leqslant \sum_{d_i \in sA - sA} P\left(B_i d_i = 0\right) < 2^m \cdot \frac{1}{2^m} = 1.$$

Therefore, the probability P_3 that for all nonzero $d \in sA - sA$, $B_i d \neq 0$ is

$$P_3 = 1 - P_2 > 0.$$

Thus, there exists $B \in \mathbb{F}_2^{m \times n}$ such that for all nonzero $d \in sA - sA$, $Bd \neq 0$, fix such a B and define ϕ as

$$\phi(a) = Ba$$

For any $x, y \in A$, $d = x - y = sx - (y + (s-1)x) \in sA - sA$, if $\phi(x) = \phi(y)$, then

$$\begin{aligned} Bx &= By \\ B(x-y) &= 0. \end{aligned}$$

By definition of ϕ, $x = y$, this implies that ϕ is injective, hence ϕ is a bijection onto its image. For any $a_1, a_2, \ldots, a_s, a_1', a_2', \ldots, a_s' \in A$ satisfying

$$a_1 + a_2 + \cdots + a_s = a_1' + a_2' + \cdots + a_s'.$$

By linearity, we have

$$\begin{aligned} &\phi(a_1) + \phi(a_2) + \cdots + \phi(a_s) \\ &= B \cdot (a_1 + a_2 + \cdots + a_s) \\ &= B \cdot (a_1' + a_2' + \cdots + a_s') \\ &= \phi(a_1') + \phi(a_2') + \cdots + \phi(a_s'). \end{aligned}$$

Thus ϕ is a Freiman s-homomorphism.
For any $\phi(a_1), \phi(a_2), \ldots, \phi(a_s), \phi(a_1'), \phi(a_2'), \ldots, \phi(a_s')$ in $\phi(A)$ satisfying

$$\sum_{i=1}^{s} \phi(a_i) = \sum_{i=1}^{s} \phi(a_i').$$

We have

$$\begin{aligned} &B \cdot (a_1 + a_2 + \cdots + a_s) \\ =&B \cdot (a_1' + a_2' + \cdots + a_s'). \end{aligned}$$

By linearity,

$$B \cdot ((a_1 + a_2 + \cdots + a_s) - (a_1' + a_2' + \cdots + a_s')) = 0.$$

For the corresponding preimages $a_1, a_2, \ldots, a_s, a_1', a_2', \ldots, a_s' \in A$, $(a_1 + a_2 + \cdots + a_s) - (a_1' + a_2' + \cdots + a_s') \in sA - sA$, by definition of ϕ,

$$\sum_{i=1}^{s} a_i - \sum_{i=1}^{s} a_i' = 0$$
$$\sum_{i=1}^{s} a_i = \sum_{i=1}^{s} a_i'.$$

Thus ϕ^{-1} is a Freiman s-homomorphism. $\square$

4.2.3 Ruzsa modeling lemma

The idea of the proof of Ruzsa modeling lemma over integer sets is quite similar to the finite field case. However, since $\mathbb{Z}$ has infinite *exponent* while a finite field has finite *exponent*, we have to shift our attention from A to $A' \subseteq A$ in order to restrict the domain. After this restriction, all the additive relations will be preserved as desired.

Theorem 4.14 (Ruzsa modeling lemma)**.** [Ruz94][Zha23, p. 250]
Let $A \subseteq \mathbb{Z}$. Let $s \geqslant 2$ and N be positive integers. Suppose $|sA - sA| \leqslant N$. Then there exists $A' \subseteq A$ with $|A'| \geqslant |A|/s$ such that A' is Freiman s-isomorphic to a subset of $\mathbb{Z}/N\mathbb{Z}$.

Proof. Choose a prime $q > \max(sA - sA)$. Thus for any non-zero $x \in sA - sA$, $x \not\equiv 0 \pmod{q}$. For each $\lambda \in \{1, \ldots, q-1\}$, define the map $\phi_\lambda : \mathbb{Z} \to \{0, 1, \ldots, q-1\}$ by

$$\phi_\lambda(x) = \lambda x \pmod{q}.$$

For any $\lambda_1, \lambda_2 \in \{1, \ldots, q-1\}, \lambda_1 \neq \lambda_2$, any nonzero $x \in sA - sA$, If

$$\lambda_1 x \equiv \lambda_2 x \pmod{q},$$

then

$$\lambda_1 x - \lambda_2 x \equiv 0$$
$$(\lambda_1 - \lambda_2)\, x \equiv 0 \pmod{q}.$$

Since $x \not\equiv 0 \pmod{q}$, $(\lambda_1 - \lambda_2) \equiv 0 \pmod{q}$, which contradicts the fact $(\lambda_1 - \lambda_2) \in \{2-q, \ldots, -1\} \cup \{1, \ldots, q-2\}$.

Thus, if λ is chosen uniformly at random from $\{1, \ldots, q-1\}$, then for any fixed non-zero $x \in sA - sA$, the value $\phi_\lambda(x)$ is uniformly distributed over $\{1, \ldots, q-1\}$. Therefore, the probability that N divides $\phi_\lambda(x)$ is

$$P_\lambda\left(N \mid \phi_\lambda(x)\right) = \frac{\lfloor (q-1)/N \rfloor}{q-1} \leq \frac{1}{N}.$$

Since $|sA - sA| \leqslant N$, $|(sA - sA) \setminus \{0\}| < N$. Lemma 4.11 gives us the probability $\mathcal{P}_\lambda$ that there exist $x \in sA - sA \setminus \{0\}$ such that $N \mid \phi_\lambda(x)$ is

$$\mathcal{P}_\lambda\left(\exists x \in sA - sA \setminus \{0\} \mid N \mid \phi_\lambda(x)\right) \leq \sum_{x \in sA - sA \setminus \{0\}} P_\lambda\left(N \mid \phi_\lambda(x)\right) < N \cdot \frac{1}{N} = 1.$$

Thus, there exists λ such that $N \nmid \phi_\lambda(x)$ for all nonzero $x \in sA - sA$. We fix such a λ and write $\phi = \phi_\lambda$.

Let us partition the codomain of ϕ, $\{0, 1, \ldots, q-1\}$, into s disjoint intervals $I_1, I_2, \ldots, I_s$, each of length at most $\lceil q/s \rceil$ thus each of diameter at most q/s. Since ϕ assigns each element of A into exactly one of these s intervals, Lemma 4.12 implies there exists at least one interval that at least $|A|/s$ elements of A are assigned by ϕ to this interval. Fix such an interval, denote it by I, and we define:

$$A' = \{a \in A : \phi(a) \in I\},$$

with

$$|A'| \geqslant |A| / s.$$

Define $\varphi : \{0, 1, \ldots, q-1\} \to \mathbb{Z}/N\mathbb{Z}$ by

$$\varphi(a) = a \pmod{N},$$

and let $\psi : \mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$ be

$$\psi = \varphi \circ \phi.$$

For $a_1, a_2 \in A' \subseteq \mathbb{Z}$, if

$$\psi(a_1) = \psi(a_2),$$

then

$$\phi(a_1) \equiv \phi(a_2) \pmod{N}.$$

Since

$$\phi(a_1 - a_2) = \lambda(a_1 - a_2),$$
$$\phi(a_1 - a_2) \equiv \lambda(a_1 - a_2) \pmod q.$$

Thus

$$\phi(a_1 - a_2) \equiv \lambda(a_1 - a_2) \equiv \lambda a_1 \pmod q - \lambda a_2 \pmod q \equiv \phi(a_1) - \phi(a_2) \pmod q.$$

Since $\phi(a_1) - \phi(a_2) < \operatorname{diam} I \leqslant q/s$, and $\phi(a_1 - a_2) \in \{0, 1, \ldots, q-1\}$,

$$\phi(a_1) - \phi(a_2) = \phi(a_1 - a_2),$$
$$\phi(a_1 - a_2) \equiv \phi(a_1) - \phi(a_2) \equiv 0 \pmod N.$$

Since $a_1 - a_2 = \underbrace{a_1 + a_2 + \cdots + a_2}_{s} - \underbrace{a_2 + \cdots + a_2}_{s} \in sA - sA$, so by the definition of ϕ,

$$a_1 - a_2 = 0,$$
$$a_1 = a_2.$$

This shows that ψ is injective, thus ψ is a bijection onto its image of A'.
For any $a_1, a_2, \ldots, a_s, a_1', a_2', \ldots, a_s' \in A'$ satisfying

$$\sum_{i=1}^{s} a_i = \sum_{i=1}^{s} a_i{}'.$$

We have

$$\sum_{i=1}^{s} \lambda a_i = \sum_{i=1}^{s} \lambda a_i{}'$$
$$\sum_{i=1}^{s} \lambda a_i \equiv \sum_{i=1}^{s} \lambda a_i{}' \pmod q.$$

By the definition of ϕ,

$$\phi(a_i) \equiv \lambda a_i \pmod q,$$

hence

$$\sum_{i=1}^{s} \phi(a_i) \equiv \sum_{i=1}^{s} \lambda a_i \pmod q$$

$$\sum_{i=1}^{s} \phi(a_i) \equiv \sum_{i=1}^{s} \lambda a_i \equiv \sum_{i=1}^{s} \lambda a_i{}' \equiv \sum_{i=1}^{s} \phi(a_i{}') \pmod q$$

$$\sum_{i=1}^{s} \phi(a_i) - \sum_{i=1}^{s} \phi(a_i{}') \equiv 0 \pmod q.$$

Notice that

$$\sum_{i=1}^{s} \phi(a_i) - \sum_{i=1}^{s} \phi(a_i{}') < s \cdot \operatorname{diam} I \leqslant s \cdot q/s = q.$$

Therefore

$$\sum_{i=1}^{s} \phi(a_i) = \sum_{i=1}^{s} \phi(a_i{}').$$

This shows that ϕ is a Freiman s-homomorphism on A'.

For any $b_1, b_2, \ldots, b_s, b_1', b_2', \ldots, b_s' \in I$ satisfying

$$\sum_{i=1}^{s} b_i = \sum_{i=1}^{s} b_i{}'.$$

We have

$$\begin{aligned} &\sum_{i=1}^{s} \varphi(b_i) - \sum_{i=1}^{s} \varphi(b_i{}') \\ &= \varphi\left(\sum_{i=1}^{s} b_i - \sum_{i=1}^{s} b_i{}'\right) \\ &= \varphi(0) \\ &= 0. \end{aligned}$$

This implies that $\sum_{i=1}^{s} \varphi(b_i) = \sum_{i=1}^{s} \varphi(b_i{}')$ and thus φ is a Freiman s-homomorphism on I.

By Exercise 4.3, we conclude that $\psi = \varphi \circ \phi$ is a Freiman s-homomorphism on A'.

For any $a_1, a_2, \ldots, a_s, a_1', a_2', \ldots, a_s' \in A'$ satisfying

$$\sum_{i=1}^{s} \psi(a_i) = \sum_{i=1}^{s} \psi(a_i').$$

We have

$$y := \sum_{i=1}^{s} \phi\left(a_i\right) - \sum_{i=1}^{s} \phi\left({a_i}'\right) \equiv 0 \pmod{N}.$$

By swapping $(a_1, a_2, \ldots, a_s)$ with $(a_1', a_2', \ldots, a_s')$ if needed, we may assume that $y \geqslant 0$. Notice that

$$y = \sum_{i=1}^{s} \phi\left(a_i\right) - \sum_{i=1}^{s} \phi\left({a_i}'\right) < s \cdot \operatorname{diam} I \leqslant s \cdot q/s = q.$$

Thus

$$0 \leqslant y < q.$$

Let $x = \sum_{i=1}^{s} a_i - \sum_{i=1}^{s} {a_i}' \in sA - sA$, then

$$\phi\left(x\right) \equiv \phi\left(\sum_{i=1}^{s} a_i - \sum_{i=1}^{s} {a_i}'\right) \equiv \sum_{i=1}^{s} \phi\left(a_i\right) - \sum_{i=1}^{s} \phi\left({a_i}'\right) \equiv y \pmod{q}.$$

Since $\phi\left(x\right), y \in [0, q) \cap \mathbb{Z}$,

$$\phi\left(x\right) = y.$$

Therefore

$$\phi\left(x\right) \equiv 0 \pmod{N}.$$

By the definition of ϕ,

$$x = 0,$$

which implies that $\sum_{i=1}^{s} a_i = \sum_{i=1}^{s} {a_i}'$.
Therefore, ψ^{-1} is a Freiman s-homomorphism on $\psi\left(A'\right)$.

The above has shown that ψ is a bijection and both ψ, ψ^{-1} are Freiman s-homomorphisms, therefore we can conclude that ψ is a Freiman s-isomorphism from A' to its image.

$\square$

CHAPTER 5

CROSS-DISCIPLINARY INTERACTIONS: HARMONIC ANALYSIS AND GEOMETRY OF NUMBERS IN ADDITIVE COMBINATORICS

In Chapter 4 we have shown how probability theory could help to build tools for additive combinatorics. In this Chapter, we will continue borrowing tools from other mathematical fields to build our toolkits. Firstly we will shift our attention to the harmonic analysis and see how it could help us to prove the Bogolyubov's lemma—the theorem claiming that sumsets necessarily contain subspaces or approximate subspaces. After that, we will introduce several concepts in the geometry of numbers, as well as an important result in this area, Minkowski's theorem, which is also a powerful tool in additive combinatorics.

5.1 Harmonic Analysis in Additive Combinatorics

Throughout the previous chapters, we have primarily relied on combinatorial tools. While these tools are effective for studying the size of a set, they struggle to research its underlying structure. In the arguments that follow, we shall study our target sets through the convolution of indicator functions. However, since this function is discrete, direct analysis rather challenging.

This is where harmonic analysis, a mathematical field dedicated to studying periodicity, comes into play. Specifically, we will use the Fourier transform to express our discrete function as a sum of periodic functions. By doing so, we bypass the discreteness of the original function; instead, we are able to study its behavior through a sum of periodic waves. But before that, let us first introduce the concepts and tools we will borrow from harmonic analysis.

5.1.1 Tools from harmonic analysis

Definition 5.1 (Convolution in $\mathbb{F}_p^n$)**.** [Zha23, p. 206] Given $f, g : \mathbb{F}_p^n \to \mathbb{C}$, define $f * g : \mathbb{F}_p^n \to \mathbb{C}$ by

$$(f * g)(x) := \mathbb{E}_{y\in\mathbb{F}_p^n} f(y)g(x-y).$$

In other words, $(f * g)(x)$ is the average of $f(y)g(z)$ over all pairs (y, z) with $y + z = x$.

Definition 5.2 (Convolution in $\mathbb{Z}/N\mathbb{Z}$)**.** Given $f, g : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$, define $f * g : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$ by

$$(f * g)(x) := \mathbb{E}_{y \in \mathbb{Z}/N\mathbb{Z}} f(y)g(x - y).$$

In other words, $(f * g)(x)$ is the average of $f(y)g(z)$ over all pairs (y, z) with $y + z = x \pmod N$.

