INFINITELY OFTEN DENSE BASES

AND

GEOMETRIC STRUCTURE OF SUMSETS

by

Jaewoo Lee

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

2006

UMI Number: 3213245

ProQuest Information and Learning Company
300 North Zeeb Road
P.O. Box 1346
Ann Arbor, MI 48106-1346

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.

Melvyn B. Nathanson

Date of Acceptance — Chair of Examining Committee

Józef Dodziuk

Date of Acceptance — Executive Officer of Mathematics

Melvyn B. Nathanson

Carlos Moreno

Mark Sheingorn

Supervision Committee

THE CITY UNIVERSITY OF NEW YORK

Abstract

INFINITELY OFTEN DENSE BASES

AND

GEOMETRIC STRUCTURE OF SUMSETS

by

Jaewoo Lee

Adviser: Professor Melvyn B. Nathanson

We'll discuss two problems related to sumsets.

Nathanson constructed bases of integers with prescribed representation functions, then asked how dense bases for integers can be in such cases. Let $A(-x, x)$ be the number of elements of A whose absolute value is less than or equal to x, then it's easy to see that $A(-x, x) \ll x^{1/2}$ if its representation function is bounded, giving us a general upper bound. Chen constructed unique representation bases for

integers with $A(-x,x) \geq x^{1/2-\epsilon}$ infinitely often. In the first chapter, we'll construct bases for integers with a prescribed representaion function with $A(-x,x) > x^{1/2}/\phi(x)$ infinitely often where $\phi(x)$ is any nonnegative real-valued function which tends to infinity.

In the second chapter, we'll see how sumsets appear geometrically. Assume A is a finite set of lattice points and

$$h * \Delta = \{h \cdot x : x \in \text{conv}(A)\}$$

is a full dimensional polytope. Then we'll see that there is a constant ρ with the following property: for any positive integer h, any integral point in the polytope $h * \Delta$, whose distance to the boundary is bigger than ρ, belongs to the sumset hA.

Acknowledgments

I want to express my deepest gratitude toward my advisor Professor Melvyn Nathanson. Without his continued guidance, this thesis would not have been possible.

I would also like to acknowledge my appreciation to my thesis committee members, Professor Carlos Moreno 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 wish to extend my appreciation to the participants of the New York Number Theory Seminar as well.

I wish to thank my wife for her patience and support all through these years. I wish to thank my parents for their continued support and never-ending love. I wish to thank my family-in-law and many other friends for their

support and prayers. And I wish to dedicate this to my son, Seungho, whom I love the most.

Lastly and most importantly, I want to thank God for his amazing love and making all this possible.

Contents

CHAPTER 1

Infinitely Often Dense Bases

1. Introduction

We'll use the following notations: For sets A, B of integers and for any integer t, we define the *sumset*

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

the *translation*

$$A + t = \{a + t : a \in A\},$$

and the *difference set*

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

And for any nonnegative integer h, we define the *h-fold sumset* hA as follows:

$$\begin{aligned} 0A &= \{0\} \\ hA &= A + (h-1)A \\ &= \{a_1 + a_2 + \ldots + a_h : a_1, a_2, \ldots, a_h \in A\}. \end{aligned}$$

In particular, $2A = A + A$. And the *dilation* is

$$h * A = \{ha : a \in A\}.$$

1.1. Case of nonnegative integers and Sidon sets.

Let A be a set of nonnegative integers. We define the representation function of A as

$$r_A(n) = \text{card}\{(a,b) : a, b \in A,\ a \leq b,\ a + b = n\},$$

where n is a nonnegative integer. A set of nonnegative integers A is called an *additive basis* for nonnegative integers if $r_A(n) \geq 1$ for all nonnegative integers n, i.e. if all nonnegative integers can be written as a sum of two elements of A.

If all but finitely many nonnegative integers can be written as a sum of two elements from A, then A is called an *asymptotic basis* for nonnegative integers. In this paper we'll try to find relationships between asymptotic bases and representation functions. The most famous one of such problems is Erdős-Turán conjecture [**23**], which states that if A is a basis of nonnegative integers, then

$$\limsup_{n\to\infty} r_A(n) = \infty. \tag{1.1}$$

For survey of this and related problems, see [**19, 49**].

What do we know about aymptotic bases for nonnegative integers and their representation functions? If f is any function from $\mathbb{N}_0$ to $\mathbb{N}_0 \cup \{\infty\}$ with $\text{card}(f^{-1}(0)) < \infty$, then Nathanson [**41**] proved that there exists at most one set A of nonnegative integers with $r_A(n) = f(n)$, i.e. if we prescribe a representation function for A, there can be at most one A with $r_A(n) = f(n)$ for nonnegative integers

case. Erdős [**18**] showed the existence of an asymptotic basis of nonnegative integers with $\log n \ll r_A(n) \ll \log n$ for large n. Other results for asymptotic bases for nonnegative integers and their representation functions are mostly negative ones. For example, Dirac [**15**] showed that the representation function of an asymptotic basis of nonnegative integers cannot be eventually constant. Then, Erdős and Fuchs[**20**] proved that the average value of a representation function cannot even be approximately constant, i.e. for every infinite set A of nonnegative integers and every real number $c > 0$,

$$\sum_{n \le N} r_A(n) \neq cN + o(N^{1/4} \log^{-1/2} N).$$

This result was then generalized by Bateman, Kohlbecker and Tull [**4**] and Vaughan [**52**].

A set of nonnegative integers, A, is called a *Sidon set* if $r_A(n) \le 1$ for all nonnegative integer n. Thus when an integer can be written as a sum of two elements of a Sidon

set, then that representation of the sum is unique up to order, that is, if A is a Sidon set and we have

$$a_1 + a_2 = a_3 + a_4 \quad \text{for} \quad a_1, a_2, a_3, a_4 \in A \tag{1.2}$$

where $a_1 \leq a_2$ and $a_3 \leq a_4$, then,

$$a_1 = a_3 \text{ and } a_2 = a_4. \tag{1.3}$$

Therefore, a Sidon set A is a set that has unique differences of its two elements when the difference is nonzero.

A set of nonnegative integers A is called a *perfect difference set* if any nonzero integer has a unique representation as a difference of two elements of A. Lev [**36**] proved the following:

THEOREM 1.1 ([**36**]). *There is a partition* $\mathbb{N} = \cup_{k=1}^{\infty} A_k$ *of the set of all positive integers such that each* A_k *is a perfect difference set and* $|A_i \cap (A_j + z)| \leq 2$ *for any* $i, j, z \in \mathbb{N}$.

For a set of nonegative integers A, we define the counting function of A, $A(n)$, to be the number of elements of A which is less than or equal to n. Lev asked if there exists a perfect difference set A such that $A(x) \gg x^{1/3+\delta}$ for some $\delta > 0$, which was answered positively by Cilleruelo and Nathanson [**14**].

In Theorem 1.1, we start with a representation function for differences and ask what kind of structure we can get for sets. It's a kind of inverse problem in that we are starting with information about sets such as representation functions, then trying to know about sets themselves. As far as we know, this kind of inverse problem was first studied by Nathanson [**41**]. In this paper, we'll investigate how dense an aymptotic basis can be given its representation function, also a kind of inverse problem in additive number theory.

In our proof, we'll use a result on Sidon sets so let's take a look at it. Let $F_2(n)$ be the maximum number of elements

that can be selected from $\{1, 2, \ldots, n\}$ to form a Sidon set A, i.e. the maximum size of a Sidon set in the $\{1, 2, \ldots, n\}$. Then all sums $a_1 + a_2$ where $a_1, a_2 \in A$ and $a_1 \leq a_2$ are different, so there are $\frac{F_2(n)(F_2(n)+1)}{2}$ sums of two elements of A. But all those sums lie between 1 and $2n$ so

$$\frac{F_2(n)(F_2(n)+1)}{2} \leq 2n.$$

Solving this for $F_2(n)$, we get $F_2(n) \ll n^{1/2}$, giving us a trivial bound for $F_2(n)$. Then Erdős and Turán [**23**], Chowla [**13**] and Bose and Chowla [**7**] proved the following result:

THEOREM 1.2 ([**23, 13, 7**]). $F_2(n) = n^{1/2} + O(n^{5/16})$.

The above theorem uses Ingham's result [**35**] on the difference between all pairs of consecutive primes. It is possible, if needed, to improve the exponent 5/16 slightly using the Riemann-Zeta function.

Infinite Sidon sets are not that well understood. Theorem 1.2 gives $\limsup n^{-1/2}A(n) \leq 1$ for any infinite Sidon set A. Then Erdős [**51**] proved the following for infinite Sidon sets :

$$\liminf_{n\to\infty} n^{-1/2}(\log n)^{1/2}A(n) \ll 1$$

for every infinite Sidon set A. He also proved that there exists an infinite Sidon set A with

$$\limsup_{n\to\infty} n^{-1/2}A(n) \geq 1/2.$$

Then Krückeberg [**34**] constructed an infinite Sidon set A with

$$\limsup_{n\to\infty} n^{-1/2}A(n) \geq 1/\sqrt{2}.$$

Erdős [**18**] has conjectured that for any $\epsilon > 0$, there exists an infinite Sidon set A with $A(n) \gg n^{1/2-\epsilon}$ for all n. Then it was pointed out by Mian-Chowla [**39**] that the greedy algorithm gives us an infinite Sidon set with $A(n) \gg n^{1/3}$ as follows : let $a_1 = 1$ and suppose $a_2, a_3, \ldots, a_m$ has

been chosen(where $m \geq 1$) so that $a_1, a_2, \ldots, a_m$ consist a Sidon set. Then take a_{m+1} to be the least natural number differing from all $a_r + a_s - a_t$ with $1 \leq r, s, t \leq m$ so that we would still have a Sidon set with $a_1, a_2, \ldots, a_m, a_{m+1}$(note that any $a_i,\ i = 1, 2, \ldots, m$ can be written as $a_i + a_i - a_i$, so all a_i's are included in $a_r + a_s - a_t$). Since there are at most m^3 triads $r, s, t,$ there are at most m^3 of $a_r + a_s - a_t$, therefore $a_{m+1} \leq (m+1)^3$. Thus $a_n \leq n^3$ for all n, giving us the formentioned result.

Then Erdős and Rényi [**22**] showed, for every $\epsilon > 0$, the existence of an infinite set A such that $A(n) \gg n^{1/2-\epsilon}$ with the property that the number of solutions of equations

$$m = a_1 + a_2, \quad a_1, a_2 \in A,\ m \text{ an interger}$$

is uniformly bounded for all natural numbers m. And Ruzsa [**48**] constructed an infinite Sidon set A with $A(n) = n^{\sqrt{2}-1+o(1)}$. For details on many of these results, see Halberstam and Roth [**28**].

