A

STUDIES IN THE STRUCTURE OF SUMSETS

by

SHU-PING SANDIE HAN

A dissertation submitted to the Graduate Faculty in Mathematics in partial fulfillment of the requirements for the degree of Doctor of Philosophy, the City University of New York

1999

UMI Number: 9946173

UMI
300 North Zeeb Road
Ann Arbor, MI 48103

This manuscript has been read and accepted for the Graduate Faculty in Mathematics in satisfaction of the dissertation requirement for the degree of Doctor of Philosophy.

9/17/99 Melvyn B. Nathanson

Date — Chair of Examining Committee

9/17/99

Date — Executive Officer

Melvyn B. Nathanson

Mark Sheingorn

Alphonse Vasquez

Supervisory Committee

THE CITY UNIVERSITY OF NEW YORK

Abstract

STUDIES IN THE STRUCTURE OF SUMSETS

by

SHU-PING SANDIE HAN

Advisor: Professor Melvyn B. Nathanson

Many studies have been done on the structure and the cardinality of sum of sets. In particular, let h be a positive integer, and let A be a finite subset of $\mathbf{Z}^n$. We are interested in hA, the h-fold sumset of A and its structure and cardinality for h sufficiently large. In this research, we are interested in extending some of the concepts on hA to $h_1A_1 + \cdots + h_rA_r$, where $A_1, \ldots, A_r$ are finite subsets of $\mathbf{Z}^n$ and $h_1, \ldots, h_r$ are positive integers.

It was found by Nathanson that when A is a set of integers, the structure of the h-fold sumset of A consists of an interval of consecutive integers and the cardinality of hA is a linear function of h. If we consider A to be a finite set of lattice points in $\mathbf{Z}^n$, Khovanskii has found a polytope in $\mathbf{R}^n$ such that hA contains all of the lattice points in the polytope. Khovanskii found the cardinality of hA to be a function of h^n.

The objective of this paper is three-fold. In Chapter 1, we let $A_1, \ldots, A_r$ be finite subsets of integers, and let $h_1, \ldots, h_r$ be positive integers. We are able to generalize Nathanson's theorem to a sum of sumsets $h_1A_1 + \cdots + h_rA_r$ and determine the structure and estimate the cardinality of $h_1A_1 + \cdots + h_rA_r$ for all sufficiently large integers h_i.

In Chapter 2, the author will present a modified proof of Khovanskii's theorems concerning hA. Furthermore, we let $A_1, \ldots, A_r$ be finite subsets of $\mathbf{Z}^n$, and $h_1, \ldots, h_r$ be positive integers, we are able to generalize Khovanskii's theorem to $h_1A_1 + \cdots + h_rA_r$ and determine its structure for h_i sufficiently large. We are also able to estimate the cardinality of the linear form in the case of $\mathbf{Z}^2$.

In Chapter 3, we look at specifically the fine structure of the h-fold sumset of a set A in $\mathbf{Z}^2$. It is found that the distribution of hA in the boundary region of the convex hull has a consistent regular pattern. To study the distribution of hA in the boundary region of the convex hull of hA, we partition the boundary region into many smaller regions and find that the distribution of hA in each small boundary region is identical, the elements from one region and the elements from another region differ by a translation.

Acknowledgments

I want to express my deepest gratitude toward my advisor Professor Melvyn Nathanson. Without his guidance and encouragement every step of the way, this thesis would not have been possible.

I would also like to acknowledge my appreciation to my thesis committee members, Professor Alphonse Vasquez and Professor Mark Sheingorn. I also wish to extend my appreciation to all the faculty members and friends from the Mathematics Department of the Graduate Center for their encouragement. I especially want to thank Martin Helm for his help and advice when I most needed them.

I wish to extend my appreciation to Professor Henry Africk and other faculty and staff of the Mathematics Department at NYC Technical College for their encouragement.

I wish to thank my husband for his support and for being so patient with me through these frustrating years. I also wish to thank my mother-in-law for always taking time out to help us with babysitting and household chores so I could study.

Finally, I want to thank my parents for their inspiration and for believing in me.

Contents

Chapter 1

The structure of sumsets in the case of the integers

1.1 Introduction

Let A be a set of integers and let h be a positive integer, Nathanson had found that the h-fold sumset of A contains an interval of consecutive integers. In this chapter, we let $A_1, \ldots, A_r$ be sets of integers, and let $h_1, \ldots, h_r$ be positive integers, we will explore the structure of $h_1A_1 + \cdots + h_rA_r$ which is the sum of sets of integers in a linear form.

In the first section of the chapter, we will go over some basic definitions and notations. In the second section of this chapter, we will look at the structure of the sum of arithmetic progressions in a linear form. Arithmetic progressions are special sets of integers. Its regularity makes it easy to study the sum in the linear form. In the third section of this chapter, we will look at the structure of the sum of arbitrary sets of integers in a linear form. It is found that, just as in the case of hA, the sum of sets of integers in the linear form also contains an interval of consecutive integers.

Throughout this chapter, we will adopt the following definitions and notations.

Let A be a finite arithmetic progression. This means that A is a set of integers of the form

$$A = \{a, a+\delta, a+2\delta, \ldots, a+(k-1)\delta\}$$

If $a = 0$, then we say A is normalized. Let $|A|$ denote the cardinality of A. Thus, for the set A mentioned above, $|A| = k$.

Let A and B be finite sets of integers. Then

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

We denote

$$2A = A + A = \{a_1 + a_2 \mid a_1, a_2 \in A\},$$

where a_1 and a_2 are not necessarily distinct. For every positive integer h, we can define the sumset hA in a similar way:

$$hA = \underbrace{A + \cdots + A}_{h \text{ times}} = \{a_1 + \cdots + a_h \mid a_i \in A, \quad \text{for} \quad i = 1, \ldots, h\},$$

where $a_1, \ldots, a_h$ are not necessarily distinct. Define $hA = \{0\}$ for $h = 0$. Let δ be a positive integer, define

$$\delta \cdot A = \{\delta \cdot a \mid a \in A\},$$

and if a_0 is an integer, define

$$a_0 + A = \{a_0 + a \mid a \in A\}.$$

Let $A_1, \ldots, A_r$ be finite sets of integers, and let $h_1, \ldots, h_r$ be positive integers. Then the sumset $h_1A_1 + \cdots + h_rA_r$ is called a *linear form* and

$$h_1A_1 + \cdots + h_rA_r = \{\alpha_1 + \cdots + \alpha_r \mid \alpha_i \in h_iA_i, \text{ for } i = 1, \ldots, r\}.$$

Also, throughout this chapter, we will denote

$$[a,\ b] = \{n \in Z \mid a \leq n \leq b\}$$

$$(a,\ b] = \{n \in Z \mid a < n \leq b\}$$

$$[a,\ b) = \{n \in Z \mid a \leq n < b\}$$

$$(a,\ b) = \{n \in Z \mid a < n < b\}$$

1.2 The structure of the sum of arithmetic progressions

Let $A_1, A_2, \ldots, A_r$ be r arithmetic progressions. In this section, the structure and the cardinality of the sum of arithmetic progressions is determined. Furthermore, let $h_1, h_2, \ldots, h_r$ be positive integers, the structure of $h_1A_1 + h_2A_2 + \cdots + h_rA_r$ is also determined.

First, let us consider the normalized arithmetic progressions A and B where $A = \{0, a, 2a, \ldots, (k-1)a\}$ and $B = \{0, b, 2b, \ldots, (l-1)b\}$. If $n \in A + B$, then there exist nonnegative integers i and j such that $0 \leq i \leq k-1$ and $0 \leq j \leq l-1$ and $n = ia + jb$. The following few lemmas prove some interesting properties of those integers n that can be expressed as $ia + jb$.

Lemma 1.1 *Let a, b be positive integers with* $\gcd(a,b) = 1$. *Let n be an integer such that $0 \leq n < ab$, then n is uniquely represented by $n = ia + jb$ where $i \in Z$, and j is an integer such that $0 \leq j \leq a - 1$.*

Proof.

Since $\gcd(a,b) = 1$, $\exists\, x, y \in Z$ such that $n = xa + yb$. Let m be an integer such that $0 \leq y - ma \leq a - 1$.

$$\begin{aligned} n &= xa + yb - mab + mab \\ &= (x + mb)a + (y - ma)b \\ &= ia + jb \end{aligned}$$

where $i = x + mb \in Z$, and $j = y - ma$, $0 \leq j \leq a - 1$.

For uniqueness: Let $x = ia + jb$, $x' = i'a + j'b$ and $0 \leq x, x' < ab$ where $i, i' \in Z$, and $0 \leq j, j' \leq a - 1$. If $i \neq i'$ and $j \neq j'$, assume $x = x'$

$$\begin{aligned} &\Rightarrow\ ia + jb = i'a + j'b \\ &\Rightarrow\ (i - i')a = (j' - j)b \end{aligned}$$

Since $\gcd(a,b) = 1$, equality occurs if $i - i' = tb$ and $j' - j = ta$, for some nonnegative integer t. $\Rightarrow i = i' + tb$, and $j' = j + ta$. Since $j' \neq j$, so $t \neq 0$. But then $j' = j + ta > a - 1$, which is a contradiction. Thus $x \neq x'$. $\square$

Lemma 1.2 *Let k and l be positive integers such that $k - 1 \geq b$ and $l - 1 \geq a$. Let $A = \{0, a, 2a, \ldots, (k-1)a\}$ and $B = \{0, b, 2b, \ldots, (l-1)b\}$,* $\gcd(a,b) = 1$. *Without* *loss of generality, we can assume $b > a$. Let*

$$S = \{n \mid n = ia + jb,\ i, j \in \mathbf{Z},\ i \geq 0,\ 0 \leq j \leq a-1,\ 0 \leq n < ab\}$$

$$S' = \{n \in A + B \mid 0 \leq n < ab\}$$

Then $S = S'$.

Proof.

Let $n \in S$, then $n = ia + jb$ such that $0 \leq n < ab$ and $i \geq 0$, $0 \leq j \leq a-1$. This implies that $0 \leq j < l-1$. We can also assume that $i \leq b \leq k-1$, otherwise, $n = ia \geq ab$. Thus, $ia \in A$, and $jb \in B$. Therefore, $n \in A + B$, this implies that $S \subseteq S'$.

On the other hand, We need to prove that $S' \subseteq S$: Let $n \in S'$, then $n = ia + jb$ for some nonnegative integers i, j. Suppose $j \geq a$, then $n = ia + jb \geq ab$, contradicting the fact that $n < ab$. Thus, $0 \leq j \leq a-1$. So $n \in S$ and $S' \subseteq S$. □

Lemma 1.3 *Let $A = \{0, a, 2a, \ldots, (k-1)a\}$ and $B = \{0, b, 2b, \ldots, (l-1)b\}$. The largest element less than ab and not in $A + B$ is $ab - b - a$.*

Proof.

From Lemma 1.1, an integer n, such that $0 \leq n < ab$, has a unique representation as $n = ia + jb$, where $i, j \in Z$ and $0 \leq j \leq a-1$. By Lemma 1.2, the elements that are less than ab and not in $A + B$ are exactly those $n = ia + jb$, where $i < 0$. To find the largest of such an element, we let i, j be the largest it can be. We let $i = -1$ and $j = a-1$. Thus we have $(a-1)b - a = ab - b - a$ as the largest element not in $A + B$ and is less than ab. □

Remark 1.1 *Let $c = ab-a-b+1$, then we have $[c, ab) \subset A+B$, since $c-1 = ab-a-b$ is the largest element less than ab that is not contained in $A+B$.*

Lemma 1.4 *Let $U = \{n \mid n = ia + jb,\ i, j \in \mathbf{Z},\ i \geq 0,\ 0 \leq j \leq a-1,\ 0 \leq n \leq (a-1)b - a\}$, then $|U| = (a-1)(b-1)/2$.*

Proof.

Let

$$V = \{n \mid n = ia + jb,\ i, j \in \mathbf{Z},\ i < 0,\ \ 0 \leq j \leq a-1,\ \ 0 \leq n \leq (a-1)b - a\}$$

Define a function $f : U \longrightarrow V$ such that

$$f(ia + jb) = -(i+1)a + [(a-1) - j]b$$

This function is well defined, one-to-one and onto since

$$f^{-1}(ia + jb) = -(i+1)a + [(a-1) - j]b$$

Thus f is an isomorphism. Therefore $U \cong V$ and $|U| = |V|$. Since $U \cap V = \emptyset$ and $U \cup V = [0, (a-1)b - a]$ we have

$$|U| = [(a-1)b - a + 1]/2 = (a-1)(b-1)/2.$$

□

Lemma 1.5 *Let $A = \{0, a, 2a, \ldots, (k-1)a = a^*\}$ and $B = \{0, b, 2b, \ldots, (l-1)b = b^*\}$, $\gcd(a, b) = 1$, $k - 1 \geq b$, and $l - 1 \geq a$. If n is an integer such that $ab \leq n \leq a^* + b^* - ab$, then $n \in A + B$.*

Proof.

Since $\gcd(a,b)=1$, there exist integers x and y such that $n = xa + yb$. Let u' be the least nonnegative residue of x mod b, then

$$n \equiv u'a \quad \mod b \qquad \text{where} \quad 0 \le u' \le b-1$$

Let v' be an integer such that

$$n = u'a + v'b$$

So

$$v'b = n - u'a \ge n - (b-1)a > n - ab \ge 0$$

Thus $v' > 0$.

If $n-(k-1)a \ge 0$, then let t be a nonnegative integer such that

$$u' + tb \;\le\; k-1 \;<\; u' + (t+1)b \tag{1.1}$$

If $n-(k-1)a < 0$, then let t be a nonnegative integer such that

$$0 \;\le\; n - (u' + tb) \;\le ab \tag{1.2}$$

Let $u = u' + tb$ and $v = v' - ta$, then

$$\begin{aligned} n &= u'a + v'b \\ &= u'a + tab + v'b - tab \\ &= (u' + tb)a + (v' - ta)b \\ &= ua + vb \end{aligned}$$

In the case of either equations (1.1) or (1.2), we have $0 \le u \le k-1$, also

$$vb \;=\; (v' - ta)b \;=\; v'b - tab \;=\; (n - u'a) - tab \;=\; n - (u' + tb)a \;=\; n - ua \;\ge\; 0$$

Implying that $v \geq 0$.

Furthermore, if $n-(k-1)a \geq 0$, then

$$\begin{aligned} vb &= n-ua \\ &= n-(tb+u')a \\ &< (k-1)a+(l-1)b-ab-(tb+u')a \\ &= [(k-1)-(tb+u')]a+(l-1)b-ab \\ &\leq ba+(l-1)b-ab \\ &= (l-1)b \end{aligned}$$

implying that $v \leq l-1$.

On the other hand, if $n-(k-1)a < 0$, then

$$vb = n-(tb+u')a \leq ab, \Rightarrow v \leq a \leq l-1.$$

also implying that $v \leq l-1$.

Thus, if n is an integer such that $ab \leq n \leq a^* + b^* - ab$, then $n = ua + vb$ where $0 \leq u \leq k-1$ and $0 \leq v \leq l-1$. Hence, $n \in A+B$. □

Remark 1.2 *Lemma 1.5 implies that $A+B$ contains an interval of consecutive integers. Specifically,*

$$[ab, a^* + b^* - ab] \subset A+B$$

Lemma 1.6 *Let $A = \{0, a, 2a, \ldots, (k-1)a = a^*\}$ and $B = \{0, b, 2b, \ldots, (l-1)b = b^*\}$, $\gcd(a,b) = 1$. If $x \in A+B$, then $a^* + b^* - x \in A+B$.*

Proof.

Let $x = ia + jb \in A + B$ where $0 \le i \le k-1$, $0 \le j \le l-1$. Then

$$\begin{aligned} a^* + b^* - x &= (k-1)a + (l-1)b - (ia + jb) \\ &= [(k-1) - i]a + [(l-1) - j]b \\ &= i'a + j'b \end{aligned}$$

where $i' = (k-1) - i$, $0 \le i' \le k-1$ and $j' = (l-1) - j$, $0 \le j' \le l-1$. Thus $a^* + b^* - x \in A + B$. □

Theorem 1.1 *Let* $A = \{0, a, 2a, \ldots, (k-1)a = a^*\}$ *and* $B = \{0, b, 2b, \ldots, (l-1)b = b^*\}$, $\gcd(a, b) = 1$, *where* $k - 1 \ge b$, *and* $l - 1 \ge a$. *Then*

$$A + B = C \cup [c, a^* + b^* - c] \cup a^* + b^* - C \tag{1.3}$$

where $c = (a-1)(b-1)$ *and* $C \subseteq [0, c-2]$. *Moreover,*

$$|A + B| = a^* + b^* - ab + a + b \quad or \quad ka + lb - ab \tag{1.4}$$

Proof.

Lemma 1.5 indicates that $[ab, a^* + b^* - ab] \subset A + B$. If we let $c = ab - a - b + 1 = (a-1)(b-1)$, Lemma 1.3 further indicates that $[c, ab) \subset A + B$. By Lemma 1.6, the symmetry of arithmetic progressions and their sum, we have, $(a^* + b^* - ab, a^* + b^* - c] \subset A + B$. Let $C = \{n \mid n = ia + jb,\ \ i \ge 0,\ \ 0 \le j \le a-1,\ \ 0 \le n < (a-1)b - a\}$. Since $(a-1)b - a \notin U$, $C = U$, and $C = [0, c-2] \cap (A + B)$. By symmetry, $a^* + b^* - C \subset A + B$. Put all these together, we have the structure

$$A + B = C \cup [c, \quad a^* + b^* - c] \cup a^* + b^* - C.$$

Since $|C| = (a-1)(b-1)/2$ and $|[c, a^* + b^* - c]| = a^* + b^* - 2c + 1$, we have the cardinality:

$$\begin{aligned} |A+B| &= a^* + b^* - 2c + 1 + 2((a-1)(b-1)/2) \\ &= a^* + b^* - 2(a-1)(b-1) + 1 + (a-1)(b-1) \\ &= a^* + b^* - (a-1)(b-1) + 1 \\ &= a^* + b^* - ab + a + b \\ \text{or } |A+B| &= (k-1)a + (l-1)b - ab + a + b = ka + lb - ab \end{aligned}$$

□

Corollary 1.1 *Let* $A = \{0, a, 2a, \ldots, (k-1)a = a^*\}$ *and* $B = \{0, b, 2b, \ldots, (l-1)b = b^*\}$, $\gcd(a,b) = 1$. *Let* h_1 *and* h_2 *be positive integers such that* $h_1(k-1) \geq b$ *and* $h_2(l-1) \geq a$, *then*

$$\begin{aligned} h_1A + h_2B &= C \cup [c, h_1a^* + h_2b^* - c] \cup h_1a^* + h_2b^* - C \\ |h_1A + h_2B| &= h_1a^* + h_2b^* - ab + a + b \end{aligned}$$

where $c = (a-1)(b-1)$ *and* $C \subseteq [0, c-2]$.

Proof.

Note that h_1A and h_2B are also arithmetic progressions where

$$\begin{aligned} h_1A &= \{0, a, 2a, \ldots, h_1a^*\} = \{0, a, 2a, \ldots, h_1(k-1)a\} \\ h_2B &= \{0, b, 2b, \ldots, h_2b^*\} = \{0, b, 2b, \ldots, h_2(l-1)b\} \end{aligned}$$

Apply the sets h_1A and h_2B to Theorem 1.1 by using h_1a^* and h_2a^* in equations (1.3) and (1.4) instead of a^* and b^*, we have the result:

$$\begin{aligned} h_1A + h_2B &= C \cup [c, h_1a^* + h_2b^* - c] \cup h_1a^* + h_2b^* - C \\ |h_1A + h_2B| &= h_1a^* + h_2b^* - ab + a + b \end{aligned}$$

where $c = (a-1)(b-1)$ and $C \subseteq [0, c-2]$. □

Remark 1.3 *For h_1, h_2 sufficiently large, $|h_1A + h_2B| = h_1a^* + h_2b^* - \rho$ is a first degree function in h_1 and h_2 with a constant term $\rho = ab - a - b$.*

Let $A_1, \ldots, A_r$ be r arithmetic progressions, such that

$$A_i = \{a_i, a_i + \delta_i, a_i + 2\delta_i, \ldots, a_i + (k_i - 1)\delta_i\} \quad \text{for} \quad i = 1, \ldots, r$$

If $\gcd(\delta_1, \ldots, \delta_r) = \delta \neq 1$, we can normalize $A_1, \ldots, A_r$ in the following way:

$$A_i^{(N)} = \frac{A_i - a_i}{\delta} = \{0, \delta_i', 2\delta_i', \ldots, (k_i - 1)\delta_i'\}, \text{ where } \delta_i' = \delta_i/\delta$$

Thus, $\gcd(\delta_i', \ldots, \delta_r') = 1$. Then

$$h_iA_i^{(N)} = \frac{h_iA_i - h_ia_i}{\delta}$$

or

$$h_iA_i = h_ia_i + \delta \cdot h_iA_i^{(N)}$$

Therefore,

$$h_1A_1 + \cdots + h_rA_r = \sum_{i=1}^{r} h_ia_i + \delta \cdot \sum_{i=1}^{r} h_iA_i^{(N)}$$

Thus, it suffices to study the structure of the normalized sets. [4]

Lemma 1.7 *Let $A_1, \ldots, A_r$ be r normalized arithmetic progressions such that*

$$A_i = \{0, a_i, 2a_i, \ldots, (k_i - 1)a_i = a_i^*\} \qquad \text{for } i = 1, \ldots, r \tag{1.5}$$

If $x \in A_1 + \cdots + A_r$, then $a_1^* + \cdots + a_r^* - x \in A_1 + \cdots + A_r$.

Proof.