Theorem 5.3 (Convolution identity in $\mathbb{F}_p^n$)**.** [Zha23, p. 206] For any $f, g : \mathbb{F}_p^n \to \mathbb{C}$ and any $r \in \mathbb{F}_p^n$,

$$\widehat{f * g}(r) = \widehat{f}(r)\widehat{g}(r).$$

Theorem 5.4 (Convolution identity in $\mathbb{Z}/N\mathbb{Z}$)**.** For any $f, g \colon \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$ and any $r \in \mathbb{Z}/N\mathbb{Z}$,

$$\widehat{f * g}(r) = \widehat{f}(r)\widehat{g}(r).$$

Theorem 5.5 (Fourier inversion formula in $\mathbb{F}_p^n$)**.** [Zha23, p. 204] Let $f \colon \mathbb{F}_p^n \to \mathbb{C}$. For every $x \in \mathbb{F}_p^n$,

$$f(x) = \sum_{r \in \mathbb{F}_p^n} \widehat{f}(r)\omega^{r \cdot x}.$$

Theorem 5.6 (Fourier inversion formula in $\mathbb{Z}/N\mathbb{Z}$)**.** Let $f \colon \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$ and let $\omega = \exp(2\pi i/N)$. For every $x \in \mathbb{Z}/N\mathbb{Z}$,

$$f(x) = \sum_{r \in \mathbb{Z}/N\mathbb{Z}} \widehat{f}(r)\omega^{rx}.$$

Theorem 5.7 (Parseval / Plancherel in $\mathbb{F}_p^n$)**.** [Zha23, p. 204] Given $f, g \colon \mathbb{F}_p^n \to \mathbb{C}$, we have

$$\mathbb{E}_{x \in \mathbb{F}_p^n} f(x)\overline{g(x)} = \sum_{r \in \mathbb{F}_p^n} \widehat{f}(r)\overline{\widehat{g}(r)}.$$

In particular, as a special case ($f = g$),

$$\mathbb{E}_{x \in \mathbb{F}_p^n} |f(x)|^2 = \sum_{r \in \mathbb{F}_p^n} |\widehat{f}(r)|^2.$$

Theorem 5.8 (Parseval / Plancherel in $\mathbb{Z}/N\mathbb{Z}$)**.** Given $f, g \colon \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$, we have

$$\mathbb{E}_{x \in \mathbb{Z}/N\mathbb{Z}} f(x)\overline{g(x)} = \sum_{r \in \mathbb{Z}/N\mathbb{Z}} \widehat{f}(r)\overline{\widehat{g}(r)}.$$

In particular, as a special case ($f = g$),

$$\mathbb{E}_{x\in\mathbb{Z}/N\mathbb{Z}}|f(x)|^2 = \sum_{r\in\mathbb{Z}/N\mathbb{Z}} |\widehat{f}(r)|^2.$$

Remark 5.9 (Proofs and Generalization to $\mathbb{Z}/N\mathbb{Z}$)**.** We omit the detailed proofs for the Fourier analytic theorems presented above. More information can be found in *Graph Theory and Additive Combinatorics* [Zha23, Chapter 6]. Furthermore, although Zhao introduces these Fourier analytic tools specifically for the finite field model $\mathbb{F}_p^n$ in the book, we will directly generalize and apply them to the cyclic group $\mathbb{Z}/N\mathbb{Z}$ in the subsequent proof of Theorem 5.13. This generalization is naturally valid as $\mathbb{F}_p^n$ and $\mathbb{Z}/N\mathbb{Z}$ share the underlying structure of finite groups.

5.1.2 Bogolyubov's lemma over finite field

Now let us see what we can do by using our newly acquired tools. As mentioned at the beginning of this Chapter, Bogolyubov's lemma allows us to find some subspaces in sumsets. However, for most integers N (namely, when N is not prime), $\mathbb{Z}/N\mathbb{Z}$ is not a field, which implies that no vector space can be based on it. Meaning the concept of "subspaces" does not exist in $\mathbb{Z}/N\mathbb{Z}$. In that case, we will construct an approximate subspace, which we will present later (Bohr sets). But before that, let us first warm up with the finite field model just as we did in Section 4.2.

Theorem 5.10 (Bogolyubov's lemma in $\mathbb{F}_p^n$)**.** [Bog39][Zha23, p. 252]
If $A \subseteq \mathbb{F}_p^n$ and $|A| = \alpha p^n > 0$, then $2A - 2A$ contains a subspace of codimension $< 1/\alpha^2$.

Proof. Let $f : \mathbb{F}_p^n \to \mathbb{R}$ be

$$f(x) = 1_A * 1_A * 1_{-A} * 1_{-A}$$

where 1_A, 1_{-A} are indicator functions.
By the definition of convolution, for any $x \in \mathbb{F}_p^n$

$$f(x) = \mathbb{E}_{z\in\mathbb{F}_p^n}\left(\mathbb{E}_{y\in\mathbb{F}_p^n} 1_A(y)\, 1_A(z-y)\, \mathbb{E}_{y\in\mathbb{F}_p^n} 1_{-A}(y)\, 1_{-A}(x-z-y)\right).$$

Since $1_A, 1_{-A} \geqslant 0$, $f(x) \geqslant 0$ and $f > 0$ if and only if there exist $x, y, z \in \mathbb{F}_p^n$ such that

$1_A(y), 1_A(z-y), 1_{-A}(y), 1_{-A}(x-z-y) > 0$, which is equivalent to

$$\begin{aligned} y &= a_1 \in A \\ z-y &= a_2 \in A \\ y &= -a_3 \in -A \\ x-z-y &= -a_4 \in -A, \end{aligned} \tag{5.1}$$

which after substitution implies that $x = a_1 + a_2 - a_3 - a_4 \in 2A - 2A$. Therefore, it suffices to find a subspace such that for all x in such subspace, $f(x) > 0$, to show that such subspace is contained in $2A - 2A$.
By Theorem 5.3, for any $x \in \mathbb{F}_p^n$

$$\hat{f}(x) = 1_A * 1_A \widehat{* 1_{-A}} * 1_{-A} = \widehat{1_A} \cdot \widehat{1_A} \cdot \widehat{1_{-A}} \cdot \widehat{1_{-A}}.$$

Notice that for any $r \in \mathbb{F}_p^n$

$$\begin{aligned} \widehat{1_A}(r) &= \mathbb{E}_{x \in \mathbb{F}_p^n} 1_A(x) \omega^{-r \cdot x} \\ \widehat{1_{-A}}(r) &= \mathbb{E}_{x \in \mathbb{F}_p^n} 1_{-A}(x) \omega^{-r \cdot x} \end{aligned}$$

where $\omega = \exp(2\pi i/p)$, we have

$$\begin{aligned} \widehat{1_A}(r) &= \mathbb{E}_{x \in \mathbb{F}_p^n} 1_A(x) \omega^{-r \cdot x} = \mathbb{E}_{x \in \mathbb{F}_p^n} 1_A(x) \exp(-2\pi i r \cdot x/p) \\ &= \mathbb{E}_{x \in \mathbb{F}_p^n} 1_A(x) (\cos(-2\pi r \cdot x/p) + i \sin(-2\pi r \cdot x/p)) \\ \overline{\widehat{1_A}(r)} &= \mathbb{E}_{x \in \mathbb{F}_p^n} 1_A(x) (\cos(-2\pi r \cdot x/p) - i \sin(-2\pi r \cdot x/p)) \\ &= \mathbb{E}_{x \in \mathbb{F}_p^n} 1_A(x) (\cos(2\pi r \cdot x/p) + i \sin(2\pi r \cdot x/p)) \\ \widehat{1_{-A}}(r) &= \mathbb{E}_{x \in \mathbb{F}_p^n} 1_{-A}(x) \omega^{-r \cdot x} = \mathbb{E}_{x \in \mathbb{F}_p^n} 1_{-A}(x) \exp(-2\pi i r \cdot x/p) \\ &= \mathbb{E}_{x \in \mathbb{F}_p^n} 1_{-A}(x) (\cos(-2\pi r \cdot x/p) + i \sin(-2\pi r \cdot x/p)) \end{aligned}$$

For any $x \in A$, $-x \in -A$, thus

$$\begin{aligned}
&\overline{\widehat{1_A}(r)} \\
&= \mathbb{E}_{x\in\mathbb{F}_p^n} 1_A(x)\left(\cos\left(2\pi r\cdot x/p\right) + i\sin\left(2\pi r\cdot x/p\right)\right) \\
&= \frac{1}{p^n}\begin{pmatrix} \sum_{x\in A} 1_A(x)\left(\cos\left(2\pi r\cdot x/p\right) + i\sin\left(2\pi r\cdot x/p\right)\right) \\ +\sum_{x\notin A} 1_A(x)\left(\cos\left(2\pi r\cdot x/p\right) + i\sin\left(2\pi r\cdot x/p\right)\right)\end{pmatrix} \\
&= \frac{1}{p^n}\sum_{x\in A} 1_A(x)\left(\cos\left(2\pi r\cdot x/p\right) + i\sin\left(2\pi r\cdot x/p\right)\right) \\
&= \frac{1}{p^n}\sum_{a} 1_A(a)\left(\cos\left(2\pi r\cdot a/p\right) + i\sin\left(2\pi r\cdot a/p\right)\right) \\
&= \frac{1}{p^n}\sum_{a} \left(\cos\left(2\pi r\cdot a/p\right) + i\sin\left(2\pi r\cdot a/p\right)\right) \\
&= \frac{1}{p^n}\sum_{-a} 1_{-A}(-a)\left(\cos\left(2\pi r\cdot a/p\right) + i\sin\left(2\pi r\cdot a/p\right)\right) \\
&= \frac{1}{p^n}\sum_{x\in -A} 1_{-A}(x)\left(\cos\left(2\pi r\cdot x/p\right) + i\sin\left(2\pi r\cdot x/p\right)\right) \\
&= \frac{1}{p^n}\begin{pmatrix} \sum_{x\in -A} 1_{-A}(x)\left(\cos\left(2\pi r\cdot x/p\right) + i\sin\left(2\pi r\cdot x/p\right)\right) \\ +\sum_{x\notin -A} 1_{-A}(x)\left(\cos\left(2\pi r\cdot x/p\right) + i\sin\left(2\pi r\cdot x/p\right)\right)\end{pmatrix} \\
&= \mathbb{E}_{x\in\mathbb{F}_p^n} 1_{-A}(x)\left(\cos\left(-2\pi r\cdot x/p\right) + i\sin\left(-2\pi r\cdot x/p\right)\right) \\
&= \widehat{1_{-A}}(r)
\end{aligned}$$

where a is in A.

Hence,

$$\begin{aligned}
\hat{f}(x) &= \widehat{1_A}\cdot\widehat{1_A}\cdot\widehat{1_{-A}}\cdot\widehat{1_{-A}} \\
&= \left(\widehat{1_A}\right)^2\cdot\left(\overline{\widehat{1_A}(r)}\right)^2 \\
&= \left|\widehat{1_A}\right|^4.
\end{aligned}$$

By Theorem 5.5, for any $x \in \mathbb{F}_p^n$

$$\begin{aligned}
f(x) &= \sum_{r\in\mathbb{F}_p^n} \hat{f}(r)\omega^{r\cdot x} \\
&= \sum_{r\in\mathbb{F}_p^n} \left|\widehat{1_A}(r)\right|^4 \omega^{r\cdot x}.
\end{aligned}$$

Notice that for $r=0$, any $x\in\mathbb{F}_p^n$

$$\begin{aligned}\left|\widehat{1_A}(0)\right|^4\omega^{0\cdot x}&=\left|\widehat{1_A}(0)\right|^4=\left|\mathbb{E}_{x\in\mathbb{F}_p^n}\widehat{1_A}(x)\,\omega^{-0\cdot x}\right|^4\\&=\left|\mathbb{E}_{x\in\mathbb{F}_p^n}\widehat{1_A}(x)\right|^4=\left|\frac{1}{p^n}\cdot|A|\right|^4=\left|\frac{1}{p^n}\cdot\alpha p^n\right|^4\\&=\alpha^4\end{aligned}$$

Let $R=\left\{r\in\mathbb{F}_p^n\setminus\{0\}\ :\left|\widehat{1_A}(r)\right|>\alpha^{3/2}\right\}$, then by Theorem 5.7 we have

$$\begin{aligned}|R|\cdot\alpha^3=|R|\cdot\left(\alpha^{3/2}\right)^2&\leqslant\sum_{r\in R}|\widehat{1_A}(r)|^2<\sum_{r\in\mathbb{F}_p^n}|\widehat{1_A}(r)|^2\\&=\mathbb{E}_{x\in\mathbb{F}_p^n}|1_A(x)|^2=\frac{1}{p^n}\cdot|A|=\frac{1}{p^n}\cdot\alpha p^n=\alpha.\end{aligned}$$

The strict inequality is used here since $0\notin R$ and $\left|\widehat{1_A}(0)\right|^2=\alpha^2>0$.
Thus we have

$$|R|<1/\alpha^2.$$

For $r\in\mathbb{F}_p^n$ and $r\notin R\cup\{0\}$, by Theorem 5.7 again we have

$$\begin{aligned}\sum_{r\notin R\cup\{0\}}|\widehat{1_A}(r)|^4&=\sum_{r\notin R\cup\{0\}}|\widehat{1_A}(r)|^2\cdot|\widehat{1_A}(r)|^2\\&\leqslant\max_{r\notin R\cup\{0\}}|\widehat{1_A}(r)|^2\cdot\sum_{r\notin R\cup\{0\}}|\widehat{1_A}(r)|^2\\&\leqslant\alpha^3\cdot\sum_{r\notin R\cup\{0\}}|\widehat{1_A}(r)|^2\\&<\alpha^3\cdot\sum_{r\in\mathbb{F}_p^n}|\widehat{1_A}(r)|^2\\&=\alpha^3\cdot\alpha=\alpha^4.\end{aligned}$$

The strict inequality is used here for the same reason as above.
Let $R^\perp$ be the orthogonal complement of R in the vector space $\mathbb{F}_p^n$, namely, for any $x\in R^\perp$, any $r\in R$, we have $x\cdot r=0$. Assume that there are exactly k elements in R, then $R=\{r_1,r_2,\ldots,r_k\}$, let $M\in\mathbb{F}_p^{k\times n}$, $M=\begin{pmatrix}r_1\\r_2\\\vdots\\r_k\end{pmatrix}$, $T:\mathbb{F}_p^n\to\mathbb{F}_p^k$,

$$T(x)=Mx.$$

It is straightforward to verify that $R^{\perp} = \ker(T)$, and hence $R^{\perp}$ is a subspace of $\mathbb{F}_p^n$.
By *Rank-nullity theorem*, we have

$$\dim(\ker(T)) + \mathrm{rank}(T) = n.$$

Since $\mathrm{rank}(M) \leqslant |R| < 1/\alpha^2$,

$$\begin{aligned}\dim(R^{\perp}) &= n - \mathrm{rank}(T) \\ &= n - \mathrm{rank}(M) \\ &> n - 1/\alpha^2.\end{aligned}$$

Therefore,

$$\mathrm{codim}(R^{\perp}) < n - \left(n - 1/\alpha^2\right) = 1/\alpha^2.$$

For any $x \in R^{\perp}$, any $r \in R$, we have $x \cdot r = 0$.

$$\begin{aligned}f(x) &= \sum_{r \in \mathbb{F}_p^n} \left|\widehat{1_A}(r)\right|^4 \mathrm{Re}\left(\omega^{r \cdot x}\right) \\ &\geqslant \left|\widehat{1_A}(0)\right|^4 + \sum_{r \in R} \left|\widehat{1_A}(r)\right|^4 - \sum_{r \notin R \cup \{0\}} |\widehat{1_A}(r)|^4 \\ &> \alpha^4 + 0 - \alpha^4 \\ &= 0.\end{aligned}$$

The inequality $\geqslant$ holds from $\mathrm{Re}\left(\omega^{r \cdot x}\right) \leqslant 1$.
We have shown that for any $x \in R^{\perp}$, $f(x) > 0$ thus $x \in 2A - 2A$, therefore, $R^{\perp}$ is a subspace with $\mathrm{codim}(R^{\perp}) < 1/\alpha^2$ that is contained in $2A - 2A$. $\square$

Remark 5.11 (The core of the proof)**.** As we mentioned previously, the above proof use the Fourier transform to express our discrete function as a sum of periodic functions. What we do next is exactly divide them into three sets ($\{0\}, R, \mathbb{F}_p^n \backslash \{0, R\}$) based on their amplitudes $\left(\left|\widehat{1_A}(r)\right|\right)$ to ensure that all elements within $R^{\perp}$ satisfy our conditions after the function transformation.