1.2. Case of integers. Now, let's talk about integer cases. Let A be a set of integers. Let $\mathbb{N}_0$ be the set of nonnegative integers. We define the representation function of A as

$$r_A(n) = \text{card}\{(a,b) : a,b \in A,\ a \leq b,\ a+b=n\},$$

where n is an integer. A set of integers A is called an *additive basis* for integers if $r_A(n) \geq 1$ for all integers n, i.e. if all integers can be written as a sum of two elements of A. If all but finitely many integers can be written as a sum of two elements from A, then A is called an *aymptotic basis* for integers. A set of integers A is called an *unique representation basis* for integers if $r_A(n) = 1$ for all integers n. Also, the *counting function* for the set A is

$$A(y,x) = \text{card}\{a \in A : y \leq a \leq x\}$$

for real numbers x and y. In particular, $A(-x,x)$ is the number of elements a of A with $|a| \leq x$.

We saw that representation function for bases of nonnegative integers was very restrictive. In the case of integers, the situation is very different. We have much more freedom. In fact, Nathanson [**46, 45**] proved the following:

THEOREM 1.3 ([**46, 45**]). *Let $f: \mathbb{Z} \to \mathbb{N}_0 \cup \{\infty\}$ be any function such that the set $f^{-1}(0)$ is a finite set.*

(1) *Let $\phi : \mathbb{N}_0 \to \mathbb{R}$ be any nonnegative function such that $\lim_{x\to\infty} \phi(x) = \infty$. Then there exist uncountably many asymptotic bases A for the integers such that $r_A(n) = f(n)$ for all integers n and $A(-x, x) \leq \phi(x)$ for all $x \geq 0$.*

(2) *There exist uncountably many aymptotic bases A of integers such that $r_A(n) = f(n)$ for all integers n and $A(-x, x) \gg x^{1/3}$ for all sufficiently large x.*

Cilleruelo and Nathason [**14**] later improved the exponent $1/3$ in the second statement of Theorem 1.3 to $\sqrt{2} - 1 + o(1)$ using Ruzsa [**48**]. Also, Łuczak and Schoen [**37**]

showed the second statement of Theorem 1.3 by showing that a set with a condition of Sidon type can be extended to a unique representation bases.

Note that if $r_A(n) = f(n)$, then the requiring the set $f^{-1}(0)$ to be finite just means that only finitely many integers cannot be written as a sum of two elements of A, i.e. A is an asymptotic basis. Thus, the situation is quite different from that of nonnegative integer case and almost all functions can be a representative function for an aymptotic basis for integers. Note that you can find an h-fold sumset analogue of Theorem 1.3 in [**46, 45**] as well.

Clearly any asymptotic basis for integers has to be an infinite set. Therefore, the first statement of Theorem 1.3 means an asymptotic basis for integers can be as sparse as we want, and the second statement of Theorem 1.3 means there is an asymptotic basis of integers with some thickness. Nathanson [**44**] also constructed an unique representation

basis A for integers with $\log x \ll A(-x,x) \ll \log x$ for all $x \geq 1$. Then Nathanson [**45**] asked how dense an aymptotic basis of integers with a prescribed representation function can be. This is still open, but some progress has been made by Chen [**12**] and again in this paper, and we'll discuss them in a moment.

Before we get to them, let A be any set of integers with $r_A(n) \leq r$ for some $r > 0$ for all integers n. Then let's take $k = A(-x,x)$. Then there are $\frac{k(k+1)}{2}$ ways to make $a_i + a_j$, where a_i, a_j are in A and $|a_i|, |a_j| \leq x$. All these sums belong in the interval $[-2x, 2x]$ and each number in that interval is represented as $a_i + a_j$ at most r times. Therefore,

$$\frac{k(k+1)}{2} \leq r(4x+1)$$

and solving this for $k = A(-x,x)$ gives

$$A(-x,x) \ll x^{1/2} \tag{1.4}$$

for all $x > 0$.

Let's go back to nonnegative integers case for a moment. The similar argument as above for a set of nonnegative integers A with $r_A(n) \leq r$ for some $r > 0$ for all nonegative integers n also yields $A(x) \ll x^{1/2}$ for all $x > 0$. That means if a set of nonnegative integers A have $\limsup_{n\to\infty} n^{-1/2}A(n) = \infty$, then $r_A(n)$ can't be bounded. Thus, for the bases of nonnegative integers A with $\limsup_{n\to\infty} n^{-1/2}A(n) = \infty$, Erdős-Turán conjecture is settled. So we only concern ourselves with the case that $\limsup_{n\to\infty} n^{-1/2}A(n)$ is bounded. Note $\limsup_{n\to\infty} n^{-1/2}A(n)$ can't be zero. To see this, let $A^{(n)} = \{a \in A : a \leq n\}$ for a positive integer n. Note the size of $A^{(n)}$ is $A(n)$. Let's take k to be the size of the sumset $A^{(n)} + A^{(n)}$. If $n = a_1 + a_2$ where $a_1, a_2 \in A$, then since A is a set of nonnegative integers, both a_1, a_2 are in $A^{(n)}$. In fact, whenever any integer $m \leq n$ is written as $a_1 + a_2$, both a_1, a_2 are in $A^{(n)}$. If A is a basis for nonnegative integers, then all positive integers up to n is a sum

of only with elements of $A^{(n)}$, i.e. the interval $[1, n]$ is a subset of $A^{(n)} + A^{(n)}$, thus $n \leq k$. But clearly $k < A(n)^2$, giving us $n < A(n)^2$, proving our claim. In short, Erdős-Turán conjecture is open only for the bases A such that $0 < \limsup_{n\to\infty} n^{-1/2} A(n) < \infty$ and these bases are called *thin bases*. For more on thin bases, see Halberstam and Roth [**28**] and Hofmeister [**31**].

Coming back to integers case, in the light of (1.4) for A with a bounded representation function, Nathanson [**44**] asked the following: Does there exist a number $\theta < 1/2$ such that $A(-x, x) \leq x^\theta$ for every unique representation basis A and for all sufficiently large x? The question was answered negatively by Chen [**12**].

THEOREM 1.4 ([**12**]). *For any $\epsilon > 0$, there exists an unique representation basis A for the integers such that for infinitely many positive integers x, we have*

$$A(-x, x) \geq x^{1/2-\epsilon}.$$

In this paper, we improve Theorem 1.4 to a basis of integers with any prescribed representation function and we also improve the upper bound, giving us an infintely often dense basis of integers with a prescribed representation function.

2. Preliminary Lemmas

From now on, f will denote a function $f : \mathbb{Z} \to \mathbb{N}_0 \cup \{\infty\}$ such that the set $f^{-1}(0)$ is a finite set. Then there exists a positive integer d_0 such that $f(n) \geq 1$ for all integers n with $|n| \geq d_0$. Nathanson [**46**] proved the following:

LEMMA 2.1 ([**46**]). *Given a function f as above, there exists a sequence $U = \{u_k\}_{k=1}^{\infty}$ of integers such that, for every $n \in \mathbb{Z}$ and $k \in \mathbb{N}$,*

$$f(n) = card\{k \geq 1 : u_k = n\}. \tag{2.1}$$

PROOF. First, we claim that every positive integer m can be written uniquely in the form

$$m = s^2 + s + 1 + r$$

where s is a nonnegative integer, r is an integer such that $|r| \leq s$. To see this, note that when $r = -s$, the expression is $s^2 + 1$, and as we increase r up to s, the expression increases up to $(s + 1)^2$. Thus, for fixed s, the list of expressions is $s^2 + 1, s^2 + 2, \ldots, (s + 1)^2$, giving us a block of consecutive integers corresponding to s. Then when we increase s by 1, the block that correponds to $s+1$ is $(s+1)^2+1, (s+1)^2+2, \ldots, (s+2)^2$ and these two blocks have no gaps between them. So as we change s, the expression will cover all the positive integers. And all positive integers are covered only once. Thus the claim is true.

We construct the sequence

$$\begin{aligned} V &= \{0, -1, 0, 1, -2, -1, 0, 1, 2, -3, -2, -1, 0, 1, 2, 3, \ldots\} \\ &= \{v_m\}_{m=1}^{\infty} \end{aligned}$$

where $v_{s^2+s+1+r} = r$ for $|r| \leq s$. For every nonnegative integer k, the first occurrence of $-k$ in this sequence is $v_{k^2+1} = -k$, and the first occurrence of k in this sequence is $v_{(k+1)^2} = k$.

The sequence U will be the unique subsequence of V constructed as below: Let $n \in \mathbb{Z}$. If $f(n) = \infty$, then U will contain the terms $v_{s^2+s+1+n}$ for every $s \geq |n|$. If $f(n) = l < \infty$, then U will contain the l terms $v_{s^2+s+1+n}$ for $s = |n|, |n|+1, \ldots, |n|+l-1$ in the subsequence U but not the terms $v_{s^2+s+1+n}$ for $s \geq |n|+l$. Let $m_1 < m_2 < \cdots$ be the strictly increasing sequence of positive integers such that $\{v_{m_k}\}_{k=1}^{\infty}$ is the resulting subsequence of V. Let $U =$

$\{u_k\}_{k=1}^{\infty}$, where $u_k = v_{m_k}$. Then $f(n) = \text{card}\{k \geq 1 : u_k = n\}$. □

LEMMA 2.2. *Let A be a finite set of integers with $r_A(n) \leq f(n)$ for all integers n, $0 \notin A$, and for all integers n,*

$$r_A(n) \geq \#\{i \leq m : u_i = n\}$$

for some integer m which depends only on the set A. Then, there exists a finite set of integers B such that $A \subseteq B$, $r_B(n) \leq f(n)$ for all integers n,

$$r_B(n) \geq \#\{i \leq m+1 : u_i = n\}$$

for all integers n, and $0 \notin B$.

PROOF. If $r_A(n) \geq \#\{i \leq m+1 : u_i = n\}$ for all n, then take $B = A$ and we are done. Otherwise, note that

$$\#\{i \leq m : u_i = n\} = \#\{i \leq m+1 : u_i = n\}$$

for all $n \neq u_{m+1}$ and

$$\#\{i \leq m : u_i = u_{m+1}\} + 1 = \#\{i \leq m+1 : u_i = u_{m+1}\}.$$

Since

$$r_A(n) \geq \#\{i \leq m : u_i = n\}$$

for all n, if

$$r_A(n) < \#\{i \leq m+1 : u_i = n\}$$

for some n as we are assuming now, then by the arguments above, we must have

$$r_A(u_{m+1}) < \#\{i \leq m+1 : u_i = u_{m+1}\} \leq f(u_{m+1}).$$

Let $d = \max\{d_0, |u_{m+1}|, |a| \ a \in A\}$. Choose $c > 4d$ if $u_{m+1} \geq 0$ and $c < -4d$ if $u_{m+1} < 0$. Note that $|c| > 4d$.