If $x \in A_1 + \cdots + A_r$, then $x = n_1 a_1 + \cdots + n_r a_r$ for some n_i such that $0 \le n_i \le k_i - 1$. Then

$$\begin{aligned} a_1^* + \cdots + a_r^* - x &= (k_1 - 1)a_1 + \cdots + (k_r - 1)a_r - (n_1 a_1 + \cdots + n_r a_r) \\ &= (k_1 - 1 - n_1)a_1 + \cdots + (k_r - 1 - n_r)a_r \\ &= n_1' a_1 + \cdots + n_r' a_r \end{aligned}$$

where $n_i' = k_i - 1 - n_i$ and $0 \le n_i' \le k_i - 1$. Thus, $a_1^* + \cdots + a_r^* - x \in A_1 + \cdots + A_r$. □

Corollary 1.2 *Let $A_1, \ldots, A_r$ be r normalized arithmetic progressions defined in equation (1.5). Let $h_1, \ldots, h_r$ be positive integers, then if $x \in h_1 A_1 + \cdots + h_r A_r$, then $h_1 a_1^* + \cdots + h_r a_r^* - x \in h_1 A_1 + \cdots + h_r A_r$.*

Proof.

Note that for $i = 1, \ldots, r$,

$$h_i A_i = \{0, a_i, 2a_i, \ldots, h_i(k_i - 1)a_i = h_i a_i^*\}$$

is an arithmetic progression. Thus, using the result of Lemma 1.7, we have $h_1 a_1^* + \cdots + h_r a_r^* - x \in h_1 A_1 + \cdots + h_r A_r$. □

We call this property the symmetry property of the arithmetic progression.

Theorem 1.2 *Let $A_1, A_2, \ldots, A_r$ be r arithmetic progressions such that*

$$A_i = \{0, a_i, 2a_i, \ldots, (k_i - 1)a_i = a_i^*\} \text{ for each } i = 0, 1, \ldots, r$$

where $\gcd(a_1, a_2, \ldots, a_r) = 1$. *For all k_i sufficiently large, there exists a nonnegative integer c, and a set $C \subseteq [0, c-2]$ such that*

$$A_1 + A_2 + \cdots + A_r = C \cup [c,\ a_1^* + \cdots + a_r^* - c] \cup a_1^* + \cdots + a_r^* - C$$

and

$$|A_1 + \cdots + A_r| = a_1^* + \cdots + a_r^* - \rho$$

for some constant ρ independent of k_i.

Proof. Define

$$m_i = a_1^* + \cdots + a_i^*$$

Prove by induction: When $r = 2$, Theorem 1.1 shows that there exists an integer c and a set $C \subseteq [0, c-2]$ such that

$$\begin{aligned} A_1 + A_2 &= C \cup [c, a_1^* + a_2^* - c] \cup a_1^* + a_2^* - C \\ &= C \cup [c, m_2 - c] \cup m_2 - C \end{aligned}$$

and

$$|A_1 + A_2| = a_1^* + a_2^* - a_1a_2 + a_1 + a_2 = m_2 - \rho$$

where $\rho = a_1a_2 - a_1 - a_2$.

Assume true for $r-1$. For $i = 1, \ldots, r-1$, let c_i denote the smallest integer ≥ 0 such that $[c_i, m_i - c_i] \subseteq A_1 + \cdots + A_i$, then $c_i - 1 \notin A_1 + \cdots + A_i$. Also note that since $0 \in A_i$ for each $i = 1, \ldots, r$, $A_1 + \cdots + A_j \subseteq A_1 + \cdots A_i$ for all $j \leq i$. Thus $c_j \geq c_i$ and $[c_j, m_j - c_j] \subseteq [c_i, m_i - c_i]$ for all $j \leq i$. Therefore,

$$0 \leq c_{r-1} \leq c_{r-2} \leq \cdots \leq c_2 = a_1 a_2 - a_1 - a_2 + 1.$$

Also denote $C_i = (A_1 + \cdots + A_i) \cap [0, c_i - 2]$. Thus by the inductive assumption,

$$A_1 + \cdots + A_{r-1} = C_{r-1} \ \cup \ [c_{r-1}, m_{r-1} - c_{r-1}] \ \cup \ (m_{r-1} - C_{r-1}).$$

We want to show the same structure for sum of r sets:

$$\begin{aligned} & A_1 + \cdots + A_{r-1} + A_r \\ = \ & (C_{r-1} \ \cup \ [c_{r-1}, m_{r-1} - c_{r-1}] \ \cup \ (m_{r-1} - C_{r-1})) \ + \ A_r \\ = \ & (C_{r-1} + A_r) \ \cup \ ([c_{r-1}, m_{r-1} - c_{r-1}] + A_r) \ \cup \ ((m_{r-1} - C_{r-1}) + A_r) \quad (1.6) \end{aligned}$$

Let us first consider

$$[c_{r-1}, m_{r-1} - c_{r-1}] + A_r = \bigcup_{j=0}^{k_r - 1} [c_{r-1}, m_{r-1} - c_{r-1}] + ja_r \qquad (1.7)$$

If k_i is sufficiently large, a_i^* will be sufficiently large so that for $j = 0, 1, \ldots, k_r - 1$,

$$m_{r-1} - c_{r-1} + ja_r \geq c_{r-1} + (j+1)a_r$$

Then the intervals on the right hand side of equation (1.7) will overlap. therefore,

$$\begin{aligned} [c_{r-1}, m_{r-1} - c_{r-1}] + A_r \ &= \ [c_{r-1}, \ \ m_{r-1} - c_{r-1} + a_r^*] \\ &= \ [c_{r-1}, \ \ m_r - c_{r-1}] \end{aligned}$$

Let us now consider the other sets in equation (1.6). Since $C_{r-1} \subseteq [0, c_{r-1} - 2]$, we have

$$C_{r-1} + A_r \subseteq [0, a_r^* + c_{r-1} - 2]$$

also

$$\begin{aligned}(m_{r-1} - C_{r-1}) + A_r &\subseteq [m_{r-1} - c_{r-1} + 2,\ m_{r-1} + a_r^*] \\ &= m_r - [0,\ a_r^* + c_{r-1} - 2]\end{aligned}$$

By Corollary 1.2, the sum of arithmetic progressions is symmetric, thus we only need to study $C_{r-1} + A_r$.

Define c_r to be the smallest integer ≥ 0 such that $[c_r, m_r - c_r] \subseteq A_1 + \cdots + A_r$. Note that $0 \leq c_r \leq c_{r-1} \leq \cdots \leq c_2$ and $c_r - 1 \notin A_1 + \cdots + A_r$ otherwise $c_r - 1$ is the smallest integer such that $[c_r - 1,\ m_r - c_r + 1] \subseteq A_1 + \cdots + A_r$ contradicting our assumption of c_r.

We will examine the elements of $C_{r-1} + A_r$ in three disjoint intervals:

$$\begin{aligned}C_{r-1} + A_r &= (C_{r-1} + A_r) \cap [0, c_r - 2] \bigcup \\ &\quad (C_{r-1} + A_r) \cap [c_r, c_{r-1}] \bigcup \\ &\quad (C_{r-1} + A_r) \cap [c_{r-1} + 1, a_r^* + c_{r-1} - 2]\end{aligned}$$

Claim

$$(C_{r-1} + A_r) \cap [c_r, c_{r-1}] = [c_r, c_{r-1}] \subset A_1 + \cdots + A_r$$

Otherwise we have an element, say d, such that $0 \leq c_r < d \leq c_{r-1}$ and d is the smallest integer ≥ 0 that satisfies $[d, m_r - d] \subseteq A_1 + \cdots + A_r$, thus implying $d - 1 \notin A_1 + \cdots + A_r$. But $c_r \leq d - 1$, contradicting the fact that c_r is the smallest integer that satisfies $[c_r, m_r - c_r] \subseteq A_1 + \cdots + A_r$. Also

$$(C_{r-1} + A_r) \cap [c_{r-1} + 1,\ a_r^* + c_{r-1} - 2] \subset [c_{r-1}, m_r - c_{r-1}]$$

$$\subset A_1 + \cdots + A_{r-1}$$

$$\subset A_1 + \cdots + A_r$$

Thus, we have

$$\begin{aligned}
A_1 + \cdots + A_r &= (C_{r-1} + A_r) \bigcup ([c_{r-1}, m_{r-1} - c_{r-1}] + A_r) \bigcup \{(m_{r-1} - C_{r-1}) + A_r\} \\
&= \{(C_{r-1} + A_r) \cap [0, c_r - 2]\} \bigcup [c_r, c_{r-1}] \bigcup [c_{r-1}, m_r - c_{r-1}] \\
&\quad \bigcup [m_r - c_{r-1}, m_r - c_r] \bigcup \{m_r - \{(C_{r-1} + A_r) \cap [0, c_r - 2]\}\} \\
&= C_r \bigcup [c_r, m_r - c_r] \bigcup m_r - C_r \\
&= C_r \bigcup [c_r, a_1^* + \cdots + a_r^* - c_r] \bigcup a_1^* + \cdots + h_r a_r^* - C_r
\end{aligned}$$

where $C_r = (C_{r-1} + A_r) \cap [0, c_r - 2]$. Let $C = C_r$ and $c = c_r$, we then have proven the theorem. Furthermore,

$$\begin{aligned}
| A_1 + \cdots + A_r | &= m_r - \rho \\
&= |C_r| + a_1^* + \cdots + a_r^* - 2c_r + 1 + |C_r| \\
&= a_1^* + \cdots + a_r^* - \rho
\end{aligned}$$

where $\rho = 2c_r - 1 - 2|C_r|$ is a constant independent of k_i. □

Corollary 1.3 *Let $A_1, A_2, \ldots, A_r$ be r arithmetic progressions such that*

$$A_i = \{0, a_i, 2a_i, \ldots, (k_i - 1)a_i = a_i^*\} \text{ for each } i = 0, 1, \ldots, r$$

where $\gcd(a_1, a_2, \ldots, a_r) = 1$. For all h_i sufficiently large, there exists a nonnegative integer c, and a set $C \subseteq [0, c-2]$ such that

$$h_1 A_1 + h_2 A_2 + \cdots + h_r A_r = C \cup [c,\ h_1 a_1^* + \cdots + h_r a_r^* - c] \cup h_1 a_1^* + \cdots + h_r a_r^* - C$$

and

$$|h_1A_1 + \cdots + h_rA_r| = h_1a_1^* + \cdots + h_ra_r^* - \rho$$

for some constant ρ independent of h_i.

Proof.

Note that for $i = 1, \ldots, r$, each h_iA_i is an arithmetic progression where

$$h_iA_i = \{0, a, 2a, \ldots, h_i(k_i - 1) = h_ia_i^*\}$$

For h_i sufficiently large, we can apply Theorem 1.2 to $\sum_{i=1}^{r} h_iA_i$, so there exist integers c and the set $C \subseteq [0, c-2]$ such that

$$\begin{aligned} h_1A_1 + \cdots + h_rA_r &= C \cup [c, h_ia_i^* + \cdots + h_ia_r^* - c] \cup h_1a_1^* + \cdots + h_ra_r^* - C \\ |h_1A_1 + \cdots + h_rA_r| &= h_1a_1^* + \cdots + h_ra_r^* - \rho \end{aligned}$$

where $\rho = 2c - 1 - 2|C_r|$ which is a constant independent of h. □

In conclusion of this section, because of the symmetry in the sum of arithmetic progressions, for $h_i's$ sufficiently large, the cardinality of the sum of the arithmetic progressions in a linear form is a linear function in $h_1, \ldots, h_r$. Its structure consists of C and $\sum h_ia_i^* - C$, and an interval of consecutive integers. The set C is contained in a finite set and the cardinality of C does not change as $h_1, \ldots, h_r$ grows into infinity.

1.3 The structure of the sum of finite sets of integers in a linear form

Let $A_1, \ldots, A_r$ be any arbitrary finite sets of integers, let $h_1, \ldots, h_r$ be positive integers. In this section, the structure of $h_1A_1 + \cdots + h_rA_r$ is determined for $h_1, \ldots, h_r$ sufficiently large. Nathanson had determined its structure for $r = 1$ and had shown that hA contains an interval of consecutive integers and that the cardinality of hA is a linear function of h. The result can be generalized to the sum of r finite sets of integers in a linear form.

An arbitrary finite set A of integers is called "normalized" if it consists of 0 and a nonempty set of relatively prime positive integers. If A is a finite set of integers with $|A| \geq 2$, we can normalize A as follows. Let a_0 be the least element of A, and let δ be the greatest common divisor of the positive integers of the form $a - a_0$ for $a \in A$. The normalized form of A is the set

$$A^{(N)} = \left\{ \frac{a - a_0}{\delta} \mid a \in A \right\}$$

Then

$$A = a_0 + \delta \cdot A^{(N)}$$

Let h be a positive integer, then

$$hA = ha_0 + \delta \cdot hA^{(N)}$$

Theorem 1.3 *(Nathanson)*

Let $k \geq 2$ and let $A = \{a_0, a_1, \ldots, a_{k-1}\}$ be a finite set of integers such that

$$0 = a_0 < a_1 < \cdots < a_{k-1}$$

and $\gcd(a_1, \ldots, a_{k-1}) = 1$. *Then there exist integers c and d and sets $C \subseteq [0, c-2]$ and $D \subseteq [0, d-2]$ such that*

$$hA = C \cup [c, ha_{k-1} - d] \cup (ha_{k-1} - D)$$

for all $h \geq max(1, (k-2)(a_{k-1} - 1)a_{k-1})$. [6]

Nathanson's Theorem has shown that hA contains a set C, an interval of consecutive integers, and the set $ha_{k-1} - D$ which is a translation of set D. The cardinality of sets C and D are constants independent of h, because, as h grows to infinity, sets C and D remain the same. Therefore, the cardinality of hA depends on the number of integers in the interval $[c, ha_{k-1} - d]$ which depends on h. Hence, we have a linear function in h for the cardinality of hA.

We say that the system of sets $A_1, \ldots, A_r$ is normalized, if each A_i is a finite set of nonnegative integers, if $0 \in A_i$ for $i = 1, \ldots, r$, and if $\bigcup_{i=1}^{r} A_i \backslash \{0\}$ is a nonempty set of relatively prime positive integers.

Let $A_1, \ldots, A_r$ be arbitrary nonempty finite sets of integers such that $|A_i| \geq 2$ for all i. We shall normalize this system of sets as follows. Let $a_{i,0}$ be the smallest element in A_i. Let δ be the greatest common divisor of the integers in the set

$$\bigcup_{i=1}^{r} \{a_{i,j} - a_{i,0} \mid a_{i,j} \in A_i\}.$$

Let

$$A_i^{(N)} = \left\{ \frac{a_{i,j} - a_{i,0}}{\delta} \mid a_{i,j} \in A_i \right\}.$$

The system of sets $A_1^{(N)}, \ldots, A_r^{(N)}$ is normalized, and

$$A_i = a_{i,0} + \delta \cdot A_i^{(N)}$$

for all $i = 1, \ldots, r$. For any positive integers $h_1, \ldots, h_r$, we have

$$\sum_{i=1}^{r} h_i A_i = \left\{ \sum_{i=1}^{r} h_i a_{i,0} \right\} + \delta \cdot \sum_{i=1}^{r} h_i A_i^{(N)}$$

To study the sum of arbitrary finite sets of integers in a linear form, it suffices to study the sum of a normalized system of finite sets of integers. [4]

Let A be a set of nonnegative integers that contains 0. Let $\gcd(A)$ denote the greatest common divisor of the elements of A. Let

$$a^* = \max(A)$$

We define the reflected set

$$\hat{A} = a^* - A = \{a^* - a \mid a \in A\}$$

The $\hat{A}$ is also a set of nonnegative integers that contains 0, and

$$\begin{aligned} \max(\hat{A}) &= \max(A) = a^* \\ \gcd(\hat{A}) &= \gcd(A) \end{aligned}$$

and

$$\hat{\hat{A}} = A$$

For any positive integer h, we have $0 \in hA$, and

$$\max(hA) = ha^*.$$

and so

$$\begin{aligned} h\hat{A} &= \left\{ \sum_{j=1}^{h} (a^* - a_j) \mid a_j \in A \right\} \\ &= ha^* - \left\{ \sum_{j=1}^{h} a_j \mid a_j \in A \right\} \\ &= ha^* - hA \\ &= \hat{hA}. \end{aligned}$$

Lemma 1.8 *Let $A_1, \ldots, A_r$ be a normalized system of finite sets of integers, and let $a_i^* = \max(A_i)$ for $i = 1, \ldots, r$. The reflected sets $\hat{A}_1, \ldots, \hat{A}_r$ also form a normalized system. For any integer x,*

$$x \in \sum_{i=1}^{r} h_i \hat{A}_i$$

if and only if

$$\sum_{i=1}^{r} h_i a_i^* - x \in \sum_{i=1}^{r} h_i A_i.$$

[4]

Proof.

For $i = 1, \ldots, r$, let $\delta_i = \gcd(A_i)$. If the system $A_1, \ldots, A_r$ is normalized, then

$$1 = \gcd\left(\bigcup_{i=1}^{r} A_i \backslash \{0\} \right) = (\delta_1, \ldots, \delta_r).$$

Since, $\gcd(\hat{A}_i) = \gcd(A_i) = \delta_i$, it follows that

$$\gcd\left(\bigcup_{i=1}^{r} \hat{A}_i \backslash \{0\} \right) = (\delta_1, \ldots, \delta_r) = 1.$$

and so the system $\hat{A}_1, \ldots, \hat{A}_r$ is also normalized.

If

$$x \in \sum_{i=1}^{r} h_i \hat{A}_i = \sum_{i=1}^{r} (h_i a_i^* - h_i A_i),$$

then there exist integers $b_i \in h_i A_i$ such that

$$x = \sum_{i=1}^{r} (h_i a_i^* - b_i),$$

and so

$$\sum_{i=1}^{r} h_i a_i^* - x \;=\; \sum_{i=1}^{r} b_i \;\in\; \sum_{i=1}^{r} h_i A_i.$$

Conversely, if

$$\sum_{i=1}^{r} h_i a_i^* - x \in \sum_{i=1}^{r} h_i A_i$$

then there exist integers $b_i \in h_i A_i$ such that

$$\sum_{i=1}^{r} h_i a_i^* - x = \sum_{i=1}^{r} b_i$$

but then we have

$$x = \sum_{i=1}^{r} h_i a_i^* - \sum_{i=1}^{r} b_i \;\in\; \sum_{i=1}^{r} h_i a_i^* - \sum_{i=1}^{*} h_i A_i$$

But

$$\sum_{i=1}^{r} h_i a_i^* - \sum_{i=1}^{*} h_i A_i \;=\; \sum_{i=1}^{r} (h_i a_i^* - h_i A_i) \;=\; \sum_{i=1}^{*} h_i \hat{A}_i \;=\; \sum_{i=1}^{r} h_i \hat{A}_i$$

Thus, we have $x \in \sum_{i=1}^{r} h_i \hat{A}_i$. □

Theorem 1.4 *Let $A_1, \ldots, A_r$ be a normalized system of finite sets of integers. Let $a_i^* = \max(A_i)$ for $i = 1, \ldots, r$. There exist integers c and d and finite sets*

$$C \subseteq [0, c-2] \qquad \text{and} \qquad D \subseteq [0, d-2]$$

and there exist integers $h_1^*, \ldots, h_r^*$ *such that, if* $h_i \geq h_i^*$ *for all* $i = 1, \ldots, r$, *then*

$$h_1 A_1 + \cdots + h_r A_r = C \cup \left[c, \sum_{i=1}^{r} h_i a_i^* - d\right] \cup \left(\sum_{i=1}^{r} h_i a_i^* - D\right).$$

Moreover, there exists a nonnegative integer ρ *independent of* h *such that*

$$|h_1 A_1 + \cdots + h_r A_r| = \sum_{i=1}^{r} h_i a_i^* - \rho$$

Proof.

