On Unique Recovery of Integer Bounded Signals

Abdullah Alasmari

2023

Submitted in partial fulfillment of

the requirements for the degree of

Doctor of Philosophy

School of Mathematics
Ysgol Mathemateg

Summary

The thesis considers the problem of unique recovery of finite-valued integer signals using a single linear integer measurement. A signal is an integer n-dimensional vector $\boldsymbol{x}$ with absolute entries bounded by a positive integer r, that is $\boldsymbol{x} \in [-r, r]^n$. We assume that the signal $\boldsymbol{x}$ is sufficiently *sparse*. Specifically, the number of nonzero entries of $\boldsymbol{x}$ is assumed to be bounded by a positive integer l with $2l < n$. A single linear integer measurement is represented by an integer $1 \times n$ measurement matrix, or row vector, H. Naturally, it is desirable to construct H with as small absolute entries as possible. We give a constructive proof for the existence of measurement matrices H with maximum absolute entry $\Delta = O(r^{2l-1})$. The capital O in this bound contains an implicit constant that depends on l and n and probably far from being optimal, however the exponent $2l-1$ is optimal. The optimality of the exponent is the main advantage of the latter upper bound. Additionally, we show that, in the above setting, a single measurement can be replaced by several measurements with absolute entries sub-linear in Δ. The proofs make use of results on admissible $(n-1)$-dimensional integer lattices for m-sparse n-cubes that are of independent interest. The main tools include the aggregation of linear Diophantine equations and Siegel's lemma. Additionally, we discuss

some probabilistic aspects of unique recovery for finite-valued integer signals.

Acknowledgements

I would like to express my gratitude to the many individuals who have played a pivotal role in helping me complete this thesis. Their unwavering support, guidance, and encouragement have been instrumental in shaping this endeavour.

First and foremost, I want to thank my parents for their constant love, encouragement, and sacrifices, which have been the cornerstone of my journey. Their unwavering belief in me has fueled my determination to reach this milestone.

I am also indebted to my wife and three daughters, whose understanding, patience, and unwavering support have sustained me throughout this academic pursuit. Your boundless love and encouragement have been my driving force.

In appreciation of their continuous encouragement and belief in me, I extend my gratitude to my brother, sisters, and relatives. Your support has been a source of strength for me.

From an educational perspective, I am grateful to Cardiff University for providing the necessary facilities and resources to complete this thesis successfully. Additionally, I would like to thank the Saudi government for its

scholarship, which eased my financial burdens and enabled me to pursue this academic degree. Throughout this research, I am indebted to my supervisor, Iskander Aliev, for providing me with invaluable guidance, mentorship, and expertise. I have greatly benefited from his insightful feedback and unwavering support.

It has been a pleasure working with my colleagues and office mates, whose camaraderie and intellectual discussion have enriched my understanding of the subject matter.

Lastly, a special mention goes to Aled Williams, a friend and confidant who has stood by me throughout this journey. Your unwavering support, guidance, and encouragement have been invaluable. I am truly grateful for your presence in my life.

Abdullah Alasmari

08/08/2023

Contents

Chapter 1

Preliminaries

1.1 Basics and notation

We denote by $\mathbb{R}$ the set of real numbers, by $\mathbb{Q}$ the set of rational numbers and by $\mathbb{Z}$ the set of integers. For a real number $x \in \mathbb{R}$, we denote by $\lceil x \rceil$ the *ceiling function* of x, that is the least integer greater than or equal to x. Similarly, $\lfloor x \rfloor$ stands for the *floor function* of x, the greatest integer less than or equal to x. The *support* of a vector $\boldsymbol{x} \in \mathbb{R}^n$ is denoted by $\operatorname{supp}(\boldsymbol{x})$. That is $\operatorname{supp}(\boldsymbol{x}) = \{i : \boldsymbol{x}_i \neq 0\}$. Given $K \subset \mathbb{R}^n$, we use the notation $\operatorname{vol}(K)$ for the volume , i.e., the n-dimensional Lebesgue measure of the set K.

Norms

A general norm on a vector space can be defined as follows.

Definition 1. A function $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}$ is called a *norm* if it satisfies three properties:

(i) $\|\boldsymbol{x}\| \geq 0$ for any vector $\boldsymbol{x} \in \mathbb{R}^n$, and $\|\boldsymbol{x}\| = 0$ if and only if $\boldsymbol{x} = \boldsymbol{0}$.