Let $B = A \cup \{-c, \ c + u_{m+1}\}$. Then $2B$ has three parts:

$$2A, \ A + \{-c, \ c + u_{m+1}\}, \ \{-2c, \ u_{m+1}, \ 2c + 2u_{m+1}\}.$$

If $a \in 2A$, then $-2d \leq a \leq 2d$. If $a \in A$, then if $u_{m+1} \geq 0$, $c > 0$, so we have

$$\begin{aligned} a - c &\leq d - 4d = -3d, \\ a + c + u_{m+1} &\geq -d + 4d + u_{m+1} \geq 3d + u_{m+1} \geq 3d\,, \end{aligned}$$

and if $u_{m+1} < 0$, $c < 0$, so we have

$$\begin{aligned} a - c &\geq -d + 4d = 3d, \\ a + c + u_{m+1} &\leq d - 4d + u_{m+1} = -3d + u_{m+1} \leq -3d\,. \end{aligned}$$

Thus,

$$2A \cap A + \{-c,\ c + u_{m+1}\} = \emptyset$$

and each element of $A + \{-c,\ c + u_{m+1}\}$ has an unique representation in the form of $a + \{-c,\ c + u_{m+1}\},\ a \in A$, and the same for $\{-2c,\ u_{m+1},\ 2c + 2u_{m+1}\}$ in the form of $\{-c,\ c + u_{m+1}\} + \{-c,\ c + u_{m+1}\}$. Also,

$$\begin{aligned} |-2c| &= 2|c| > 8d, \\ |2c + 2u_{m+1}| &= 2|c + u_{m+1}| \geq 2|c| \geq 8d\,, \end{aligned}$$

thus $2A \cap \{-2c, 2c + 2u_{m+1}\} = \emptyset$ (recall c and u_{m+1} has the same sign). Also note that $A + \{-c,\ c + u_{m+1}\}$ and $\{-2c,\ u_{m+1},\ 2c + 2u_{m+1}\}$ are disjoint. To see this, for example, if $a - c = 2c + 2u_{m+1}$ for some $a \in A$, then $a = 3c + 2u_{m+1}$ so $|a| = |3c + 2u_{m+1}| \geq |3c| > 12d$, giving us a contradiction. Other cases are similar.

Thus, we have

$$r_B(n) = \begin{cases} r_A(n) + 1 & \text{if } n = u_{m+1} \\ r_A(n) & \text{if } n \in 2A \setminus \{u_{m+1}\} \\ 1 & \text{if } n \in 2B \setminus \big\{2A \cup \{u_{m+1}\}\big\}. \end{cases}$$

Now, we have $r_A(u_{m+1}) < f(u_{m+1})$, so

$$r_B(u_{m+1}) = r_A(u_{m+1}) + 1 \ \leq f(u_{m+1}).$$

And, if $n \in 2B \setminus \big\{2A \cup \{u_{m+1}\}\big\}$, then $|n| \geq d_0$, so $f(n) \geq 1 = r_B(n)$. Thus, $r_B(n) \leq f(n)$ for all n.

Now, $r_A(u_{m+1}) \geq \#\{i \leq m : u_i = u_{m+1}\}$ so

$$\begin{aligned} r_A(u_{m+1}) + 1 &\geq \#\{i \leq m : u_i = u_{m+1}\} + 1 \\ &= \#\{i \leq m+1 : u_i = u_{m+1}\}, \end{aligned}$$

therefore,

$$r_B(u_{m+1}) \geq \#\{i \leq m+1 : u_i = u_{m+1}\}.$$

If $n \in 2A \setminus \{u_{m+1}\}$, then

$$r_B(n) = r_A(n) \geq \#\{i \leq m : u_i = n\} = \#\{i \leq m+1 : u_i = n\}.$$

If $n \in 2B \setminus \big\{2A \cup \{u_{m+1}\}\big\}$, then

$$0 = r_A(n) \geq \#\{i \leq m : u_i = n\} = \#\{i \leq m+1 : u_i = n\}$$

so

$$0 = \#\{i \leq m+1 : u_i = n\} \leq 1 = r_B(n).$$

Thus,

$$r_B(n) \geq \#\{i \leq m+1 : u_i = n\}$$

for all n. □

LEMMA 2.3. *Let A be a finite set of integers with $r_A(n) \leq f(n)$ for all n, and $0 \notin A$. Let $\phi(x)\colon \mathbb{N}_0 \to \mathbb{R}$ be a nonnegative function such that $\lim_{x\to\infty} \phi(x) = \infty$. Then for any $M > 0$, there exists an integer $x > M$ and a finite set of integers B with $0 \notin B$, $A \subseteq B$, $r_B(n) \leq f(n)$ for all n, and $B(-x, x) > \sqrt{x}/\phi(x)$.*

PROOF. By theorem 1.2, for all $n \geq 1$, there exists a Sidon set $D \subseteq [1, n]$ such that $|D| = n^{1/2} + O(n^{5/16}) = n^{1/2} + o(n^{1/2})$. Choose an integer x which satisfies following:

(1) $\phi(x) > M + \sqrt{20T}$ where $T = \max\{d_0,\ |a| \text{ where } a \in A\}$.

(2) x is a multiple of $5T$.

(3) $x > M$.

(4) If n is large enough, $|D| = \sqrt{n} + o(\sqrt{n}) > \sqrt{n} - \frac{1}{2}\sqrt{n} = \sqrt{n}/2$. Let x be large enough so that $n = x/5T$ is large enough to satisfy the above.

Let $B = A \cup \{5Td : d \in D\}$ where $D \subseteq [1, n]$ with $n = x/5T$ as above. Then

$$\begin{aligned} B(-x, x) &\geq B(0, x) \geq D(1, n) = |D| \\ &> \frac{\sqrt{n}}{2} = \frac{1}{2}\sqrt{\frac{x}{5T}} = \frac{\sqrt{x}}{\sqrt{20T}} > \frac{\sqrt{x}}{\phi(x) - M} > \frac{\sqrt{x}}{\phi(x)}. \end{aligned}$$

Now, note that $2B$ has three parts:

$$2A,\ A + 5Td \text{ for } d \in D, \text{ and } 5T(d_1 + d_2) \text{ for } d_1, d_2 \in D.$$

If $m \in 2A$, then $-2T \leq m \leq 2T$. If $a \in A$, $d \in D$, then $a + 5Td \geq -T + 5T = 4T$. For $d_1, d_2 \in D$, $5T(d_1 + d_2) \geq 10T$. Thus, we have $2A \cap (A + 5T*D) = \emptyset$ and $2A \cap \{5T(d_1 + d_2) : d_1, d_2 \in D\} = \emptyset$. Now, if $a + 5Td_1 = 5T(d_2 + d_3)$ for $a \in A$, $d_i \in D$, then $|a| = 5T\,|d_2 + d_3 - d_1|$. If $|\,d_2 + d_3 - d_1| = 0$, then $a = 0 \in A$, a contradiction. And if $|\,d_2 + d_3 - d_1| \geq 1$, $|\,a| \geq 5T$, a contradiction. Thus

$$(A + 5T*D) \cap \{5T(d_1 + d_2) : d_1, d_2 \in D\} = \emptyset.$$

If $a_1 + 5Td_1 = a_2 + 5Td_2$ for $a_1, a_2 \in A,\ d_1, d_2 \in D$, then $|a_1 - a_2| = 5T|d_1 - d_2|$. As above, this can't happen unless $a_1 = a_2$ and $d_1 = d_2$. And if $5T(d_1 + d_2) = 5T(d_3 + d_4)$ for $d_i \in D$ with $d_1 \le d_2$, $d_3 \le d_4$, then $d_1 + d_2 = d_3 + d_4$. Since D is a Sidon set, we have $d_1 = d_3,\ d_2 = d_4$. Thus we have

$$r_B(n) = \begin{cases} r_A(n) & \text{if } n \in 2A \\ 1 & \text{if } n \in 2B \setminus 2A. \end{cases}$$

If $n \in 2B \setminus 2A, \quad n \ge T \ge d_0$, so $f(n) \ge 1 = r_B(n)$. Thus, $r_B(n) \le f(n)$ for all n. □

3. Main Result

THEOREM 3.1. *Let $f\colon \mathbb{Z} \to \mathbb{N}_0 \cup \{\infty\}$ be a function such that the set $f^{-1}(0)$ is a finite set. Let $\phi\colon \mathbb{N}_0 \to \mathbb{R}$ be any nonnegative function such that $\lim_{x\to\infty} \phi(x) = \infty$. Then, there exists an asymptotic basis A for integers such that $r_A(n) = f(n)$ for all n, and for infinitely many positive integers x, we have $A(-x, x) > \sqrt{x}/\phi(x)$.*

PROOF. Recall that given such a function f, we have d_0 and $\{u_k\}$ as defined in Section 2. We use induction to get an infinite sequence of finite sets of integers $A_1 \subseteq A_2 \subseteq \cdots$ and a sequence of positive integers $\{x_i\}_{i=1}^{\infty}$ with $x_{i+1} > x_i$ such that, for all positive integers l, we have

(1) $r_{A_l}(n) \leq f(n)$ for all n.

(2) $r_{A_{2l}}(n),\ r_{A_{2l+1}}(n) \ \geq \#\{i \leq l+1 : u_i = n\}$ for all n.

(3) $A_{2l-1}(-x_l, x_l) > \sqrt{x_l}/\phi(x_l)$.

(4) $0 \notin A_l$.

If $u_1 \geq 0$, take $c = 4d_0 > 0$. If $u_1 < 0$, take $c = -4d_0 < 0$. Let $\alpha = |2c + 2u_1| > 0$ (thus $\alpha > |c|, |u_1|, d_0$). As before, if n is large enough, there exists a Sidon set $D \subseteq [1, n]$ such that $|D| > \sqrt{n}/2$. Take such an integer n which also satisfies that $\phi(3\alpha n) > 2\sqrt{3\alpha}$.