5.1.3 Bogolyubov's lemma

As mentioned before, here is the definition of *Bohr sets*:

Definition 5.12 (Bohr sets in $\mathbb{Z}/N\mathbb{Z}$)**.** Let $R \subseteq \mathbb{Z}/N\mathbb{Z}$. Define

$$\mathrm{Bohr}(R, \varepsilon) = \left\{x \in \mathbb{Z}/N\mathbb{Z} : \|rx/N\|_{\mathbb{R}/\mathbb{Z}} \leqslant \varepsilon, \text{ for all } r \in R\right\}$$

where $\|\cdot\|_{\mathbb{R}/\mathbb{Z}}$ denotes the distance to the nearest integer. Its *dimension* is $|R|$ and *width* is ε. (Strictly speaking, the definition of a Bohr set includes the data of R and ε and not just the set of elements above.)

Now let us prove the Bogolyubov's lemma in $\mathbb{Z}/N\mathbb{Z}$ with this approximate subspace.

Theorem 5.13 (Bogolyubov's lemma in $\mathbb{Z}/N\mathbb{Z}$)**.** [Bog39][Zha23, p. 253]
If $A \subseteq \mathbb{Z}/N\mathbb{Z}$ and $|A| = \alpha N$, then $2A - 2A$ contains some Bohr set $\mathrm{Bohr}(R, 1/4)$ with $|R| < 1/\alpha^2$.

Proof. Let $f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{R}$ be

$$f(x) = 1_A * 1_A * 1_{-A} * 1_{-A}$$

where 1_A, 1_{-A} are indicator functions.
By the definition of convolution, for any $x \in \mathbb{Z}/N\mathbb{Z}$,

$$f(x) = \mathbb{E}_{z\in\mathbb{Z}/N\mathbb{Z}}\left(\mathbb{E}_{y\in\mathbb{Z}/N\mathbb{Z}} 1_A(y)\, 1_A(z-y)\, \mathbb{E}_{y\in\mathbb{Z}/N\mathbb{Z}} 1_{-A}(y)\, 1_{-A}(x-z-y)\right).$$

Since $1_A, 1_{-A} \geqslant 0$, $f(x) \geqslant 0$ and $f > 0$ if and only if there exist $x, y, z \in \mathbb{F}_p^n$ such that $1_A(y), 1_A(z-y), 1_{-A}(y), 1_{-A}(x-z-y) > 0$, which is equivalent to

$$\begin{aligned} y &= a_1 \in A \\ z - y &= a_2 \in A \\ y &= -a_3 \in -A \\ x - z - y &= -a_4 \in -A, \end{aligned} \tag{5.2}$$

which after substitution implies that $x = a_1 + a_2 - a_3 - a_4 \in 2A - 2A$. Therefore, it suffices to find a Bohr set $\mathrm{Bohr}(R, 1/4)$ such that for all x in such set, $f(x) > 0$, to show that such Bohr set is contained in $2A - 2A$.
By Theorem 5.4, for any $x \in \mathbb{Z}/N\mathbb{Z}$,

$$\hat{f}(x) = 1_A * \widehat{1_A * 1_{-A}} * 1_{-A} = \widehat{1_A} \cdot \widehat{1_A} \cdot \widehat{1_{-A}} \cdot \widehat{1_{-A}}.$$

Notice that for any $r \in \mathbb{Z}/N\mathbb{Z}$,

$$\widehat{1_A}(r) = \mathbb{E}_{x\in\mathbb{Z}/N\mathbb{Z}} 1_A(x)\,\omega^{-r\cdot x}$$
$$\widehat{1_{-A}}(r) = \mathbb{E}_{x\in\mathbb{Z}/N\mathbb{Z}} 1_{-A}(x)\,\omega^{-r\cdot x}$$

where $\omega = \exp(2\pi i/N)$, we have

$$\begin{aligned}
\widehat{1_A}(r) &= \mathbb{E}_{x\in\mathbb{Z}/N\mathbb{Z}} 1_A(x)\,\omega^{-r\cdot x} = \mathbb{E}_{x\in\mathbb{Z}/N\mathbb{Z}} 1_A(x)\exp(-2\pi i r\cdot x/N) \\
&= \mathbb{E}_{x\in\mathbb{Z}/N\mathbb{Z}} 1_A(x)\left(\cos(-2\pi r\cdot x/N) + i\sin(-2\pi r\cdot x/N)\right) \\
\overline{\widehat{1_A}(r)} &= \mathbb{E}_{x\in\mathbb{Z}/N\mathbb{Z}} 1_A(x)\left(\cos(-2\pi r\cdot x/N) - i\sin(-2\pi r\cdot x/N)\right) \\
&= \mathbb{E}_{x\in\mathbb{Z}/N\mathbb{Z}} 1_A(x)\left(\cos(2\pi r\cdot x/N) + i\sin(2\pi r\cdot x/N)\right) \\
\widehat{1_{-A}}(r) &= \mathbb{E}_{x\in\mathbb{Z}/N\mathbb{Z}} 1_{-A}(x)\,\omega^{-r\cdot x} = \mathbb{E}_{x\in\mathbb{Z}/N\mathbb{Z}} 1_A(x)\exp(-2\pi i r\cdot x/N) \\
&= \mathbb{E}_{x\in\mathbb{Z}/N\mathbb{Z}} 1_{-A}(x)\left(\cos(-2\pi r\cdot x/N) + i\sin(-2\pi r\cdot x/N)\right)
\end{aligned}$$

For any $x \in A$, $-x \in -A$, thus

$$\begin{gathered}
\overline{\widehat{1_A}(r)} \\
= \mathbb{E}_{x\in\mathbb{Z}/N\mathbb{Z}} 1_A(x)\left(\cos(2\pi r\cdot x/N) + i\sin(2\pi r\cdot x/N)\right) \\
= \frac{1}{N}\left(\begin{array}{c} \sum_{x\in A} 1_A(x)\left(\cos(2\pi r\cdot x/N) + i\sin(2\pi r\cdot x/N)\right) \\ +\sum_{x\notin A} 1_A(x)\left(\cos(2\pi r\cdot x/N) + i\sin(2\pi r\cdot x/N)\right) \end{array}\right) \\
= \frac{1}{N}\sum_{x\in A} 1_A(x)\left(\cos(2\pi r\cdot x/N) + i\sin(2\pi r\cdot x/N)\right) \\
= \frac{1}{N}\sum_{a} 1_A(a)\left(\cos(2\pi r\cdot a/N) + i\sin(2\pi r\cdot a/N)\right) \\
= \frac{1}{N}\sum_{a} \left(\cos(2\pi r\cdot a/N) + i\sin(2\pi r\cdot a/N)\right) \\
= \frac{1}{N}\sum_{-a} 1_{-A}(-a)\left(\cos(2\pi r\cdot a/N) + i\sin(2\pi r\cdot a/N)\right) \\
= \frac{1}{N}\sum_{x\in -A} 1_{-A}(x)\left(\cos(2\pi r\cdot x/N) + i\sin(2\pi r\cdot x/N)\right) \\
= \frac{1}{N}\left(\begin{array}{c} \sum_{x\in -A} 1_{-A}(x)\left(\cos(2\pi r\cdot x/N) + i\sin(2\pi r\cdot x/N)\right) \\ +\sum_{x\notin -A} 1_{-A}(x)\left(\cos(2\pi r\cdot x/N) + i\sin(2\pi r\cdot x/N)\right) \end{array}\right) \\
= \mathbb{E}_{x\in\mathbb{Z}/N\mathbb{Z}} 1_{-A}(x)\left(\cos(-2\pi r\cdot x/N) + i\sin(-2\pi r\cdot x/N)\right) \\
= \widehat{1_{-A}}(r).
\end{gathered}$$

Hence,

$$\begin{aligned}\hat{f}(x) &= \widehat{1_A} \cdot \widehat{1_A} \cdot \widehat{1_{-A}} \cdot \widehat{1_{-A}} \\ &= \left(\widehat{1_A}\right)^2 \cdot \left(\overline{\widehat{1_A}(r)}\right)^2 \\ &= \left|\widehat{1_A}\right|^4.\end{aligned}$$

By Theorem 5.6, for any $x \in \mathbb{Z}/N\mathbb{Z}$,

$$\begin{aligned}f(x) &= \sum_{r \in \mathbb{Z}/N\mathbb{Z}} \hat{f}(r)\omega^{r \cdot x} \\ &= \sum_{r \in \mathbb{Z}/N\mathbb{Z}} \left|\widehat{1_A}(r)\right|^4 \omega^{r \cdot x}.\end{aligned}$$

Notice that for $r = 0$, any $x \in \mathbb{Z}/N\mathbb{Z}$,

$$\begin{aligned}\left|\widehat{1_A}(0)\right|^4 \omega^{0 \cdot x} = \left|\widehat{1_A}(0)\right|^4 &= \left|\mathbb{E}_{x \in \mathbb{Z}/N\mathbb{Z}} \widehat{1_A}(x)\,\omega^{-0 \cdot x}\right|^4 \\ = \left|\mathbb{E}_{x \in \mathbb{Z}/N\mathbb{Z}} \widehat{1_A}(x)\right|^4 &= \left|\frac{1}{N} \cdot |A|\right|^4 = \left|\frac{1}{N} \cdot \alpha N\right|^4 \\ &= \alpha^4\end{aligned}$$

Let $R = \left\{r \in \mathbb{Z}/N\mathbb{Z} \setminus \{0\} \ : \left|\widehat{1_A}(r)\right| > \alpha^{3/2}\right\}$, then by Theorem 5.8 we have

$$\begin{aligned}|R| \cdot \alpha^3 = |R| \cdot \left(\alpha^{3/2}\right)^2 &\leqslant \sum_{r \in R} |\widehat{1_A}(r)|^2 < \sum_{r \in \mathbb{Z}/N\mathbb{Z}} |\widehat{1_A}(r)|^2 \\ &= \mathbb{E}_{x \in \mathbb{Z}/N\mathbb{Z}} |1_A(x)|^2 = \frac{1}{N} \cdot |A| = \frac{1}{N} \cdot \alpha N = \alpha.\end{aligned}$$

The strict inequality is used here since $0 \notin R$ and $\left|\widehat{1_A}(0)\right|^2 = \alpha^2 > 0$.
Thus we have

$$|R| < 1/\alpha^2.$$

For $r \in \mathbb{Z}/N\mathbb{Z}$ and $r \notin R \cup \{0\}$, by Theorem 5.8 again we have

$$\begin{aligned}\sum_{r \notin R \cup \{0\}} |\widehat{1_A}(r)|^4 &= \sum_{r \notin R \cup \{0\}} |\widehat{1_A}(r)|^2 \cdot |\widehat{1_A}(r)|^2 \\ &\leqslant \max_{r \notin R \cup \{0\}} |\widehat{1_A}(r)|^2 \cdot \sum_{r \notin R \cup \{0\}} |\widehat{1_A}(r)|^2 \\ &\leqslant \alpha^3 \cdot \sum_{r \notin R \cup \{0\}} |\widehat{1_A}(r)|^2 \\ &< \alpha^3 \cdot \sum_{r \in \mathbb{Z}/N\mathbb{Z}} |\widehat{1_A}(r)|^2 \\ &= \alpha^3 \cdot \alpha = \alpha^4.\end{aligned}$$

The strict inequality is used here for the same reason as above.

For any $x \in \text{Bohr}\,(R, 1/4)$, every $r \in R$ satisfies

$$\|rx/N\|_{\mathbb{R}/\mathbb{Z}} \leqslant 1/4.$$

By the definition of $\|\cdot\|_{\mathbb{R}/\mathbb{Z}}$, there exists

$$\beta \in [-1/4, 1/4]$$

such that

$$\beta \equiv \frac{rx}{N} \pmod 1.$$

Therefore,

$$\begin{aligned}2\pi\beta &\in [-\pi/2, \pi/2] \\ \cos(2\pi\beta) &\geq 0.\end{aligned}$$

Hence, for some $m \in \mathbb{Z}$,

$$\cos\left(2\pi\frac{rx}{N}\right) = \cos\left(2\pi\left(\beta + m\right)\right) \geq 0,$$

therefore,

$$\begin{aligned}&\sum_{r \in R} \left|\widehat{1_A}(r)\right|^4 \operatorname{Re}\left(\omega^{r \cdot x}\right) \\ = &\sum_{r \in R} \left|\widehat{1_A}(r)\right|^4 \cos\left(2\pi r x/N\right) \geqslant 0.\end{aligned}$$

Then for any $x \in \text{Bohr}\,(R, 1/4)$,

$$\begin{aligned}
f\,(x) &= \sum_{r\in\mathbb{Z}/N\mathbb{Z}} \left|\widehat{1_A}\,(r)\right|^4 \mathrm{Re}\,(\omega^{r\cdot x}) \\
&= \left|\widehat{1_A}\,(0)\right|^4 + \sum_{r\in R} \left|\widehat{1_A}\,(r)\right|^4 \mathrm{Re}\,(\omega^{r\cdot x}) + \sum_{r\notin R\cup\{0\}} \left|\widehat{1_A}\,(r)\right|^4 \mathrm{Re}\,(\omega^{r\cdot x}) \\
&\geqslant \left|\widehat{1_A}\,(0)\right|^4 + 0 - \sum_{r\notin R\cup\{0\}} |\widehat{1_A}\,(r)\,|^4 \\
&> \alpha^4 - \alpha^4 \\
&= 0.
\end{aligned}$$

The inequality $\geqslant$ holds from $\mathrm{Re}\,(\omega^{r\cdot x}) \leqslant 1$.

We have shown that for any $x \in \text{Bohr}\,(R, 1/4)$, $f\,(x) > 0$ thus $x \in 2A - 2A$, therefore, Bohr $(R, 1/4)$ is contained in $2A - 2A$ with $|R| < 1/\alpha^2$. □

Remark 5.14. The idea of the proof of Bogolyubov's lemma over $\mathbb{Z}/N\mathbb{Z}$ is quite similar to the finite field case. The primary difference is the way we find the special sets $(R^{\perp}, \mathrm{Bohr}(R, 1/4))$, which are all used to control the Fourier character $\omega^{r\cdot x}$ of $r \in R$ and all x in these two sets, to be at least zero. Specifically, $R^{\perp}$ is found relying on the properties of finite field, and $\mathrm{Bohr}(R, 1/4)$ is what we defined for our specific purpose.

5.2 Geometry of Numbers

In Section 5.1.3 we have found that there is some Bohr set in sumsets, by the end of this Chapter, we will show that there is a large GAP contained in some Bohr set. However, it is required to use the tools like Minkowski's second theorem, which we state in Section 5.2.3, and that is the reason why Geometry of Numbers comes in.

5.2.1 Basic concepts in geometry of numbers

Definition 5.15 (Lattice). [Zha23, p. 255] A *lattice* in $\mathbb{R}^d$ is a set of the form

$$\Lambda = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_d = \{n_1v_1 + \cdots + n_dv_d : n_1, \ldots, n_d \in \mathbb{Z}\}$$

where $v_1, \ldots, v_d \in \mathbb{R}^d$ are linearly independent vectors.

The *fundamental parallelepiped* of a lattice Λ with respect to the basis $v_1, \ldots, v_d$ is

$$\{x_1v_1 + \cdots + x_dv_d : x_1, \ldots, x_d \in [0, 1)\}.$$

The *determinant* of this lattice is defined to be

$$\det \Lambda := \left| \det \begin{pmatrix} | & & | \\ v_1 & \cdots & v_d \\ | & & | \end{pmatrix} \right|.$$

This is the absolute value of the determinant of a matrix with $v_1, \ldots, v_d$ as columns.

Definition 5.16 (Lattice in Tao's book)**.** [TV06, p. 114]
A lattice Λ in $\mathbb{R}^d$ is any additive subgroup of the Euclidean space $\mathbb{R}^d$ which is discrete(i.e.,every point in Λ is isolated). The rank of Λ is defined as the dimension of the linear space spanned by the elements of Λ. If the rank is d, we say that Λ has full rank.