For $i = 1, \ldots, r$, let

$$A_i = \{a_{i,0}, a_{i,1}, \ldots, a_{i,k_i-1}\},$$

where $k_i = |A_i|$, and

$$0 = a_{i,0} < a_{i,1} < \cdots < a_{i,k_i-1} = a_i^*.$$

For $i = 1, \ldots, r$, let

$$\delta_i = \gcd(a_{i,1}, \ldots, a_{i,k_i})$$

Since $\bigcup_{i=1}^{r} A_i \backslash \{0\}$ is a nonempty set of relatively prime positive integers, it follows that $\gcd(\delta_1, \ldots, \delta_r) = 1$. Let

$$A_i' = \left\{\frac{a_{i,j}}{\delta_i} \mid a_{i,j} \in A_i\right\},$$

then

$$\begin{aligned} A_i &= \delta_i \cdot A_i' \\ h_i A_i &= \delta_i \cdot h_i A_i' \end{aligned}$$

we have $\gcd(A_i') = 1$. Let

$$\max(A_i') = b_i^* = \frac{a_i^*}{\delta_i} = \frac{a_{i,k_i-1}}{\delta_i}$$

Applying Theorem 1.3 to each of the set A_i', we have for h_i sufficiently large that there exist integers c_i and d_i and sets C_i and D_i such that $C_i \subseteq [0, c_i - 2]$ and $D_i \subseteq [0, d_i - 2]$,

$$h_i A_i' = C_i \cup [c_i, h_i b_i^* - d_i] \cup (h_i b_i^* - D_i).$$

Then

$$\begin{aligned}
\delta_i \cdot h_i A_i' &= \delta_i \cdot C_i \cup \delta_i \cdot [c_i, h_i b_i^* - d_i] \cup \delta_i \cdot (h_i b_i^* - D_i) \\
&= \delta_i \cdot C_i \cup (\delta_i c_i + \delta_i \cdot [0, h_i b_i^* - c_i - d_i]) \cup (\delta_i h_i b_i^* - \delta_i \cdot D_i) \\
&= \delta_i \cdot C_i \cup (\delta_i c_i + \delta_i \cdot [0, h_i b_i^* - c_i - d_i]) \cup (h_i a_i^* - \delta_i \cdot D_i)
\end{aligned}$$

Note that for $i = 1, \ldots, r$, $\gcd(\delta_1, \ldots, \delta_r) = 1$, so we have that $\delta_i \cdot [0, h_i b_i^* - c_i - d_i]$ is a system of arithmetic progressions in the normalized form. Thus, by Theorem 1.2, we have for all $h_i \geq h_i'$, h_i' sufficiently large, there exists a nonnegative integer c' and a set $C' \subseteq [0, c' - 2]$ such that

$$\begin{aligned}
&\sum_{i=1}^{r} \delta_i \cdot [0, h_i b_i^* - c_i - d_i] \\
&= C' \cup [c', \sum_{i=1}^{r} \delta_i (h_i b_i^* - c_i - d_i) - c'] \cup \sum_{i=1}^{r} \delta_i (h_i b_i^* - c_i - d_i) - C' \\
&= C' \cup [c', \sum_{i=1}^{r} (h_i a_i^* - \delta_i c_i - \delta_i d_i) - c'] \cup \sum_{i=1}^{r} (h_i a_i^* - \delta_i c_i - \delta_i d_i) - C'
\end{aligned}$$

Thus, we have

$$\begin{aligned}
\sum_{i=1}^{r} (\delta_i c_i + \delta \cdot [0, \quad h_i b_i^* - c_i - d_i]) &= \sum_{i=1}^{r} \delta_i c_i + \left[c', \quad \sum_{i=1}^{r} h_i a_i^* - \delta_i c_i - \delta_i d_i - c'\right] \\
&= \left[c' + \sum_{i=1}^{r} \delta_i c_i, \quad \sum_{i=1}^{r} \delta_i c_i + \sum_{i=1}^{r} (h_i a_i^* - \delta_i c_i - \delta_i d_i) - c'\right] \\
&= [c' + \sum_{i=1}^{r} \delta_i c_i, \quad \sum_{i=1}^{r} (h_i a_i^* - \delta_i d_i) - c'] \\
&\subseteq h_1 A_1 + \cdots + h_r A_r
\end{aligned}$$

Let c and d be the nonnegative integers with the property that $[c, \sum h_i a_i^* - d]$ is the largest interval of integers contained in $h_1A_1 + \cdots + h_rA_r$. This implies that

$$c - 1 \notin \sum h_i A_i$$

and

$$d - 1 \notin \sum h_i a_i^* - \sum h_i A_i.$$

We see that

$$\begin{aligned} 0 \leq c &\leq c' + \sum_{i=1}^{r} \delta_i c_i \\ 0 \leq d &\leq c' + \sum_{i=1}^{r} \delta_i d_i \end{aligned}$$

thus, c and d are bounded and are constants independent of h_i. Let

$$\begin{aligned} C &= [0, c-2] \cap (h_1A_1 + \cdots + h_rA_r) \\ D &= [0, d-2] \cap \left(\sum_{i=1}^{r} h_i a_i^* - h_1A_1 + \cdots + h_rA_r \right) \end{aligned}$$

Then

$$h_1A_1 + \cdots + h_rA_r = C \cup [c, \sum h_i a_i^* - d] \cup \sum_{i=1}^{r} h_i a_i^* - D$$

We need to show that C and D are independent of h_i. Let $a_{i,0} = \min(A_i \backslash \{0\})$, let $b_i \in h_iA_i \backslash (h_i - 1)A_i$, then for all $h_i \geq c$,

$$\sum_{i=1}^{r} b_i \geq \sum_{i=1}^{r} h_i a_{i,0} \geq c \quad \Rightarrow \quad \sum_{i=1}^{r} b_i \notin C$$

This implies that result from the sum of $h_iA_i \backslash (h_i - 1)A_i$ does not show up in the set C. Thus, C is stabilized. Let $\rho_1 = |C|$, then ρ_1 is independent of h_i.

Similarly, let

$$\hat{a_{i,0}} = \min(\hat{A}_i \backslash \{0\}) = \min(a_i^* - a_i \mid a_i \in A_i \backslash \{0\})$$

And let

$$\hat{b_i} \in h_i\hat{A}_i \backslash (h_i - 1)\hat{A}_i$$

Then for all $h_i \geq d$,

$$\sum_{i=1}^{r} \hat{b_i} \geq \sum_{i=1}^{r} h_i \hat{a_{i,0}} \geq d$$

This implies that $\sum \hat{b_i} \notin D$, by Lemma 1.8, this implies $\sum b_i \notin \sum h_i a_i^* - D$. This means new result from the sum of h_iA_i does not show up in D, hence, in $\sum h_i a_i^* - D$. Thus we say D is stabilized. Let $\rho_2 = |D|$, then ρ_2 is independent of h_i.

It follows that for all nonnegative integers $h_1, \ldots, h_r$, such that if

$$h_i \geq h_i^* = \max\{h_i', c, d\},$$

then there exist sets $C \subseteq [0, c-2]$ and $D \subseteq [0, d-2]$ such that

$$h_1A_1 + \cdots + h_rA_r = C \cup \left[c, \sum_{i=1}^{r} h_i a_i^* - d\right] \cup \left(\sum_{i=1}^{r} h_i a_i^* - D\right).$$

Furthermore, we conclude

$$\begin{aligned} |h_1A_1 + \cdots + h_rA_r| &= \rho_1 + \sum_{i=1}^{r} h_i a_i^* - c - d + 1 + \rho_2 \\ &= \sum_{i=1}^{r} h_i a_i^* - \rho \end{aligned}$$

where $\rho = c + d - \rho_1 - \rho_2 - 1$ which is a constant independent of h. □

In conclusion, if we consider the sum of arbitrary finite sets of integers in a linear form, for $h_i's$ sufficiently large, the structure consists of an interval of consecutive integers depending on the $h_i's$. Its cardinality is a linear function in $h_1, \ldots, h_r$.

Chapter 2

The structure of sumsets in the case of the lattice points

2.1 Introduction

One of the conclusions of Chapter One is that if A is a finite set of integers, hA consists of an interval of consecutive integers and the cardinality of hA is a linear function of h. In this chapter, we consider a finite set, A, of lattice points in $\mathbf{Z}^n$. Khovanskii was able to find a polytope such that hA contains all of the lattice points in the polytope. Khovanskii called this polytope $\triangle(h, C)$. The cardinality of hA is bounded by the cardinality of $\triangle_{hA} \cap \mathbf{Z}^n$ and $\triangle(h, C) \cap \mathbf{Z}^n$ which is a function of h^n.

In the first section of this chapter, we will go over the notations used throughout the chapter. In the second section of the chapter, the author will present Khovanskii's theorems concerning the sets $h \cdot \triangle_A$, $\triangle(h, C)$, and hA, with proofs provided by the author. In the last section of this chapter, the author will generalize Khovanskii's theorems to sets in the linear form, $h_1A_1 + \cdots + h_rA_r$ where $A_1, \ldots, A_r$ are subsets of $\mathbf{Z}^n$, and $h_1, \ldots, h_r$ are positive integers. The author will estimate the cardinality of $h_1A_1 + \cdots + h_rA_r$ for A_i the subsets of $\mathbf{Z}^2$.

Let A be a finite subset of $\mathbf{Z}^n$, $\mathbf{Z}^n \subset \mathbf{R}^n$. Denote the convex hull of A by $\triangle_A$. Throughout most of the paper, we assume that A contains the origin. Since otherwise we may consider the shifted set $A - a$, where $a \in A$. Let $A = \{a_i\}_{i=1}^k$ where $k = |A|$ is the cardinality of A. Thus, we define $\triangle_A$ for A that contains the origin to be

$$\triangle_A = \left\{\sum \lambda_i a_i \in \mathbf{R}^n \mid a_i \in A,\ \lambda_i \in \mathbf{R},\ 0 \le \lambda_i \le 1, \sum \lambda_i \le 1\right\}$$

Let h be a positive integer, we define h times the convex hull of A as:

$$h \cdot \triangle_A = \{h\gamma \in \mathbf{R}^n \mid \gamma \in \triangle_A\}$$

Lemma 2.1

$$h \cdot \triangle_A = \left\{\sum \lambda_i a_i \mid a_i \in A,\ \lambda_i \in \mathbf{R},\ \lambda_i \ge 0,\ \sum \lambda_i \le h\right\}$$

Proof.

Let $x \in h \cdot \triangle_A$ such that $x = h\gamma$ where $\gamma \in \triangle_A$. But by definition of $\triangle_A$, if we let $a_i \in A$, then $\gamma = \sum \lambda_i a_i$ for some $\lambda_i \in \mathbf{R}$, and $\sum \lambda_i \le 1$. Therefore,

$$x = h\gamma = h\sum \lambda_i a_i = \sum h\lambda_i a_i \qquad \text{where} \qquad \sum h\lambda_i = h\sum \lambda_i \le h$$

On the other hand, let $x \in h \cdot \triangle_A$ such that $x = \sum \lambda_i a_i$ where $a_i \in A$ and $\sum \lambda_i \le h$. Let $\delta_i = \frac{\lambda_i}{h}$, then

$$\begin{aligned} x &= \sum \lambda_i a_i = \sum h\left(\frac{\lambda_i}{h}\right) a_i \\ &= h\sum \delta_i a_i \end{aligned}$$

where

$$\sum \delta_i = \sum \frac{\lambda_i}{h} = \frac{\sum \lambda_i}{h} \leq \frac{h}{h} = 1$$

thus, if let $\gamma = \sum \delta_i a_i$ then $\gamma \in \triangle_A$ and $x = h\gamma$. □

We define the h-fold sumset of convex hull of A as

$$h\triangle_A = \{\gamma_1 + \cdots + \gamma_h \mid \gamma_i \in \triangle_A\}$$

Lemma 2.2 $h \cdot \triangle_A = h\triangle_A$.

Proof.

Let $x \in h \cdot \triangle_A$ such that $x = h\gamma$ for some $\gamma \in \triangle_A$. Note that

$$x = h\gamma = \underbrace{\gamma + \cdots + \gamma}_{h \text{ times}}$$

Thus $x \in h\triangle_A$.

Conversely, let $x \in h\triangle_A$, such that $x = \gamma_1 + \cdots + \gamma_h$ where $\gamma_i \in \triangle_i$. For $i = 1, \ldots, h$, let $\gamma_i = \sum \lambda_{ij} a_j$, where $a_i \in A$ and $\sum_j \lambda_{ij} \leq 1$. Then

$$x = \gamma_1 + \cdots + \gamma_h = \sum \lambda_{1j} a_j + \cdots + \sum \lambda_{hj} a_j$$

Let

$$\delta_j = \lambda_{1j} + \cdots + \lambda_{hj}$$

Then

$$x = \sum \delta_j a_j \quad \text{where} \quad \sum \delta_j = \sum_{i=1}^{h} \sum_{j} \lambda_{ij} \leq h$$

Thus, $x \in h \cdot \triangle_A$. □

We also define the h-fold sumset of the finite subset A of $\mathbf{Z}^n$ as

$$\begin{aligned} hA &= \{a_1 + \cdots + a_h \mid a_i \in A\} \\ &= \left\{\sum h_i a_i \mid a_i \in A,\ h_i \in \mathbf{Z},\ h_i \geq 0,\ \sum h_i \leq h\right\} \end{aligned}$$

Denote by Δ_{hA} to be the convex hull of the set hA, defined by:

$$\Delta_{hA} = \left\{\sum \lambda_i b_i \in \mathbf{R}^n \mid b_i \in hA,\ \lambda_i \in \mathbf{R},\ 0 \leq \lambda_i \leq 1,\ \sum \lambda_i \leq 1\right\}$$

Lemma 2.3 $h \cdot \Delta_A = h\Delta_A = \Delta_{hA}$.

Proof.

The first part of the equality is proven by Lemma 2.2. It remains to show that $h \cdot \Delta_A = \Delta_{hA}$. Let $x \in h \cdot \Delta_A$, then from the definition,

$$x = \sum \lambda_i a_i, \quad \text{where} \quad a_i \in A,\ \lambda_i \in \mathbf{R},\ \lambda_i \geq 0,\ \sum \lambda_i \leq h.$$

Let

$$\delta_i = \frac{\lambda_i}{h} \quad \text{and} \quad b_i = ha_i$$

Then

$$x = \sum \lambda_i a_i = \sum \left(\frac{\lambda_i}{h}\right)(ha_i) = \sum \delta_i b_i$$

But $b_i \in hA$ and $\delta_i \geq 0$. Moreover,

$$\sum \delta_i = \sum \frac{\lambda_i}{h} = \frac{\sum \lambda_i}{h} \leq 1$$

Thus, $x \in \Delta_{hA}$, implying that $h \cdot \Delta_A \subset \Delta_{hA}$.

Conversely, let $|A| = k$ and $|hA| = k'$. And if $x \in \Delta_{hA}$, then

$$x = \sum_{i=1}^{k'} \lambda_i b_i \quad \text{where} \quad b_i \in hA,\ \lambda_i \in \mathbf{R},\ \lambda_i \geq 0,\ \sum \lambda_i \leq 1.$$

Since $b_i \in hA$, for $i = 1, \ldots, k'$, there are integers $h_{i1}, \ldots, h_{ik}$ such that

$$b_i = h_{i1}a_1 + \cdots + h_{ik}a_k, \qquad \text{where} \quad \sum_{j=1}^{k} h_{ij} \leq h$$

Then

$$x = \sum_{i=1}^{k'} \lambda_i b_i = \sum_{i=1}^{k'} \lambda_i \left(\sum_{j=1}^{k} h_{ij} a_j \right) = \sum_{j=1}^{k} \sum_{i=1}^{k'} \lambda_i h_{ij} a_j$$

Let

$$\delta_j = \sum_{i=1}^{k'} \lambda_i h_{ij},$$

for $j = 1, \ldots, k$. Then

$$x = \sum_{j=1}^{k} \delta_j a_j$$

where

$$\begin{aligned} \sum_{j=1}^{k} \delta_j &= \sum_{j=1}^{k} \sum_{i=1}^{k'} \lambda_i h_{ij} \\ &= \sum_{i=1}^{k'} \lambda_i \sum_{j=1}^{k} h_{ij} \\ &\leq \sum_{i=1}^{k'} \lambda_i h \\ &= h \sum_{i=1}^{k'} \lambda_i \\ &\leq h \cdot 1 \\ &= h \end{aligned}$$

□

Let $A_1, \ldots, A_r$ be finite subsets of $\mathbf{Z}^n$, $\mathbf{Z}^n \subset \mathbf{R}^n$, and $\triangle_{A_1}, \ldots, \triangle_{A_r}$ be their convex hulls, respectively. Let $h_1, \ldots, h_r$ be positive integers, then

$$\begin{aligned} h_1 \triangle_{A_1} + \cdots + h_r \triangle_{A_r} &= \triangle_{h_1 A_1} + \cdots + \triangle_{h_r A_r} \\ &= \{\gamma_1 + \cdots + \gamma_r \in \mathbf{R}^n \mid \gamma_i \in \triangle_{h_i A_i}\} \end{aligned}$$

and the sum of $A_1, \ldots, A_r$ in the linear form is

$$h_1 A_1 + \cdots + h_r A_r = \{\alpha_1 + \cdots + \alpha_r \in \mathbf{Z}^n \mid \alpha_i \in h_i A_i\}.$$

If for $i = 1, \ldots, r$,

$$A_i = \{a_{ij}\}_{j=1}^{k_i} \quad \text{and} \quad 0 \in A_i$$

where $k_i = |A_i|$ is the cardinality of A_i, then

$$\begin{aligned} &h_1 \triangle_{A_1} + \cdots + h_r \triangle_{A_r} \\ &\quad = \left\{ \sum_{i=1}^{r} \sum_{j=1}^{k_i} \lambda_{ij} a_{ij} \in \mathbf{R}^n \mid a_{ij} \in A_i,\ \lambda_{ij} \in \mathbf{R},\ \lambda_{ij} \geq 0, \text{ and } \sum_{j=1}^{k_i} \lambda_{ij} \leq h_i \right\} \end{aligned} \tag{2.1}$$

and the sum of $A_1, \ldots, A_r$ in the linear form is

$$\begin{aligned} &h_1 A_1 + \cdots + h_r A_r \\ &\quad = \left\{ \sum_{i=1}^{r} \sum_{j=1}^{k_i} h_{ij} a_{ij} \mid a_{ij} \in A_i,\ h_{ij} \in \mathbf{Z},\ h_{ij} \geq 0, \text{ and } \sum_{j=1}^{k_i} h_{ij} \leq h_i \right\} \end{aligned} \tag{2.2}$$

Throughout most of the chapter, we will assume that A_i contains the origin, thus we will work mostly with definitions (2.1) and (2.2).

Let x and y be two points in $\mathbf{R}^n$, let $dist(x, y) = |x - y|$ denote the distance between x and y. Let X and Y be two finite subsets of $\mathbf{R}^n$. Define the distance between and sets to be

$$dist(X, Y) = \min_{\substack{x \in X \\ y \in Y}} dist(x, y)$$

Similarly, we define the distance between a point $x \in \mathbf{R}^n$ and the set $Y \subset \mathbf{R}^n$ to be

$$dist(x, Y) = \min_{y \in Y} dist(x, y)$$

Also let ∂X denote the boundary of the set X. Throughout the paper, we will make numerous references to $\partial \triangle_{hA}$ which will mean the boundary of the convex hull of hA.

Also throughout the paper we will make references to polytopes. Here, a polytope is the convex hull of a finite subset of $\mathbf{R}^n$. By lattice polytope we mean a polytope whose vertices are lattice points of $\mathbf{R}^n$.

2.2 The structure of the h-fold sumset of a finite set in $\mathbf{Z}^n$

Let A be a finite subset of $\mathbf{Z}^n$, $\mathbf{Z}^n \subset \mathbf{R}^n$. Let h be a positive integer. Khovanskii had shown that for large h, if A generates $\mathbf{Z}^n$, then the cardinality of hA is of order $V_n(\triangle_A)h^n$, where $V_n(\triangle_A)$ is the volume of the convex hull of A in $\mathbf{R}^n$. The author will present Khovanskii's theorems in this section. See [5].

Let A be a finite subset of $\mathbf{Z}^n$ containing the origin, such that the subgroup generated by the elements of A coincides with the group $\mathbf{Z}^n$. Let $|A| = k$ be the cardinality of A. Let X be a subset of lattice points in $\mathbf{Z}^n$ defined in the following way:

$$X = \{x \in \mathbf{Z}^n \mid x = \sum \lambda_i a_i,\ 0 \leq \lambda_i \leq 1,\ a_i \in A\}$$

Lemma 2.4 *X is finite.*

Proof.

If $x \in X$, then $x = \sum \lambda_i a_i$ such that $0 \leq \lambda_i \leq 1$, where $a_i \in A$. This implies

$$\begin{aligned} |x| &= |\sum_{i=1}^{k} \lambda_i a_i| \\ &\leq \sum_{i=1}^{k} \lambda_i |a_i| \end{aligned}$$

$$\leq \; k \max_i |a_i|$$

There are finitely many lattice points whose distance from the origin is bounded by $k \max |a_i|$, thus, X is finite. □

For every $x \in X$, we fix a representation of the form $x = \sum p_i(x) a_i$, where $p_i(x) \in \mathbf{Z}$. Such a representation exists because the elements $a_i \in A$ generate the group $\mathbf{Z}^n$. Define

$$C = \max_{x \in X} \sum_{i=1}^{k} |p_i(x)|$$

Next, we will define a polytope, $\triangle(h, C)$, which is a subset of $\triangle_{hA}$:

$$\triangle(h,C) = \left\{ \sum_{i=1}^{k} \lambda_i a_i \in \mathbf{R}^n \mid a_i \in A,\ \lambda_i \in \mathbf{R},\ \lambda_i \geq C,\ \sum_{i=1}^{k} \lambda_i \leq h - C \right\}. \tag{2.3}$$

We note that for h sufficiently large, $\triangle(h, C) \neq \emptyset$.

Theorem 2.1 *Let A be a finite subset of $\mathbf{Z}^n$ containing the origin. Let the group $Z^n(A)$ generated by the elements of A coincide with $\mathbf{Z}^n$. Then every lattice point of the polytope $\triangle(h, C)$ belongs to the sumset hA.*

Proof.

Let $|A| = k$. Let z be an arbitrary lattice point of $\triangle(h, C)$, then $z = \sum_{i=1}^{k} \lambda_i a_i$ for some $\lambda_i \in \mathbf{R}$, $\lambda_i \geq C$ and $\sum_{i=1}^{k} \lambda_i \leq h - C$.

Let $[\lambda_i]$ denote the greatest integer less than or equal to λ_i and let $\{\lambda_i\} = \lambda_i - [\lambda_i]$. Then

$$z \;=\; \sum_{i=1}^{k} \lambda_i a_i$$

$$
\begin{aligned}
&= \sum_{i=1}^{k}([\lambda_i] + \{\lambda_i\}a_i) \\
&= \sum_{i=1}^{k}[\lambda_i]a_i + \sum_{i=1}^{k}\{\lambda_i\}a_i
\end{aligned}
$$

Since z is a lattice point and $\sum_{i=1}^{k}[\lambda_i]a_i$ is a lattice point, thus $\sum_{i=1}^{k}\{\lambda_i\}a_i$ is a lattice point. Furthermore, $0 \leq \{\lambda_i\} \leq 1$. If we let $x = \sum_{i=1}^{k}\{\lambda_i\}a_i$, we have $x \in X$. Then x has a representation of the form $x = \sum_{i=1}^{k} p_i(x)a_i$, where $p_i(x) \in \mathbf{Z}$. Therefore,

$$
\begin{aligned}
z &= \sum_{i=1}^{k}[\lambda_i]a_i + x \\
&= \sum_{i=1}^{k}[\lambda_i]a_i + \sum p_i(x)a_i \\
&= \sum_{i=1}^{k} n_i a_i
\end{aligned}
$$

where $n_i = [\lambda_i] + p_i(x)$.

Since the set A contains the origin, the sumset hA consists of the points of the form $\sum_{i=1}^{k} n_i a_i$, where $a_i \in A$, $n_i \in \mathbf{Z}$, $n_i \geq 0$, and $\sum_{i=1}^{k} n_i \leq h$. We need to show that $z \in hA$.

For each i, we note that $[\lambda_i] > \lambda_i - 1 \geq C - 1$. Since C is an integer, this implies that $[\lambda_i] \geq C$. Hence,

$$n_i = [\lambda_i] + p_i(x) \geq C + p_i(x) \geq 0$$

Also,

$$
\begin{aligned}
\sum_{i=1}^{k} n_i &= \sum_{i=1}^{k}[\lambda_i] + p_i(x) \\
&= \sum_{i=1}^{k}[\lambda_i] + \sum_{i=1}^{k} p_i(x)
\end{aligned}
$$

$$\leq \sum_{i=1}^{k} \lambda_i + \sum_{i=1}^{k} |p_i(x)|$$
$$\leq h - C + C$$
$$= h$$

Thus, z belongs to hA. □

Let us index the elements of A:

$$A = \{a_i\}, \quad i = 1, \ldots, k$$

so that $a_1, \ldots, a_r$ are the vertices of the convex hull of A. The elements $a_{r+1}, \ldots, a_k$ are those elements of A that are in the interior of the convex hull of A.