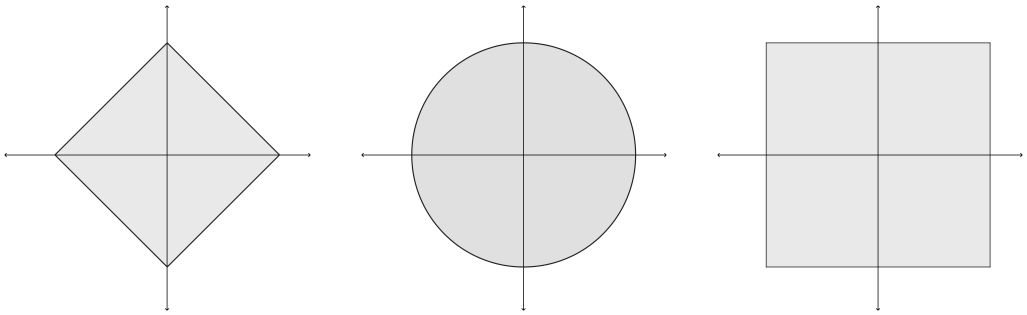


Figure 1.1: The unit norm balls for ℓ_p-norms.

(ii) $\|\alpha \boldsymbol{x}\| = |\alpha| \, \|\boldsymbol{x}\|$ for any vector $\boldsymbol{x} \in \mathbb{R}^n$ and any scalar $\alpha \in \mathbb{R}$.

(iii) $\|\boldsymbol{x} + \boldsymbol{y}\| \leq \|\boldsymbol{x}\| + \|\boldsymbol{y}\|$ for any vectors $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^n$.

The first property is referred to as the positivity of the norm, and the second expresses its homogenity, while the third is known as the triangle inequality.

The most commonly used norms belong to the family of ℓ_p*-norms*, which are defined for $\boldsymbol{x} \in \mathbb{R}^n$ as

$$\|\boldsymbol{x}\|_p = \left(\sum_{i=1}^{n} |x_i|^p \right)^{1/p},$$

where $p \geq 1$ is a real number.

Here are some particularly important ℓ_p-norms:

- $p = 1$: the ℓ_1*-norm*, which is also referred to as the *Manhattan norm*, is

$$\|\boldsymbol{x}\|_1 = |x_1| + |x_2| + \cdots + |x_n| \, .$$

- $p = 2$: the ℓ_2*-norm*, which is also referred to as the *Euclidean norm*, is

$$\|\boldsymbol{x}\|_2 = \sqrt{x_1^2 + x_2^2 + \cdots + x_n^2}.$$

- As p approaches the infinity, the ℓ_p norm approaches the ℓ_∞-*norm*, which is also referred to as the *maximum norm*,

$$\|\boldsymbol{x}\|_\infty = \max_{1\le i\le n} |x_i| .$$

The unit norm balls $\{\boldsymbol{x} \in \mathbb{R}^2 : \|\boldsymbol{x}\|_p \le 1\}$ for the above norms are shown in Figure 1.1.

In this thesis, an important role will be played by the ℓ_0-"*norm*", widely used in the theory of compressed sensing.

Definition 2. For a given vector $\boldsymbol{x} \in \mathbb{R}^n$, the ℓ_0-*norm* $\|\boldsymbol{x}\|_0$ is the cardinality of the support of $\boldsymbol{x}$, that is the number of non-zero entries of $\boldsymbol{x}$

$$\|\boldsymbol{x}\|_0 = |\operatorname{supp}(\boldsymbol{x})|.$$

In fact ℓ_0-norm is not a proper norm, as it is not homogeneous. If $\boldsymbol{x}$ is a non-zero vector and $\alpha \neq 1$, then

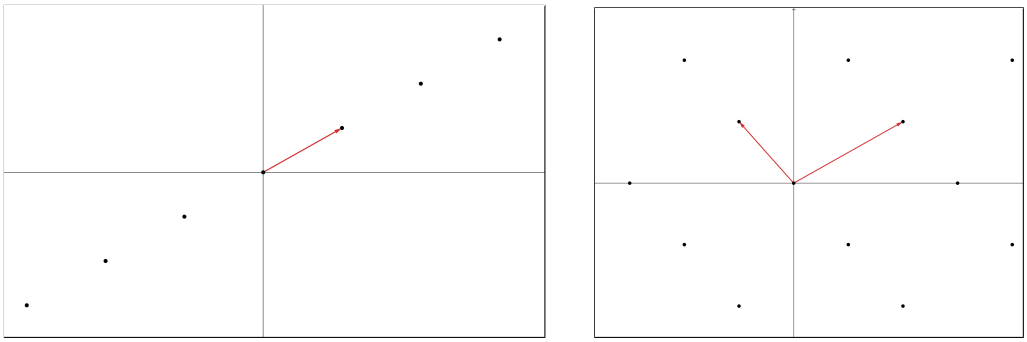
$$\|\alpha\boldsymbol{x}\|_0 \neq \alpha \|\boldsymbol{x}\|_0.$$

ℓ_∞-norm of a matrix

The ℓ_∞-norm for a vector $\boldsymbol{x}$ is the largest absolute value of its components. For a matrix $A = (a_{ij}) \in \mathbb{R}^{m\times n}$ we define the ℓ_∞-*norm* $\|A\|_\infty$ in a similar way.