Take $A_1 = 3\alpha * D \ \cup \{-c,\ c + u_1\}$ and $x_1 = 3\alpha n$. Then $2A_1$ has three parts:

$$2(3\alpha * D),\quad 3\alpha * D + \{-c,\ c + u_1\},\quad \{-2c,\ u_1,\ 2c + 2u_1\}.$$

If $3\alpha d_1 + 3\alpha d_2 = 3\alpha d_3 - c$, then $c = 3\alpha(d_3 - d_2 - d_1)$. If $d_3 \neq d_2 + d_1$, then $|c| \geq 3\alpha$, a contradiction. So $d_3 = d_2 + d_1$ and $c = 0$, again yielding a contradiction. And if $3\alpha d_1 + 3\alpha d_2 = 3\alpha d_3 + c + u_1$, then $c + u_1 = 3\alpha(d_1 + d_2 - d_3)$. If $d_1 + d_2 - d_3 \neq 0$, then $|c + u_1| \geq 3\alpha$, a contradiction. If $d_1 + d_2 - d_3 = 0$, then $c + u_1 = 0$, also a contradiction. Thus, $2(3\alpha * D) \cap 3\alpha * D + \{-c,\ c + u_1\} = \emptyset$. If $x \in 2(3\alpha * D)$, then $x \geq 6\alpha$, thus $2(3\alpha * D) \cap \{-2c,\ u_1,\ 2c + 2u_1\} = \emptyset$. Also, we have $3\alpha * D + \{-c,\ c + u_1\} \cap \{-2c,\ u_1,\ 2c + 2u_1\} = \emptyset$. To see this, for example, if $3\alpha d - c = 2c + 2u_1$, then $3\alpha d = 3c + 2u_1$, so $3\alpha \leq |3c + 2u_1| < |4c + 4u_1| = 2\alpha$, a contradiction. Other cases are similar.

Now, if $3\alpha d_1 + 3\alpha d_2 = 3\alpha d_3 + 3\alpha d_4$ with $d_1 \leq d_2$, $d_3 \leq d_4$, then $d_1 + d_2 = d_3 + d_4$, but D is a Sidon set, thus $d_1 = d_3$, $d_2 = d_4$. If $3\alpha d_1 - c = 3\alpha d_2 + c + u_1$, then $2c + u_1 = 3\alpha(d_1 - d_2)$. If $d_1 \neq d_2$, then $|2c + u_1| \geq 3\alpha$ but $|2c + u_1| < |2c + 2u_1| = \alpha$. So $d_1 = d_2$. Then $-c = c + u_1$,

so $-2c = u_1$, a contradiction. Thus,

$$r_{A_1}(n) = \begin{cases} 1 & \text{if } n \in 2A_1 \\ 0 & \text{if } n \notin 2A_1. \end{cases}$$

Now, $3\alpha d - c \geq 3\alpha - \alpha = 2\alpha$, and also $3\alpha d + c + u_1 \geq 3\alpha - \alpha - \alpha = \alpha$. So if $n \in 2A_1 \setminus \{u_1\}$ then $|n| \geq d_0$, so $f(n) \geq 1$. For $n = u_1$, by the definition of $\{u_k\}$, we have $f(u_1) = \#\{k : u_k = u_1\} \geq 1$. Thus, for all $n \in 2A_1$, $r_{A_1}(n) = 1 \leq f(n)$. If $n \notin 2A_1$, $r_{A_1}(n) = 0 \leq f(n)$. Therefore, for all n, $r_{A_1}(n) \leq f(n)$. Now, we have $1 = r_{A_1}(u_1) \geq \#\{i \leq 1 : u_i = u_1\}$. For other $n \neq u_1$, $r_{A_1}(n) \geq \#\{i \leq 1 : u_i = n\} = 0$. Thus, $r_{A_1}(n) \geq \#\{i \leq 1 : u_i = n\}$ for all n. Also,

$$\begin{aligned} A_1(-x_1, x_1) &\geq A_1(1, 3\alpha n) \geq D(1, n) = |D| \\ &> \frac{\sqrt{n}}{2} = \frac{\sqrt{3\alpha n}}{2\sqrt{3\alpha}} > \frac{\sqrt{3\alpha n}}{\phi(3\alpha n)} = \frac{\sqrt{x_1}}{\phi(x_1)}. \end{aligned}$$

Thus A_1 satisfies all the conditions (1) to (4).

Now, suppose we have $A_1 \subseteq A_2 \subseteq \cdots \subseteq A_{2l-1}$ and $x_1 < x_2 < \cdots < x_l$. By Lemma 2.2, there exist A_{2l} such that $A_{2l-1} \subseteq A_{2l}$ with $r_{A_{2l}}(n) \leq f(n)$ for all n and

$$r_{A_{2l}}(n) \geq \#\{i \leq l+1 : u_i = n\}$$

for all n, and $0 \notin A_{2\,l}$. Now, by Lemma 2.3, there exists an integer $x_{l+1} > x_l$ and A_{2l+1} with $0 \notin A_{2l+1}$, $A_{2l} \subseteq A_{2l+1}$, $r_{A_{2l+1}}(n) \leq f(n)$ for all n, and

$$A_{2l+1}(-x_{l+1}\,,\, x_{l+1}) > \frac{\sqrt{x_{l+1}}}{\phi(x_{l+1})}\,.$$

Also, $r_{A_{2l+1}}(n) \geq r_{A_{2l}}(n) \geq \#\{i \leq l+1 : u_i = n\}$ for all n.

Now, let $A = \cup_{l=1}^{\infty} A_l$. By conditions (1) and (2), $r_A(n) = f(n)$ for all n and

$$A(-x_k\,,\, x_k) \geq A_{2k-1}(-x_k\,,\, x_k) > \frac{\sqrt{x_k}}{\phi(x_k)}$$

for all k. □

CHAPTER 2

Geometric Structure of Sumsets

1. Introduction

1.1. Definitions. From now on, we'll stay in $\mathbb{R}^n$.

Affine Subspaces are the translation of linear subspaces. The *dimension* of an affine subspace is the dimension of the linear subspace corresponding to the affine subspace. An *affine hull*, $\text{aff}(x_1, x_2, \ldots, x_l)$, of $x_1, x_2, \ldots, x_l$ where $x_i \in \mathbb{R}^n$ is

$$\{x \in \mathbb{R}^n : x = \lambda_1 x_1 + \lambda_2 x_2 + \ldots + \lambda_l x_l \text{ for } \lambda_i \in \mathbb{R}, \sum_{i=1}^{l} \lambda_i = 1\},$$

or equivalently, the intersection of all affine subspaces that contain $x_1, x_2, \ldots, x_l$. A set of $d+1$ points $x_1, x_2, \ldots, x_{d+1}$ are called *affinely independent* if its affine hull has the dimension d, or equivalently, $x_2 - x_1, x_3 - x_1, \ldots, x_{d+1} - x_1$ are

linearly independent. If $x_1, x_2, \ldots, x_{d+1}$ are affinely independent, then in their *affine sum* $\lambda_1 x_1 + \lambda_2 x_2 + \ldots + \lambda_{d+1} x_{d+1}$ with $\sum \lambda_i = 1$, all λ_i's are uniquely determined, and vice versa.

A *hyperplane* H is the set $\{x \in \mathbb{R}^n : (x, u) = \alpha\}$ for some nonzero $u \in \mathbb{R}^n$ and some number α, where $(\cdot, \cdot)$ indicates an inner product in $\mathbb{R}^n$. The vector u is called a *normal vector* to H. A hyperplane divides $\mathbb{R}^n$ into two closed halfspaces H^+ and H^- where

$$H^+ = \{x \in \mathbb{R}^n : (x, u) \geq \alpha\}$$

$$H^- = \{x \in \mathbb{R}^n : (x, u) \leq \alpha\}.$$

We write $d(x, y)$ to denote the distance between two points $x, y \in \mathbb{R}^n$. If $S, T \subseteq \mathbb{R}^n$, then

$$d(x, S) = \inf_{s \in S} d(x, s),$$

$$d(S, T) = \inf_{s \in S, t \in T} d(s, t).$$

In particular, the distance from a point $x \in \mathbb{R}^n$ to a hyperplane H where $x \notin H$, is given by the length of the perpendicular line segment from x to H. For, if not, say $y \in H$ is a point with $d(x, y) < d(x, x')$ where x' is the intersection of H and the perpendicular line segment. Then the points x, x', y form a right triangle whose hypotenuse is given by x and y, and the hypotenuse's length is shorter than that of the side given by x and x', which is impossible.

If two hyperplanes H_1, H_2 are parallel, their normal vectors are mutiples of each other, so we can take a same normal vector u and write $H_1 = \{x : (x, u) = \alpha_1\}$ and $H_2 = \{x : (x, u) = \alpha_2\}$. Take any $x \in H_1$. Then $d(x, H_2)$ is given by the perpendicular line segment. To calculate the distance, note that $x+tu$ where $t \in \mathbb{R}$ gives the perpendicular ray from x to H_2. If the ray meets H_2 when $t = t_2$, then $t_2 = (\alpha_2 - \alpha_1)/|u|^2$. Thus, $d(x, H_2) = |t_2 u| = (\alpha_2 - \alpha_1)/|u|$, which is independent of the choice of x. Therefore, when

H_1 and H_2 are parallel, $d(H_1, H_2)$ is given by any perpendicular line segment joining them.

The *convex hull* , $\text{conv}(x_1, x_2, \ldots, x_l)$, of $x_1, x_2, \ldots, x_l$ is

$$\{x \in \mathbb{R}^n : \ x = \lambda_1 x_1 + \lambda_2 x_2 + \ldots + \lambda_l x_l \,, \quad \lambda_i \geq 0 \text{ for all } i,$$

$$\text{and } \textstyle\sum_{i=1}^{l} \lambda_i = 1\} \,.$$

A *polytope* is the convex hull of a finite set of points in some $\mathbb{R}^n$, or equivalently, a bounded set which is an intersection of finitely many closed halfspaces. A *d-simplex* is the convex hull of any $d + 1$ affinely independent points in some $\mathbb{R}^n$. If the hyperplane H intersects the polytope and the whole polytope lies in one of H^+ or H^-, then it's called a *supporting hyperplane.* A *face* is the intersection of the polytope and a supporting hyperplane. The *dimension* of a polytope is the dimension of its affine hull. A *facet* is a face whose dimension is one less than that of the polytope.