Denote by $\partial\triangle_{hA}$ the boundary of $\triangle_{hA}$. Denote by $\partial\triangle(h, C)$ the boundary of $\triangle(h, C)$. The vertices of the convex set $\triangle_{hA}$ are $\{0, ha_1, \ldots, ha_r\}$. Define

$$a^* = C \cdot \sum_{i=1}^{k} a_i$$

We also notice that the vertices of the convex set $\triangle(h, C)$ are

$$\{a^*,\ a^* + (h - C(k+1))a_1,\ \ldots, a^* + (h - C(k+1))a_r\}.$$

The next lemma summarizes our observation about $\triangle(h, C)$.

Lemma 2.5 *Let A be a finite set of lattice points in $\mathbf{Z}^n$ containing 0, and A generates $\mathbf{Z}^n$, then*

$$\triangle(h, C) = a^* + \triangle_{h'A} \qquad \textit{where} \qquad h' = h - C(k+1)$$

Proof.

Let $|A| = k$. By (2.3), we have the definition

$$\triangle(h, C) = \left\{ \sum_{i=1}^{k} \lambda_i a_i \in \mathbf{R}^n \mid a_i \in A,\ \lambda_i \in \mathbf{R},\ \lambda_i \geq C,\ \sum_{i=1}^{k} \lambda_i \leq h - C \right\}$$

Since A contains the origin. We also have for the definition of $a^* + \triangle_{h'A}$,

$$a^* + \triangle_{h'A} = a^* + \left\{ \sum_{i=1}^{k} \lambda_i a_i \in \mathbf{R}^n \mid a_i \in A,\ \lambda_i \in \mathbf{R},\ \lambda_i \geq 0,\ \sum \lambda_i \leq h' \right\}$$

where $h' = h - (k+1)C$.

Let $x \in \triangle(h, C)$, then $x = \sum_{i=1}^{k} \lambda_i a_i$ for some $\lambda_i \in \mathbf{R}$ such that $\lambda_i \geq C$ and $\sum_{i=1}^{k} \lambda_i \leq h - C$. Thus,

$$x = \sum_{i=1}^{k} \lambda_i a_i = a^* + \sum_{i=1}^{k} (\lambda_i - C) a_i$$

where $\lambda_i - C \geq 0$, and

$$\begin{aligned} \sum_{i=1}^{k} (\lambda_i - C) &= \sum_{i=1}^{k} \lambda_i - kC \\ &\leq h - C - kC \\ &= h - (k+1)C \end{aligned}$$

Thus $x \in a^* + \triangle_{h'A}$.

On the other hand, let $x \in a^* + \triangle_{h'A}$, then $x = a^* + \sum_{i=1}^{k} \lambda_i a_i$ where $\lambda_i \geq 0$, and $\sum_{i=1}^{k} \lambda_i \leq h'$.

$$\begin{aligned} x &= a^* + \sum_{i=1}^{k} \lambda_i a_i \\ &= \sum_{i=1}^{k} (\lambda_i + C) a_i \\ &= \sum_{i=1}^{k} \delta_i a_i \end{aligned}$$

where $\delta_i = \lambda_i + C$, thus $\delta_i \geq C$ and

$$\begin{aligned}\sum_{i=1}^{k}\delta_i &= \sum_{i=1}^{k}(\lambda_i + C)\\ &= \sum_{i=1}^{k}\lambda_i + kC\\ &\leq h' + kC\\ &= h - (k+1)C + kC\\ &= h - C\end{aligned}$$

Thus, $x \in \triangle(h, C)$. Hence, we have proven $\triangle(h, C) = a^* + \triangle_{h'A}$. □

Let us consider a simple example: Let A be a subset of $\mathbf{Z}^2$ consisting of three elements: {(0,0), (1,1), (1,0)}. Thus, $|A| = k = 3$, and the convex hull of A is a triangle. Let $h = 30$, then $\triangle_{hA}$ is the triangle with vertices $\{(0,0), (30,30), (30,0)\}$. If we let $C = 5$, then $\triangle(h, C)$ is the triangle with vertices $\{b_1,\ b_2,\ b_3\}$, where

$$\begin{aligned}b_1 &= a^* = 5(0,0) + 5(1,1) + 5(1,0) = (10,5)\\ b_2 &= a^* + (30 - 5(3+1))(1,1) = (10,5) + 10(1,1) = (20,15)\\ b_3 &= a^* + (30 - 5(3+1))(1,0) = (10,5) + 10(1,0) = (20,5)\end{aligned}$$

Please see Figure 1 for an illustration.

Lemma 2.6 *There exists a nonnegative real number ρ independent of h such that if $y \in \partial\triangle_{hA}$, then*

$$dist(y, \triangle(h, C)) \leq \rho$$

Proof.

Let $y \in \partial\triangle_{hA}$. Let F be the face that contains y. Suppose F contains the vertices $\{ha_{i_1}, \ldots, ha_{i_t}\}$ where t is a positive integer less than or equal to r and $a_{i_j} \in \{a_1, \ldots, a_r\}$ is the set of vertices of $\triangle_A$. Note that F is the convex hull of the set $\{ha_{i_j}\}_{j=1}^t$. Then

$$y = \sum_{j=1}^{t} \lambda_j h a_{i_j} \qquad \text{where} \qquad \sum \lambda_j = 1$$

Let x be an element such that

$$x = a^* + \sum \lambda_j h' a_{i_j}$$

where $h' = h - (k+1)C$, then $x \in \triangle(h, C)$. Thus,

$$\begin{aligned} dist(y, \triangle(h,C)) &\leq |y - x| \\ &= \left| \sum \lambda_j h a_{i_j} - (a^* + \sum \lambda_j h' a_{i_j}) \right| \\ &\leq |a^*| + |h - h'| \left| \sum \lambda_j a_{i_j} \right| \\ &\leq |a^*| + (k+1)C \left(\sum_{j=1}^{t} |a_{i_j}| \right) \\ &\leq |a^*| + (k+1)C \left(\sum_{i=1}^{r} |a_i| \right) \end{aligned}$$

Let $\rho = |a^*| + (k+1)C\,(\sum |a_i|)$. Since the expression of ρ is independent of h, this proves that ρ is independent of h, thus proves the lemma. □

Theorem 2.2 *Let $P_1, \ldots, P_r$ be lattice polytopes in $\mathbf{R}^n$. Let $h_1, \ldots, h_r$ be integers ≥ 0. Define*

$$h_i P_i = \{\lambda p \mid \lambda \in \mathbf{R},\ 0 \leq \lambda \leq h_i,\ p \in P_i\}$$

then the cardinality $|(h_1 P_1 + \cdots + h_r P_r) \cap \mathbf{Z}^n|$ is a polynomial in $h_1, \ldots, h_r$.

[1]

When $r = 1$, we have the explicit formula

$$|(hP) \cap Z^n| = a_n h^n + a_{n-1} h^{n-1} + \cdots + a_1 h + a_0$$

The polynomial is called the Ehrhart Polynomial, because Ehrhart was the first to study the "polynomiality" of the number of lattice points in a polytope. This polynomial was later shown to have the coefficients:

$$a_n = V_n(P), \quad a_{n-1} = \frac{1}{2} V_{n-1}(\sum_{f \in F} f), \quad \text{and } a_0 = V_0 = 1$$

where V_i is the volume computed in its ith dimension, F is the set of all faces of P, and f is a face of P. [3]

Theorem 2.3 *Let A be a finite subset of $\mathbf{Z}^n$. Suppose that the group $\mathbf{Z}^n(A)$ generated by the differences in the elements of A coincides with $\mathbf{Z}^n$. Then the ratio of the number of points lying in hA to the number $V_n(\triangle_A)h^n$ tends to 1 as $h \to \infty$, where $V_n(\triangle_A)$ is the volume of the convex hull of A.*

Proof.

The convex hull, $\triangle_A$, of A is a lattice polytope. Applying the Ehrhart Polynomial to $h\triangle_A$ and applying Lemma 2.3 which says $\triangle_{hA} = h\triangle_A$, we have a formula for the cardinality of the lattice points contained in $\triangle_{hA}$:

$$|\triangle_{hA} \cap \mathbf{Z}| = |h\triangle_A \cap \mathbf{Z}^n| = V_n(\triangle_A)h^n + a_{n-1}h^{n-1} + \cdots + a_0.$$

Lemma 2.5 and Lemma 2.3 give us the relationship

$$\triangle(h, C) = a^* + \triangle_{h'A} = a^* + h'\triangle_A$$

where $a^* \in \mathbf{Z}^n$. we have a similar formula for the cardinality of the lattice points contained in $\triangle(h, C)$:

$$\begin{aligned} |\triangle(h,C) \cap \mathbf{Z}^n| &= |h'\triangle_A \cap \mathbf{Z}^n| \\ &= V_n(\triangle_A)(h')^n + b_{n-1}(h')^{n-1} + \cdots + b_0 \\ &= V_n(\triangle_A)(h - C(k+1))^n + b_{n-1}(h - C(k+1))^{n-1} + \cdots + b_0 \\ &= V_n(\triangle_A)h^n + b'_{n-1}h^{n-1} + \cdots + b'_0 \end{aligned}$$

We can see that both $|\triangle_{hA} \cap \mathbf{Z}^n|$ and $|\triangle(h,C) \cap \mathbf{Z}^n|$ are of order $V_n(\triangle_A)h^n$ as $h \to \infty$. We also have the set relationship:

$$\triangle_{hA} \cap \mathbf{Z}^n \supseteq hA \supseteq \triangle(h,C) \cap \mathbf{Z}^n$$

thus the cardinality of hA is bounded above by the cardinality of $\triangle_{hA} \cap \mathbf{Z}^n$ and below by the cardinality of $\triangle(h,C) \cap \mathbf{Z}^n$:

$$|\triangle_{hA} \cap \mathbf{Z}^n| \geq |hA| \geq |\triangle(h,C) \cap \mathbf{Z}^n|$$

Both the upper and lower bounds are of order $V_n(\triangle_A)h^n$, therefore $|hA|$ is also of the order $V_n(\triangle_A)h^n$. In other words,

$$\frac{|hA|}{V_n(\triangle_A)h^n} \longrightarrow 1, \text{ as } h \longrightarrow \infty$$

□

Corollary 2.1 *Let $\mathbf{Z}^n(A)$ be the group generated by A. Suppose that the lattice $\mathbf{Z}^n(A)$ has a finite index in $\mathbf{Z}^n$, denote it by ind A. Then the ratio of the number of points lying in hA to $(ind\ A)^{-1}V_n(\triangle_A)h^n$ tends to 1 as $h \to \infty$.*

Proof.

We may assume that the set A is contained in the group $\mathbf{Z}^n(A)$, otherwise we consider a shifted set $A-a$, where $a \in A$. Let $u_1, \ldots, u_n$ be the basis of $\mathbf{Z}^n(A)$ and $e_1, \ldots, e_n$ be the basis of $\mathbf{Z}^n$. Let $F(\mathbf{Z}^n(A))$ denote the fundamental parallelepiped of the lattice $\mathbf{Z}^n(A)$ with respect to the basis $u_1, \ldots, u_n$. Let $F(\mathbf{Z}^n)$ denotes the fundamental parallelepiped of the lattice $\mathbf{Z}^n$ with respect to the basis $e_1, \ldots, e_n$. Then the ratio of the volumes of $F(\mathbf{Z}^n(A))$ to $F(\mathbf{Z}^n)$ is equal to the *ind* A. Let $V_n(\triangle_A, \mathbf{Z}^n(A))$ be the volume of the convex hull of A with respect to the lattice $\mathbf{Z}^n(A)$. Let $V_n(\triangle_A)$ be the volume of the convex hull of A with respect to the lattice $\mathbf{Z}^n$. Then

$$V_n(\triangle_A, \mathbf{Z}^n(A)) = \frac{V_n(\triangle_A)}{ind\ A} = (ind\ A)^{-1} V_n(\triangle_A)$$

Thus

$$\frac{hA}{(ind\ A)^{-1} V_n(\triangle_A) h^n} \longrightarrow 1, \quad \text{as } h \longrightarrow \infty.$$

□

2.3 The structure of the sum of finite sets in $\mathbf{Z}^n$ in a linear form

Let $A_1, \ldots, A_r$ be finite subsets of $\mathbf{Z}^n$, $\mathbf{Z}^n \subset \mathbf{R}^n$, and $h_1, \ldots, h_r$ be positive integers. The author will generalize Khovanskii's theorem concerning the cardinality of the set hA to the cardinality of the sums of sets in a linear form: $h_1A_1 + h_2A_2 + \cdots + h_rA_r$. We will use some basic concepts concerning sum of convex sets to prove the generalization of Khovanskii's theorem. The notation becomes much more complex. The result yields a mixed volume problem.

We will first prove some fundamental concepts concerning sum of convex sets.

Lemma 2.7 *Let K_1 and K_2 be two convex sets in $\mathbf{R}^n$. Then $K_1 + K_2$ is also convex.*

Proof.

Let $x, y \in K_1 + K_2$. We need to show that $\lambda x + (1-\lambda)y \in K_1 + K_2$ for some λ such that $0 \leq \lambda \leq 1$. Since $x \in K_1 + K_2$, there exist elements x_1, x_2 such that $x = x_1 + x_2$ wherer $x_1 \in K_1$ and $x_2 \in K_2$. Similarly, there exist y_1, y_2 such that $y = y_1 + y_2$ where $y_1 \in K_1$ and $y_2 \in K_2$.

Since K_1 and K_2 are convex, for some λ such that $0 \leq \lambda \leq 1$, we have

$$\begin{aligned} z_1 &= \lambda x_1 + (1-\lambda)y_1 \in K_1 \\ z_2 &= \lambda x_2 + (1-\lambda)y_2 \in K_2 \end{aligned}$$

then

$$\begin{aligned} \lambda x + (1-\lambda)y &= \lambda(x_1 + x_2) + (1-\lambda)(y_1 + y_2) \\ &= \lambda x_1 + (1-\lambda)y_1 + \lambda x_2 + (1-\lambda)y_2 \\ &= z_1 + z_2 \\ &\in K_1 + K_2 \end{aligned}$$

Thus, $K_1 + K_2$ is convex. □

Lemma 2.8 *Let K_1 and K_2 be two convex sets in $\mathbf{R}^n$. Let $y \in \partial(K_1 + K_2)$. Suppose $y = y_1 + y_2$ where $y_1 \in K_1$, and $y_2 \in K_2$, then $y_1 \in \partial K_1$ and $y_2 \in \partial K_2$.*

Proof.

Suppose either $y_1 \notin \partial K_1$ or $y_2 \notin \partial K_2$. Without loss of generality, we can assume that $y_1 \notin \partial K_1$, then $y_1 \in Int(K_1)$. Then there exists an open ball $B(y_1)$ centered around y_1 such that $B(y_1) \subset Int(K_1)$. But $B(y_1)+y_2$ is an open ball centered around y_1+y_2 such that $B(y_1)+y_2 \subset Int(K_1+K_2)$. Thus, $y = y_1+y_2$ is an element of the interior of K_1+K_2, contradicting our assumption that $y \in \partial(K_1+K_2)$. □

Lemma 2.9 *Let K be a convex set, let δ be a nonnegative real number. define*

$$K(\delta) = \{x \in K \mid dist(x, \partial K) \geq \delta\}$$

Then $K(\delta)$ is also a convex set.

Proof.

Let $x, y \in K(\delta)$, then $dist(x, \partial K) \geq \delta$ and $dist(y, \partial K) \geq \delta$. Let $z = \lambda x + (1-\lambda)y$, we need to show that $dist(z, \partial K) \geq \delta$.

Let $B_\delta(z)$ be a ball of radius δ around z. Let $z' \in B_\delta(z)$, then $|z'-z| \leq \delta$. Let $w = z'-z$. Then $w+x$ and $w+y$ are in $B_\delta(x)$ and $B_\delta(y)$ respectively. But both $B_\delta(x)$ and $B_\delta(y)$ are contained in K because $dist(x, \partial K) \geq \delta$ and $dist(y, \partial K) \geq \delta$. Thus, $w+x$ and $w+y$ are in K. Since K is convex,

$$\lambda(w+x) + (1-\lambda)(w+y) \in K$$

Then

$$\lambda(w+x) + (1-\lambda)(w+y) \;=\; w + \lambda x + (1-\lambda)y \;=\; z+w \;=\; z' \in K$$

This is true for all $z' \in B_\delta(z)$, thus $B_\delta(z) \subset K$. Furthermore, $B_\delta(z) \subset K$ implies that $dist(z, \partial K) \geq \delta$. Therefore, $z \in K(\delta)$, hence $K(\delta)$ is convex. □

If $K(\delta) \neq \emptyset$, then $K(\delta)$ is a convex set contained inside K. Throughout the rest of this chapter, we will assume that $K(\delta) \neq \emptyset$.

Lemma 2.10 *Let K be a convex set and K' a convex subset of K, then if $y \in \partial K$, then*

$$dist(y, K') = dist(y, \partial K')$$

Proof. By definition,

$$dist(y, K') = \min_{x \in K'} dist(y, x)$$

Let $x \in K'$ such that $dist(y, K') = dist(y, x)$. Suppose $x \notin \partial K'$, then $x \in Int(K')$. There exists an open ball of radius ϵ such that $B_\epsilon(x) \subset K'$. Then there exists an element $x_1 \in B_\epsilon(x) \subset K'$ such that $dist(y, x_1) < dist(y, x)$ contradicting our assumption that $dist(y, x)$ is the minimum distance between y and the elements of K'. Hence, $x \in \partial K'$. □

Let K_1, K_2 be two convex sets of $\mathbf{R}^n$. For $i = 1, 2$, define

$$K_i(\delta_i) = \{x \in K_i \mid dist(x, \partial K_i) \geq \delta_i\} \tag{2.4}$$

and define

$$D(K_i(\delta_i)) = \max_{y \in \partial K_i} dist(y, K_i(\delta_i)) \tag{2.5}$$

to be the maximum distance from the boundary of K_i to the convex subset $K_i(\delta_i)$. Also define

$$D(K_1(\delta_1) + K_2(\delta_2)) = \max_{y \in \partial(K_1 + K_2)} dist(y, K_1(\delta_1) + K_2(\delta_2)) \tag{2.6}$$

to be the maximum distance from the boundary of the sum $K_1 + K_2$ to the convex subset $K_1(\delta_1) + K_2(\delta_2)$.

Lemma 2.11

$$D(K_1(\delta_1) + K_2(\delta_2)) \leq D(K_1(\delta_1)) + D(K_2(\delta_2))$$

Proof.

Let $y \in \partial(K_1 + K_2)$ such that

$$dist(y, K_1(\delta_1) + K_2(\delta_2)) = D(K_1(\delta_1) + K_2(\delta_2))$$

There exist elements $y_1 \in K_1$ and $y_2 \in K_2$ such that $y = y_1 + y_2$. By Lemma 2.8, we have $y_1 \in \partial K_1$ and $y_2 \in \partial K_2$. Let $x_1 \in K_1(\delta_1)$ such that

$$dist(y_1, x_1) = dist(y_1, K_1(\delta_1))$$

Let $x_2 \in K_2(\delta_2)$ such that

$$dist(y_2, x_2) = dist(y_2, K_2(\delta_2))$$

Note that for $i = 1, 2$, $dist(y_i, K_i(\delta_i)) \leq D(K_i(\delta_i))$. Let $x = x_1 + x_2$, then $x \in K_1(\delta_1) + K_2(\delta_2)$. Therefore we have,

$$\begin{aligned}
D(K_1(\delta_1) + K_2(\delta_2)) &= dist(y, K_1(\delta_1) + K_2(\delta_2)) \\
&= \min_{z \in K_1(\delta_1) + K_2(\delta_2)} dist(y, z) \\
&\leq dist(y, x) \\
&= |y - x| \\
&= |y_1 + y_2 - (x_1 + x_2)|
\end{aligned}$$

$$
\begin{aligned}
&\leq |y_1 - x_1| + |y_2 + x_2| \\
&= dist(y_1, x_1) + dist(y_2, x_2) \\
&= dist(y_1, K_1(\delta_1)) + dist(y_2, K_2(\delta_2)) \\
&\leq D(K_1(\delta_1)) + D(K_2(\delta_2))
\end{aligned}
$$

□

Lemma 2.12 *Let $K_1, \ldots, K_r$ be r convex sets in $\mathbf{R}^n$. For $i = 1, \ldots, r$, let $K_i(\delta_i)$ be a convex subset of K_i defined by (2.4) and let $D(K_i(\delta_i))$ be the property of $K_i(\delta_i)$ defined by (2.5). Let*

$$D(K_1(\delta_1) + \cdots + K_r(\delta_r)) = \max_{y \in \partial K_1 + \cdots + K_r} dist(y, K_1(\delta_1) + \cdots + K_r(\delta_r))$$

$$D(K_1(\delta_1) + \cdots + K_r(\delta_r)) \leq D(K_1(\delta_1)) + \cdots + D(K_r(\delta_r))$$

Proof.