Lemma 5.17 (Fundamental theorem of lattices)**.** [TV06, p. 115]
If Λ is a lattice in R^d of rank k, then there exist linearly independent vectors $v_1, v_2, \ldots, v_k$ in $\mathbb{R}^d$ such that $\Lambda = \mathbb{Z}^d \cdot v$.

Remark 5.18 (Two definitions of lattice)**.** The two definitions of *Lattice* are equivalent. Furthermore, the linearly independent vectors $v_1, v_2, \ldots, v_k$ in Lemma 5.17 (with rank d) are exactly the basis vectors $v_1, \ldots, v_d$ in Definition 5.15.

Remark 5.19 (Determinant of a lattice)**.** [Zha23, p. 255]
The determinant of a lattice does not depend on the choice of a basis, and equals the volume of every fundamental parallelepiped.

Proof. Recall from linear algebra that the volume of the fundamental parallelepiped generated by $v_1, \ldots, v_d$ is the absolute value of the determinant of its basis matrix, namely,

$$\operatorname{vol}(P) = \left| \det \begin{pmatrix} | & & | \\ v_1 & \cdots & v_d \\ | & & | \end{pmatrix} \right| = \det \Lambda.$$

Let $V = \{v_1, v_2, \ldots, v_d\}, U = \{u_1, u_2, \ldots, u_d\}$ be bases of Λ. Notice that $u_i \in \Lambda$, for $i = 1, 2, \ldots, d$, thus there exist $n_{i1}, \ldots, n_{id} \in \mathbb{Z}$ such that

$$u_i = n_{i1}v_1 + \cdots + n_{id}v_d.$$

Then

$$
\begin{aligned}
U = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_d \end{pmatrix} &= \begin{pmatrix} n_{11}v_1 + \cdots + n_{1d}v_d \\ n_{21}v_1 + \cdots + n_{2d}v_d \\ \vdots \\ n_{d1}v_1 + \cdots + n_{dd}v_d \end{pmatrix} \\
&= \begin{pmatrix} n_{11} & n_{12} & \cdots & n_{1d} \\ n_{21} & n_{22} & \cdots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ n_{d1} & \cdots & \cdots & n_{dd} \end{pmatrix} \cdot \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_d \end{pmatrix} \\
&= N_1 V.
\end{aligned}
$$

By a similar process, we have

$$V = N_2 U,$$

where $N_2 \in \mathbb{Z}^{d \times d}$. Notice that

$$V = N_2 U = N_2 N_1 V.$$

Thus

$$N_2 N_1 = I.$$

Therefore by multiplicativity of the determinant,

$$\det(N_2)\det(N_1) = \det(N_2 N_1) = \det(I) = 1.$$

Since $N_1, N_2 \in \mathbb{Z}^{d \times d}$, the determinants of N_1, N_2 must be integers. Consequently, we must have

$$\det(N_2) = \det(N_1) = \pm 1.$$

Therefore,

$$
\begin{aligned}
|\det(U)| = \left| \det \begin{pmatrix} | & & | \\ u_1 & \cdots & u_d \\ | & & | \end{pmatrix} \right| &= \left| \det(N_1 V)^\mathsf{T} \right| \\
&= |\det(N_1 V)| = |\det(N_1)\det(V)| \\
&= |\det(V)| \\
&= \det \Lambda.
\end{aligned}
$$

□

Definition 5.20 (Successive minima)**.** [Zha23, p. 256] Let Λ be a lattice in $\mathbb{R}^d$ and $K \subseteq \mathbb{R}^d$ a centrally symmetric convex body. For each $1 \leqslant i \leqslant d$, the *ith successive minimum* of K with respect to Λ is defined to be

$$\lambda_i = \inf\{\lambda \geqslant 0 : \dim(\mathrm{span}(\lambda K \cap \Lambda)) \geqslant i\}.$$

Equivalently, λ_i is the minimum λ such that λK contains i linearly independent lattice vectors from Λ.

A *directional basis* of K with respect to Λ is a basis $\mathbf{b}_1, \ldots, \mathbf{b}_d$ of $\mathbb{R}^d$ such that $\mathbf{b}_i \in \lambda_i K \cap \Lambda$ for each $i = 1, \ldots, d$.

Remark 5.21 (Equivalence of Successive Minima)**.** Let Ω_i be the collection of λ such that λK contains at least i linearly independent lattice vectors from Λ, equivalently,

$$\Omega_i = \{\lambda \geqslant 0 : \dim(\mathrm{span}(\lambda K \cap \Lambda)) \geqslant i\}.$$

Suppose that $\lambda_i = \inf \Omega_i \notin \Omega_i$, then

$$\dim(\mathrm{span}(\lambda_i K \cap \Lambda)) < i.$$

Let $\{v_1, v_2, \ldots, v_j\}$ be the set of linearly independent lattice points in $\lambda_i K$, where $j < i$. Let v_i be the lattice point that $v_i \notin \lambda_i K$ and minimizes the distance between v_i and $\lambda_i K$

$$d(v_i, \lambda_i K),$$

where v_i is linearly independent of $\{v_1, v_2, \ldots, v_j\}$. Since $K \subseteq \mathbb{R}^d$ a centrally symmetric convex body, K is compact. Then $\lambda_i K$ is compact. Therefore, for any $x \in \lambda_i K$,

$$\|x - v_i\| \neq 0.$$

where $\|\cdot\|$ denotes a norm on $\mathbb{R}^d$. Let $d = \min_{x \in \lambda_i K} \|x - v_i\| > 0$. Let $D = \max_{y \in K} \|y\|$, denote such a $y \in K$ as y_D, namely

$$D = \max_{y \in K} \|y\| = \|y_D\|.$$

Let $\delta = \frac{d}{2D} > 0$, $\lambda_i' = \lambda_i + \delta$. For any $y \in K$, let

$$\Delta_y = \|\lambda_i' y - \lambda_i y\| = \|(\lambda_i + \delta)y - \lambda_i y\| = \|\delta y\| = \delta\|y\| \leqslant \delta D = \frac{d}{2D} \cdot D = \frac{d}{2}.$$

Thus

$$\begin{aligned}\|\lambda_i'y - v_i\| &= \|(\lambda_i + \delta)y - v_i\| = \|\lambda_i y - v_i + \delta y\| \\ &\geqslant \|\lambda_i y - v_i\| - \|\delta y\| \\ &\geqslant d - \Delta_y \geqslant d - \frac{d}{2} = \frac{d}{2} \\ &> 0.\end{aligned}$$

Let Λ_L be the collection of points in $(\Lambda \setminus \{v_1, v_2, \ldots, v_j, v_i\})$ that is linearly independent of $\{v_1, v_2, \ldots, v_j\}$. We claim that $\lambda_i'K \cap \Lambda_L = \emptyset$. Assume for contradiction, if v_k is a lattice point in $\lambda_i'K$ that is linearly independent of $\{v_1, v_2, \ldots, v_j\}$, then by above argument. We must have $d(v_k, \lambda_i K) \leqslant \frac{d}{2} < d$. This contradicts the fact that v_i minimizes the distance $d(v_i, \lambda_i K)$.

Therefore we have $\lambda_i' > \lambda_i$ such that

$$\begin{gathered} v_i \notin \lambda_i'K \\ \dim(\mathrm{span}(\lambda_i'K \cap \Lambda)) < i. \end{gathered}$$

Since $\lambda_i = \inf \Omega_i$, for any $\epsilon > 0$, we have $\lambda_i + \epsilon \in \Omega_i$, which is equivalent to

$$\dim(\mathrm{span}((\lambda_i + \epsilon)K \cap \Lambda)) \geqslant i$$

This contradicts above corollary. Therefore, we must have $\lambda_i = \inf \Omega_i \in \Omega_i$. This concludes that λ_i is the minimum λ such that λK contains i linearly independent lattice vectors from Λ.

5.2.2 Blichfeldt's theorem and Minkowski's first theorem

This section will present a beautiful result in geometry of numbers, Blichfeldt's theorem. After that, we will present a direct result of it.

Theorem 5.22 (Blichfeldt's theorem)**.** [Bli14][Zha23, p. 257]
Let $\Lambda \subseteq \mathbb{R}^d$ be a lattice and $K \subseteq \mathbb{R}^d$ be a measurable set with vol$(K) > \det(\Lambda)$. Then there are distinct points $x, y \in K$ with $x - y \in \Lambda$.

Proof. Let P be the fundamental parallelepiped of Λ with respect to the basis $v_1, \ldots, v_d$, namely,

$$P = \{x_1 v_1 + \cdots + x_d v_d : x_1, \ldots, x_d \in [0, 1)\}.$$

For any $x \in \mathbb{R}^d$,

$$x = r_1 v_1 + \cdots + r_d v_d$$

where $r_1, \ldots, r_d \in \mathbb{R}$, there exist $n_1, \ldots, n_d \in \mathbb{Z}$ such that for $i \in \{1, \ldots, d\}$, $x_i \in [0, 1)$,

$$r_i = n_i + x_i.$$

Thus,

$$x = \sum_i r_i v_i = \sum_i (n_i + x_i) v_i = \sum_i n_i v_i + \sum_i x_i v_i = \lambda + p$$

for some $\lambda \in \Lambda$ and $p \in P$.

Therefore,

$$\mathbb{R}^d = \Lambda + P.$$

For some $\lambda \in \Lambda$, let

$$K_\lambda := (\lambda + P) \cap K,$$

translate it by $-\lambda$ to bring it back inside P. Then all the parts of K end up back inside P via translations by some $\lambda \in \Lambda$.

By definition of the determinant of lattice,

$$\det \Lambda = \left| \det \begin{pmatrix} | & & | \\ v_1 & \cdots & v_d \\ | & & | \end{pmatrix} \right| = |\det(V)|.$$

Let $I^d = [0, 1)^d$, notice that

$$P = V(I^d) = \{Vx : x \in I^d\}.$$

Thus, by applying the change of variables formula for multiple integrals, we have

$$\begin{aligned}
\text{vol}(P) &= \int_P 1\, dy \\
&= \int_{V(I^d)} 1\, dy \\
&= \int_{I^d} |\det(V)|\, dx \\
&= |\det(V)| \int_{I^d} 1\, dx \\
&= |\det(V)| \cdot \text{vol}(I^d) \\
&= |\det(V)| \cdot 1 \\
&= \det(\Lambda) \\
&< \text{vol}\,(K)\,.
\end{aligned}$$

Since K is the disjoint union of all K_λ,

$$\begin{aligned}
\sum_{\lambda\in\Lambda} \mathrm{vol}(K_\lambda - \lambda) &= \sum_{\lambda\in\Lambda} m(K_\lambda - \lambda) \\
&= \sum_{\lambda\in\Lambda} m(K_\lambda) \\
&= \sum_{\lambda\in\Lambda} \mathrm{vol}(K_\lambda) \\
&= \mathrm{vol}\left(\bigcup_{\lambda\in\Lambda} K_\lambda\right) \\
&= \mathrm{vol}(K) \\
&> \mathrm{vol}(P)
\end{aligned}$$

where m is the Lebesgue measure.
Assume that $(K_\lambda - \lambda)$ are pairwise disjoint, notice that $(K_\lambda - \lambda)$ are subsets of P, we must have

$$\sum_{\lambda\in\Lambda} \mathrm{vol}(K_\lambda - \lambda) \leqslant \mathrm{vol}(P),$$

which contradicts $\sum_{\lambda\in\Lambda} \mathrm{vol}(K_\lambda - \lambda) > \mathrm{vol}(P)$. Thus, there exist $\lambda_1, \lambda_2 \in \Lambda$ with $\lambda_1 \neq \lambda_2$ such that

$$(K_{\lambda_1} - \lambda_1) \cap (K_{\lambda_2} - \lambda_2) \neq \emptyset.$$

This implies that there must exist distinct points $x, y \in K$, such that

$$x - \lambda_1 = y - \lambda_2,$$

which is equivalent to

$$x - y = \lambda_1 - \lambda_2 = \lambda_3 \in \Lambda.$$

□

Minkowski's first theorem is a direct corollary of Blichfeldt's theorem, the following is the statement.

Theorem 5.23 (Minkowski's first theorem)**.** [Min96][Zha23, p. 257]
Let Λ be a lattice in $\mathbb{R}^d$ and $K \subseteq \mathbb{R}^d$ a centrally symmetric convex body. If $\mathrm{vol}(K) > 2^d \det(\Lambda)$, then K contains a nonzero point of Λ.

Proof. Since K is a measurable set in $\mathbb{R}^d$,

$$\mathrm{vol}\left(\frac{1}{2}K\right) = m\left(\frac{1}{2}K\right) = \left(\frac{1}{2}\right)^d m\left(K\right) = 2^{-d}\mathrm{vol}\left(K\right) > 2^{-d} \cdot 2^d \det\left(\Lambda\right) = \det\left(\Lambda\right).$$

By Theorem 5.22, there exist distinct points $x, y \in \frac{1}{2}K$ such that $x - y = \lambda \neq 0 \in \Lambda$. Observe that $2x, 2y \in K$, since K is centrally symmetric, $-2y \in K$, since K is convex, for any $t \in [0, 1]$,

$$t\left(2x\right) + \left(1 - t\right)\left(-2y\right) \in K.$$

Setting $t = \frac{1}{2}$, we obtain

$$\frac{1}{2}\left(2x\right) + \frac{1}{2}\left(-2y\right) = x - y = \lambda \in K.$$

□

5.2.3 Minkowski's second theorem

Minkowski's second theorem is a remarkable tool that helps us to find a GAP in some Bohr set. Specifically, it allows us to show that the GAP that we find is large enough.

Theorem 5.24 (Minkowski's second theorem)**.** [Min96][Zha23, p. 257]
Let $\Lambda \subseteq \mathbb{R}^d$ be a lattice and $K \subseteq \mathbb{R}^d$ a centrally symmetric convex body. Let $\lambda_1 \leqslant \cdots \leqslant \lambda_d$ be the successive minima of K with respect to Λ. Then

$$\lambda_1 \cdots \lambda_d \mathrm{vol}(K) \leqslant 2^d \det(\Lambda).$$

Proof. Let $U = \mathrm{int}(K)$ be the interior of K, which is an open centrally symmetric convex set. For each $1 \leqslant i \leqslant d$, let λ_i be the *ith successive minimum* of K with respect to Λ. Let $\{b_1, b_2, \ldots, b_d\}$ be a fixed directional basis of K with respect to Λ. Notice that U and K share the same successive minima $\lambda_1 \leqslant \cdots \leqslant \lambda_d$ with respect to Λ. We will proceed by working with the open set U.

Since $\lambda_i U$ is the interior of $\lambda_i K$ and b_i lies exactly on the boundary of $\lambda_i K$, for $1 \leqslant i \leqslant d$ we have

$$b_i \notin \left(\lambda_i U \cap \Lambda\right).$$

For any $x \in (\lambda_i U \cap \Lambda)$, suppose that $x \notin \mathrm{span}(b_1, b_2, \ldots, b_{i-1})$. We must have

$$b_1, b_2, \ldots, b_{i-1}, x$$

are linearly independent. Since $(\lambda_i U \cap \Lambda) \subseteq (\lambda_i K \cap \Lambda)$, we have

$$x \in (\lambda_i K \cap \Lambda).$$

By the definition of directional basis, we can select x as b_i such that $b_i = x$ and

$$b_1, b_2, \ldots, b_i$$

is a directional basis of K with respect to Λ. This contradicts the fact that $b_i = x \notin (\lambda_i U \cap \Lambda)$.