Now, let $\Delta \neq \emptyset$ be a polytope and $\Delta = H_1^+ \cap \ldots \cap H_l^+$. We may assume that $H_i \cap \Delta \neq \emptyset$ for all i, because: assume $H_1 \cap \Delta = \emptyset$, then let $K = H_2^+ \cap \ldots \cap H_l^+ \supseteq \Delta \neq \emptyset$, so K is nonempty and convex. If $H_1^- \cap K = \emptyset$, then $K \subseteq H_1^+$ and $K = K \cap H_1^+ = \Delta$, so we are done. If $x \in H_1^- \cap K$, choose $y \in H_1^+ \cap K = \Delta$. Then connect x and y by a straight line, which meets H_1 at z. Since K is convex, $z \in K$ and $z \in H_1 \subseteq H_1^+$. Thus, $z \in \Delta \cap H_1$, a contradiction.

Let h be a positive integer and $\Delta = \text{conv}(a_1, a_2, \ldots, a_m)$ where $a_i \in \mathbb{Z}^n$. Then define the *dilation of* Δ, $h * \Delta$, as

$$\begin{aligned} h * \Delta &= \{hx : x \in \Delta\} \\ &= \{\sum \lambda_i a_i : \lambda_i \geq 0, \sum \lambda_i = h\} \\ &= \text{conv}(ha_1, \ldots, ha_m)\,. \end{aligned}$$

We present some elementary facts without proof. The details can be found in [**9**], [**55**], and [**24**].

PROPOSITION 1.1. *We have the following:*

(1) *Any polytope is a compact set.*

(2) *Every polytope is the convex hull of its vertices.*

(3) *If a polytope can be written as the convex hull of a finite point set S, then the finite set S contains all the vertices of the polytope, i.e. all the vertices of the polytope belong to S.*

(4) *The face F is a polytope, with the vertex set of F equals the intersection of F with the vertex set of the polytope.*

(5) *Every intersection of faces is a face of the polytope.*

PROPOSITION 1.2. *Let Δ be a polytope in $\mathbb{R}^n$. Then the following are equivalent for $x \in \Delta$.*

(1) *x is not contained in a face of Δ .*

(2) *x can be represented in the form $x = \sum_{i=0}^{n} \lambda_i x_i$ for $n+1$ affinely independent points $x_0, x_1, \ldots, x_n \in \Delta$ with $\lambda_i > 0$ and $\sum_{i=0}^{n} \lambda_i = 1$.*

If one of the conditions in Proposition 1.2 holds, then the point is called an *interior point* of Δ. It can be checked that this definition agrees with the usual definition of interior points using topology. The *boundary* of Δ, written $\partial(\Delta)$, is the union of all faces of Δ.

1.2. Background. It was Minkowski who first studied the geometry of numbers. General survey on this subject and Minkowski's theorems can be found on Cassels [**10**] and Siegel [**50**]. Also, Erdős, Gruber and Hammer [**21**] gave a nice problem-oriented survey.

When $\Delta \subseteq \mathbb{R}^2$ is a lattice polytope (a polytope whose vertices are lattice points), Pick [**47**] proved that

$$|\Delta \cap \mathbb{Z}^2| = \text{area}(\Delta) + \frac{|\partial(\Delta) \cap \mathbb{Z}^2|}{2} + 1\,.$$

More generally, assume that $\Delta \subseteq \mathbb{R}^n$ is an n-dimensional nonempty lattice polytope, and h is a positive integer. Then Ehrhart [**17**] showed that there is a polynomial $p(h)$, called

the *Ehrhart polynomial*, such that

$$|(h * \Delta) \cap \mathbb{Z}^n| = p(h)$$

where

$$p(h) = \mathrm{Vol}(\Delta)h^n + \frac{\mathrm{Vol}(\partial(\Delta))}{2}h^{n-1} + \cdots + \chi(\Delta)\,.$$

Here, $\chi(\Delta)$ is the Euler characteristic of Δ, and $\mathrm{Vol}(\partial(\Delta))$ is the surface area of Δ normalized with respect to the sublattice on each face of Δ. The Ehrhart-MacDonald reciprocity law states that $p(-h) = (-1)^n|\mathrm{interior}(h\Delta) \cap \mathbb{Z}^n|\,.$

Many people have worked on other coefficients of $p(h)$, and although no simple geometric meaning is known for other coefficients, some results are known. For example, it is known that the kth coefficient of $p(h)$ can be expressed as $\sum_\Gamma \mu(\Gamma)\mathrm{Vol}(\Gamma)$, where the sum is taken over all k-faces Γ of Δ and $\mu(\Gamma)$ is some value of a certain additive measure (see, for example, McMullen [**38**]). It's also known that the coefficients can be written with Dedekind sum,

and Chen [**11**] gave an elementary proof for some of these expressions. Chen [**11**] also gave a formula for the coefficients in terms of the elementary symmetric functions when Δ is a simplex. Beck [**5**] has expressed $p(h)$ as an integral in several complex variables.

The Ehrhart's theorem was studied extensively partly because it has a lot of connections with other branches of mathematics. For example, Ehrhart's theorem turns out to be equivalent to the so-called Riemann-Roch-Hirzebruch theorem related to toric varieties. Algebraic geometers have shown that the Hilbert polynomials of toric varieties associated to lattice polytopes describe the number of lattice points inside their dilates. Differential geometers are interested in it in connection with the Durfree conjecture. Beck, Diaz and Robins [**6**] considered the connection between counting lattice points inside a rational polytope and the Frobenius problem.

Let's consider a rational polytope (a polytope with vertices of rational coordinates), and let D be the smallest positive integer such that $D*\Delta$ has integral vertices. Then Ehrhart [**16**] showed that

$$|(h*\Delta)\cap\mathbb{Z}^n| = p(h)$$

where $p(h)$ is a quasi-polynomial function with a period of D, i.e. there exist polynomials $f_0(h), f_1(h), \ldots, f_{D-1}(h)$ such that $p(h) = f_j(h)$ for $h \equiv j(\text{mod } D)$. Woods [**54**] proved that, for fixed dimension, there is a polynomial time algorithm which decides whether an integer is a period of $p(h)$. In particular, there is a polynomial time algorithm to decide whether $p(h)$ is a polynomial. And Barvinok [**3**] described an algorithm which counts lattice points in fixed dimension in polynomial time.

If $\Delta = \text{conv}(A)$ where A is a finite set of integral points in some $\mathbb{R}^n$, then $|(h*\Delta)\cap\mathbb{Z}^n| \geq |hA|$. Then we can

consider the growth of hA. Nathanson [**40**] proved the following theorem.

THEOREM 1.3. *Let $k \geq 2$ and let $A = \{a_1, \ldots, a_k\}$ be a finite set of integers such that*

$$0 = a_1 < a_2 < \cdots < a_k \text{ and } \gcd(a_2, \ldots, a_k) = 1.$$

Then there exists integers c and d and sets $C \subseteq [0, c-2]$ and $D \subseteq [0, d-2]$ such that

$$hA = C \cup [\, c, ha_k - d \,] \cup (ha_k - D)$$

for all sufficiently large h.

In particular, the growth of hA is a linear function when A is a subset of integers. When we have $A_1, A_2, \ldots, A_r$ and B as finite subsets of $\mathbb{N}_0$, normalized similarly as above, then Han, Kirfel, and Nathanson [**29**] showed that $|B + h_1A_1 + \cdots + h_rA_r|$ is a multilinear function of $h_1, \ldots, h_r$ eventually. If $A_1, A_2, \ldots, A_r$ and B are finite subsets of

an abelian semigroup which contains 0, then $|B + h_1A_1 + \cdots + h_rA_r|$ is a polynomial of $h_1, \ldots, h_r$ for all sufficiently large $h_1, \ldots, h_r$, which was proven by Khovanskiĭ [**33**] when $r = 1$, and by Nathanson [**43**] for $r \geq 2$. And if A, B are finite subsets of an abelian group without elements of finite order, then Khovanskiĭ [**33**] computed the degree and the leading coefficient of the polynomial above (although his proof contained a gap since he failed to prove Theorem 2.4, which we prove later).

Let A be a finite set in $\mathbb{R}^n$. There is a kind of inverse problem we can answer: if the sumset $2A$ is small, i.e. if $|2A| \leq c|A|$ where $1 < c < 2^n$, then a positive proportion of A must lie on a hyperplane. For proof, see Nathanson [**42**].

2. Khovanskiĭ's Work

Let's see what Khovanskiĭ did in his paper [**33**]. Let A be a finite subset of $\mathbb{Z}^n$, $A = \{a_1, \ldots, a_m\}$, with $|A| = m$

and $\Delta = conv(A)$. Also assume that A generate $\mathbb{Z}^n$ as a group.

LEMMA 2.1. *There exists a constant C with the following property: for all linear combination $\sum \lambda_i a_i$ of $a_i \in A$ with real coefficients λ_i such that $\sum \lambda_i a_i$ is an integral point, there exists a linear combination $\sum n_i a_i$ of a_i with integer coefficients such that $\sum n_i a_i = \sum \lambda_i a_i$, with $\sum |n_i - \lambda_i| < C$.*

PROOF. Let $X = \{x : x \in \mathbb{Z}^n, x = \sum \lambda_i a_i, \text{ with } 0 \leq \lambda_i \leq 1\}$, which is a finite set. Since A generate $\mathbb{Z}^n$, each $x \in X$ can be written as $x = \sum_{i=1}^m n_i(x) a_i$, where $n_i(x) \in \mathbb{Z}$. So for each $x \in X$, we fix one representation $\sum_{i=1}^m n_i(x) a_i$ with $n_i(x) \in \mathbb{Z}$. Let $q = \max_{x \in X} \sum_{i=1}^m |n_i(x)|$ and let $C = m + q$, a positive integer. Then for any $z = \sum \lambda_i a_i \in \mathbb{Z}^n$, $x = z - \sum [\lambda_i] a_i \in X$. So $x = \sum_{i=1}^m n_i(x) a_i$ with $n_i(x) \in \mathbb{Z}$ and $z = \sum_{i=1}^m \big(n_i(x) + [\lambda_i]\big) a_i = \sum_{i=1}^m \lambda_i a_i$ with $\sum |n_i(x) + [\lambda_i] - \lambda_i| < \sum_{i=1}^m \big(|n_i(x)| + 1\big) \leq q + m = C$. $\square$

Let h be a positive integer and assume $0 \in A$. Then

$$\Delta = \{ \sum \lambda_i a_i : \lambda_i \geq 0, \sum \lambda_i \leq 1\}$$

and

$$h * \Delta = \{ \sum \lambda_i a_i : \lambda_i \geq 0, \sum \lambda_i \leq h\} .$$

Define

$$\Delta(h, C) = \{ \sum \lambda_i a_i : \lambda_i \geq C , \sum \lambda_i \leq h - C\}$$

with C as in Lemma 2.1.

Then, if $x = \sum \lambda_i a_i \in \Delta(h, C)$, let $\lambda_i = \alpha_i + C$, $\alpha_i \geq 0$.