We will prove by induction. By Lemma 2.11, the statement is true for $r = 2$. Assume it is true for $r - 1$. Thus,

$$D(K_1(\delta_1) + \cdots + K_{r-1}(\delta_{r-1})) \leq D(K_1(\delta_1)) + \cdots + D(K_{r-1}(\delta_{r-1}))$$

Let $y \in \partial(K_1 + \cdots + K_r)$ such that

$$dist(y, K_1(\delta_1) + \cdots + K_r(\delta_r)) = D(K_1(\delta_1) + \cdots + K_r(\delta_r))$$

There exist elements $y_1 \in K_1 + \cdots + K_{r-1}$ and $y_2 \in K_r$ such that $y = y_1 + y_2$. By Lemma 2.8, we have

$$
\begin{aligned}
y_1 &\in \partial(K_1 + \cdots + K_{r-1}) \\
y_2 &\in \partial K_r
\end{aligned}
$$

Let $x_1 \in K_1(\delta_1) + \cdots + K_{r-1}(\delta_{r-1})$ such that

$$dist(y_1, x_1) = dist(y_1, K_1(\delta_1) + \cdots + K_{r-1}(\delta_{r-1}))$$

By the inductive hypothesis

$$\begin{aligned} dist(y_1, x_1) &= dist(y_1, K_1(\delta_1) + \cdots + K_{r-1}(\delta_{r-1})) \\ &\leq D(K_1(\delta_1) + \cdots + K_{r-1}(\delta_{r-1})) \\ &\leq D(K_1(\delta_1)) + \cdots + D(K_{r-1}(\delta_{r-1})) \end{aligned}$$

On the other hand, let $x_2 \in K_r(\delta_r)$ such that

$$dist(y_2, x_2) = dist(y_2, K_r(\delta_r)) \leq D(K_r(\delta_r))$$

Let $x = x_1 + x_2$, then $x \in K_1(\delta_1) + \cdots + K_{r-1}(\delta_{r-1}) + K_r(\delta_r)$. Therefore,

$$\begin{aligned} D(K_1(\delta_1) + \cdots + K_r(\delta_r)) &= dist(y, K_1(\delta_1) + \cdots + K_r(\delta_r)) \\ &= \min_{z \in K_1(\delta_1) + \cdots + K_r(\delta_r)} dist(y, z) \\ &\leq dist(y, x) \\ &= |y - x| \\ &= |y_1 + y_2 - (x_1 + x_2)| \\ &\leq |y_1 - x_1| + |y_2 - x_2| \\ &= dist(y_1, x_1) + dist(y_2, x_2) \\ &\leq D(K_1(\delta_1)) + \cdots + D(K_{r-1}(\delta_{r-1})) + D(K_r(\delta_r)) \end{aligned}$$

□

Let A_1 and A_2 be two finite subsets of $\mathbf{Z}^n$ such that each contains the origin and the subgroup generated by each set A_1 and A_2 is $\mathbf{Z}^n$. Let $\triangle_{h_1A_1}$ and $\triangle_{h_2A_2}$ be the convex hulls of h_1A_1 and h_2A_2. Let $\triangle_1(h_1, C_1)$ and $\triangle_2(h_2, C_2)$ be subsets of $\triangle_{h_1A_1}$ and $\triangle_{h_2A_2}$ respectively and define them similar to definition (2.3) from the previous section:

$$\triangle_i(h_i, C_i) = \left\{ \sum \lambda_{ij} a_{ij} \in \mathbf{R}^n \mid a_{ij} \in A_i,\ \lambda_{ij} \in \mathbf{R},\ \lambda_{ij} \geq C_i,\ \sum_j \lambda_{ij} \leq h_i - C_i \right\} \tag{2.7}$$

for $i = 1, 2$. By Lemma 2.6, there exists a positive real number ρ_i such that if $y \in \partial \triangle_{h_iA_i}$, then

$$dist(y,\ \triangle_i(h_i, C_i)) \leq \rho_i$$

Let us denote $\triangle_{h_iA_i}(\rho_i)$ to be the set such that

$$\triangle_{h_iA_i}(\rho_i) = \{x \in \triangle_{h_iA_i} \mid dist(x, \partial \triangle_{h_iA_i}) \geq \rho_i\}$$

we note that for h_i sufficiently large $\triangle_{h_iA_i}(\rho_i) \neq \emptyset$. It also follows from Lemma 2.9 that $\triangle_{h_iA_i}(\rho_i)$ is convex.

Lemma 2.13 *For h_i sufficiently large,*

$$\triangle_{h_iA_i}(\rho_i) \subseteq \triangle_i(h_i, C_i)$$

Proof.

For h_i sufficiently large, We note that $\triangle_{h_iA_i}(\rho_i)$ and $\triangle_i(h_i, C_i)$ are both nonempty convex subsets of $\triangle_{h_iA_i}$. Suppose that $\triangle_{h_iA_i}(\rho_i) \not\subseteq \triangle_i(h_i, C_i)$, there exists an element $y \in \partial \triangle_{h_iA_i}$ such that

$$dist(y, \triangle_{h_iA_i}(\rho_i)) \leq dist(y, \triangle_i(h_i, C_i)) \leq \rho_i$$

This implies that there is an element $x \in \triangle_{h_iA_i}(\rho_i)$ such that

$$dist(x,y) \leq \rho_i$$

contradicting our definition of $\triangle_{h_iA_i}(\rho_i)$. Thus, we have $\triangle_{h_iA_i}(\rho_i) \subseteq \triangle_i(h_i, C_i)$. □

Remark 2.1 *We have the relationship*

$$\triangle_{h_iA_i}(\rho_i) \quad \subseteq \quad \triangle_i(h_i, C_i) \quad \subseteq \quad \triangle_{h_iA_i}$$

Theorem 2.4 *Let A be a finite subset of $\mathbf{Z}^n$. Suppose that the group $\mathbf{Z}^n(A)$ generated by the differences of the elements of A coincides with $\mathbf{Z}^n$. Let h be a positive integer. Then for h sufficiently large, there exists a nonnegative real number ρ independent of h such that every latttice point of the polytope $\triangle_{hA}$ whose distance from the boundary of the polytope is more than or equal to ρ belongs to hA.*

Proof.

We can assume that A contains 0, otherwise, we can consider a shifted set $A - a$ for $a \in A$. By Lemma 2.6, there exists a nonnegative real number ρ such that for $y \in \partial\triangle_{hA}$, we have $dist(y, \triangle(h, C)) \leq \rho$. Also by Lemma 2.6, we let $\rho = |a^*| + (k+1)C(\sum |a_i|)$ which is independent of h. The set of lattice points whose distance from the boundary of $\triangle_{hA}$ is greater than or equal to ρ is precisely the set $\triangle_{hA}(\rho)$. By Lemma 2.13,

$$\triangle_{hA}(\rho) \subseteq \triangle(h, C)$$

Thus, by Theorem 2.1,

$$\triangle_{hA}(\rho) \cap \mathbf{Z}^n \ \subseteq \ \triangle(h, C) \cap \mathbf{Z}^n \ \subseteq hA$$

Proving the theorem. □

Although we know that each lattice point of $\triangle_i(h_i, C_i)$ belongs to h_iA_i, it does not guarantee that each lattice point of the sum $\triangle_1(h_1, C_1) + \triangle_2(h_2, C_2)$ is a sum of the lattice points from $\triangle_1(h_1, C_1)$ and $\triangle_2(h_2, C_2)$. Let m_i be a positive real number, we define a smaller set $\triangle_{h_iA_i}(\rho_i + m_i)$ in a similar manner:

$$\triangle_{h_iA_i}(\rho_i + m_i) = \{x \in \triangle_{h_iA_i} \mid dist(x, \partial\triangle_{h_iA_i}) \geq \rho_i + m_i\} \tag{2.8}$$

Specifically, if we look instead at the sum of the smaller sets,

$$\triangle_{h_1A_1}(\rho_1) + \triangle_{h_2A_2}(\rho_2 + 2\sqrt{n})$$

where n is the dimension of $\mathbf{Z}^n$, then we can show that every lattice point of $\triangle_{h_1A_1}(\rho_1)+ \triangle_{h_2A_2}(\rho_2 + 2\sqrt{n})$ is a sum of lattice points from $\triangle_1(h_1, C_1)$ and $\triangle_2(h_2, C_2)$.

Before presenting the next proof, we will first introduce a subset of $\mathbf{R}^n$ defined by:

$$R = \left\{\sum \lambda_i e_i \mid \lambda_i \in \mathbf{R},\ |\lambda_i| \leq 1\right\}$$

where e_i is the standard basis of $\mathbf{R}^n$. Let $r = \sum \lambda_i e_i$ be an element of R, then

$$\begin{aligned} |r| &\leq |\sum \lambda_i e_i| \\ &\leq |\sum e_i| \\ &= \sqrt{n} \end{aligned}$$

Theorem 2.5 *Let A_1 and A_2 be finite subsets of $\mathbf{Z}^n$. For $i = 1, 2$, let $\triangle_{h_iA_i}$ be the convex hull of h_iA_i, and let $\triangle_i(h_i, C_i)$ be defined by (2.7) and $\triangle_{h_iA_i}(\rho_i + m_i)$ be* *defined by (2.8). Then for* h_1 *and* h_2 *sufficiently large, every lattice point of the set* $\triangle_{h_1A_1}(\rho_1) + \triangle_{h_2A_2}(\rho_2 + 2\sqrt{n})$ *is an element of* $h_1A_1 + h_2A_2$.

Proof.

Let z be an lattice point of $\triangle_{h_1A_1}(\rho_1) + \triangle_{h_2A_2}(\rho_2 + 2\sqrt{n})$. Then there exist $z_1 \in \triangle_{h_1A_1}(\rho_1)$, and $z_2 \in \triangle_{h_2A_2}(\rho_2 + 2\sqrt{n})$ such that $z = z_1 + z_2$. If z_1 and z_2 are both lattice points, then we are done. Suppose they are not.

Let $z_1 = x_1 + y_1$ such that x_1 is a lattice point of $\triangle_{h_1A_1}(\rho_1)$ and $y_1 \in R$. Then,

$$|y_1| \;=\; |z_1 - x_1| \;\leq\; \sqrt{n}$$

Similarly, let $z_2 = x_2 + y_2$ such that x_2 is a lattice point of $\triangle_{h_2A_2}(\rho_2 + 2\sqrt{n})$ and $y_2 \in R$. Then,

$$|y_2| \;=\; |z_2 - x_2| \;\leq\; \sqrt{n}$$

Note that $y_1 + y_2$ is a lattice point, and

$$|y_1 + y_2| \;\leq\; |y_1| + |y_2| \;\leq\; 2\sqrt{n}$$

Thus, if we let

$$\begin{aligned} \overline{z}_1 &= x_1 \\ \overline{z}_2 &= x_2 + y_1 + y_2 \end{aligned}$$

then both $\overline{z}_1$ and $\overline{z}_2$ are lattice points. Since $\overline{z}_1 = x_1$ is a lattice point of $\triangle_{h_1A_1}(\rho_1)$ which is a subset of $\triangle_1(h_1, C_1)$, this implies that $\overline{z}_1$ is an element of h_1A_1.

Also, since x_2 is a lattice point of $\triangle_{h_2A_2}(\rho_2 + 2\sqrt{n})$ we have $\overline{z}_2 = x_2 + y_1 + y_2$ is a lattice point of $\triangle_{h_2A_2}(\rho_2)$ which is a subset of $\triangle_2(h_2, C_2)$. This implies that $\overline{z}_2$ is an element of h_2A_2. Thus,

$$z = z_1 + z_2 = \overline{z}_1 + \overline{z}_2 \in h_1A_1 + h_2A_2$$

□

Lemma 2.14 *Let A be a finite set of lattice points in $\mathbf{Z}^n$. Let h be a positive integer. Let ρ be a nonnegative real number independent of h. Then*

$$\triangle_{hA}(\rho) + \triangle_A \subseteq \triangle_{(h+1)A}(\rho).$$

Proof.

If $x_1 \in \triangle_{hA}(\rho)$, and $x_2 \in \triangle_A$. There exists an open ball $B_\rho(x_1)$ centered around x_1 with radius ρ such that $B_\rho(x_1) \subset \triangle_{hA}$, then $B_\rho(x_1) + x_2$ is an open ball centered around $x_1 + x_2$ with radius ρ such that

$$B_\rho(x_1) + x_2 \subset \triangle_{hA} + \triangle_A = h\triangle_A + \triangle_A = (h+1)\triangle_A = \triangle_{(h+1)A}$$

Thus, $x_1 + x_2 \in \triangle_{(h+1)A}(\rho)$. □

Lemma 2.15 *Let h_0 be the minimum nonnegative integer such that $\triangle_{h_0A}(\rho) \neq \emptyset$. Then for all $h \geq h_0$, $D(\triangle_{hA}(\rho))$ is a constant independent of h.*

Proof.

For all $h \geq h_0$, the set $\triangle_{hA}(\rho) \neq \emptyset$. Let $y \in \partial\triangle_{(h+1)A}$. There exist y_1 and y_2 such that $y_1 \in \partial\triangle_{hA}$ and $y_2 \in \partial\triangle_A$. Let $x_1 \in \triangle_{hA}(\rho)$ such that $dist(y_1, x_1) = dist(y_1, \triangle_{hA}(\rho))$. Also let $x_2 = y_2 \in \triangle_A$. Then $x = x_1 + x_2 \in \triangle_{(h+1)A}(\rho)$ by Lemma 2.14. Thus,

$$dist(y, \triangle_{(h+1)A}(\rho)) \leq dist(y, x)$$

$$
\begin{aligned}
&= |y - x| \\
&= |y_1 + y_2 - (x_1 + x_2)| \\
&= |y_1 - x_1| \\
&= dist(y, \triangle_{hA}(\rho)) \\
&\leq D(\triangle_{hA}(\rho))
\end{aligned}
$$

Since this is true for all $y \in \partial\triangle_{(h+1)A}$, we conclude that

$$D(\triangle_{(h+1)A}(\rho)) \leq D(\triangle_{hA}(\rho))$$

Hence, $D(\triangle_{hA}(\rho))$ is independent of h, for all $h \geq h_0$, □

Corollary 2.2 *There exists a nonnegative real number ρ independent of h_i such that every lattice point that is more than or equal to ρ distance away from the boundary of $\triangle_{h_1A_1} + \triangle_{h_2A_2}$ belongs to $h_1A_1 + h_2A_2$.*

Proof.

Let $\rho = D(\triangle_{h_1A_1}(\rho_1)) + D(\triangle_{h_2A_2}(\rho_2 + 2\sqrt{n}))$. By Lemma 2.15, we see that $D(\triangle_{h_iA_i})$ is independent of h_i, thus, ρ is independent of h_i. Define the set

$$(\triangle_{h_1A_1} + \triangle_{h_2A_2})(\rho) = \{x \in \triangle_{h_1A_1} + \triangle_{h_2A_2} \mid dist(x, \partial(\triangle_{h_1A_1} + \triangle_{h_2A_2})) \geq \rho\}$$

Claim that

$$(\triangle_{h_1A_1} + \triangle_{h_2A_2})(\rho) \subseteq \triangle_{h_1A_1}(\rho_1) + \triangle_{h_2A_2}(\rho_2 + 2\sqrt{n})$$

Suppose not. Then there exists an element $y \in \partial(\triangle_{h_1A_1} + \triangle_{h_2A_2})$ such that

$$dist(y, (\triangle_{h_1A_1} + \triangle_{h_2A_2})(\rho)) < dist(y, \triangle_{h_1A_1}(\rho_1) + \triangle_{h_2A_2}(\rho_2 + 2\sqrt{n}))$$

$$\leq D(\triangle_{h_1A_1}(\rho_1) + \triangle_{h_2A_2}(\rho_2 + 2\sqrt{n}))$$

$$\leq D(\triangle_{h_1A_1}(\rho_1)) + D(\triangle_{h_2A_2}(\rho_2 + 2\sqrt{n}))$$

$$= \rho$$

Thus, there exists an element $x \in (\triangle_{h_1A_1} + \triangle_{h_2A_2})(\rho)$ such that $dist(x, y) < \rho$ contradicting our assumption of the set.

By Theorem 2.5 every lattice point that is more than or equal to ρ distance away from the boundary $\partial(\triangle_{h_1A_1} + \triangle_{h_2A_2})$ belongs to $\triangle_{h_1A_1}(\rho_1) + \triangle_{h_2A_2}(\rho + 2\sqrt{n})$, thus, belongs to $h_1A_1 + h_2A_2$. □

Let $A_1, A_2, \ldots, A_r$ be finite subsets of $\mathbf{Z}^n$, $\mathbf{Z}^n \subset \mathbf{R}^n$, such that the subgroup generated by the elements of each set A_i coincides with the group $\mathbf{Z}^n$. Suppose that the cardinality $|A_i| = k_i$, for each $i = 1, \ldots, r$.

Let $\triangle_{h_iA_i}$ be the convex hull of h_iA_i and define $\triangle_i(h_i, C_i)$ the same as in equation (2.7). Also for each pair $\triangle_{h_iA_i}$ and $\triangle_i(h_i, C_i)$, there exists a real number ρ_i such that if $y \in \partial\triangle_{h_iA_i}$, then

$$dist(y,\ \triangle_i(h_i, C_i)) \leq \rho_i$$

Let $\triangle_{h_iA_i}(\rho_i)$ be a subset of $\triangle_{h_iA_i}$ defined in equation (2.8). Let m_i be a positive real number, we note the set relationship:

$$\triangle_{h_iA_i}(\rho_i + m_i) \subset \triangle_{h_iA_i}(\rho_i) \subset \triangle_i(h_i, C_i) \subset \triangle_{h_iA_i}$$

Thus, each lattice point of $\triangle_{h_iA_i}(\rho_i)$ belongs to h_iA_i.

Theorem 2.6 *Let $A_1, \ldots, A_r$ be finite subsets of $\mathbf{Z}^n$. For $i = 1, \ldots, r$, let $\triangle_i(h_i, C_i)$ be defined in equation (2.7), and $\triangle_i(\rho_i)$ be defined in equation (2.8). Then every lattice point of the set*

$$\triangle_{h_1A_1}(\rho_1) + \triangle_{h_2A_2}(\rho_2 + 2\sqrt{n}) + \cdots + \triangle_{h_rA_r}(\rho_r + 2\sqrt{n})$$

belongs to $h_1A_1 + \cdots + h_rA_r$.

Proof.

We will prove by induction. Theorem 2.5 shows that the statement is true for $r = 2$. Assume the statement is true for $r - 1$. Thus, every lattice point of the set

$$\triangle_{h_1A_1}(\rho_1) + \triangle_{h_2A_2}(\rho_2 + 2\sqrt{n}) + \cdots + \triangle_{h_{r-1}A_{r-1}}(\rho_{r-1} + 2\sqrt{n})$$

belongs to $h_1A_1 + \cdots + h_{r-1}A_{r-1}$.

Let z be a lattice point of the set $\triangle_{h_1A_1}(\rho_1) + \triangle_{h_2A_2}(\rho_2 + 2\sqrt{n}) + \cdots + \triangle_{h_rA_r}(\rho_r + 2\sqrt{n})$ Then there exist elements z_1 and z_2 such that $z = z_1 + z_2$ and

$$\begin{aligned} z_1 &\in \triangle_{h_1A_1}(\rho_1) + \triangle_{h_2A_2}(\rho_2 + 2\sqrt{n}) + \cdots + \triangle_{h_{r-1}A_{r-1}}(\rho_{r-1} + 2\sqrt{n}) \\ z_2 &\in \triangle_{h_rA_r}(\rho_r + 2\sqrt{n}) \end{aligned}$$

If z_1 and z_2 are lattice points, then we are done. Assume z_1 and z_2 are not lattice points. Let

$$z_1 = x_1 + y_1$$

such that x_1 is a lattice point of $\triangle_{h_1A_1}(\rho_1) + \triangle_{h_2A_2}(\rho_2 + 2\sqrt{n}) + \cdots + \triangle_{h_{r-1}A_{r-1}}(\rho_{r-1} + 2\sqrt{n})$, and $y_1 \in R$, then

$$|y_1| = |z_1 - x_1| \leq \sqrt{n}$$

Similarly, let

$$z_2 = x_2 + y_2$$

such that x_2 is a lattice point of $\triangle_{h_r A_r}(\rho_r + 2\sqrt{n})$, and $y_2 \in R$, then

$$|y_2| = |z_2 - x_2| \leq \sqrt{n}$$

Note that $y_1 + y_2$ is an integral point such that

$$|y_1 + y_2| \leq |y_1| + |y_2| \leq \sqrt{n} + \sqrt{n} = 2\sqrt{n}$$

Thus, if we let

$$\begin{aligned} \overline{z}_1 &= x_1 \\ \overline{z}_2 &= x_2 + y_1 + y_2 \end{aligned}$$

then both $\overline{z}_1$ and $\overline{z}_2$ are lattice points. Since x_1 is a lattice point of $\triangle_{h_1 A_1}(\rho_1) + \triangle_{h_2 A_2}(\rho_2 + 2\sqrt{n}) + \cdots + \triangle_{h_{r-1} A_{r-1}}(\rho_{r-1} + 2\sqrt{n})$, by the inductive hypothesis,

$$\overline{z}_1 = x_1 \in h_1 A_1 + \cdots + h_{r-1} A_{r-1}$$

Since x_2 is a lattice point of $\triangle_{h_r A_r}(\rho_r + 2\sqrt{n})$, we have $x_2 + y_1 + y_2$ is a lattice point of $\triangle_{h_r A_r}(\rho_r)$, thus implies

$$\overline{z}_2 = x_2 + y_1 + y_2 \in h_r A_r$$

Together,

$$z = z_1 + z_2 = \overline{z}_1 + \overline{z}_2 \in h_1 A_1 + \cdots + h_r A_r$$

□

Corollary 2.3 *There exists a nonnegative real number ρ independent of h such that every lattice point that is more than or equal to ρ distance away from the boundary $\triangle_{h_1A_1} + \cdots + \triangle_{h_rA_r}$ belongs to $h_1A_1 + \cdots + h_rA_r$.*

Proof. Let

$$\rho = D(\triangle_{h_1A_1}(\rho_1)) + D(\triangle_{h_2A_2}(\rho_2 + 2\sqrt{n})) + \cdots + D(\triangle_{h_rA_r}(\rho_r + 2\sqrt{n}))$$

By Lemma 2.15, we see that $D(\triangle_{h_iA_i}(\rho_i + m_i))$ is independent of h_i, thus, ρ is independent of h_i. Define

$$(\triangle_{h_1A_1}+\cdots+\triangle_{h_rA_r})(\rho) = \{x \in \triangle_{h_1A_1} + \cdots + \triangle_{h_rA_r} \mid dist(x, \partial(\triangle_{h_1A_1} + \cdots + \triangle_{h_rA_r}) \geq \rho\} \tag{2.9}$$

then we claim that

$$(\triangle_{h_1A_1} + \cdots + \triangle_{h_rA_r})(\rho) \subseteq \triangle_{h_1A_1}(\rho_1) + \triangle_{h_2A_2}(\rho_2 + 2\sqrt{n}) + \cdots + \triangle_{h_rA_r}(\rho_r + 2\sqrt{n})$$

The rest of proof is similar to the proof of Lemma 2.2 □

Let P be a lattice polytope in $\mathbf{R}^2$, then the Pick's identity says:

$$|P \cap \mathbf{Z}^2| = V(P) + \frac{|(\text{boundary of } P) \cap \mathbf{Z}^2|}{2} + 1$$

[3]. By using Pick's theorem we can derive a similar conclusion for sums of sets in a linear form $h_1A_1 + \cdots + h_rA_r$ in $\mathbf{Z}^2$ as Khovanskii did for sum of one set hA.