Therefore, for any $x \in (\lambda_i U \cap \Lambda)$ we must have

$$x \in \operatorname{span}(b_1, b_2, \ldots, b_{i-1}).$$

For each $1 \leqslant j \leqslant d$, define map $\phi_j : U \to U$ as

$$\phi_j(x) = \sum_{i<j} c_{j,i}(x_j, \ldots, x_d)\, b_i + \sum_{i \geqslant j} x_i b_i,$$

where $x_i \in \mathbb{R}$ is the i-th coordinate of x with respect to the directional basis $\{b_1, b_2, \ldots, b_d\}$ and $c_{j,i}$ is i-th coordinate of the center of mass of $(j-1)$-dimensional slice of U which contains x and is parallel to $\operatorname{span}_{\mathbb{R}}(b_1, b_2, \ldots, b_{j-1})$. In particular, $\phi_1(x) = x$ for all $x \in U$. For any $x = \sum_{i=1}^{d} x_i b_i \in U$, define $\psi : U \to \mathbb{R}^d$ by:

$$\psi(x) = \sum_{j=1}^{d} \left(\frac{\lambda_j - \lambda_{j-1}}{2}\right) \phi_j(x).$$

Notice that $\psi(x)$ is sum of weighted $\phi_j(x)$ where $j \in \{1, 2, \ldots, d\}$, we can determine the i-th coordinate of $\psi(x)$ (with respect to b_i) by summing the weighted i-th coordinates of each $\phi_j(x)$. Let

$$\begin{aligned}
\psi_i(x) &= \sum_{j=1}^{d} \left(\frac{\lambda_j - \lambda_{j-1}}{2}\right)(\phi_j(x))_i \\
&= \sum_{j=1}^{i} \left(\frac{\lambda_j - \lambda_{j-1}}{2}\right)(\phi_j(x))_i + \sum_{j=i+1}^{d} \left(\frac{\lambda_j - \lambda_{j-1}}{2}\right)(\phi_j(x))_i \\
&= \psi_{i1}(x) + \psi_{i2}(x).
\end{aligned}$$

Recall that

$$\phi_j(x) = \sum_{i<j} c_{j,i}(x_j, \ldots, x_d)\, b_i + \sum_{i \geqslant j} x_i b_i.$$

Therefore, for $j \in \{1, 2, \ldots, i\}$, the i-th coordinate of $\phi_j(x)$ is x_i, and for $j \in \{i+1, i+2, \ldots, d\}$, the i-th coordinate of $\phi_j(x)$ is $c_{j,i}(x_j, \ldots, x_d)$. Thus we have

$$\begin{aligned}
\psi_{i1}(x) &= \sum_{j=1}^{i} (\frac{\lambda_j - \lambda_{j-1}}{2})(\phi_j(x))_i \\
&= (\frac{\lambda_1 - \lambda_0}{2})x_i + (\frac{\lambda_2 - \lambda_1}{2})x_i + \cdots + (\frac{\lambda_i - \lambda_{i-1}}{2})x_i \\
&= (\frac{\lambda_1 - \lambda_0}{2} + \frac{\lambda_2 - \lambda_1}{2} + \cdots + \frac{\lambda_i - \lambda_{i-1}}{2})x_i \\
&= \frac{\lambda_i - \lambda_0}{2}x_i \\
&= \frac{\lambda_i}{2}x_i, \\
\psi_{i2}(x) &= \sum_{j=i+1}^{d} (\frac{\lambda_j - \lambda_{j-1}}{2})c_{j,i}(x_j, \ldots, x_d).
\end{aligned}$$

and then

$$\psi_i(x) = \psi_{i1}(x) + \psi_{i2}(x) = \frac{\lambda_i}{2}x_i + \psi_{i2}(x).$$

Recall that $c_{j,i}$ is i-th coordinate of the center of mass of $(j-1)$-dimensional slice of U which contains x and is parallel to $\mathrm{span}_{\mathbb{R}}(b_1, b_2, \ldots, b_{j-1})$, which depends only on $x_j, \ldots, x_d$ thus $\psi_{i2}(x)$, a sum of weighted $c_{i+1,i}, \ldots, c_{d,i}$, depends only on $x_{i+1}, \ldots, x_d$, which implies that for any $j < i$, $\psi_{i2}(x)$ is independent of x_j, therefore

$$\begin{aligned}
\frac{\partial \psi_i}{\partial x_j} &= \frac{\partial}{\partial x_j}\left(\frac{\lambda_i}{2}x_i + \psi_{i2}(x)\right) \\
&= \frac{\partial \frac{\lambda_i}{2}x_i}{\partial x_j} + \frac{\partial \psi_{i2}(x)}{\partial x_j} \\
&= 0 + 0 \\
&= 0.
\end{aligned}$$

Then the Jacobian matrix of $\psi(x) = \begin{bmatrix} \psi_1(\mathbf{x}) \\ \psi_2(\mathbf{x}) \\ \vdots \\ \psi_d(\mathbf{x}) \end{bmatrix}$ is

$$J = \begin{bmatrix} \frac{\partial \psi_1}{\partial x_1} & \frac{\partial \psi_1}{\partial x_2} & \cdots & \frac{\partial \psi_1}{\partial x_d} \\ \frac{\partial \psi_2}{\partial x_1} & \ddots & \vdots & \vdots \\ \vdots & \cdots & \ddots & \vdots \\ \frac{\partial \psi_d}{\partial x_1} & \cdots & \cdots & \frac{\partial \psi_d}{\partial x_d} \end{bmatrix} = \begin{bmatrix} \frac{\lambda_1}{2} & \frac{\partial \psi_1}{\partial x_2} & \cdots & \frac{\partial \psi_1}{\partial x_d} \\ 0 & \ddots & \vdots & \vdots \\ \vdots & \cdots & \ddots & \vdots \\ 0 & \cdots & \cdots & \frac{\lambda_d}{2} \end{bmatrix},$$

which is an upper triangular matrix.

Therefore,

$$\det(J) = \prod_{i=1}^{d} \frac{\lambda_i}{2} = \frac{\lambda_1 \lambda_2 \cdots \lambda_d}{2^d}$$

and thus

$$\begin{aligned} \mathrm{vol}(\psi(U)) &= |\det(J)| \, \mathrm{vol}(U) \\ &= \frac{\lambda_1 \lambda_2 \cdots \lambda_d}{2^d} \, \mathrm{vol}(U). \end{aligned}$$

Assume that $\lambda_1 \cdots \lambda_d \, \mathrm{vol}(U) > 2^d \det(\Lambda)$, which contradicts our statement, then

$$\mathrm{vol}(\psi(U)) = \frac{\lambda_1 \lambda_2 \cdots \lambda_d}{2^d} \, \mathrm{vol}(U) > \frac{1}{2^d} \cdot 2^d \det(\Lambda) = \det(\Lambda).$$

By Theorem 5.22, there exist $x, y \in U$, $x \neq y$ such that

$$\psi(x) - \psi(y) \in \Lambda \setminus \{0\}.$$

Since $x \neq y$, there exists a maximum index k such that $x_k \neq y_k$. Consequently, for any $j > k$, we have $x_j = y_j$, this implies that for any $j > k$ and $i < j$,

$$c_{j,i}(x_j, \ldots, x_d) = c_{j,i}(y_j, \ldots, y_d).$$

Therefore,

$$\begin{aligned} \phi_j(x) - \phi_j(y) &= \left(\sum_{i<j} c_{j,i}(x_j, \ldots, x_d) \, b_i + \sum_{i \geqslant j} x_i b_i \right) - \left(\sum_{i<j} c_{j,i}(y_j, \ldots, y_d) \, b_i + \sum_{i \geqslant j} y_i b_i \right) \\ &= \left(\sum_{i<j} c_{j,i}(x_j, \ldots, x_d) \, b_i - \sum_{i<j} c_{j,i}(y_j, \ldots, y_d) \, b_i \right) + \left(\sum_{i \geqslant j} x_i b_i - \sum_{i \geqslant j} y_i b_i \right) \\ &= 0 + 0 \\ &= 0. \end{aligned}$$

Thus, for any $j > k$, we conclude that

$$\phi_j(x) = \phi_j(y).$$

Then we have

$$\begin{aligned}\psi(x)-\psi(y) &= \sum_{j=1}^{d}(\frac{\lambda_j-\lambda_{j-1}}{2})\phi_j(x)-\sum_{j=1}^{d}(\frac{\lambda_j-\lambda_{j-1}}{2})\phi_j(y)\\ &= \sum_{j=1}^{d}(\frac{\lambda_j-\lambda_{j-1}}{2})\left(\phi_j(x)-\phi_j(y)\right)\\ &= \sum_{j=1}^{k}(\frac{\lambda_j-\lambda_{j-1}}{2})\left(\phi_j(x)-\phi_j(y)\right)\end{aligned}$$

Notice that $\phi_j(y)$ is in U, as ϕ_j preserves the i-th coordinate of y for $i \geqslant j$, and replaces the i-th coordinate of y for $i < j$ with the corresponding coordinate of center of mass of $(j-1)$-dimensional slice of U which contains y and is parallel to $\mathrm{span}_{\mathbb{R}}(b_1, b_2, \ldots, b_{j-1})$. We claim that such a center of mass is in U. Let S be the slice above, then

$$S = U \cap \{y + \mathrm{span}_{\mathbb{R}}(b_1, b_2, \ldots, b_{j-1})\}.$$

Since U and $\{y+\mathrm{span}_{\mathbb{R}}(b_1, b_2, \ldots, b_{j-1})\}$ are both convex, S is convex. Suppose the center of mass of S, $C(S) := \frac{1}{\mathrm{vol}(S)}\int_S x dx \notin S$, where $\mathrm{vol}(S)$ and dx are taken with respect to the $(j-1)$-dimensional Lebesgue measure on the affine subspace containing S. By *Hyperplane separation theorem*, there exist $v \in \mathbb{R}^d \setminus \{0\}, c \in \mathbb{R}$ such that

$$\begin{aligned} v\cdot x > c, \text{for all } x \in S \\ v \cdot C(S) \leqslant c. \end{aligned} \tag{5.3}$$

Notice that (5.3) implies that

$$v \cdot C(S) = \frac{1}{\mathrm{vol}(S)}\int_S v\cdot x dx > \frac{1}{\mathrm{vol}(S)}\int_S c dx = c,$$

which contradicts the fact that $v \cdot C(S) \leqslant c$.

Therefore, $C(S) \in S$ and thus $C(S) \in U$.

Since U is symmetric, we have $-\phi_j(y) \in U$. Since U is convex, for any $t \in [0, 1]$,

$$t\left(\phi_j(x)\right) + (1-t)\left(-\phi_j(y)\right) \in U.$$

Setting $t = \frac{1}{2}$, we obtain

$$\frac{1}{2}\left(\phi_j(x)\right) + \frac{1}{2}\left(-\phi_j(y)\right) = \frac{1}{2}(\phi_j(x) - \phi_j(y)) = u_j \in U.$$

Since U is convex, for any $a, b \geqslant 0$, we have $aU + bU = (a+b)U$, since $\lambda_j - \lambda_{j-1} \geqslant 0$, we have

$$\begin{aligned}
\psi(x) - \psi(y) &= \sum_{j=1}^{k} (\frac{\lambda_j - \lambda_{j-1}}{2}) \, (\phi_j(x) - \phi_j(y)) \\
&= \sum_{j=1}^{k} (\lambda_j - \lambda_{j-1}) \, u_j \in \sum_{j=1}^{k} (\lambda_j - \lambda_{j-1}) \, U \\
&= (\lambda_1 - \lambda_0 + \lambda_2 - \lambda_1 + \cdots + \lambda_k - \lambda_{k-1}) U \\
&= (\lambda_k - \lambda_0) \, U \\
&= \lambda_k U.
\end{aligned}$$

This implies that $m = \psi(x) - \psi(y) \in (\lambda_k U \cap \Lambda)$. Recall that for any $x \in (\lambda_i U \cap \Lambda)$ we must have

$$x \in \operatorname{span}(b_1, b_2, \ldots, b_{i-1}).$$

Therefore

$$m \in \operatorname{span}(b_1, b_2, \ldots, b_{k-1}).$$

Since for any $j > k$, $x_j = y_j$, we have $\psi_{k2}(x) = \psi_{k2}(y)$, thus the k-th coordinate of m is:

$$\begin{aligned}
m_k &= \psi_k(x) - \psi_k(y) \\
&= \left(\frac{\lambda_k}{2} x_k + \psi_{k2}(x)\right) - \left(\frac{\lambda_k}{2} y_k + \psi_{k2}(y)\right) \\
&= \left(\frac{\lambda_k}{2} x_k - \frac{\lambda_k}{2} y_k\right) + (\psi_{k2}(x) - \psi_{k2}(y)) \\
&= \frac{\lambda_k}{2} \left(x_k - y_k\right).
\end{aligned}$$

Notice that $m_k \neq 0$ as $x_k \neq y_k$, which contradicts $m \in \operatorname{span}(b_1, b_2, \ldots, b_{k-1})$.
Therefore, we must have

$$\lambda_1 \cdots \lambda_d \operatorname{vol}(U) \leqslant 2^d \det(\Lambda).$$

Since K and U share the same *successive minima*, and $\operatorname{vol}(\partial(K)) = 0$ as $\partial(K)$ has measure zero, we have

$$\begin{aligned}
\lambda_1 \cdots \lambda_d \operatorname{vol}(K) &= \lambda_1 \cdots \lambda_d \operatorname{vol}(U) + \lambda_1 \cdots \lambda_d \operatorname{vol}(\partial(K)) \\
&= \lambda_1 \cdots \lambda_d \operatorname{vol}(U) \leqslant 2^d \det(\Lambda).
\end{aligned}$$

$\square$

5.2.4 Finding a GAP in a Bohr Set

Recall that our ultimate goal is to prove that a subset $A \subseteq \mathbb{Z}$ is contained within a GAP. Let us check the tools in our current toolkits. Bogolyubov's lemma allows us to find a Bohr set within a sumset. If we can find a GAP in such a Bohr set, we will have essentially bridged the gap to our original goal. However, Bogolyubov's lemma operates in the cyclic group $\mathbb{Z}/N\mathbb{Z}$, whereas our target set A resides in the integer $\mathbb{Z}$. This is exactly where the Ruzsa modeling lemma, introduced in Section 4.2.3, makes a difference. It allows us to find a "not too small" subset $A' \subseteq A \subseteq \mathbb{Z}$ that can be mapped to a subset of $\mathbb{Z}/N\mathbb{Z}$ while preserving all its additive relations. This implies that if we can successfully identify a GAP within the Bohr set in $\mathbb{Z}/N\mathbb{Z}$, we can use this map to pull the GAP structure back into $\mathbb{Z}$. This transfer is precisely as the Ruzsa modeling lemma preserves all additive properties. Therefore, in the following section, we will demonstrate exactly how to find a GAP in a Bohr set.

Theorem 5.25 (Large GAP in a Bohr set)**.** [Zha23, p. 259]
Let N be a prime. Every Bohr set of dimension d and width $\varepsilon \in (0,1)$ in $\mathbb{Z}/N\mathbb{Z}$ contains a proper GAP with dimension at most d and volume at least $(\varepsilon/d)^d N$.