So

$$\begin{aligned} \Delta(h, C) &= \{ \sum (\alpha_i + C) a_i : \alpha_i \geq 0 , \\ &\qquad \sum \alpha_i \leq h - C - mC\} \\ &= C \sum a_i + \{ \sum \alpha_i a_i : \alpha_i \geq 0 , \\ &\qquad \sum \alpha_i \leq h - C - mC\} \\ &= C \sum a_i + (h - C - mC) * \Delta . \end{aligned}$$

Note $\Delta(h, C)$ is an empty set when $h < C + mC$, a single point $C \sum a_i$ when $h = C + mC$, and a dilation of Δ translated by an integral point when $h \geq C + mC + 1$.

If $x \in h * \Delta$, then $x = h(\sum \lambda_i a_i)$ where $\lambda_i \geq 0$, $\sum \lambda_i = 1$, so $x = \sum \lambda_i (ha_i) \in \text{conv}(hA)$. Now, if $x \in \text{conv}(hA)$, then

$$\begin{aligned} x &= \sum \lambda_i (a_i^1 + \ldots + a_i^h), \ \lambda_i \geq 0, \ \sum \lambda_i = 1 \\ &= h \sum_{i=1}^{m} \frac{\lambda_i}{h} (a_i^1 + \ldots + a_i^h) \\ &= h \sum_{i=1}^{m} \mu_j a_j \text{ where } \mu_j \geq 0, \sum_{j=1}^{m} \mu_j = \sum_{i=1}^{m} \frac{\lambda_i}{h} \cdot h = 1 \end{aligned}$$

by collecting for each a_j's. So, $x \in h * \Delta$. Thus, $h * \Delta = \text{conv}(hA)$. Also, $h * \Delta = \text{conv}(ha_1, \ldots, ha_m)$.

Let $\mathbb{Z}^n(A)$ be the group generated by the differences of the elements of A.

LEMMA 2.2. *Assume $\mathbb{Z}^n(A) = \mathbb{Z}^n$, and $0 \in A$. Then, every integral point in $\Delta(h, C)$ belongs to the sumset hA.*

PROOF. Let z be an integral point in $\Delta(h, C)$. Then

$$z = \sum \lambda_i a_i, \quad \lambda_i \geq C\,, \sum \lambda_i \leq h - C\,.$$

By Lemma 2.1, $z = \sum n_i a_i\,,\ n_i \in \mathbb{Z}\,, \sum |n_i - \lambda_i| < C$. If $n_i < 0$ for some i, then $|n_i - \lambda_i| > C$, so all n_i must be nonnegative. And $\sum n_i = \sum |n_i| = \sum |n_i - \lambda_i + \lambda_i| \leq \sum |n_i - \lambda_i| + \sum |\lambda_i| < C + h - C = h$. Thus $z = \sum n_i a_i\,,\ n_i \geq 0\,, \sum n_i < h$. Since $0 \in A$,

$$hA = \{ \sum n_i a_i : n_i \geq 0, \sum n_i \leq h \}\,,$$

therefore $z \in hA$. □

Let K be the convex hull of $\{e_o, e_1, \ldots, e_n\}$ in $\mathbb{R}^n$ where $e_0 = 0$, and e_i for $i \geq 1$ is the ith standard basis in $\mathbb{R}^n$. Then

$$\begin{aligned} h * K &= \{ \sum_{i=0}^{n} \lambda_i e_i : \lambda_i \geq 0, \sum_{i=0}^{n} \lambda_i \leq h \} \\ &= \{ \sum_{i=1}^{n} \lambda_i e_i : \lambda_i \geq 0, \sum_{i=1}^{n} \lambda_i \leq h \} \end{aligned}$$

and

$$\begin{aligned} K(h,C) &= \{\sum_{i=0}^{n}\lambda_i e_i : \lambda_i \geq C,\ \sum_{i=0}^{n}\lambda_i \leq h - C\} \\ &= \{\sum_{i=1}^{n}\lambda_i e_i : \lambda_i \geq C,\ \sum_{i=1}^{n}\lambda_i \leq h - 2C\}\,. \end{aligned}$$

LEMMA 2.3. *For any positive integer h, if a point in $h * K$ has the distance to $\partial(h * K)$ bigger than $2C$, then it belongs to $K(h,C)$.*

PROOF. Let $z = \sum_{i=1}^{n}\lambda_i e_i$, $\lambda_i \geq 0$, $\sum\lambda_i \leq h$ be such a point. Note we have $h * K = H_1^+ \cap \ldots \cap H_n^+ \cap H_{n+1}^-$ where $H_i = \{x_i = 0\}$ for $i = 1, \ldots, n$ and $H_{n+1} = \{\sum_{i=1}^{n} x_i = h\} = \{x : (x, \mathfrak{u}) = h\}$ where $\mathfrak{u}$ is the vector whose coordinates are all 1. So $h * K$ has boundaries given by hyperplanes $H_1, \ldots, H_n, H_{n+1}$. Since $d(z, H_i) > 2C$, $\lambda_i > 2C$ for all $i = 1, \ldots, n$. Now, let $H = \{x : (x, \mathfrak{u}) = h - 2C\}$, a hyperplane which is parallel to H_{n+1}. Let $z_1 \in H$. Then, $z_1 + t\mathfrak{u}$, $t \in \mathbb{R}$ is a ray starting from z_1, is perpendicular to H_{n+1}, and it will intersect H_{n+1} at $t = t_2$. Then

$z_1 + t_2\mathfrak{u} \in H_{n+1}$, so $(z_1 + t_2\mathfrak{u}, \mathfrak{u}) = h$, giving $t_2 = 2C/n$. Thus, $d(H, H_{n+1}) = t_2|\mathfrak{u}| = 2C/\sqrt{n}$. Now take any point x which lies between H and H_{n+1}. Then $d(x, H_{n+1})$ is given by a line segment which is perpendicular to H_{n+1}. If you extend this line segment so that it joins H and H_{n+1}, this extended line segment, which is perpendicular to both H and H_{n+1}, gives $d(H, H_{n+1})$. Therefore, $d(x, H_{n+1}) < d(H, H_{n+1}) = 2C/\sqrt{n}$ for any point x which lies between H and H_{n+1}. Therefore, any point in $h * K$ whose distance to H_{n+1} is bigger than $2C/\sqrt{n}$ belongs to $H^- = \{x : (x, \mathfrak{u}) \leq h - 2C\}$. Therefore, $z \in H^-$, i.e. $\sum \lambda_i \leq h - 2C$. So $z \in K(h, C)$. □

Using these results, Khovanskiĭ in [**33**] tried to prove the following, with some error.

THEOREM 2.4. *Suppose $\mathbb{Z}^n(A) = \mathbb{Z}^n$. Then, there exists a constant ρ with the following property: for any positive*

integer h, every integral point of $h * \Delta$, whose distance to $\partial(h * \Delta)$ is more than ρ, belongs to hA.

In general, hA is a proper subset of $(h * \Delta) \cap \mathbb{Z}^n$. Theorem 2.4, which we will prove later, states that hA takes all of the central region in $h * \Delta$. Note that a particular case of Theorem 1.3 supports Theorem 2.4.

Let's take a look at how Khovanskiĭ tried to prove Theorem 2.4. First, without loss of generality, we may assume $0 \in A$ because: if not, by Proposition 1.1, all vertices of Δ belong to A. So take any $a \in A$ which is also a vertex of Δ, then take $\bar{\Delta} = \Delta - a$ so that $0 \in \bar{\Delta}$. Then $\bar{\Delta} = \text{conv}(A - a)$ and $h * \bar{\Delta} = h * \Delta - ha = h * \text{conv}(A - a)$. And, for any positive integer h, if $x \in (h * \Delta) \cap \mathbb{Z}^n$ with $d(x, \partial(h * \Delta)) > \rho$, then $x - ha \in h * \bar{\Delta}$, and $d(x - ha, \partial(h * \bar{\Delta})) > \rho$ since a translation doesn't change the distance. Thus $x - ha \in h(A - a) = hA - ha$. So $x \in hA$, proving our claim. We will assume $a_1 = 0$ from now on.

Recall that $|A| = m$. Consider $\pi : \mathbb{R}^{m-1} \to \mathbb{R}^n$ where $\pi(e_i) = a_{i+1}$ with $e_0, \ldots, e_{m-1}$ defined as before, and $K = \text{conv}(\{e_0, \ldots, e_{m-1}\})$. Then,

$$\pi(h * K) = h * \Delta$$

and

$$\pi(K(h, C)) = \Delta(h, C).$$

By Lemma 2.3, each point in $h * K$ whose distance to $\partial(h * K)$ is more than $2C$ belongs to $K(h, C)$. Then, Khovanskiĭ mistakenly claimed that *each point in* $h * \Delta$ *whose distance to boundary is more than* $\rho = 2C||\pi||$*, where* $||\pi||$ *is the norm of* π*, lies in* $\Delta(h, C)$. But the problem with this argument is that some boundary of $h * K$ might be mapped into the interior of $h * \Delta$. For example, take $a_1 = (0, 0)$, $a_2 = (0, 1)$, $a_3 = (1, 0)$ and $a_4 = (1, 1)$, and let $A = \text{conv}(\{a_1, a_2, a_3, a_4\})$. Then the boundary $\{x_1 = 0\} = \{\lambda_0 e_0 + \lambda_2 e_2 + \lambda_3 e_3,\ \lambda_i \geq 0, \sum \lambda_i \leq 1\}$ in

$h*K$ is mapped to $\{\lambda_0 a_1+\lambda_2 a_3+\lambda_3 a_4 : \lambda_i \geq 0, \sum \lambda_i \leq 1\}$, which is $\text{conv}(a_1, a_3, a_4)$, and that is not in the boundary of $h*\Delta$.

Thus, a point in $h*\Delta$ close to $\partial(h*\Delta)$ is not necessarily an image of a point which is close to all boundaries of $h*K$. In fact, we can give a counterexample to his claim below.

Let $a_1 = 0, a_2 = 1, a_3 = 10$ and let $A = \{a_1, a_2, a_3\}$. Then $m = 3$. We'll follow his construction of the constant C. We have

$$X = \{x : x \in \mathbb{Z},\, x = \sum \lambda_i a_i\,, 0 \leq \lambda_i \leq 1\}.$$

If $x \in X$, then $0 \leq x = \lambda_2 a_2 + \lambda_3 a_3 \leq 11$. Thus, for each $x \in X$, we fix the representation $x = \sum n_i(x) a_i$ as follows; For $0 \leq x \leq 9$, we write $x = x \cdot a_2$. For $x = 10$, $x = 1 \cdot a_3$. For $x = 11$, $x = a_2 + a_3$. Then $q = \max_{x\in X} \sum |n_i(x)| = 9$, giving us $C = m + q = 12$.