Theorem 2.7 *Let $A_1, \ldots, A_r$ be finite subsets of $\mathbf{Z}^2$ containing 0. Suppose that the group generated by the the elements of each set A_i coincides with $\mathbf{Z}^2$. Then*

$$\frac{|h_1A_1 + \cdots + h_rA_r|}{V(\triangle_{h_1A_1} + \cdots + \triangle_{h_rA_r})} \longrightarrow 1, \quad \textit{as each } h_i \longrightarrow \infty, \textit{ for all } i = 1, \ldots, r,$$

where $V(\triangle_{h_1A_1}+\cdots+\triangle_{h_rA_r})$ *is the volume of the sum of the convex hulls measured in* $\mathbf{R}^2$.

Proof.

Let $K=\triangle_{h_1A_1}+\cdots+\triangle_{h_rA_r}$, then K is a lattice polytope. Applying Pick's identity, we have:

$$|K\cap\mathbf{Z}^2| \;=\; V(K)+\frac{|(\text{boundary of } K)\cap\mathbf{Z}^2|}{2}+1$$

where

$$V(K)=\sum\sum V(\triangle_{A_i},\triangle_{A_j})h_ih_j$$

and the coefficient $V(\triangle_{A_i},\triangle_{A_j})$ is called the mixed volume of $\triangle_{A_i}$ and $\triangle_{A_j}$. [2]

Also

$$|(\text{boundary of } K)\cap\mathbf{Z}^2| \;\le\; \text{length of boundary of } K=\sum_{f\in F} l(f)$$

where F is the set of all faces of K and $l(f)$ is the length of a face of K. So $\sum l(f)$ measures the total length of the boundary of K. However, the boundary of K does not contribute significantly compared with $V(K)$ as $h_i\to\infty$. Since the boundary is of the order h_i and $V(K)$ is of the order h_ih_j. Thus

$$\frac{|K\cap Z^2|}{V(K)}\longrightarrow 1,\quad \text{as } h_i\longrightarrow\infty$$

On the other hand, let

$$\rho=D(\triangle_{h_1A_1}(\rho_1))+D(\triangle_{h_2A_2}(\rho_2+2\sqrt{n}))+\cdots+D(\triangle_{h_rA_r}(\rho_r+2\sqrt{n}))$$

which is independent of h_i, and let

$$K'=(\triangle_{h_1A_1}+\cdots+\triangle_{h_rA_r})(\rho)$$

be the set defined by (2.9). We estimate the cardinality of the lattice points in K':

$$\begin{aligned} |K' \cap \mathbf{Z}^2| &= |K \cap \mathbf{Z}^2| - |\text{ lattice points that are in } K \text{ but not in } K'\ | \\ &\geq |K \cap \mathbf{Z}^2| - \rho(\text{length of the boundary of } K) \end{aligned}$$

But ρ is independent of the h_i and the length of the boundary of K is of the order h_i, which does not contribute significantly compared with $|K \cap \mathbf{Z}^2|$ which is of the order $h_i h_j$. Thus $|K' \cap \mathbf{Z}^2|$ is also of the order as $|K \cap \mathbf{Z}^n|$ which is $V(K)$. Since $h_1 A_1 + \cdots + h_r A_r$ is bounded above by $K \cap \mathbf{Z}^2$ and below by $K' \cap \mathbf{Z}^2$,

$$|K \cap \mathbf{Z}^2| \geq |h_1 A_1 + \cdots + h_r A_r| \geq |K' \cap \mathbf{Z}^2|$$

So $|h_1 A_1 + \cdots + h_r A_r|$ is also of order $V(K)$. Thus

$$\frac{|h_1 A_1 + \cdots + h_r A_r|}{V(K)} = \frac{|h_1 A_1 + \cdots + h_r A_r|}{V(\Delta_{h_1 A_1} + \cdots + \Delta_{h_r A_r})} \longrightarrow 1, \quad \text{as } h_i \longrightarrow \infty$$

□

Chapter 3

The fine structure of sumsets in the case of $\mathbf{Z}^2$

3.1 Introduction

In the second chapter, we have found that the integral points that are ρ distance interior of the convex hull of hA belong to hA. This discovery has permitted us to use the volume of the convex hull for the approximation of the cardinality of hA. In the third chapter, we will instead look at the distribution of the elements of hA within ρ distance of the boundary. In the case of $\mathbf{Z}^2$, we not only have found that the cardinality of the elements of hA in the boundary area to be linear, we have also noticed a regular pattern in the distribution of these elements.

We will first go over some notations used in this chapter and present two simple examples in $\mathbf{Z}^2$. In the second section of this chapter, we will restrict our attention to the distribution of hA in the boundary region, where A is a subset of $\mathbf{Z}^2$. We will partition the boundary region of $\triangle_{hA}$ into congruent parallelograms. We find that the elements of hA in one parallelogram are a translation of the elements of hA in another parallelogram, thus indicating that the cardinality in each parallelogram is identical. Finally, in the third section of this chapter, we will put the result obtained from Chapter 2 together with the result obtained from Section 3.2 to give us a better idea of the distribution of the elements of hA in the case of $\mathbf{Z}^2$.

Let x, y, a, b be elements in $\mathbf{R}^2$. Let $l(x, y)$ denote the line segment connecting the two points x and y. Let $dist(a, b)$ denotes the distance between the two points a and b. The set

$$\{a \mid dist(a, l(x, y)) < \rho\}$$

denotes the set of all elements a such that a is less than ρ distance away from the line segment $l(x, y)$. Similarly, the set

$$\{a \mid dist(a, l(x, y)) = \rho\}$$

denotes the set of all elements a such that a is exactly ρ distance away from the line segment $l(x, y)$.

Let us look at some simple examples.

Suppose A is a set of integral points in $\mathbf{Z}^2$ such that A contains only three elements. Let $A = \{0, a_1, a_2\}$, where $0 = (0, 0)$ and $a_1 \neq ka_2$ for some real number k. The convex hull of A is a triangle. Let h be a positive integer, then

$$hA = \{k_1 a_1 + k_2 a_2 \mid k_1 = 0, 1, \ldots, h \text{ and } k_2 = 0, 1, \ldots, h - k_1\}$$

The cardinality of hA is

$$|hA| = \frac{(h+2)(h+1)}{2} = \frac{h^2}{2} + \frac{3h}{2} + 1$$

Looking at the boundary in particular:

$$|hA \cap boundary| = 3h$$

To compute the cardinality of hA in the boundary area with a thickness ρ, we define the following boundary areas:

$$\begin{aligned}
F_1 &= F_1(h,\rho) = \{a \in \triangle_{hA} \mid dist(a, l(0, ha_1) < \rho\} \\
F_2 &= F_2(h,\rho) = \{a \in \triangle_{hA} \mid dist(a, l(0, ha_2) < \rho\} \\
F_3 &= F_3(h,\rho) = \{a \in \triangle_{hA} \mid dist(a, l(ha_1, ha_2) < \rho\}
\end{aligned}$$

Let m_1, m_2, m_3 be three positive integers. Each m_i computes the number of layers of hA contained in F_i. A layer of hA consists of all those elements of hA that are the same distance away from one face of the boundary, for instance, $F_i \cap$ (boundary of $\triangle_{hA}$). We formally define m_i as follows:

$$\begin{aligned}
m_1 &= |\{n \in \text{ nonnegative integer}|dist(na_2, l(0, ha_1) < \rho\}| = |\{0, 1, \ldots, m_1 - 1\}| \\
m_2 &= |\{n \in \text{ nonnegative integer}|dist(na_1, l(0, ha_2) < \rho\}| = |\{0, 1, \ldots, m_2 - 1\}| \\
m_3 &= |\{n \in \text{ nonnegative integer}|dist(ha_1 - na_1, l(ha_1, ha_2) < \rho\}| = |\{0, 1, \ldots, m_3 - 1\}|
\end{aligned}$$

The cardinality of hA in the boundary areas can be computed:

$$\begin{aligned}
|hA \cap (F_1 \cup F_2 \cup F_3)| &= |hA \cap F_1| + |hA \cap F_2| + |hA \cap F_3| \\
&\quad - |hA \cap (F_1 \cap F_2)| - |hA \cap (F_2 \cap F_3)| - |hA \cap (F_1 \cap F_3)|
\end{aligned}$$

Note that here we make the assumption that ρ is small in comparison to the set $\triangle_{hA}$ so that $F_1 \cap F_2 \cap F_3 = \emptyset$.

To compute the cardinality of hA contained in each F_i, we notice that $F_i \cap$ (boundary of $\triangle_{hA}$) contains $h+1$ elements of hA. We call this the 0th layer. Each jth layer contains $(h+1)-i$ elements of hA, thus

$$\begin{aligned} |hA \cap F_i| &= \sum_{j=0}^{m_i-1} h+1-i \\ &= hm_i + \frac{3m_i}{2} - \frac{m_i^2}{2} \end{aligned}$$

and

$$|hA \cap (F_i \cap F_j)| = m_i m_j$$

Then the number of elements of hA that are less than ρ distance of the boundary of the convex hull of hA is

$$\begin{aligned} |hA \cap (F_1 \cup F_2 \cup F_3)| &= \sum_{i=1}^{3} hm_i + \frac{3m_i}{2} - \frac{m_i^2}{2} - \sum_{i<j} m_i m_j \\ &= Ch - D \end{aligned}$$

Since m_1, m_2, m_3 are constants, we have C and D are constants where

$$\begin{aligned} C &= m_1 + m_2 + m_3 \\ D &= \sum_{i=1}^{3} \frac{m_i^2 - 3m_i}{2} + \sum_{i<j} m_i m_j \end{aligned}$$

Please see Figure 2 for an illustration.

Next, we look at the set $A = \{0, a_1 = (n_1, 0), a_2 = (0, n_2), a_3 = (n_1, n_2)\}$, where $n_i \in \mathbf{Z}$. We can also easily see that the convex hull of A is a rectangle, and the set hA consist of elements in this form:

$$hA = \{k_1 a_1 + k_2 a_2 \mid k_1 = 0, 1, \ldots, h, \text{ and } k_2 = 0, 1, \ldots, h\}$$

thus the cardinality can be computed easily:

$$|hA| = (h+1)^2 = h^2 + 2h + 1$$

Clearly, the distribution of the elements of hA in the boundary area is regular, see Figure 3. Thus we can easily figure out the number of hA in the boundary:

$$|hA \cap boundary| = 4h$$

Define boundary areas:

$$\begin{aligned}
F_1 &= F_1(h,\rho) = \{a \in \triangle_{hA} \mid dist(a, l(0, ha_1) < \rho\} \\
F_2 &= F_2(h,\rho) = \{a \in \triangle_{hA} \mid dist(a, l(0, ha_1) < \rho\} \\
F_3 &= F_3(h,\rho) = \{a \in \triangle_{hA} \mid dist(a, l(0, ha_1) < \rho\} \\
F_4 &= F_4(h,\rho) = \{a \in \triangle_{hA} \mid dist(a, l(0, ha_1) < \rho\}
\end{aligned}$$

Also define

$$\begin{aligned}
m_1 &= |\{n \in \text{ nonnegative integer} \mid dist(na_2, l(0, ha_1) < \rho\}| \\
m_2 &= |\{n \in \text{ nonnegative integer} \mid dist(ha_1 - na_1, l(ha_1, ha_3) < \rho\}| \\
m_3 &= |\{n \in \text{ nonnegative integer} \mid dist(ha_2 - na_2, l(ha_2, ha_3) < \rho\}| \\
m_4 &= |\{n \in \text{ nonnegative integer} \mid dist(na_1, l(0, ha_2) < \rho\}|
\end{aligned}$$

Note that $m_1 = m_3$ and $m_2 = m_4$.

Since the intersection of any three boundary strips is empty, using the basic rectangular formula, we can compute the number of hA within ρ distance of the boundary to be:

$|hA \cap (F_1 \cup F_2 \cup F_3 \cup F_4)|$

$$
\begin{aligned}
&= |hA\cap F_1|+|hA\cap F_2|+|hA\cap F_3|+|hA\cap F_4| \\
&\quad -|hA\cap(F_1\cap F_2)|-|hA\cap(F_2\cap F_3)|-|hA\cap(F_3\cap F_4)|-|hA\cap(F_1\cap F_4)| \\
&= (h+1)m_1+(h+1)m_2+(h+1)m_3+(h+1)m_4-m_1m_2-m_2m_3-m_3m_4-m_1m_4 \\
&= hm_1+hm_2+hm_3+hm_4+m_1+m_2+m_3+m_4-m_1m_2-m_2m_3-m_3m_4-m_1m_4 \\
&= Ch-D
\end{aligned}
$$

where

$$
\begin{aligned}
C &= m_1+m_2+m_3+m_4 \\
D &= m_1m_2+m_2m_3+m_3m_4+m_1m_4-m_1-m_2-m_3-m_4
\end{aligned}
$$

3.2 Distribution of hA in the boundary region of $\triangle_{hA}$ in $\mathbf{Z}^2$

Let A be a finite set of integral points in $\mathbf{Z}^2$. Let h be an integer ≥ 0. Let $\triangle_A$, $\triangle_{hA}$, and hA be defined the same way as in Chapter 2 to denote the convex set of A, h times the convex set of A, and the h-fold sumset of A, respectively. Let ρ be a real number. In this section, we will examine the distribution of the elements of hA within a distance ρ from the boundary of $\triangle_{hA}$. The two examples in $\mathbf{Z}^2$ from Section 3.1 illustrate that the distribution of the elements of hA in the boundary area has a regular pattern, and the cardinality of hA in the boundary area can be easily computed to be a linear term. Although, an arbitrary set hA may not exhibit such a regular pattern as seen in the two examples, the author has found that if we consider the special case where the set A is a finite subset of $\mathbf{Z}^2$ such that no element of A is contained in the convex hull formed by the other elements of A, then the distribution of hA in the boundary area is shown to have a consistent pattern. This consistent and repeating pattern allows us to study the structure of the boundary area in details and allows us to estimate the cardinality of hA in the boundary area.

Let $A = \{a_0 = (0,0), a_1, a_2\}$ be a subset of $\mathbf{Z}^2$. For an integer h, the convex hull of hA is a triangle. We would like to partition this triangle into h strips of trapezoids with equal width, in the following way: For n such that $0 \leq n \leq h-1$, $l(na_1, na_1 + (h-n)a_2)$ is the line segment that marks the boundary of each partition. Each of these line segments is parallel to the vector a_2. (See figure 4) Let $a_1 = (x_1, y_1)$ and $a_2 = (x_2, y_2)$. If we consider the line segment as part of the infinite line, the slope of the infinite line is $m = \frac{y_2}{x_2}$. Thus, the general equations for these infinite lines are

$$y - ny_1 = \frac{y_2}{x_2}(x - nx_1)$$

Lemma 3.1 *Let l_n be the infinite line that coincides with the line segment $l(na_1, na_1 + (h-n)a_2)$, then*

$$l_{n+1} = l_n + a_1 - a_2$$

Proof.

Let $a_1 = (x_1, y_1)$ and $a_2 = (x_2, y_2)$, then the infinite line l_n has the equation $y - ny_1 = \frac{y_2}{x_2}(x - nx_1)$. We want to prove $l_{n+1} = l_n + a_1 - a_2$, we let $(x_0, y_0) \in l_n$, we want to show that $(x_0 + x_1 - x_2, y_0 + y_1 - y_2) \in l_{n+1}$. Thus, let

$$y_0 = \frac{y_2}{x_2}(x_0 - nx_1) + ny_1$$

$$
\begin{aligned}
y-(y_0+y_1-y_2) &= \frac{y_2}{x_2}(x-(x_0+x_1-x_2)) \\
y-y_0-y_1+y_2 &= \frac{y_2}{x_2}(x-x_0-x_1+x_2) \\
y-(\frac{y_2}{x_2}(x-nx_1)+ny_1)-y_1+y_2 &= \frac{y_2}{x_2}(x-x_0-x_1)+y_2 \\
y-\frac{y_2}{x_2}(x_0-nx_1)-ny_1-y_1+y_2 &= \frac{y_2}{x_2}(x-x_0-x_1)+y_2 \\
y-(n+1)y_1 &= \frac{y_2}{x_2}(x-x_0-x_1)+\frac{y_2}{x_2}(x_0-nx_1) \\
y-(n+1)y_1 &= \frac{y_2}{x_2}(x-x_0-x_1+x_0-nx_1) \\
y-(n+1)y_1 &= \frac{y_2}{x_2}(x-(n+1)x_1)
\end{aligned}
$$

Remark 3.1 *Although, it is also true that $l_{n+1} = l_n + a_1$ or that $l_{n+1} = l_n + a_2$, the reason for choosing to prove $l_{n+1} = l_n + a_1 - a_2$ is that $a_1 - a_2$ is parallel to the boundary line $l(ha_1, ha_2)$. Translation by $a_1 - a_2$ will preserve the distance between the point being translated and the boundary line $l(ha_1, ha_2)$.*

Let us consider a special subset of $\mathbf{Z}^2$. Let A be a finite set of lattice points in $\mathbf{Z}^2$ such that $0 \in A$ and no element of A is contained in the convex hull formed by the other elements of A. In other words, let V be the set of vertices of the convex hull of A, then $V = A$.

Definition 3.1 *Let a and b be two vertices of a polytope. We say that a and b are adjacent vertices if the line segment connecting a and b is an edge of the polytope.*

Let k be the cardinality of A. Since all the elements of A are the vertices of the convex hull of A, $\triangle_A$, we will number the elements of A clockwise:

$$A = \{a_0 = 0, a_1, a_2, \ldots, a_{k-1}\}$$

so that a_i and a_{i+1} are the adjacent vertices of $\triangle_A$, and a_{k-1} is adjacent to $a_0 = 0$.

We can partition the convex hull of hA into $k-2$ triangles. Each triangle has vertices $\{0, ha_i, ha_{i+1}\}$. We will consider one triangle at a time.

Let $A_i = \{0, a_i, a_{i+1}\}$ for $i = 1, \ldots, k-2$. We denote by $\triangle_{hA_i}$ the convex hull formed by $0, ha_i, ha_{i+1}$. We know $\triangle_{hA_i}$ has the shape of a triangle. Let $l_{i,n}$ denote the infinite line which coincides with the line segment $l(na_i, na_i + (h-n)a_{i+1})$. Define

$$F_i(h,\rho) = \{x \in \triangle_{hA_i} | dist(x, l(ha_i, ha_{i+1})) < \rho\}$$

to be the region containing all those elements of $\triangle_{hA_i}$ that is less than ρ from the boundary line $l(ha_i, ha_{i+1})$. Define

$$l_i(h,\rho) = \{x \in \triangle_{hA_i} \mid dist(x, l(ha_i, ha_{i+1})) = \rho\}$$

to be the line that intersects $\triangle_{hA_i}$, parallel to $l(ha_i, ha_{i+1})$ and is ρ distance away from $l(ha_i, ha_{i+1})$.

Let us define a subset of $\triangle_{hA}$: Let $a \in A$, define $\triangle_{h(A \backslash \{a\})}$ to be the convex hull of the set hA', where $A' = A \backslash \{a\}$ is the subset of A which contains all elements of A except for one element. Let

$$\triangle_i = \triangle_{hA_i} \backslash \left(\triangle_{h(A\backslash\{a_i\})} \cup \triangle_{h(A\backslash\{a_{i+1}\})}\right)$$

denote the subset of $\triangle_{hA_i}$ that does not intersect with the convex hulls of $\triangle_{h(A\backslash\{a_i\})}$ and $\triangle_{h(A\backslash\{a_{i+1}\})}$. This set $\triangle_i$ represents a small region in the boundary area. We will partition $F_i(h,\rho) \cap \triangle_i$ by the infinite lines $l_{i,n}$ for $n_{i,1} \le n \le h - n_{i,2}$. The values of $n_{i,1}$ and $n_{i,2}$ depend on where $l(ha_{i-1}, ha_{i+1})$ and $l(ha_i, ha_{i+2})$ intersect $l_i(h,\rho)$. Note that

$l(ha_{i-1}, ha_{i+1})$ and $l(ha_i, ha_{i+2})$ are the boundary lines of $\triangle_{h(A\setminus\{a_i\})}$ and $\triangle_{h(A\setminus\{a_{i+1}\})}$ respectively.

The reason for such a restriction is because if we select $w \in hA \cap \triangle_i$, then w can be translated by $a_i - a_{i+1}$ and $w + a_i - a_{i+1} \in hA$. The details are presented later in this section.

Also note that the two lines $l(ha_{i-1}, ha_{i+1})$ and $l(ha_i, ha_{i+2})$ intersect each other in $\triangle_{hA_i}$. Consider an h large enough so that $l(ha_i, ha_{i+2})$ and $l(ha_{i-1}, ha_{i+1})$ intersect in the region that is outside of $F_i(h, \rho)$. In other words, pick an h large enough so that if $x \in l(ha_i, ha_{i+2}) \cap (l(ha_{i-1}, ha_{i+1}))$, then $x \in \triangle_{hA_i} \setminus F_i(h, \rho)$. (See Figure 5)

Let u_1 be the intersection of $l(ha_{i-1}, ha_{i+1})$ with $l_i(h, \rho)$ and let u_2 be the intersection of $l(ha_i, ha_{i+2})$ with $l_i(h, \rho)$. Let v_1 and v_2 be two points on the line $l(0, ha_i)$ such that the lines $l(u_1, v_1)$ and $l(u_2, v_2)$ both have slopes equal to the vector a_{i+1} thus, parallel to $l(0, ha_{i+1})$. Since $v_1, v_2 \in l(0, ha_i)$, there exist real numbers λ_1 and λ_2 such that $v_1 = \lambda_1 a_1$ and $v_2 = (h - \lambda_2)a_1$. Note that we assume $\lambda_1 < (h - \lambda_2)$. If we consider a h large enough so that the intersection of $l(ha_i, ha_{i+2})$ and $l(ha_{i-1}, ha_{i+1})$ occurs in $\triangle_{hA_i} \setminus F_i(h, \rho)$, then we will have $\lambda_1 < (h - \lambda_2)$.