Proof. Let $R = \{r_1, r_2, \dots, r_d\} \subseteq \mathbb{Z}/N\mathbb{Z}$. Recall that

$$\mathrm{Bohr}(R, \varepsilon) = \{x \in \mathbb{Z}/N\mathbb{Z} : \|xr/N\|_{\mathbb{R}/\mathbb{Z}} \leqslant \varepsilon, \text{for all } r \in R\}.$$

Let

$$v = \left(\frac{r_1}{N}, \frac{r_2}{N}, \dots, \frac{r_d}{N}\right).$$

We claim that for each $x = 0, 1, \dots, N-1$, $x \in \mathrm{Bohr}(R, \varepsilon)$ if and only if some element of $xv + \mathbb{Z}^d$ lies in $[-\varepsilon, \varepsilon]^d$. We first prove the forward implication, suppose that for some of $x \in \{0, 1, \dots, N-1\}$, $x \in \mathrm{Bohr}(R, \varepsilon)$. Notice that

$$xv = \left(\frac{xr_1}{N}, \frac{xr_2}{N}, \dots, \frac{xr_d}{N}\right),$$

for each $\frac{xr_i}{N}$, $i = 1, 2, \dots, N$, since $x \in \mathrm{Bohr}(R, \varepsilon)$,

$$\left\|\frac{xr_i}{N}\right\|_{\mathbb{R}/\mathbb{Z}} \leqslant \varepsilon.$$

Since

$$\frac{xr_i}{N} + z \equiv \frac{xr_i}{N} \pmod 1, \text{for } z \in \mathbb{Z},$$

by definition of $\|\cdot\|_{\mathbb{R}/\mathbb{Z}}$,

$$\left\|\frac{xr_i}{N}+z\right\|_{\mathbb{R}/\mathbb{Z}}=\left\|\frac{xr_i}{N}\right\|_{\mathbb{R}/\mathbb{Z}}\leqslant\varepsilon.$$

Therefore, there exist $z_i\in\mathbb{Z}$ such that

$$\frac{xr_i}{N}+z_i\in[-1,1], \tag{5.4}$$

$$\left\|\frac{xr_i}{N}+z_i\right\|_{\mathbb{R}/\mathbb{Z}}\leqslant\varepsilon. \tag{5.5}$$

Combining 5.4 and 5.5 we have

$$\frac{xr_i}{N}+z_i\in[-\varepsilon,\varepsilon].$$

Then there exist $\mathbf{z}=(z_1,z_2,\ldots,z_n)\in\mathbb{Z}^d$ such that

$$xv+\mathbf{z}\in[-\varepsilon,\varepsilon]^d.$$

Conversely, suppose that for each $x=0,1,\ldots,N-1$, there exist $\mathbf{z}=(z_1,z_2,\ldots,z_n)\in\mathbb{Z}^d$ such that

$$xv+\mathbf{z}\in[-\varepsilon,\varepsilon]^d.$$

For each coordinate of $xv+\mathbf{z}$, $\frac{xr_i}{N}+z_i$, we have

$$\frac{xr_i}{N}+z_i\leqslant\varepsilon.$$

Since $\varepsilon\in(0,1)$, by definition of $\|\cdot\|_{\mathbb{R}/\mathbb{Z}}$,

$$\left\|\frac{xr_i}{N}+z_i\right\|_{\mathbb{R}/\mathbb{Z}}\leqslant\varepsilon.$$

Since

$$\frac{xr_i}{N}+z_i\equiv\frac{xr_i}{N}\pmod 1,$$

we have

$$\left\|\frac{xr_i}{N}\right\|_{\mathbb{R}/\mathbb{Z}}=\left\|\frac{xr_i}{N}+z_i\right\|_{\mathbb{R}/\mathbb{Z}}\leqslant\varepsilon.$$

Therefore we conclude that

$$x\in\mathrm{Bohr}(R,\varepsilon).$$

Let

$$\Lambda=\mathbb{Z}^d+\mathbb{Z}v\subseteq\mathbb{R}^d.$$

We claim Λ is a full-rank lattice in $\mathbb{R}^d$. It suffices to show that Λ satisfies the three properties of Definition 5.16. For any $x_1, x_2 \in \Lambda$, there exist $\mathbf{z_1}, \mathbf{z_2} \in \mathbb{Z}^d$ and $z_1, z_2 \in \mathbb{Z}$ such that

$$x_1 = \mathbf{z_1} + z_1 v, x_2 = \mathbf{z_2} + z_2 v$$

and

$$\begin{aligned} x_1 - x_2 &= (\mathbf{z_1} + z_1 v) - (\mathbf{z_2} + z_2 v) = (\mathbf{z_1} - \mathbf{z_2}) + (z_1 - z_2)v \\ &= \mathbf{z_3} + z_3 v, \end{aligned}$$

where $\mathbf{z_3} = \mathbf{z_1} - \mathbf{z_2} \in \mathbb{Z}^d$, $z_3 = z_1 - z_2 \in \mathbb{Z}$. Thus $x_3 = x_1 - x_2 \in \Lambda$.

It suffices to show that for any $x_1 \neq x_2 \in \Lambda$, $\|x_1 - x_2\| \geqslant \frac{1}{N}$ to show that every point in Λ is isolated. For any $x_1 \neq x_2 \in \Lambda$, there exist at least one coordinate of x_1 and x_2, say, i-th coordinate, such that

$$a_1 + b_1 \cdot \frac{r_i}{N} = (x_1)_i \neq (x_2)_i = a_2 + b_2 \cdot \frac{r_i}{N},$$

where $a_1, b_1, a_2, b_2 \in \mathbb{Z}$. Then

$$\begin{aligned} \|x_1 - x_2\| &\geqslant \sqrt{((a_1 + b_1 \cdot \frac{r_i}{N}) - (a_2 + b_2 \cdot \frac{r_i}{N}))^2} \\ &= \sqrt{((a_1 - a_2) + (b_1 - b_2) \cdot \frac{r_i}{N})^2}. \end{aligned}$$

- If $a_1 \neq a_2$, since $a_1, a_2 \in \mathbb{Z}$, we have $\|x_1 - x_2\| \geqslant \sqrt{(a_1 - a_2)^2} \geqslant 1$.
- If $b_1 \neq b_2$, since $b_1, b_2 \in \mathbb{Z}$, we have $\|x_1 - x_2\| \geqslant \sqrt{((b_1 - b_2) \cdot \frac{r_i}{N})^2} \geqslant \sqrt{(\frac{r_i}{N})^2} \geqslant \frac{1}{N}$.
- $a_1 = a_2$ and $b_1 = b_2$ contradicts our assumption.

Therefore we have

$$\|x_1 - x_2\| \geqslant \frac{1}{N}.$$

Notice that $\mathbb{Z}^d \subseteq \Lambda$, consequently e_i's are in Λ and therefore

$$\operatorname{rank}(\Lambda) = \dim(\operatorname{span}(e_1, e_2, \ldots, e_d)) = d.$$

By Lemma 5.17, there exist linearly independent vectors $v_1, v_2, \ldots, v_k$ in $\mathbb{R}^d$ such that $\Lambda = \mathbb{Z}^d \cdot v$. Notice that such a vector set is exactly the basis in Definition 5.15.

We have shown that $\mathbb{R}^d$ can be covered by *fundamental parallelepiped* P and all its translations by Λ in Theorem 5.22. Notice that there is only one lattice point in P and any of its translations. Furthermore, since translations do not change the volume, it follows that $\mathrm{vol}(P)$ is exactly the reciprocal of density of Λ in $\mathbb{R}^d$, where the density is equal to the number of elements of Λ in a unit cube of $\mathbb{R}^d$, $[0,1)^d$.

To intuitively visualize this conclusion, we provide an example in $\mathbb{R}^2$. We will show that via geometric translations, an unit cube is seamlessly tiled by exactly 5 copies of the fundamental parallelepiped, where 5 is the density of Λ_2 and Λ_2 is the 2-dimensional version of Λ with $r_1 = 1, r_2 = 2$ and $N = 5$.

Since $\mathbb{Z}^2 \subseteq \Lambda_2$, the distribution of lattice points within the unit cube and any of its integer translations is strictly identical. Its suffices to analyze the unit cube $[0,1)^2$. Figure 5.1 illustrates the unit cube $[0,1)^2$ in blue, the fundamental parallelepiped in green, and its translations in red. Points P, P_i, $i = 1,2,3,4$, are the lattice points in $\Lambda_2 \cap [0,1)^2$.

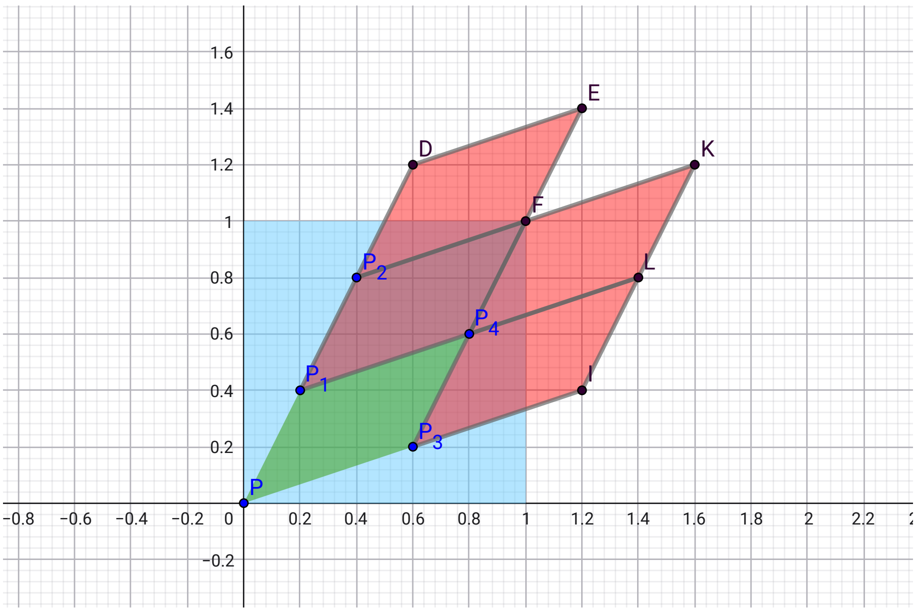

Figure 5.1: Unit cube $[0,1)^2$, fundamental parallelepiped and its translations.

To highlight the parts that need to be translated, we color the parts of parallelepipeds that intersect the cube green, the parts of parallelepipeds that exceed the cube brown and the parts of cube that do not intersect the parallelepipeds blue as shown in Figure 5.2.

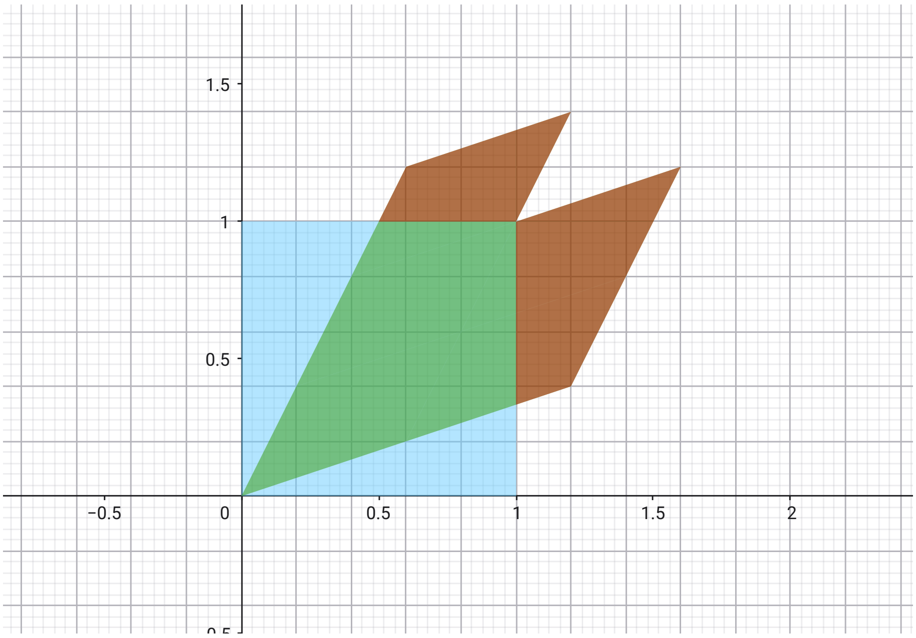

Figure 5.2: Categorization of the unit cube and parallelepipeds.

Figure 5.3 illustrates that we could partition the brown part in Figure 5.2 into 5 parts, which after integer translations can exactly cover the blue parts in Figure 5.2. For instance, the lower-left yellow triangle is exactly the upper-right yellow triangle after being translated by $(-1,-1)$.

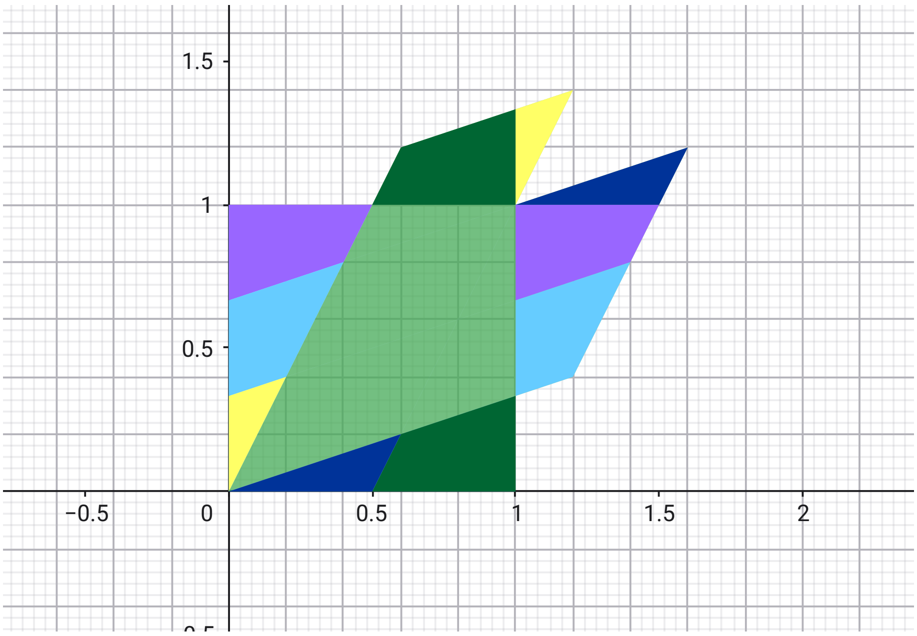

Figure 5.3: The geometric translation from Brown to Blue.

The above shows that the volume of the *fundamental parallelepiped* of Λ_2 is exactly $1/5$.

The geometric translation method above relies on the fact that the distribution of lattice points within unit cube and any of its integer translations is strictly identical. Since $\mathbb{Z}^d \subseteq \Lambda$, the above precondition is satisfied in $\mathbb{R}^d$ as well. This gives that the similar geometric translation is repeatable in d dimensions as well. Therefore our statement above is satisfied.

Now let us check the number of elements of Λ in the unit cube of $\mathbb{R}^d$, $[0,1)^d$, recall that $\Lambda = \mathbb{Z}^d + \mathbb{Z}v \subseteq \mathbb{R}^d$, then it suffices to check the number of distinct combinations of decimal part of $x \in \mathbb{Z}v$ as $\mathbb{Z}^d \in \Lambda$, to check the number of elements of Λ in such cube. For any $z \in \mathbb{Z}$, there exist $q \in \mathbb{Z}$ and $k \in \{0, 1, \ldots, N-1\}$ such that

$$z = qN + k.$$

Then

$$\begin{aligned} zv = (qN+k)v &= (qN+k)\left(\frac{r_1}{N}, \frac{r_2}{N}, \ldots, \frac{r_d}{N}\right) \\ &= q(r_1, r_2, \ldots, r_d) + k\left(\frac{r_1}{N}, \frac{r_2}{N}, \ldots, \frac{r_d}{N}\right) \\ &\equiv k\left(\frac{r_1}{N}, \frac{r_2}{N}, \ldots, \frac{r_d}{N}\right) \pmod{\mathbb{Z}^d}. \end{aligned}$$

This implies that the number of distinct combinations of decimal part of $x \in \mathbb{Z}v$ is at most N.