Now, $||\pi|| = \sup_{|x|=1} |\pi(x)|$ where $\pi : \mathbb{R}^2 \to \mathbb{R}$ is defined as earlier. If $x = \sum_{i=0}^{2} \lambda_i e_i$ with $|x| = 1$, then $|\lambda_1|, |\lambda_2| \leq 1$

so $|\pi(x)| = |\lambda_1 + \lambda_2 \cdot 10| \leq 11$ so $||\pi|| \leq 11$. Thus we have $\rho = 2C||\pi|| \leq 264$. Let $h = 53$. Then $h*\Delta = [\,0, 530\,]$. Now consider 265. If $265 \in \Delta(h, C) = \Delta(53, 12)$, then by the definition of $\Delta(h, C)$, $265 = \lambda_2 + \lambda_3 \cdot 10$ for some $\lambda_2, \lambda_3 \geq 12$, $\lambda_2 + \lambda_3 \leq 29$. But after a simple calculation, we see that this is impossible. So $265 \notin \Delta(h, C)$ but $d(265, \partial(h * \Delta)) = 265 > \rho$.

3. Proof of Theorem

Khovanskiĭ's argument can be modified to prove the following.

PROPOSITION 3.1. *Suppose* $\mathbb{Z}^n(A) = \mathbb{Z}^n$, $|A| = n + 1$, *and* $A = \{a_1, a_2, \ldots, a_{n+1}\}$ *are affinely independent. Then there exists a constant* ρ *with the following property: for any positive integer* h, *every integral point of* $h * \Delta$, *whose distance to* $\partial(h * \Delta)$ *is more than* ρ, *belongs to* hA.

The affine hull $\text{aff}(A)$ is an affine subspace, which is a translation of a linear subspace L, i.e. $\text{aff}(A) = x + L$ for some $x \in \mathbb{R}^n$. So $A \subseteq x + L$. Therefore, if $\mathbb{Z}^n(A) = \mathbb{Z}^n$, then $\dim(\text{aff}(A)) = \dim \Delta = n$.

PROOF. Consider $\pi : \mathbb{R}^n \to \mathbb{R}^n$ where $\pi(e_i) = a_{i+1}$, i.e. $\pi(x) = Tx$ where T is the matrix whose ith column is given by the coordinates of a_{i+1} for $i = 1, \ldots, n$. Recall that $a_1 = 0$. Since $a_2 - a_1, \ldots, a_{n+1} - a_1$ are linearly independent, i.e. $a_2, \ldots, a_{n+1}$ are linearly independent, T is invertible so π is injective. Also, $\pi(h*K) = h*\Delta$ and $\pi(K(h, C)) = \Delta(h, C)$. By Proposition 1.1, every face of $h * K$ is the convex hull of up to n vertices, and so is every face of $h * \Delta$.

Now, suppose $x \in h * \Delta$ belongs to a convex hull of up to n vertices. Recall that all the vertices belong to the set $\{ha_1, \ldots, ha_{n+1}\}$ by Proposition 1.1. Thus, x belongs to a convex hull of proper subset of $\{ha_1, \ldots, ha_{n+1}\}$. Take, for example, $x = \sum_{i=1}^{n} \lambda_i(ha_i)$, $\lambda_i \geq 0$, $\sum \lambda_i = 1$ (other

cases are similar). Assume x is an interior point. Then by Proposition 1.2, x can be written as

$$x = \sum_{j=1}^{n+1} \gamma_j x_j\,, \qquad \text{where } \sum \gamma_j = 1,$$

$$x_j \in h * \Delta = \operatorname{conv}(ha_1, \ldots, ha_{n+1}),$$

$$x_j \text{ are affinely independent}$$

$$\text{and } \gamma_j > 0.$$

Then $x_j = \sum_{l=1}^{n+1} \alpha_{lj}(ha_l)$ with $\sum_{l=1}^{n+1} \alpha_{lj} = 1,\ \alpha_{lj} \geq 0$. So

$$\sum_{i=1}^{n} \lambda_i(ha_i) = \sum_{j=1}^{n+1}\sum_{l=1}^{n+1} \gamma_j \alpha_{lj}(ha_l) \tag{3.1}$$

$$\text{where } \sum_{j=1}^{n+1}\sum_{l=1}^{n+1} \gamma_j \alpha_{lj} = 1.$$

Since ha_i's are affinely independent, the affine combinations of them are unique, so the coefficient of a_{n+1} in the right hand side of (3.1) must be 0. Therefore, $\sum_{j=1}^{n+1} \gamma_j \alpha_{(n+1)j} = 0$, but $\alpha_{lj} \geq 0$ and $\gamma_j > 0$. So $\alpha_{(n+1)j} = 0$ for all $j = 1, \ldots, n+1$. Thus $x_1, \ldots, x_{n+1} \in \operatorname{aff}(ha_1, \ldots, ha_n)$, which means there are $n+1$ affinely independent vectors in the

affine hull aff$(ha_1, \ldots, ha_n)$, whose dimension is $n-1$, giving us a contradiction. Therefore, $x \in \partial(h * \Delta)$. Similarly, if $x \in h * K$ belongs to a convex hull of up to n vertices, $x \in \partial(h * K)$. Thus we have just proved that

$$\partial(h * \Delta) = \{x \in h * \Delta : \ x \text{ belongs to a convex hull of up to } n \text{ vertices}\}$$

$$\partial(h * K) = \{x \in h * K : \ x \text{ belongs to a convex hull of up to } n \text{ vertices}\}.$$

Therefore, π maps $\partial(h * K)$ onto $\partial(h * \Delta)$.

Now, let $x \in h * \Delta$ be an integral point with $d(x, \partial(h * \Delta)) > 2C||\pi||$. Then, for any $\bar{y} \in \partial(h * K)$, $\pi(\bar{y}) = y \in \partial(h * \Delta)$ and

$$|\pi^{-1}(x) - \bar{y}| \geq \frac{|x - y|}{||\pi||} > \frac{2C||\pi||}{||\pi||} = 2C.$$

Then, by Lemma 2.3, $\pi^{-1}(x) \in K(h, C)$. Therefore, $x \in \Delta(h, C)$. Thus, by Lemma 2.2, $x \in hA$. $\square$

Now we prove Theorem 2.4.

PROOF OF THEOREM 2.4. Take any hyperplane

$$H = \{x : (x, u) = \alpha\}.$$

Then, for a positive integer h,

$$h * H = \{x : (x, u) = h\alpha\},$$

so the dilation of a hyperplane results in another hyperplane which is parallel to the original one. And

$$H - b = \{x : (x, u) = \alpha - (b, u)\}$$

where $b \in \mathbb{R}^n$, so the translation of a hyperplane is another hyperplane that's parallel to the original one.

Now, let's calculate the distance between

$$H_1 = h * H\ ,$$

$$H_2 = g * H - b,$$

where $h > g$, h, g are positive integers, and $b \in \mathbb{R}^n$. Then $H_1 = \{x : (x, u) = h\alpha\}$, $H_2 = \{x : (x, u) = g\alpha - (b, u)\}$, so H_1 is parallel to H_2. Take any point $x_1 \in H_1$. Then $x_1 + tu$, $t \in \mathbb{R}$ is a ray perpendicular to both H_1 and H_2. Let's say $x_1 + tu \in H_2$ when $t = t_2$. Then

$$t_2 = \frac{(g-h)\alpha - (b,u)}{|u|^2},$$

$$d(H_1, H_2) = |t_2 u| = \frac{|(g-h)\alpha - (b,u)|}{|u|}.$$

Now, recall that, for $h \geq C + mC + 1$,

$$\Delta(h, C) = C \sum a_i + (h - C - mC) * \Delta.$$

Let $\Delta = G_1^+ \cap \ldots \cap G_l^+$ where G_i's are hyperplanes $\{x : (x, u_i) = \alpha_i\}$ with $G_i \cap \Delta \neq \emptyset$. Then $h * \Delta = H_1^+ \cap \ldots \cap H_l^+$ and $\Delta(h, C) = H_1^{'+} \cap \ldots \cap H_l^{'+}$ where $H_i = h * G_i$, $H_i^{'} = (h - C - mC) * G_i + C \sum a_i$. And for all $h \geq C + mC + 1$,

$$d(H_i, H_i^{'}) = \frac{|(-C - mC)\alpha_i + (C \sum a_i, u_i)|}{|u_i|}$$

for $i = 1, \ldots, l$. Thus, for all $i = 1, \ldots, l$, the distance $d(H_i, H_i^{'})$ remains same for all $h \geq C + mC + 1$.

Thus, fix any $h \geq C + mC + 1$. Define

$$\rho = \max \{ \, \delta\big((C + mC) * \Delta\big), \, d(H_i, H_i^{'}), i = 1, \ldots, l \, \}$$

where $\delta(S)$ represents the diameter of the set S. Then ρ is independent of h. Let $z \in h * \Delta$ be an integral point with $d(z, \partial(h * \Delta)) > \rho$. Note that if $h \leq C + mC$, then by the definition of ρ, such z doesn't exist.

Let $F_i = H_i \cap (h * \Delta) \neq \emptyset$ be the face of $h * \Delta$ and $F_i^{'} = H_i^{'} \cap \Delta(h, C) \neq \emptyset$ be the face of $\Delta(h, C)$. If $z \in H_1^{'-} \setminus H_1^{'}$, then $d(z, H_1) < d(H_1^{'}, H_1) \leq \rho$, but $d(z, F_1) > \rho$. Thus the perpendicular ray to H_1 from z doesn't intersect F_1 . It's a well known fact that every compact convex body in $\mathbb{R}^n$ with nonempty interior is homeomorphic to the closed n-ball, and its boundary is homeomorphic to the $(n-1)$-sphere. So $\partial(h * \Delta)$ is homeomorphic to the $(n-1)$-sphere. Thus, the perpendicular ray above intersects $\partial(h * \Delta)$, say, at z_2 which

is a point of a face F_2, $F_2 \neq F_1$. Then $z_2 \in F_2 \subseteq h * \Delta$, so $z_2 \in H_1^+$. Then $d(z, F_2) \leq d(z, z_2) \leq d(z, H_1) < \rho$, a contradiction. Therefore, $z \in H_1^{'+}$, and it's true for all $H_i^{'+}$. Thus, $z \in H_1^{'+} \cap \ldots \cap H_l^{'+} = \Delta(h, C)$. Then, by Lemma 2.2, $z \in hA$. □

4. Historical Perspective and Some Open Problems

A polytope of dimension d is a *simplicial polytope* if all of its proper faces are simplices, i.e. every facet has the minimal number of d vertices. A polytope of dimension d is a *simple polytope* if every vertex is contained in the minimal number of only d facets. Two polytopes Δ and Δ' are *combinatorially equivalent*, denoted $\Delta \simeq \Delta'$, if there is a bijection between their faces that preserves the inclusion relation.