Lemma 3.2 *λ_1 and λ_2 are both constants independent of h.*

Proof.

First, we will prove that λ_1 is a constant independent of h. Let $u_1(h')$ and $u_1(h'')$ be two points defined in the following ways for two different values of h.

$$u_1(h') = l(h'a_{i-1}, h'a_{i+1}) \cap l(h', \rho)$$

$$u_1(h'') = l(h''a_{i-1}, h''a_{i+1}) \cap l(h'', \rho)$$

Let $w(h') = u_1(h') - h'a_{i+1}$ and $w(h'') = u_1(h'') - h''a_{i+1}$. Let $r(h')$ be a point on $l(h'a_i, h'a_{i+1})$, the boundary of $\triangle_{h'A_i}$, such that $|u_1(h') - r(h')| = \rho$. Let $r(h'')$ be a point on $l(h''a_i, h''a_{i+1})$, the boundary of $\triangle_{h''A_i}$, such that $|u_1(h'') - r(h'')| = \rho$. Since the two triangles formed by the vertices $\{u_1(h'), r(h'), h'a_{i+1}\}$ and $\{u_1(h''), r(h''), h''a_{i+1}\}$ are congruent, we conclude $w(h') = w(h'')$. Let $w = w(h') = w(h'')$, also assume $h'' > h'$, then,

$$\begin{aligned} u_1(h') &= h'a_{i+1} + w \\ u_1(h'') &= h''a_{i+1} + w \\ \text{thus, } u_1(h'') &= u_1(h') + (h'' - h')a_{i+1} \end{aligned}$$

Let $l_{u_1(h')}$ be the line that goes through the point $u_1(h')$ with the slope that is equal to the vector a_{i+1} and $l_{u_1(h'')}$ be the line that goes through the point $u_1(h'')$ with the same slope a_{i+1}. Then the infinite line $l_{u_1(h')}$ coincides with $l_{u_1(h'')}$. Thus, if $v_1(h') = l_{u_1(h')} \cap l(0, h'a_i)$, and if $v_1(h'') = l_{u_1(h'')} \cap l(0, h''a_i)$, we conclude that $v_1(h') = v_1(h'')$, since $l_{u_1(h')} = l_{u_1(h'')}$. Let $v_1 = v_1(h') = v_1(h'')$, v_1 is independent of h. Furthermore, let λ_1 be a constant such that $v_1 = \lambda_1 a_i$, then λ_1 is a constant independent of h.

Next, we will prove that λ_2 is a constant independent of h. Similarly, let $l_{u_2(h')}$ and $l_{u_2(h'')}$ be two lines that pass through the points $u_2(h')$ and $u_2(h'')$ respectively and both with slopes equal to a_{i+1}. Let $v_2(h')$ be the point where $l_{u_2(h')}$ intersects the line $l(0, h'a_i)$ and let $v_2(h'')$ be the point where $l_{u_2(h'')}$ intersects the line $l(0, h''a_i)$. We note that the two triangles formed by the vertices $\{u_2(h'), v_2(h'), h'a_i\}$, and $\{u_2(h''), v_2(h''), h''a_i\}$ are congruent. Thus, $h'a_i - v_2(h') = h''a_i - v_2(h'')$. Let λ_2 be a constant such that $h'a_i - v_2(h') = \lambda_2 a_i$ $v_2 = \lambda_2 a_i$, then λ_2 is a constant independent of h. Let $v_2 = (h - \lambda_2)a_i$, then $ha_i - v_2 = \lambda_2 a_1$ is a vector independent of h.

Let $n_{i,1} = \lceil \lambda_1 \rceil$ the least integer greater than λ_1 and let $n_{i,2} = \lfloor \lambda_2 \rfloor$ the greatest integer less than λ_2. Note that $n_{i,1}$ and $n_{i,2}$ are both constants independent of h, since λ_1 and λ_2 are constants independent of h. □

Let $b_{i,n}(h)$ be a point on the line segment $l(ha_i, ha_{i+1})$ determined by n and h:

$$b_{i,n}(h) = na_i + (h - n)a_{i+1}$$

Let γ_i be a real number such that $(h - \gamma_i)a_{i+1} \in l_i(h, \rho)$. Then for each nonnegative integer n, $0 \leq n \leq h - 1$, we can define a parallelogram:

$$B_{i,n}(h) = b_{i,n}(h) - \delta_1 a_{i+1} + \delta_2(a_i - a_{i+1}) \tag{3.1}$$

$$\text{where} \quad 0 \leq \delta_1 < \gamma_i, \quad 0 \leq \delta_2 < 1$$

Note that for those n such that $n_{i,1} \leq n \leq h - n_{i,2} - 1$, each $B_{i,n}(h)$ is a parallelogram bounded by the lines $l_{i,n}$, $l_{i,n+1}$,$l(ha_i, ha_{i+1})$, and $l_i(h, \rho)$, including the sides bounded by $l_{i,n}$, $l(ha_i, ha_{i+1})$, but not including the side bounded by $l_{i,n+1}$ and $l_i(h, \rho)$. Furthermore,

$$B_{i,n}(h) \subset F_i(h, \rho) \cap \Delta_i$$

Define

$$B_{i,F}(h) = \bigcup_{n=1}^{n_{i,1}-1} B_{i,n}(h) \tag{3.2}$$

$$B_{i,L}(h) = \left(\bigcup_{n=h-n_{i,2}}^{h-1} B_{i,n}(h) \right) \cap F_i(h, \rho) \tag{3.3}$$

So, $B_{i,F}(h)$ is the area that is bounded by the lines $l(ha_i, ha_{i+1})$, $l_i(h,\rho)$, $l(0, ha_{i+1}$, and $l_{i,n_{i,1}}(h)$ including the sides bounded by $l(ha_i, ha_{i+1})$, and $l(0, ha_{i+1})$, but not including the side that is $l_{i,n_{i,1}}(h)$ and $l_i(h,\rho)$. On the other hand, $B_{i,L}(h)$ is the area that is bounded by the lines $l(ha_i, ha_{i+1})$, $l_i(h,\rho)$, $l_{i,n_{i,2}}(h)$, and $l(0, ha_i)$ including all the sides except $l_i(h,\rho)$.

Let $S_{i,n}(h)$ denote the subset of hA that belongs in the parallelogram. Let $U_i(h)$ and $V_i(h)$ denote the subset of hA that belong in the first and the last cell respectively, thus, we have the following definitions:

$$S_{i,n}(h) = hA \cap B_{i,n}(h) \qquad \text{for } n_{i,1} \leq n \leq h - n_{i,2} - 1 \tag{3.4}$$

$$U_i(h) = hA \cap B_{i,F}(h) \tag{3.5}$$

$$V_i(h) = hA \cap B_{i,L}(h) \tag{3.6}$$

The interesting finding of this research is that for all $n_{i,1} \leq n \leq h - n_{i,2} - 1$, we can translate each element of $S_{i,n}(h)$ by $a_i - a_{i+1}$ to get $S_{i,n+1}(h)$, thus indicating $|S_{i,n}(h)| = |S_{i,n+1}(h)|$. Furthermore, as h increases to infinity, $|S_{i,n}(h)|$ stays a constant, thus indicating that the cardinality of hA in each parallelogram is a constant independent of h. The researcher has also found that the cardinality of $U_i(h)$ and $V_i(h)$, the first and the last cell of each $\triangle_{hA_i}$, is a constant independent of h. Therefore, the cardinality of hA in the boundary region of $\triangle_{hA_i}$ is

$$|S_{i,n}(h)| \cdot (\text{ number of cells }) + |U_i(h)| + |V_i(h)|$$

The only component of the above expression that depends on h is the number of cells which is determined by the number of partitions into parallelograms. The details of the proof are presented next.

Lemma 3.3 *Let A be a finite set of lattice points in $\mathbf{Z}^2$ containing 0 such that no element of A is contained in the convex hull formed by the other elements of A. Let h be a positive integer. Let i be an integer $\in [1, k-2]$. Let $A_i = \{0, ha_i, ha_{i+1}\}$, define*

$$\triangle_i = \triangle_{hA_i} \setminus \left(\triangle_{h(A \setminus \{a_i\})} \cup \triangle_{h(A \setminus \{a_{i+1}\})} \right)$$

If $w \in hA$ and if $w \in \triangle_i$, then $w - a_i$ and $w - a_{i+1}$ are both in $(h-1)A$.

Proof.

Let

$$w = \sum_{j=0}^{k-1} h_j a_j \qquad \text{where} \qquad \sum_{j=0}^{k-1} h_j = h$$

If both $h_i \neq 0$ and $h_{i+1} \neq 0$, then we are done with the proof. So we can assume that either $h_i = 0$ or $h_{i+1} = 0$. If $h_i = 0$, then $w \in \triangle(0, ha_1, \ldots, ha_{i-1}, ha_{i+1}, \ldots, ha_{k-1})$ contradicting our assumption of w. If $h_{i+1} = 0$, then $w \in \triangle(0, ha_1, \ldots, ha_i, ha_{i+2}, \ldots, ha_{k-1})$ again contradicting our assumption of w. Thus, $h_i \neq 0$ and $h_{i+1} \neq 0$, therefore,

$$w - a_i \;=\; (h_i - 1)a_i + \sum_{j \neq i} h_j a_j \;\in\; (h-1)A$$

and

$$w - a_{i+1} \;=\; (h_{i+1} - 1)a_{i+1} + \sum_{j \neq i+1} h_j a_j \;\in\; (h-1)A$$

□

Note that $\triangle_i \neq \emptyset$, since $w = (h-1)a_i + a_{i+1} \in \triangle_i$.

Claim 3.1 *Let h be a fixed positive integer, n a nonnegative integer. For $0 \leq n \leq h-2$, $B_{i,n+1}(h) = B_{i,n}(h) + a_i - a_{i+1}$.*

Proof.

Let $x = b_{i,n}(h) - \delta_1 a_{i+1} + \delta_2(a_i - a_{i+1}) \in B_{i,n}(h)$ for some δ_1 and δ_2 such that $0 \le \delta_1 < \gamma_i$, and $0 \le \delta_2 < 1$. Then

$$\begin{aligned}
x &= b_{i,n}(h) - \delta_1 a_{i+1} + \delta_2(a_i - a_{i+1}) \\
&= na_i + (h-n)a_{i+1} - \delta_1 a_{i+1} + \delta_2(a_{i+1} - a_i) \\
x + a_i - a_{i+1} &= (n+1)a_i + (h-(n+1))a_{i+1} - \delta_1 a_{i+1} + \delta_2(a_{i+1} - a_i) \\
&= b_{i,n+1}(h) - \delta_1 a_{i+1} + \delta_2(a_{i+1} - a_i)
\end{aligned}$$

By definition, $x + a_i - a_{i+1} \in B_{i,n+1}(h)$. Thus, $B_{i,n}(h) + a_i - a_{i+1} \subset B_{i,n+1}(h)$.

Conversely, if $x \in B_{i,n+1}(h)$, then

$$\begin{aligned}
x &= b_{i,n+1}(h) - \delta_1 a_{i+1} + \delta_2(a_i - a_{i+1}) \\
&= (n+1)a_i + (h-(n+1))a_{i+1} - \delta_1 a_{i+1} + \delta_2(a_i - a_{i+1}) \\
&= na_i + (h-n)a_{i+1} - \delta_1 a_{i+1} + \delta_2(a_i - a_{i+1}) + a_i - a_{i+1} \\
&= b_{i,n}(h) - \delta_1 a_{i+1} + \delta_2(a_i - a_{i+1}) + a_i - a_{i+1}
\end{aligned}$$

Let $y = b_{i,n}(h) - \delta_1 a_{i+1} + \delta_2(a_i - a_{i+1}) \in B_{i,n}(h)$, so $x = y + a_i - a_{i+1} \in B_{i,n}(h) + a_i - a_{i+1}$. Thus, $B_{i,n+1}(h) \subset B_{i,n}(h) + a_i - a_{i+1}$. Therefore $B_{i,n+1}(h) = B_{i,n}(h) + a_i - a_{i+1}$. □

Claim 3.2 *For n such that $n_{i,1} \le n \le h - n_{i,2} - 2$, $S_{i,n+1}(h) = S_{i,n}(h) + a_i - a_{i+1}$.*

Proof.

Let $x \in S_{i,n}(h)$, then $x \in hA$ and $x \in B_{i,n}(h)$. We want to prove that $x + a_i - a_{i+1} \in B_{i,n+1}(h)$. Claim 3.1 implies that $x + a_i - a_{i+1} \in B_{i,n+1}(h)$. We need to prove that $x + a_i - a_{i+1} \in hA$. Since for n such that $n_{i,1} \le n \le h - n_{i,2} - 1$,

$B_{i,n}(h) \subset (F_i(h,\rho) \cap \Delta_i)$, thus, $x \in \Delta_i$. By the previous lemma, both $x - a_i$ and $x - a_{i+1}$ are in $(h-1)A$. Thus,

$$x + a_i - a_{i+1} = (x - a_{i+1}) + a_i \in (h-1)A + A = hA$$

Therefore, $x + a_i - a_{i+1} \in S_{i,n+1}(h)$ and thus $S_{i,n}(h) + a_i - a_{i+1} \subset S_{i,n+1}(h)$

Conversely, if $x \in S_{i,n+1}(h)$, by definition, $x \in hA$ and $x \in B_{i,n+1}(h)$. The previous claim shows that there exists an element $y \in B_{i,n}(h)$ such that $x = y + a_i - a_{i+1}$. So $y = x - a_i + a_{i+1}$. Again, since $B_{i,n+1}(h) \subset F_i(h,\rho) \cap \Delta_i$, meaning $x \in \Delta_i$, thus $x - a_i$ and $x - a_{i+1}$ are both in $(h-1)A$. Therefore,

$$y = x - a_i + a_{i+1} = (x - a_i) + a_{i+1} \in (h-1)A + A = hA$$

implying $y \in S_{i,n}(h)$ which implies $x \in B_{i,n}(h) + a_i - a_{i+1}$. Hence, $S_{i,n+1}(h) \subset S_{i,n}(h) + a_i - a_{i+1}$. Hence, $S_{i,n+1}(h) = S_{i,n}(h) + a_i - a_{i+1}$. □

Claim 3.3 *For n such that $0 \leq n \leq h-1$, $B_{i,n}(h+1) = B_{i,n}(h) + a_{i+1}$.*

Proof.

Again, let $x \in B_{i,n}(h)$, then for some δ_1 and δ_2 such that $0 \leq \delta_1 < \gamma_i$, $0 \leq \delta_2 < 1$, we have

$$\begin{aligned} x &= b_{i,n}(h) - \delta_1 a_{i+1} + \delta_2(a_i - a_{i+1}) \\ &= na_i + (h-n)a_{i+1} - \delta_1 a_{i+1} + \delta_2(a_i - a_{i+1}) \\ x + a_{i+1} &= na_i + ((h+1) - n)a_{i+1} - \delta_1 a_{i+1} + \delta_2(a_i - a_{i+1}) \\ &= b_{i,n}(h+1) - \delta_1 a_{i+1} + \delta_2(a_i - a_{i+1}) \end{aligned}$$

Thus, $x + a_{i+1} \in B_{i,n}(h+1)$ implying $B_{i,n}(h) + a_{i+1} \subset B_{i,n}(h+1)$.

Conversely, if $x \in B_{i,n}(h+1)$, then

$$\begin{aligned} x &= b_{i,n}(h+1) - \delta_1 a_{i+1} + \delta_2(a_i - a_{i+1}) \\ &= na_i + ((h+1)-n)a_{i+1} - \delta_1 a_{i+1} + \delta_2(a_i - a_{i+1}) \\ &= na_i + (h-n)a_{i+1} - \delta_1 a_{i+1} + \delta_2(a_i - a_{i+1}) + a_{i+1} \\ &= b_{i,n}(h) - \delta_1 a_{i+1} + \delta_2(a_i - a_{i+1}) + a_{i+1} \end{aligned}$$

There exists an element $y = b_{i,n}(h) - \delta_1 a_{i+1} + \delta_2(a_i - a_{i+1}) \in B_{i,n}(h)$ such that $x = y + a_{i+1}$, thus, $x \in B_{i,n}(h) + a_{i+1}$ implying $B_{i,n}(h+1) \subset B_{i,n}(h) + a_{i+1}$. Hence, $B_{i,n}(h+1) = B_{i,n}(h) + a_{i+1}$. □

Claim 3.4 *For n such that $n_{i,1} \leq n \leq h - n_{i,2} - 1$, $S_{i,n}(h+1) = S_{i,n}(h) + a_{i+1}$.*

Proof.

Let $x \in S_{i,n}(h)$, then $x \in hA$ and $x \in B_{i,n}(h)$. By Claim 3.3, $x + a_{i+1} \in B_{i,n}(h+1)$ and $x + a_{i+1} \in hA + A = (h+1)A$. Thus $x + a_{i+1} \in S_{i,n}(h+1)$ implying $S_{i,n}(h) + a_{i+1} \subset S_{i,n}(h+1)$.

Conversely, let $x \in S_{i,n}(h+1)$, then $x \in (h+1)A$ and $x \in B_{i,n}(h+1)$. Again by Claim 3.3, there exists an element $y \in B_{i,n}(h)$ such that $x = y + a_{i+1}$. Since $y = x - a_{i+1} \in hA$, $x \in S_{i,n}(h) + a_{i+1}$, thus, $S_{i,n}(h+1) \subset S_{i,n}(h) + a_{i+1}$. Hence, $S_{i,n}(h+1) = S_{i,n}(h) + a_{i+1}$. □

Claim 3.5 $B_{i,F}(h+1) = B_{i,F}(h) + a_{i+1}$.

Proof.

Using equation (3.2), we have

$$B_{i,F}(h) + a_{i+1} = \bigcup_{n=0}^{n_{i,1}-1} B_{i,n}(h) + a_{i+1}$$

$$= \bigcup_{n=0}^{n_{i,1}-1} B_{i,n}(h+1)$$
$$= B_{i,F}(h+1)$$

Thus proving the claim. □

Claim 3.6 $B_{i,L}(h+1) = B_{i,L}(h) + a_{i+1}$

Proof.

Let $x \in B_{i,L}(h)$, then $x \in F_i(h,\rho)$ and $x \in B_{i,n}(h)$ for some n such that $h - n_{i,2} \leq n \leq h-1$. By Claim 3.3, we have $x + a_{i+1} \in B_{i,n}(h+1)$. We now need to prove that $x + a_{i+1} \in F_i(h+1,\rho)$. Let w be a point on the line $l(ha_i, ha_{i+1})$, such that $|w - x| = d < \rho$. Since $w + a_{i+1}$ is a point on the line $l((h+1)a_i,(h+1)a_{i+1})$, then

$$|x + a_{i+1} - l((h+1)a_i,(h+1)a_{i+1})| < (w + a_{i+1}) - (x + a_{i+1})| = |w - x| = d < \rho$$

Thus, $x+a_{i+1} \in F_i((h+1),\rho)$, therefore $x+a_{i+1} \in B_{i,L}(h+1)$ implying $B_{i,L}(h)+a_{i+1} \subset B_{i,L}(h+1)$.

Conversely, let $x \in B_{i,L}(h+1)$, then $x \in F_i(h+1,\rho)$ and $x \in B_{i,n}(h+1)$. There exists an element $y \in B_{i,n}(h)$ such that $x = y + a_{i+1}$. Using similar argument as above shows that $y \in F_i(h,\rho)$, thus $y \in B_{i,L}(h)$ implying $x \in B_{i,L}(h) + a_{i+1}$. Hence, proving the claim. □

Claim 3.7 $U_i(h+1) = U_i(h) + a_{i+1}$ *and* $V_i(h+1) = V_i(h) + a_{i+1}$.

Proof.

Refer to equations (3.5) and (3.6) for the definitions of $U_i(h)$ and $V_i(h)$. The result follows directly from Claims 3.5 and 3.6. □

Theorem 3.1 *Let i be an integer $\in [1, k-2]$. Let $A = \{a_0 = 0, a_1, a_2, \ldots, a_{k-1}\}$ be a finite set of lattice points in $\mathbf{Z}^2$ such that A generates $\mathbf{Z}^2$ and that no element of A is contained in the convex hull formed by the other elements of A. Also the elements of A are numbered so that consecutive elements are the adjacent vertices of $\triangle_A$. Let h be a positive integer and ρ a nonnegative real number. For $i = 1, \ldots, k-2$, let $A_i = \{0, a_i, a_{i+1}\}$. Define*

$$F_i(h,\rho) = \{x \in \triangle_{hA_i} | dist(x, l(ha_i, ha_{i+1})) < \rho\} \tag{3.7}$$

Then for h sufficiently large

$$|\ F_i(h,\rho) \cap hA\ | = \ C_i \cdot h - D_i$$

where C_i and D_i are some constants.

Proof.

Let $n_{i,1}$ and $n_{i,2}$ be two constants determined by the intersections of the lines $l(ha_{i-1}, ha_{i+1})$ and $l(ha_i, ha_{i+2})$ with ρ. Recall that $n_{i,1}$ and $n_{i,2}$ do not depend on h. For all integers n such that $n_{i,1} \leq n \leq h - n_{i,2} - 1$, let $l_{i,n}$ be the infinite line that passes through the point na_i and has slope equal to the vector a_{i+1}. By Lemma 3.1, $l_{i,n}$ and $l_{i,n+1}$ are parallel, and

$$l_{i,n+1} = l_{i,n} + a_i - a_{i+1}$$

Refer to equations (3.1), (3.4), (3.5), and (3.6) for the definitions of $B_{i,n}(h)$, $S_{i,n}(h)$, $U_i(h)$, and $V_i(h)$.