Since there exists at least one $r_i \neq 0$, in order to show that the number of distinct combinations of decimal part of $x \in \mathbb{Z}v$ is at least N, it suffices to show that for any $k_j \neq k_k \in \{0, 1, \ldots, N-1\}$, the i-th coordinate of $k_j v$ and $k_k v$ are distinct. Let $e_{ji} \in [0,1)$ such that

$$\frac{k_j r_i}{N} \equiv e_{ji} \pmod{1}.$$

if $e_{ji} = e_{ki}$, then

$$\begin{aligned} \frac{k_j r_i}{N} &\equiv \frac{k_k r_i}{N} \pmod{1}, \\ \frac{k_j r_i}{N} - \frac{k_k r_i}{N} &= Z \\ \frac{(k_j - k_k) r_i}{N} &= Z, \end{aligned}$$

where $Z \in \mathbb{Z}$. This contradicts the fact that N is a prime and $r_i \in \mathbb{Z}/N\mathbb{Z} \setminus \{0\}$ and $k_j \neq k_k \in \{0, 1, \ldots, N-1\}$. Therefore we conclude that the i-th coordinate of $k_j v$ and $k_k v$ are distinct and consequently $k_j v$ and $k_k v$ are distinct.

Thus we conclude that the number of distinct combinations of decimal part of $x \in \mathbb{Z}v$ is exactly N, and then the density of Λ in $\mathbb{R}^d$ is N, hence $\mathrm{vol}(P)$, the reciprocal of such density, is $1/N$. By Remark 5.19,

$$\det \Lambda = \mathrm{vol}(P) = 1/N.$$

Consider a convex body $K = [-\varepsilon, \varepsilon]^d$. Let $\lambda_1, \lambda_2, \ldots, \lambda_d$ be the *successive minima* of K with respect to Λ. Let $b_1, b_2, \ldots, b_d$ be the directional basis. We know

$$\|b_j\|_\infty \leqslant \lambda_j \varepsilon, \text{ for all } j,$$

where $\|b_j\|_\infty$ denotes the maximum absolute coordinate of b_j. Such inequality holds since $b_j \in \lambda_j K$ and $K = [-\varepsilon, \varepsilon]^d$.

For each $1 \leqslant j \leqslant d$, let $L_j = \lceil 1/(\lambda_j d) \rceil$. For $l_j \in \mathbb{Z}$, if $0 \leqslant l_j < L_j$, notice that $L_j \in \mathbb{Z}$, then

$$l_j \leqslant L_j - 1 < 1/(\lambda_j d).$$

Thus for k-th coordinate of each $l_j b_j$, $l_j b_{j_k}$, we have

$$l_j b_{j_k} < 1/(\lambda_j d) b_{j_k}$$

Then

$$\begin{aligned} \|l_j b_j\|_\infty &< \|1/(\lambda_j d) b_j\|_\infty \\ &= 1/(\lambda_j d) \cdot \|b_j\|_\infty \\ &\leqslant 1/(\lambda_j d) \cdot \lambda_j \varepsilon \\ &= \frac{\varepsilon}{d}. \end{aligned}$$

Therefore

$$\|l_1 b_1 + l_2 b_2 + \cdots + l_d b_d\|_\infty \leqslant \sum_{i=1}^{d} \|l_i b_i\|_\infty \leqslant \frac{\varepsilon}{d} \cdot d = \varepsilon.$$

Since $b_j \in \Lambda$, there exist $\mathbf{z} \in \mathbb{Z}^d$ and $c \in \mathbb{Z}$ such that

$$b_j = \mathbf{z} + cv.$$

Notice that $c = qN + k$ for some $q \in \mathbb{Z}$ and $k \in \{0, 1, \ldots, N-1\}$, thus there exists $\mathbf{z}' \in \mathbb{Z}^d$

such that

$$\begin{aligned}
b_j &= \mathbf{z} + cv \\
&= \mathbf{z} + (qN+k)v \\
&= \mathbf{z} + (qN+k)\left(\frac{r_1}{N}, \frac{r_2}{N}, \ldots, \frac{r_d}{N}\right) \\
&= \mathbf{z} + q(r_1, r_2, \ldots, r_d) + kv \\
&= \mathbf{z}' + kv.
\end{aligned}$$

Thus for each $1 \leqslant j \leqslant d$, there is some $x_j \in \{0, 1, \ldots, N-1\}$ so that $b_j \in x_j v + \mathbb{Z}^d$, so its i-th coordinate lies in $x_j r_i/N + \mathbb{Z}$. Notice that $\|l_1 b_1 + l_2 b_2 + \cdots + l_d b_d\|_\infty \leqslant \varepsilon$ implies

$$\max_{i \in \{1,\ldots,d\}} \left| \left(\sum_{j=1}^{d} l_j b_j \right)_i \right| \leqslant \varepsilon.$$

Since the i-th coordinate of b_j lies in $x_j r_i/N + \mathbb{Z}$, by the definition of $\|\cdot\|_{\mathbb{R}/\mathbb{Z}}$, we have

$$\begin{aligned}
\left\| \frac{\sum_{j=1}^{d} (l_j x_j) r_i}{N} \right\|_{\mathbb{R}/\mathbb{Z}} &= \left\| \left(\sum_{j=1}^{d} (l_j b_j) \right)_i \right\|_{\mathbb{R}/\mathbb{Z}} \\
&\leqslant \max_{i \in \{1,\ldots,d\}} \left| \left(\sum_{j=1}^{d} l_j b_j \right)_i \right| \\
&\leqslant \varepsilon.
\end{aligned}$$

Here the first inequality holds since $\varepsilon \in (0,1)$. Thus there exist $m_i \in \mathbb{Z}$ such that

$$\left\| \sum_{j=1}^{d} (l_j x_j) v_i + m_i \right\| \in [-\varepsilon, \varepsilon].$$

Thus there exist $M = (m_1, m_2, \ldots, m_d) \in \mathbb{Z}^d$ such that

$$\sum_{j=1}^{d} (l_j x_j) v + M \in [-\varepsilon, \varepsilon]^d.$$

Therefore, $\sum_{j=1}^{d} (l_j x_j) v + \mathbb{Z}^d$ lies in $[-\varepsilon, \varepsilon]^d$. Recall that for each $x = 0, 1, \ldots, N-1$, $x \in \mathrm{Bohr}(R, \varepsilon)$ if and only if some element of $xv + \mathbb{Z}^d$ lies in $[-\varepsilon, \varepsilon]^d$. Therefore the GAP

$$l_1 x_1 + l_2 x_2 + \cdots + l_d x_d, \qquad 0 \leqslant l_i < L_i, \text{ for each } i = 1, \ldots, d$$

is contained in $\mathrm{Bohr}(R, \varepsilon)$. It remains to show that this GAP is large and proper. By Theorem 5.24 we have its volume is

$$L_1 \cdots L_d \geqslant \frac{1}{\lambda_1 \cdots \lambda_d \cdot d^d} \geqslant \frac{\mathrm{vol}(K)}{2^d \det(\Lambda) d^d} = \frac{(2\varepsilon)^d}{2^d (1/N) d^d} = (\frac{\varepsilon}{d})^d N.$$

The first inequality holds as $L_j = \lceil 1/(\lambda_j d) \rceil \geqslant \frac{1}{\lambda_j d}$. Now we check that the GAP is proper. It suffices to show that if

$$l_1 x_1 + l_2 x_2 + \cdots + l_d x_d \equiv l'_1 x_1 + l'_2 x_2 + \cdots + l'_d x_d \pmod N,$$

then we must have $l_i = l'_i$ for all i. Setting

$$\mathbf{b} = \sum_{j=1}^{d} (l_j - l'_j) b_j.$$

Then

$$\|\mathbf{b}\|_\infty = \|\sum_{j=1}^{d} (l_j - l'_j) b_j\|_\infty \leqslant \sum_{j=1}^{d} \|l_j - l'_j\| \cdot \|b_j\|_\infty.$$

Since

$$\|l_j - l'_j\| \leqslant L_j - 1 < \frac{1}{\lambda_j d}$$

$$\|b_j\|_\infty \leqslant \lambda_j \varepsilon,$$

we have

$$\|\mathbf{b}\|_\infty < d \cdot \frac{1}{\lambda_j d} \cdot \lambda_j \varepsilon = \varepsilon < 1.$$

Recall that for each $1 \leqslant j \leqslant d$, there is some $x_j \in \{0, 1, \ldots, N-1\}$ so that $b_j \in x_j v + \mathbb{Z}^d$, let $k_j \in \mathbb{Z}^d$, then

$$\begin{aligned}\mathbf{b} &= \sum_{j=1}^{d} (l_j - l'_j) b_j \\ &= \sum_{j=1}^{d} (l_j - l'_j) x_j v + k_j \\ &= \sum_{j=1}^{d} (l_j - l'_j) x_j v + \sum_{j=1}^{d} (l_j - l'_j) k_j. \end{aligned} \tag{5.6}$$

For the first part of (5.6), let

$$\Gamma = \sum_{j=1}^{d} (l_j - l'_j) x_j v = \sum_{j=1}^{d} (l_j - l'_j) x_j \left(\frac{r_1}{N}, \frac{r_2}{N}, \ldots, \frac{r_d}{N}\right).$$

Since by our assumption, $\sum_{j=1}^{d}(l_j - l'_j)x_j \equiv 0 \pmod N$, there exist $n \in \mathbb{Z}$ such that

$$\sum_{j=1}^{d}(l_j - l'_j)x_j = nN$$

and then

$$\begin{aligned}\Gamma &= nN\left(\frac{r_1}{N}, \frac{r_2}{N}, \dots, \frac{r_d}{N}\right) \\ &= n(r_1, r_2, \dots, r_d) \in \mathbb{Z}^d.\end{aligned}$$

It is trivial to show that the second part of (5.6) is in $\mathbb{Z}^d$. Therefore

$$\mathbf{b} \in \mathbb{Z}^d.$$

Since $\|\mathbf{b}\|_\infty < 1$, we must have

$$\mathbf{b} = 0.$$

This implies that $l_i = l'_i$ for all i as $b_1, b_2, \dots, b_d$ form a directional basis. $\square$

CHAPTER 6

PROOF OF FREIMAN'S THEOREM

6.1 Overall Approach

We have collected all the tools we need for our ultimate goal—Freiman's theorem—in all previous Chapters. While the toolkit we obtained is extremely powerful, the proof of Freiman's theorem remains somewhat complicated. As preparation for Section 6.2, let us first go through the overall approach.

Step 1: From $\mathbb{Z}$ to $\mathbb{Z}/N\mathbb{Z}$.

The first step is to shift our perspective from $\mathbb{Z}$ to $\mathbb{Z}/N\mathbb{Z}$. We will use the Ruzsa modeling lemma to find a subset A' within our target set A that is Freiman isomorphic to some subset B in $\mathbb{Z}/N\mathbb{Z}$. Then we will use Bogolyubov's lemma to show that $2B-2B$ contains a Bohr set, after which we will apply Theorem 5.25 to show that this Bohr set contains a large, proper GAP. Consequently, we establish that $2B-2B$ contains this large, proper GAP.

Step 2: Return to $\mathbb{Z}$.

Then we will shift our perspective back from $\mathbb{Z}/N\mathbb{Z}$ to $\mathbb{Z}$. By the properties of the Freiman isomorphism, we will demonstrate that the GAP found in $\mathbb{Z}/N\mathbb{Z}$ can be mapped back into $\mathbb{Z}$. We will also prove that this GAP in $\mathbb{Z}$, Q, is contained within $2A'-2A'$. After that, we will use the Ruzsa covering lemma to show that there exists a subset X of A such that A can be covered by $X+Q-Q$. The remaining part is quite straightforward: we simply need to show that both X and $Q-Q$ are contained in a GAP, which naturally implies that A is contained in this GAP.

6.2 Freiman's Theorem

Following the approach in the previous Section, the following is the proof of Freiman's theorem.

Theorem 6.1 (Freiman's theorem)**.** [Fre73][Zha23, p. 260]
Let $A \subseteq \mathbb{Z}$ be a finite set satisfying $|A+A| \leqslant K|A|$. Then A is contained in a GAP

of dimension at most $d(K)$ and volume at most $f(K)|A|$, where $d(K) \leqslant \exp(K^C)$ and $f(K) \leqslant \exp(\exp(K^C))$ for some absolute constant C.

Proof. By Theorem 3.7, we have

$$|8A - 8A| \leqslant K^{16}|A|.$$

By *Bertrand-Chebyshev theorem*, there exists a prime N such that

$$K^{16}|A| \leqslant N \leqslant 2K^{16}|A|.$$

By Theorem 4.14, there exists $A' \subseteq A$ with $|A'| \geqslant |A|/8$ such that A' is Freiman 8-isomorphic to a subset B of $\mathbb{Z}/N\mathbb{Z}$.

By Theorem 5.13 on $B \subseteq \mathbb{Z}/N\mathbb{Z}$, with

$$\alpha = \frac{|B|}{N} = \frac{|A'|}{N} \geqslant \frac{|A|}{8N} \geqslant \frac{\frac{N}{2K^{16}}}{8N} = \frac{1}{16K^{16}},$$

we deduce that $2B-2B$ contains a Bohr set with dimension $< 256K^{32}$ with width $1/4$. By Theorem 5.25, $2B - 2B$ contains a proper GAP with dimension $d < 256K^{32}$ and volume $\geqslant (\frac{1}{4}/d)^d = (4d)^{-d}N$.

Since B is Freiman 8-isomorphic to A', we claim that $2B - 2B$ is Freiman 2-isomorphic to $2A' - 2A'$. For any $\beta_1, \beta_2, \beta_1', \beta_2' \in 2B - 2B$, there exist $b_i, b_i' \in B$, $i = 1, \ldots, 8$, such that

$$\beta_1 = b_1 + b_2 - b_5 - b_6, \quad \beta_2 = b_3 + b_4 - b_7 - b_8,$$
$$\beta_1' = b_1' + b_2' - b_5' - b_6', \quad \beta_2' = b_3' + b_4' - b_7' - b_8'.$$

If

$$\beta_1 + \beta_2 = \beta_1' + \beta_2',$$

then

$$\sum_{i=1}^{4} b_i - \sum_{i=5}^{8} b_i = \sum_{i=1}^{4} b_i' - \sum_{i=5}^{8} b_i'$$
$$\sum_{i=1}^{4} b_i + \sum_{i=5}^{8} b_i' = \sum_{i=1}^{4} b_i' + \sum_{i=5}^{8} b_i.$$

Since B is Freiman 8-isomorphic to A', there exists $\phi : B \to A'$ such that

$$\sum_{i=1}^{4} \phi(b_i) + \sum_{i=5}^{8} \phi(b_i') = \sum_{i=1}^{4} \phi(b_i') + \sum_{i=5}^{8} \phi(b_i). \tag{6.1}$$

For any $\beta = b_i + b_j - b_k - b_m \in 2B - 2B$ define $\Phi : (2B - 2B) \to (2A' - 2A')$ as

$$\Phi(\beta) = \Phi(b_i + b_j - b_k - b_m) = \phi(b_i) + \phi(b_j) - \phi(b_k) - \phi(b_m).$$

Then (6.1) implies that

$$\begin{gathered} \sum_{i=1}^{4} \phi(b_i) - \sum_{i=5}^{8} \phi(b_i) = \sum_{i=1}^{4} \phi(b_i') - \sum_{i=5}^{8} \phi(b_i') \\ \Phi(\beta_1) + \Phi(\beta_2) = \Phi(\beta_1') + \Phi(\beta_2'). \end{gathered}$$

Therefore Φ is a Freiman 2-homomorphism. By a similar method we can show that Φ^{-1} is also a Freiman 2-homomorphism. It remains to show that Φ is a bijection. For any $\beta_m, \beta_n \in 2B - 2B$, if

$$\Phi(\beta_m) = \Phi(\beta_n).$$

Then

$$\begin{aligned} \phi(m_1) + \phi(m_2) - \phi(m_3) - \phi(m_4) &= \phi(n_1) + \phi(n_2) - \phi(n_3) - \phi(n_4) \\ \phi(m_1) + \phi(m_2) + \phi(n_3) + \phi(n_4) &= \phi(n_1) + \phi(n_2) + \phi(m_3) + \phi(m_4), \end{aligned} \tag{6.2}$$

where $\beta_m = m_1 + m_2 - m_3 - m_4$, $\beta_n = n_1 + n_2 - n_3 - n_4$. By Exercise 4.4, ϕ is a Freiman 4-isomorphism, therefore (6.2) implies that

$$\begin{aligned} &\phi^{-1}(\phi(m_1)) + \phi^{-1}(\phi(m_2)) + \phi^{-1}(\phi(n_3)) + \phi^{-1}(\phi(n_4)) \\ = &\phi^{-1}(\phi(n_1)) + \phi^{-1}(\phi(n_2)) + \phi^{-1}(\phi(m_3)) + \phi^{-1}(\phi(m_4)). \end{aligned}$$

Then

$$\begin{gathered} m_1 + m_2 + n_3 + n_4 = n_1 + n_2 + m_3 + m_4 \\ \beta_m = m_1 + m_2 - m_3 - m_4 = n_1 + n_2 - n_3 - n_4 = \beta_n. \end{gathered}$$

Since ϕ is a Freiman 8-isomorphism,

$$|B| = |A'|.$$

let us map each $b_i \in B$ to a unique $a_i \in A'$ by $a = \phi(b)$. For any $\beta = b_i + b_j - b_k - b_m \in 2B - 2B$, we have $\phi(b_i), \phi(b_j), \phi(b_k), \phi(b_m) \in A'$, thus there exists $\alpha \in 2A' - 2A'$ such that

$$\alpha = \phi(b_i) + \phi(b_j) - \phi(b_k) - \phi(b_m) = a_i + a_j - a_k - a_m$$

such α is unique since each $b_i \in B$ corresponds to a unique $a_i \in A'$. Thus $|2B - 2B| = |2A' - 2A'|$ and we conclude that Φ is a bijection.