In Lemma 2.1, we found that we can perturb the coordinates a little to get integer coefficients. In fact, it is

known that there exists a combinatorially equivalent polytope $\Delta' \simeq \Delta$ with integral vertex coordinates for every simple or simplicial polytope Δ. Is this true for all polytopes? It is true for polytopes of dimension $d \leq 3$ but it is false in general. Another question; if the integral coordinates exist, can we keep them small? The answer is yes in low dimension, but in general, we have coordinates that grow doubly exponential in terms of the number of vertices (Goodman, Pollack and Sturmfels [**26**]).

It's known that every polytope is a "projection" of a simplex. When Khovanskiĭ tried to use the map π to prove Theorem 2.4, he maybe was trying to use this idea. For other similar results, see, for example, Grünbaum [**27**].

Another way we can try to visualize objects in dimension $d \geq 4$ is by using its projection on $(d-1)$-polytope, which is called a *Schlegel diagram*. Then, we can ask if what looks like a projection is indeed a Schlegel diagram.

The answer is no. In fact, it's an open problem to find necessary and sufficient condition for a sphere with a "face-like" structure on it to be isomorphic to the boundary of a polytope (called *Steinitz problem*). For more on classifying polytopes, see Ziegler [**55**], Ewald [**24**], Alon [**1**] and Goodman and Pollack [**25**] for the classification using the number of vertices and the dimension, Bárány and Vershik [**2**] for the classification using the volume and the dimension, and Karpenkov [**32**] for the classification using affine transformations.

By Theorem 2.4, the sumset hA in $\mathbb{R}^n$ takes over the central region of dilalated polytopes. Han [**30**] showed that, for $A \subseteq \mathbb{R}^2$ satisfying some conditions, the cardinality of hA in boundary region of dilated polytopes is a linear function of h when h is sufficiently large. For the problems counting lattice points in "thin" annuli, Wigman [**53**] studied the statistical behaviour of the counting function. It will be

interesting if we can tell something more about the density or distribution of sumsets in the boundary region.

Bibliography

[1] N. Alon, *The number of polytopes, configurations and real matroids*, Mathematika **33** (1986), no. 1, 62-71.

[2] I. Bárány and A. M. Vershik, *On the number of convex lattice polytopes*, GAFA J., **12** (1992), 381-393.

[3] A. I. Barvinok, *A polynomial time algorithm for counting integral points in polyhedra when the dimension is fixed*, Math. Oper. Res. **19** (1994), no. 4, 769-779.

[4] P. T. Bateman, E. E. Kohlbecker and J. P. Tull, *On a theorem of Erdős and Fuchs in additive number theory*, Proc. Amer. Math. Soc., **14** (1963), 278-284.

[5] M. Beck, *Counting lattice points by means of the residue theorem*, Ramanujan J. **4** (2000), no. 3, 299-310.

[6] M. Beck, R. Diaz and S. Robins, *The Frobenius problem, rational polytopes, and Fourier-Dedekind sums*, J. Number Theory **96** (2002), no. 1, 1-21.

[7] R. C. Bose and S. Chowla, *Theorems in the additive theory of numbers*, Comment. math. helvet. **37** (1962-1963), 141-147.

[8] G. Bredon, *Topology and Geometry*, Springer, 1993.

[9] A. Brøndsted, *An introduction to convex polytopes*, Springer, 1983.

[10] J. W. S. Cassels, *An introduction to the geometry of numbers*, Springer, 1997.

[11] B. Chen, *Lattice points, Dedekind sums, and Ehrhart polynomials of lattice polyhedra*, Discrete Comput. Geom. **28** (2002), no. 2, 175-199.

[12] Y. Chen, *A problem on unique representation bases*, European J. Combin. *to appear*.

[13] S. Chowla, *Solution of a problem of Erdős and Turán in additive number theory*, Proc. Natn. Acad. Sci. India **14** (1944), 1-2.

[14] J. Cilleruelo and M. B. Nathanson, *Dense sets of integers with prescribed representation functions*, preprint, 2006.

[15] G. A. Dirac, *Note on a problem in additive number theory*, J. London Math. Soc., **26** (1951), 312-313.

[16] E. Ehrhart, *Sur les polyèdres rationnels homothétiques à n dimensions*, C. R. Acad. Sci. Paris, **254** (1962) 616-618.

[17] E. Ehrhart, *Sur un problème de géométrie diophantienne linéaire II*, J. Reine Angew. Math. **227** (1967), 25-49.

[18] P. Erdős, *Colloque sur la Théorie des Nombres*, Bruxelles, 1956

[19] P. Erdős, *Some applications of Ramsey's theorem in additive number theory*, European J. Combin. **1** (1980), 43-46.

[20] P. Erdős and W. H. J. Fuchs, *On a problem of additive number thoery*, J. London Math. Soc., **31** (1956), 67-73.

[21] P. Erdős, P. Gruber and J. Hammer, *Lattice point problems*, Pitman Monographs and Surveys in Pure and Applied Mathematics **39**, Longman, Essex, and John Wiley and Sons, New York 1989.

[22] P. Erdős and A. Rényi, *Additive properties of random sequences of positive integers*, Acta arith. **6** (1960), 83-110.

[23] P. Erdős and P. Turán, *On a problem of Sidon in additive number theory, and on some related problems*, J. London Math. Soc. **16** (1941), 212-215. Addendum (by P. Erdős), ibid. **19** (1944), 208.

[24] G. Ewald, *Combinatorial convexity and algebraic geometry*, Springer, 1996.

[25] J. E. Goodman and R. Pollack, *New bounds on higher-dimensional configurations and polytopes*, Combinatorial Mathematics: Proceedings of the Third International Conference(New York, 1985), 205-212, Ann. New York Acad. Sci., 555, New York Acad. Sci., New York, 1989.

[26] J. E. Goodman, R. Pollack and B. Sturmfels, *The intrinsic spread of a configuration in* $\mathbb{R}^d$, J. Amer. Math. Soc. **3** (1990), no. 3, 639-651.

[27] B. Grünbaum, *Convex Polytopes*, Springer, 2nd edition, 2003.

[28] H. Halberstam and K. F. Roth, *Sequences*, Springer, 1983.

[29] S. Han, C. Kirfel and M. B. Nathanson, *Linear forms in finite sets of integers*, Ramanujan J. **2** (1998), 271-281.

[30] S. S. Han, *The boundary structure of the sumset in* $\mathbb{Z}^2$, Number theory (New York, 2003), 201-218, Springer, New York, 2004.

[31] G. Hofmeister, *Thin basis of order two*, J. Number Theory **86** (2001), 118-132.

[32] O. Karpenkov, *Classification of lattice-regular lattice convex polytopes*, preprint.

[33] A. G. Khovanskiĭ, *The Newton polytope, the Hilbert polynomial and sums of finite sets*(Russian), Funktsional. Anal. i Prilozhen. **26** (1992), no. 4, 57-63, 96; translation in Funct. Anal. Appl. **26** (1992), no.4, 276-281 (1993).

[34] F. Krückeberg, *B_2-Folgen und verwandte Zahlenfolgen*, J. reine angew. Math. **206** (1961), 53-60.

[35] A. E. Ingham, *On the difference between consecutive primes*, Quart. J. Math. **8** (1937), 255-266.

[36] V. F. Lev, *Reconstructing integer sets from their representation functions*, Electron. J. Combin. **11** (2004), no. 1, Research paper 78, 6 pp.(electronic).

[37] T. Łuczak and T. Schoen, *A note on unique representation bases for the integers*, Funct. Approx. Comment. Math. **32** (2004), 67-70.

[38] P. McMullen, *Handbook of convex geometry, Vol. A, B*, North-Holland, 1993.

[39] A. Mian and S. Chowla, *On the B_2-sequences of Sidon*, Proc. natn. Acad. Sci. India, Sect. A, **14** (1944), 3-4.

[40] M. B. Nathanson, *Sums of finite sets of integers*, Amer. Math. Monthly **79** (1972), 1010-1012.

[41] M. B. Nathanson, *Representation functions of sequences in additive number theory*, Proc. Amer. Math. Soc. **72** (1978), no. 1, 16-20.

[42] M. B. Nathanson, *Additive number theory-Inverse problems and the geometry of sumsets*, Springer, 1996.

[43] M. B. Nathanson, *Growth of sumsets in abelian semigroups*, Semigroup Forum **61** (2000), no. 1, 149-153.

[44] M. B. Nathanson. *Unique representation bases for the integers*, Acta Arith. **108** (2003), no. 1, 1-8.

[45] M. B. Nathanson, *The inverse problem for representation functions of additive bases*, in : Number Theory (New York, 2003), 253-262, Springer, New York, 2004.

[46] M. B. Nathanson, *Every function is the representation function of an additive basis for the integers*, Port. Math. (N.S.) **62** (2005), no. 1, 55-72.

[47] G. Pick, *Geometrisches zur Zahlentheorie*, Sitzenber. Lotos (Prague) **19** (1899), 311-319.

[48] I. Z. Ruzsa, *An infinite Sidon sequence*, J. Number Theory, **68** (1998), 63-71.

[49] A. Sárközy and V. Sós, *On additive representation functions*, in: The Mathematics of Paul Erdős, R.L. Graham and J. Nešetřil (eds.), Springer, 1991, 129-150.

[50] C. L. Siegel, *Lectures on the geometry of numbers*, Springer, 1989.

[51] A. Stöhr, *Gelöste und ungelöste Fragen über Basen der natürlichen Zahlenreihe' II*, J. reine angew. Math. **194** (1955), 111-140. Theorems 8 and 9 are due to Erdős although paper is written by Stöhr.

[52] R.C. Vaughan, *On the addition of sequences of integers*, J. Number Theory, **4** (1972), 1-16.

[53] I. Wigman, *Statistics of lattice points in thin annuli for generic lattices*, preprint.

[54] K. Woods, *Computing the period of an Ehrhart quasi-polynomial*, Electron. J. Combin. **12** (2005), Research

Paper 34, 12pp.(electronic).

[55] G. M. Ziegler, *Lectures on polytopes*, Springer, 1995