For h sufficiently large, we have

$$F_i(h,\rho) \cap hA \ = \ \bigcup_{i=n_{i,1}}^{h-n_{i,2}-1} S_{i,n}(h) \ \cup \ U_i(h) \ \cup \ V_i(h)$$

where the intersection of any two sets in the union is empty. Thus the cardinality is

$$|F_i(h,\rho) \cap hA| \;=\; \sum_{i=n_{i,1}}^{h-n_{i,2}-1} |S_{i,n}(h)| \;+\; |U_i(h)| \;+\; |V_i(h)|$$

By Claim 3.2, we see that for n such that $n_{i,1} \leq n \leq h - n_{i,2} - 1$,

$$S_{i,n+1}(h) = S_{i,n}(h) + a_i - a_{i+1}$$

we see that the distribution of the elements of hA is identical in each set $S_{i,n}(h)$. Thus,

$$|S_{i,n+1}(h)| \;=\; |S_{i,n}(h)|$$

Furthermore, by Lemma 3.4, the cardinality of $S_{i,n}(h)$ is independent of h. For all n such that $n_{i,1} \leq n \leq h - n_{i,2} - 1$, let $C_i = |S_{i,n}(h)|$, then C_i is a constant independent of h.

Moreover, by claim 3.7, we have the cardinality of $U_i(h)$ and $V_i(h)$ are both constants independent of h.

Therefore, the number of elements of hA that are within ρ distance away from the face $l(ha_i, ha_{i+1})$ is:

$$\begin{aligned} |\ F_i(h,\rho) \cap hA\ | &= \sum_{i=n_{i,1}}^{h-n_{i,2}-1} |S_{i,n}(h)| \;+\; |U_i(h)| \;+\; |V_i(h)| \\ &= (h - n_{i,2} - n_{i,1})C_i + |\ U_i(h)\ | + |\ V_i(h)\ | \\ &= C_i \cdot h - D_i \end{aligned}$$

where $D_i = (n_{i,1} + n_{i,2}) \cdot C_i \;-\; |U_i(h)| \;-\; |V_i(h)|$. □

Theorem 3.2 *Let A be a finite set of lattice points in $\mathbf{Z}^2$ such that A generates $\mathbf{Z}^2$ and that no element of A is contained in the convex hull formed by the other elements of A. Let h be a positive integer. Define*

$$F_A(h,\rho) = \{x \in \triangle_{hA} \mid dist(x, \partial\triangle_{hA}) < \rho\}$$

to be the region that is less than ρ distance away from the boundary. Then for h sufficiently large

$$|\, hA \cap F_A(h,\rho) \,| = \; C \cdot h + D$$

where C and D are some constants independent of h.

Proof.

We can assume that $0 \in A$, since if $0 \notin A$, we can translate the set A by an element of A. Let $A = \{a_0 = 0, a_1, a_2, \ldots, a_{k-1}\}$, where the elements of A are numbered so that the consecutive elements are the adjacent vertices of $\triangle_A$. For $i = 1, \ldots, k-2$, let $F_i(h,\rho)$ be the set defined in (3.7). For $i = 1, \ldots, k-2$, apply Theorem 3.1 to the set $A_i = \{0, a_i, a_{i+1}\}$, we have

$$|hA \cap F_i(h,\rho)| = C_i h - D_i$$

Define the remaining two boundary regions of $\triangle_{hA}$ in the following way:

$$\begin{aligned} F_0(h,\rho) &= \{x \in \triangle_{hA_1} \mid dist(x, l(0, ha_1)) < \rho\} \\ F_{k-1}(h,\rho) &= \{x \in \triangle_{hA_{k-2}} \mid dist(x, l(0, ha_{k-1})) < \rho\} \end{aligned}$$

To be able to apply Theorem 3.1 to the case of $|hA \cap F_0(h,\rho)|$ and $|hA \cap F_{k-1}(h,\rho)|$, we will translate the set A by a_{k-2}. Thus we will consider the set $A' = A - a_{k-2}$. Let

$a'_0 = a_{k-2} - a_{k-2} = 0$; $a'_1 = a_{k-1} - a_{k-2}$; $a'_2 = a_0 - a_{k-2}$; and $a'_3 = a_1 - a_{k-2}$. Now we can apply Theorem 3.1 to $\{0, a'_1, a'_2\}$ and $\{0, a'_2, a'_3\}$. Thus,

$$|hA \cap F_0(h,\rho)| = |hA' \cap F_0(h,\rho)|$$

and

$$|hA \cap F_{k-1}(h,\rho)| = |hA' \cap F_{k-1}(h,\rho)|$$

Putting it all together we have for $i = 0$, and $k-1$,

$$|hA \cap F_i(h,\rho)| = |hA' \cap F_i(h,\rho)| = C_i h - D_i$$

For $i = 0, 1, \ldots, k-2$, let

$$T_i(h) = hA \cap F_i(h,\rho) \cap F_{i+1}(h,\rho)$$

For $i = k-1$, let

$$T_{k-1}(h) = hA \cap F_{k-1}(h,\rho) \cap F_0(h,\rho)$$

We note that for all $i = 0, 1, \ldots, k-1$,

$$T_i(h) \subseteq (U_i(h) \cup V_{i+1}(h))$$

By Claim 3.7, we see the elements of $U_i(h+1)$ and $V_i(h+1)$ are simply the translation of the elements of $U_i(h)$ and $V_i(h)$ by a_{i+1}. Thus, the elements of $T_i(h+1)$ are also translation of the elements of $T_i(h)$ by a_{i+1}. Thus, if we let $t_i = |T_i(h)|$, then t_i is a constant independent of h. Therefore, we have the cardinality of hA in the boundary region to be:

$$|\, hA \cap F_A(h,\rho)\,| = \sum_{i=0}^{k-1} |\, hA \cap F_i(h,\rho)\,| - \sum_{i=0}^{k-1} t_i$$

$$
\begin{aligned}
&= \sum_{i=0}^{k-1} C_i \cdot h - D_i - t_i \\
&= C \cdot h - D
\end{aligned}
$$

where $C = \sum_{i=0}^{k-1} C_i$ and $D = \sum_{i=0}^{k-1} D_i + t_i$. □

Theorem 3.3 *Let A be a finite subset of $\mathbf{Z}^2$ such that no element of A is contained in the convex hull formed by the other elements of A. Let h be a positive integer. Then for h sufficiently large, there exists a nonnegative real number ρ independent of h such that*

$$hA = \left(\triangle_{hA}(\rho) \cap \mathbf{Z}^2\right) \cup (F_A(h,\rho) \cap hA)$$

where $|F_A(h,\rho) \cap hA|$ is a linear function in h.

Proof.

By definition

$$
\begin{aligned}
\triangle_{hA}(\rho) &= \{x \in \triangle_{hA} \mid dist(x, \partial\triangle_{hA}) \geq \rho\} \\
F_A(h,\rho) &= \{x \in \triangle_{hA} \mid dist(x, \partial\triangle_{hA}) < \rho\}
\end{aligned}
$$

we see that

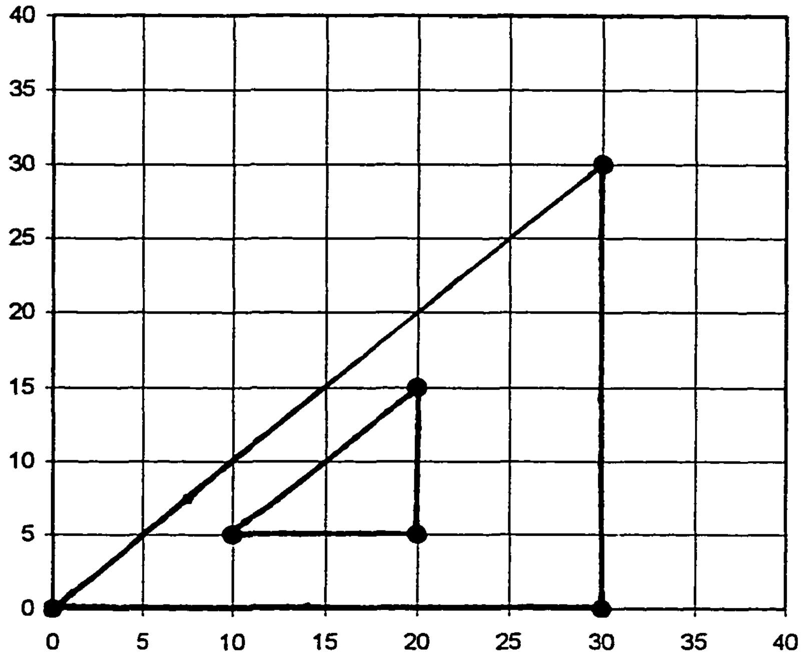
$$\triangle_{hA}(\rho) \ \cap \ F_A(h,\rho) = \emptyset.$$

By Theorem 2.4, there exists a real number ρ such that $\triangle_{hA}(\rho) \cap \mathbf{Z}^2 \subseteq hA$. Also by Theorem 3.2, $|F_A(h,\rho) \cap hA|$ is a linear function in h. Thus proven the theorem. □

In conclusion, Theorem 3.3 has presented a general structure for hA where A is the special finite subset of $\mathbf{Z}^2$ such that no elements of A is contained in the convex hull formed by the other elements of A. The general structure is this: There exists a nonnegative real number ρ such that all lattice points whose distance from the boundary of $\triangle_{hA}$ is greater or equal to ρ belong to hA. If we look at the distribution of hA less than ρ distance away from the boundary of $\triangle_{hA}$, we see a regular repeating pattern. Moreover, the cardinality of hA in the boundary region is $|F_A(h, \rho) \cap \mathbf{Z}^2|$ which is a linear function in h. We also know from Theorem 2.3 that hA is of the order $V_2(\triangle_A)h^2$. Thus, the cardinality of hA in the boundary region is one less degree in h than the cardinality of hA.

It is the author's wish to continue with the research in the structure of hA and hope to obtain a result similar to that of the Ehrhart's polynomial in the general case.

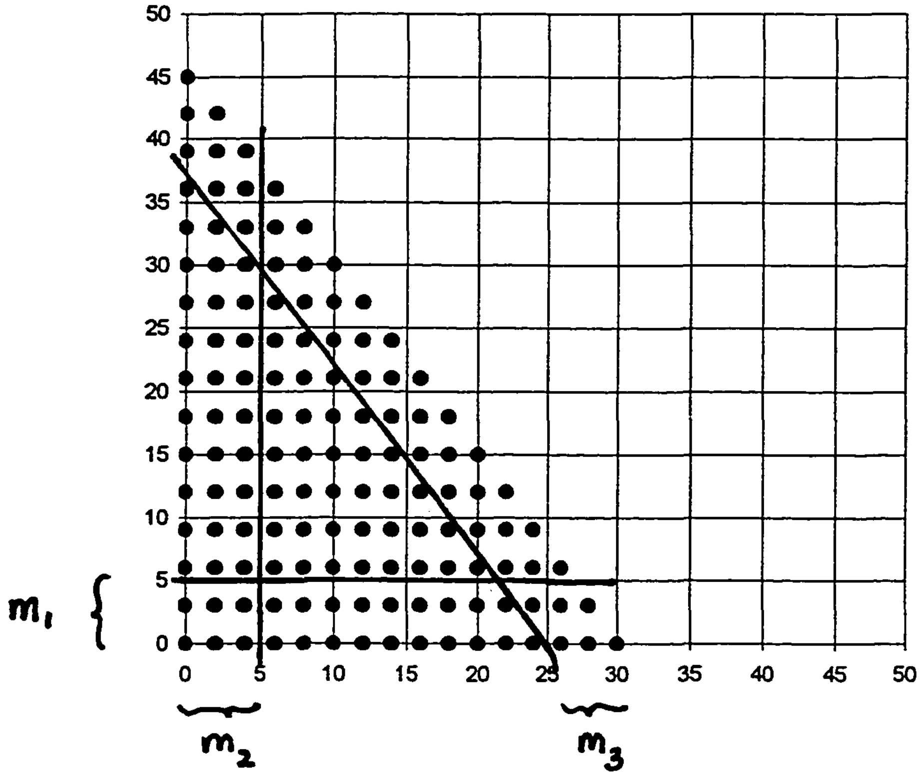
Figure #1



0	0
30	0
30	30
10	5
20	15
20	5

A={(0,0),(1,1),(1,0)}
h=30
C=5
The outside triangle is Δ_{hA}
The inside triangle is $\Delta(h,C)$

Figure #2

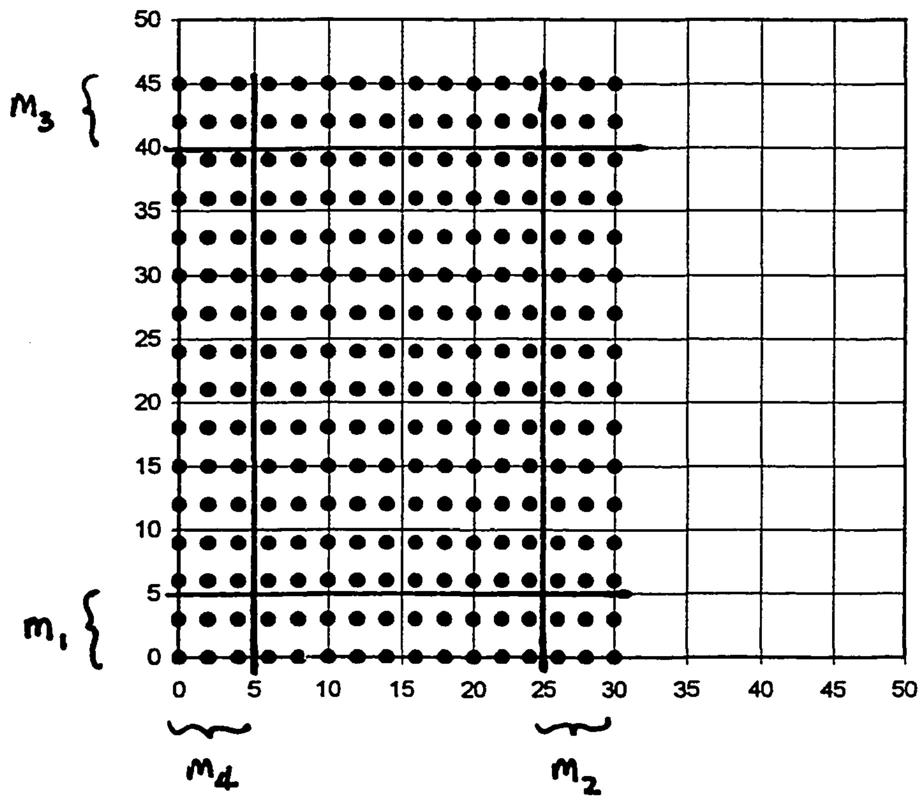


A={(0,0),(2,0),(0,3)}
h=15
ρ = 5

a_1=(2,0)
a_2=(0,3)

m_1=2
m_2=3
m_3=3

Figure #3



A={(0,0),(2,0),(0,3),(2,3)}
h=15
ρ = 5

a_1=(2,0)
a_2=(0,3)
a_3=(2,3)

m_1=2
m_2=3
m_3=2
m_4=3

Figure #4

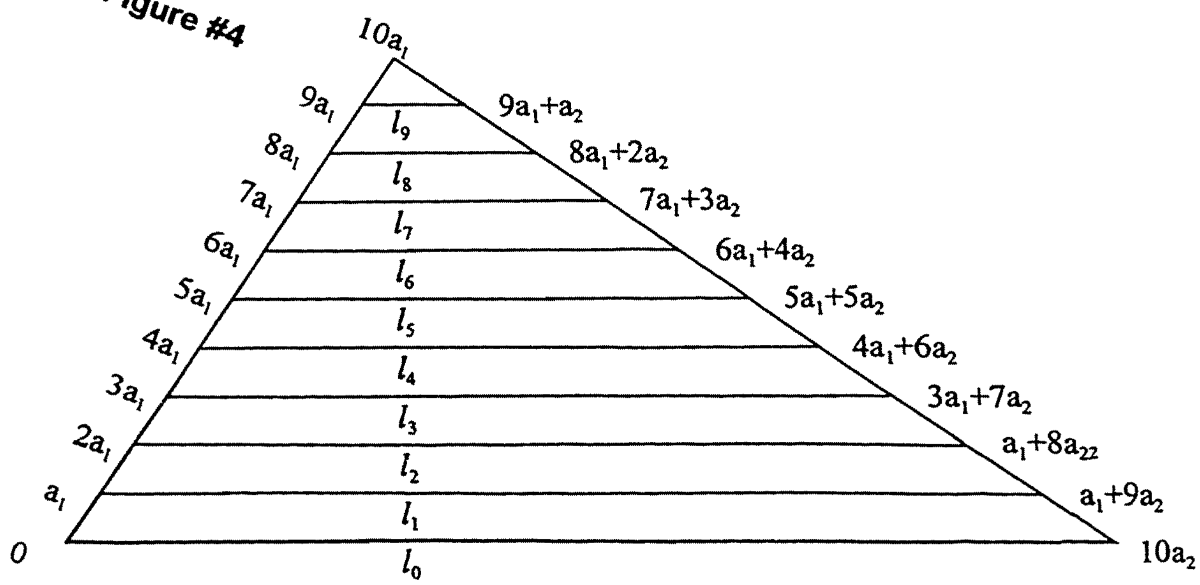
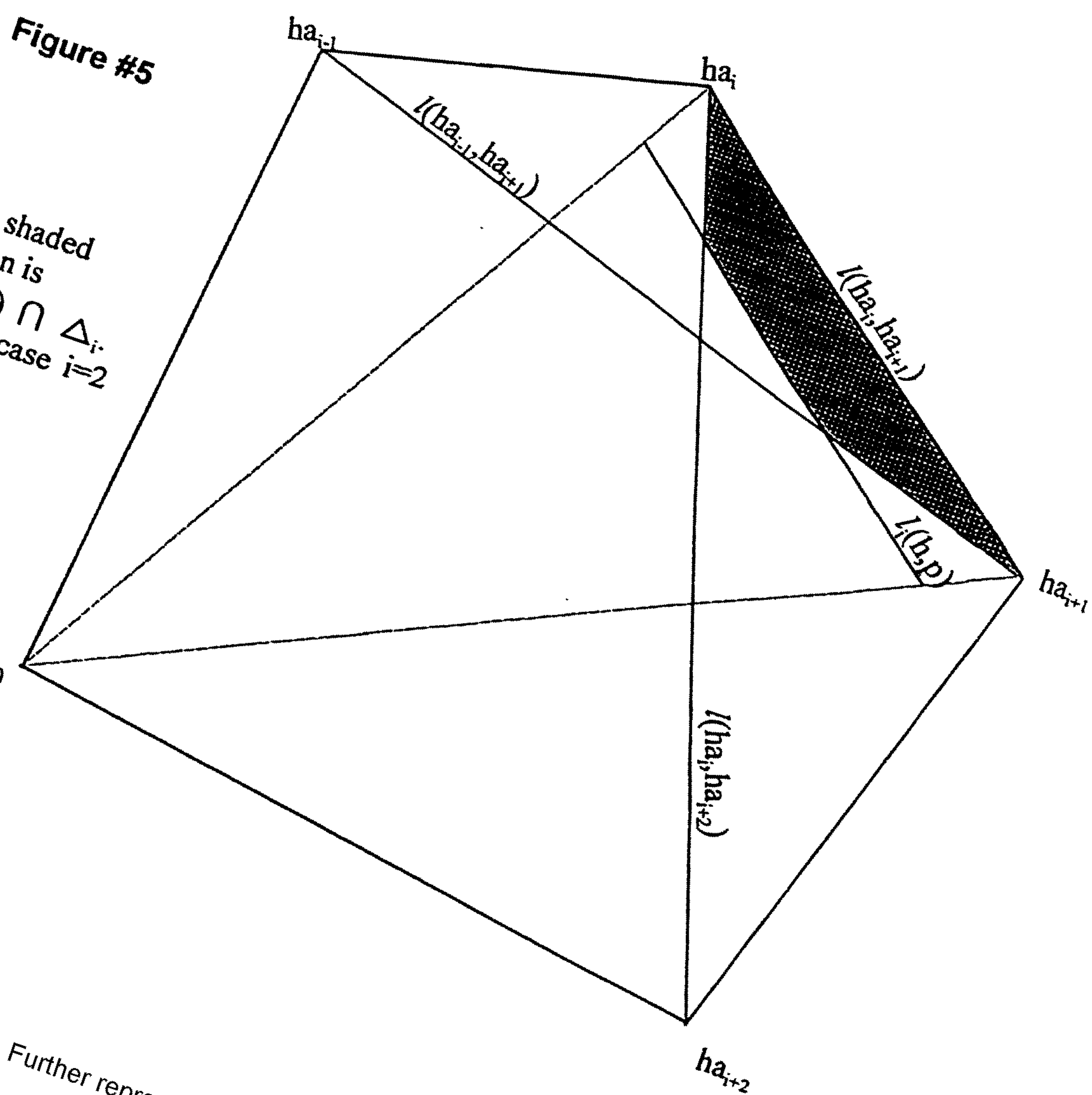


Figure #5

The shaded region is $F_i(h,p) \cap \Delta_i$. In this case i=2



Bibliography

[1] D,N. Berstein, "The number of integral points in integral polyhedra," *Functional Anal. Appl.* **10**(3)(1976), pp. 223-224.

[2] G. Ewald, *Combinatorial Convexity and Algebraic Geometry,* volume 168 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1996.

[3] P.M. Gruber and J.M. Wills, *Handbook of Convex Geometry, Volume B.* Elsevier Science Publishers B.V., Amsterdam, 1993, pp.767-797.

[4] S. Han, C. Kirfel, and M. Nathanson, "Linear forms in finite sets of integers," *The Ramanujan Journal.* 2(1998), pp.271-281.

[5] A.G. Khovanskii, "Newton polyhedron, Hilbert polynomial, and sums of finite sets," *Funksional. Anal. Prilozhen.* **26** (1992), pp. 276-281.

[6] M.B. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, volume 165 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1996.