We claim that GAPs are preserved by Freiman 2-isomorphisms. Let G be a proper GAP of dimension d generated by a base point $g_0 \in U$, basis vectors $v_1, \ldots, v_d \in U$, and lengths $L_1, \ldots, L_d \in \mathbb{Z}$

$$G = \left\{ g_0 + \sum_{i=1}^{d} x_i v_i \mid 0 \leqslant x_i < L_i \text{ for } i = 1, \ldots, d \right\}.$$

Since G is proper, its volume is: $|G| = \prod_{i=1}^{d} L_i$.

We claim that $\Phi(Q)$ is a GAP in U' with the base point $\Phi(g_0)$ and basis vectors $v'_i = \Phi(g_0 + v_i) - \Phi(g_0)$ for $i = 1, \ldots, d$. We use induction to prove that:

$$\Phi\left(g_0 + \sum_{i=1}^{d} x_i v_i\right) = \Phi(g_0) + \sum_{i=1}^{d} x_i v'_i. \tag{6.3}$$

Notice that the inputs of left-hand side of (6.3) are in G.

Let $S = \sum_{i=1}^{d} x_i$ be the sum of coefficients of some $g \in G$. For the base case, when $S = 0$, all $x_i = 0$, implying that the input is g_0, and $\Phi(g_0) = \Phi(g_0) + 0$, (6.3) holds. When $S = 1$, the input is $g_0 + v_j$ for some j. By definition of v'_j, we have $\Phi(g_0 + v_j) = \Phi(g_0) + v'_j$, (6.3) also holds.

For the induction step, assume that (6.3) holds for all elements in G with $S = k$. Now consider $g' \in G$ with sum $S = k + 1$. Then g' can be written as $g + v_j$ for some $j \in \{1, \ldots, d\}$ and some $g \in G$ where the sum of coefficients of g is k.

Notice that

$$g' + g_0 = (g + v_j) + g_0 = g + (g_0 + v_j).$$

Since Φ is a Freiman 2-isomorphism, we have

$$\Phi(g') + \Phi(g_0) = \Phi(g) + \Phi(g_0 + v_j).$$

Rearranging the terms, we have

$$\begin{aligned}\Phi(g') &= \Phi(g) + \Phi(g_0 + v_j) - \Phi(g_0) \\ &= \Phi(g) + v'_j. \end{aligned} \tag{6.4}$$

The second equality holds as the case that $S = 1$ we shown above.

By the induction hypothesis, $\Phi(g) = \Phi(g_0) + \sum_{i=1}^{d} x_i v'_i$, where $\sum_{i=1}^{d} x_i = k$. Substitute this into (6.4) we have

$$\begin{aligned}\Phi(g') &= \Phi(g) + v'_j \\ &= \Phi(g_0) + \sum_{i=1}^{d} x_i v'_i + v'_j \\ &= \Phi(g_0) + \sum_{i=1}^{d} x'_i v'_i,\end{aligned}$$

where $\sum_{i=1}^{d} x'_i = k + 1$. This proves that $\Phi(G)$ is indeed a GAP with lengths $L_1, \ldots, L_d$ and dimension $\leqslant d$.

It remains to show that $\Phi(G)$ is proper. Since Φ is a Freiman 2-isomorphism, which implies that Φ is a bijection from G to $\Phi(G)$, therefore we have

$$|\Phi(G)| = |G| = \prod_{i=1}^{d} L_i.$$

Since the number of elements in $\Phi(G)$ is exactly $\prod_{i=1}^{d} L_i$, this implies that for distinct combinations of coefficients, the values in $\Phi(G)$ that corresponding to these distinct combinations will be distinct. Therefore, $\Phi(G)$ is a proper GAP.

Hence, the proper GAP in $2B - 2B$ is mapped to a proper GAP $Q \subseteq 2A' - 2A'$ with the same dimension ($\leqslant d$) and volume ($\geqslant (4d)^{-d}N$). Since $B \subseteq \mathbb{Z}/N\mathbb{Z}$, $|B| \leqslant |N|$, since $|Q| \geqslant (4d)^{-d}N$, we have $N \leqslant (4d)^d|Q|$, therefore we have

$$|A| \leqslant 8|A'| = 8|B| \leqslant 8|N| \leqslant 8((4d)^d)|Q|.$$

Since $Q \subseteq 2A' - 2A' \subseteq 2A - 2A$, we have

$$Q + A \subseteq 3A - 2A.$$

By Theorem 3.7,

$$|Q + A| \leqslant |3A - 2A| \leqslant K^5|A| \leqslant 8K^5(4d)^d|Q|.$$

By Theorem 3.9, there exists a subset X of A, $X \subseteq A$, with $|X| \leqslant 8K^5(4d)^d$ such that

$$A \subseteq X + Q - Q.$$

Since $Q \subseteq 2A - 2A$, by Theorem 3.7 we have

$$|Q| \leqslant |2A - 2A| \leqslant K^4|A|.$$

Suppose that $|X| = n$, $X = \{x_1, \ldots, x_n\}$, let

$$v_1 = x_2 - x_1, \;\; v_2 = x_3 - x_1, \;\; \ldots, \;\; v_{n-1} = x_n - x_1$$

and

$$P = \left\{ x_1 + \sum_{i=1}^{n-1} e_i v_i \mid e_i \in \{0, 1\} \right\}.$$

Then P is a GAP with dimension $(n-1) \leqslant 8K^5(4d)^d - 1$ and volume $|P| \leqslant 2^{n-1} \leqslant 2^{8K^5(4d)^d-1}$ such that $X \subseteq P$.

Since Q is proper GAP with dimension d, let

$$Q = \{a_0 + \sum_{i=1}^{d} y_i w_i \mid 0 \leqslant y_i < L_i.\}$$

Then

$$Q - Q = \{\sum_{i=1}^{d} y_i' w_i \mid -L_i < y_i' < L_i\}$$

is a GAP with dimension d and volume $|Q - Q| \leqslant (2L_i)^d = 2^d(L_i)^d \leqslant 2^d|Q| \leqslant 2^d K^4|A|$. Therefore, $P + Q - Q$ is a GAP with

$$\text{dimension} \leqslant 8K^5(4d)^d - 1 + d$$

and

$$\text{volume} \leqslant |P| \cdot |Q - Q| \leqslant 2^{8K^5(4d)^d-1} 2^d K^4|A| = 2^{8K^5(4d)^d-1+d} K^4|A|$$

such that contains A.

Recall that the dimension $d < 256K^{32}$, which implies $d = K^{O(1)}$. Therefore, for $(4d)^d$ we have

$$(4d)^d = e^{d\ln(4d)} \leqslant e^{K^{O(1)}\ln(K^{O(1)})} = e^{K^{O(1)}\cdot O(1)\ln(K)} = e^{K^{O(1)}}.$$

Since $8K^5$ and $d-1$ grow much slower than the exponential function $e^{K^{O(1)}}$, the dimension of the GAP can be bounded by the exponential term:

$$\text{dimension} \leqslant 8K^5(4d)^d - 1 + d = e^{K^{O(1)}}. \tag{6.5}$$

Substituting (6.5) into the volume bound we have:

$$\begin{aligned}\text{volume} \leqslant 2^{8K^5(4d)^d-1+d}K^4|A| &\leqslant 2^{e^{K^{O(1)}}}e^{O(\log K)}|A| \\ &\leqslant e^{e^{K^{O(1)}}}e^{O(\log K)}|A| = e^{e^{K^{O(1)}}+O(\log K)}|A| \\ &= e^{e^{K^{O(1)}}}|A|.\end{aligned}$$

Therefore, we conclude that A is contained in a GAP with dimension at most $e^{K^{O(1)}}$ and volume at most $e^{e^{K^{O(1)}}}|A|$. This completes the proof of Freiman's theorem. $\square$

CHAPTER 7

CONCLUSIONS AND RECOMMENDATIONS

7.1 Conclusions

Eventually, we have finished the proof of the classic Freiman's theorem in our last chapter. It is not hard to see that at the end of the proof, the volume bound of the GAP that can cover A is at a double-exponential level. As we mentioned in the introduction, the polynomial Freiman's theorem was already proved by four mathematicians in 2023[GGMT25]. A natural question arises: why is our classic Freiman's theorem still so important in this situation? We can answer this question from two aspects.

First, the classic proof is still a great exercise. The proof is an excellent starting point to get into additive combinatorics. For one, it perfectly shows us the interdisciplinary property of additive combinatorics. It not only uses traditional combinatorics tools, but also borrows tools from seemingly unrelated fields like probability theory, harmonic analysis, and the geometry of numbers. At the same time, it shows us a great way of thinking when researching additive combinatorics, or even math in general: if we get stuck in one place, a shift of perspective can sometimes help us to solve it. For instance, in our thesis, this is when we found it extremely difficult to directly study the structure of sumsets in the integers $\mathbb{Z}$, we shifted our focus to the finite cyclic group $\mathbb{Z}/N\mathbb{Z}$, where things are a bit easier. Then, by using certain tools, we shift our perspective back to our original integer group, and then the problem can be solved.

Furthermore, you will find that the statement of the paper "On a conjecture of Marton"[GGMT25] is slightly different from our classic Freiman's theorem. For the classic one, we are discussing sets from the perspective of integers, while that paper is based on the linear space $\mathbb{F}_2^n$ over the finite field $\mathbb{F}_2$. Also, in our thesis, the target we want to find to cover A is a GAP, but in that paper, the target becomes cosets. To answer why there is this difference, we have to go back to the essence of the statement of Freiman's theorem. In fact, the cores of both statements are both trying to find a perfectly structured set in their respective environments ($\mathbb{Z}$ and $\mathbb{F}_2^n$) that can cover set A. This is because the essence of studying the

Freiman problem is trying to reveal the structure of A through its doubling constant. If a set can be covered by a well-structured set, it somehow shows that A itself has a good structure. In $\mathbb{Z}$, a GAP is naturally the one with the best structure. And in $\mathbb{F}_2^n$, what kind of set has the best structure? That would be our cosets. For instance, if the set A is a coset in $\mathbb{F}_2^n$, then A can be written in the form of an element x in $\mathbb{F}_2^n$ plus a finite subgroup H in $\mathbb{F}_2^n$. In this case, $A + A$ becomes $x + x + H + H = H$, then the *doubling constant* is 1! This is exactly why the target of study in the polynomial Freiman's theorem is the coset. However, unlike $\mathbb{F}_2^n$, the integer group $\mathbb{Z}$ has no non-trivial finite subgroups, therefore, we cannot use cosets of finite subgroups to cover sets in $\mathbb{Z}$.

7.2 Recommendations

The starting point of the polynomial version's proof is also very interesting and brilliant. The authors directly shifted from sets to probability theory, using X_A to represent a uniformly distributed random variable over A. This turns the set A we are studying into a random variable X_A in a probability space which is uniformly distributed, and introduces the concept of Shannon entropy to perfectly represent the size of A. The advantage of this idea of turning A into X_A is that the traditional approach can only study the size of set A and its sumset, which is just the number of their elements. However, in this process, it is extremely difficult to find the differences in the "origins" of elements in the sumset. For example, if set A consists of the integers 1 to 6 (imagine all possible outcomes of a die), then the sumset is 2 to 12 (imagine rolling two dice at the same time and adding all possible outcomes together). With the traditional method, we only know there are 11 elements in the sumset, but we cannot really study the "origins" of these elements. For instance, '2' can only be obtained through $1 + 1$, but '6' can be obtained through $1 + 5$, $2 + 4$, $3 + 3$. Although both '2' and '6' are in the sumset, the properties of their "origins" are obviously not the same. But if we switch it to probability, things change. If we represent A and $A' = A$ using random variables, denoted as X_A and $X_{A'}$, respectively, then the addition of these two random variables can represent our sumset, and we will find that adding random variables solves the problem we just mentioned. For example, the probability of '2' is $1/36$ (die 1=1, die 2=1), and the probability of '6' is $6/36 = 1/6$ (die 1=1, die 2=5, etc.). This perfectly reflects the difference in the properties of their "origins". Of course, here we are just briefly touching on the ideas of this paper and a comprehensive exposition would be a future work for us.

REFERENCES

[Bli14] Hans F. Blichfeldt. A new principle in the geometry of numbers, with some applications. *Transactions of the American Mathematical Society*, 15(3):227–235, 1914. MR:1500976.

[Bog39] Nikolay N. Bogolyubov. Sur quelques propriétés arithmétiques des presque-périodes. *Ann. Chaire Phys. Math. Kiev*, 4:185–205, 1939. MR:20164.

[Fre73] Gregory A. Freiman. *Foundations of a structural theory of set addition*. American Mathematical Society, Providence, R.I., 1973. Translated from the Russian. MR:360496.

[GGMT25] W. T. Gowers, Ben Green, Freddie Manners, and Terence Tao. On a conjecture of Marton. *Annals of Mathematics*, 201(2):515–549, 2025. MR:4880432.

[Min96] Hermann Minkowski. *Geometrie der Zahlen*. Teubner, Leipzig, 1896. MR:249269.

[Pet12] Giorgis Petridis. New proofs of Plünnecke-type estimates for product sets in groups. *Combinatorica*, 32(6):721–733, 2012. MR:3063158.

[Plü70] Helmut Plünnecke. Eine zahlentheoretische anwendung der graphentheorie. *Journal für die reine und angewandte Mathematik*, 243:171–183, 1970. MR:266892.

[Ruz89] Imre Z. Ruzsa. An application of graph theory to additive number theory. *Sci. Ser. A Math. Sci.*, 3:97–109, 1989. MR:2314377.

[Ruz94] Imre Z. Ruzsa. Generalized arithmetical progressions and sumsets. *Acta Mathematica Hungarica*, 65(4):379–388, 1994. MR:1281447.

[Ruz99] Imre Z. Ruzsa. An analog of Freiman's theorem in groups. *Astérisque*, 258:323–326, 1999. MR:1701207.

[TV06] Terence Tao and Van H. Vu. *Additive Combinatorics*. Cambridge University Press, 2006. MR:2289012.

[Zha23] Yufei Zhao. *Graph Theory and Additive Combinatorics*. Cambridge University Press, 2023. MR:4603631.