Definition 3. For a matrix $A = (a_{ij}) \in \mathbb{R}^{m\times n}$, the ℓ_∞-*norm* is the maximum absolute value of the entries of A, that is

$$\|A\|_\infty = \max_{\substack{1\le i\le m\\ 1\le j\le n}} \left|a_{ij}\right| .$$



(a) One-dimensional lattice in $\mathbb{Z}^2$. (b) Two- dimensional lattice in $\mathbb{Z}^2$.

Figure 1.2: Comparison of different lattices in $\mathbb{Z}^2$.

1.2 Lattices

Minkowski's Geometry of Numbers provides a mathematical toolbox for this thesis. One of the most important mathematical instruments that we use are the lattices. We refer the reader to [30, 13] for an extensive introduction to the geometry of numbers.

Definition 4. Let $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_k \in \mathbb{R}^n$ be linearly independent vectors. The set

$$\Lambda = \left\{ \sum_{i=1}^{k} x_i \boldsymbol{b}_i : x_i \in \mathbb{Z} \right\}$$

is a k-dimensional lattice with basis $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_k$. If $n = k$, then Λ is a full-dimensional lattice, as illustrated in Figure 1.2b.

Let $B = (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_k) \in \mathbb{R}^{n \times k}$ be a matrix with columns $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_k$, referred to as a *basis matrix*. We can define the lattice $\Lambda = \Lambda(B)$ as

$$\Lambda = \left\{ B\boldsymbol{x} : \boldsymbol{x} \in \mathbb{Z}^k \right\}.$$

Notice that, since the basis vectors $\mathbf{b}_1, \ldots, \mathbf{b}_k$ are linearly independent, any point $\boldsymbol{y}$ in the subspace spanned by the basis vectors can be written as a

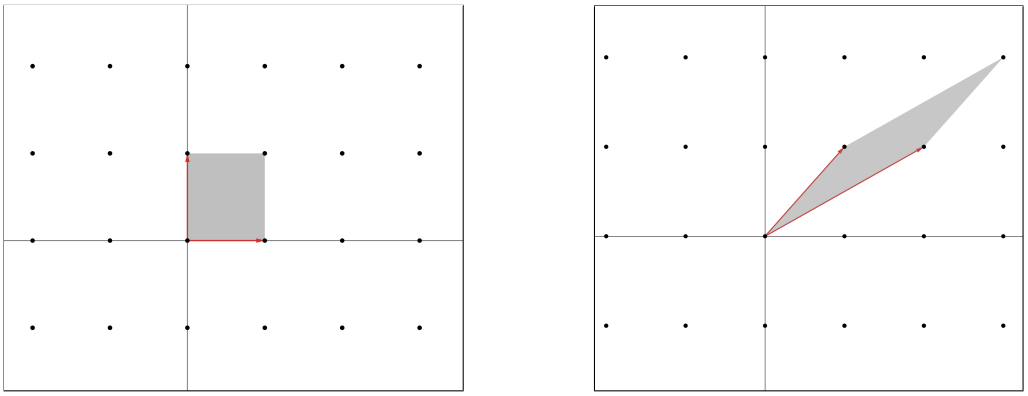


Figure 1.3: Two different bases generate the same lattice.

unique linear combination $\boldsymbol{y} = x_1\mathbf{b}_1 + x_2\mathbf{b}_2 + \cdots + x_k\mathbf{b}_k$, for some $x_1, x_2, \ldots, x_k \in \mathbb{R}$. Therefore, $\boldsymbol{y} \in \Lambda$ if and only if $x_j \in \mathbb{Z}$ for all $j \in \{1, 2, \ldots, k\}$.

Note that the choice of a lattice basis is not unique, the same lattice can be generated by different bases, as we can see in the next example.

Example 1. *Take*

$$B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \text{ and } C = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}.$$

Then as it is illustrated by Figure 1.3, B and C generate the same lattice $\mathbb{Z}^2$*, that is* $\Lambda(B) = \Lambda(C) = \mathbb{Z}^2$.

In general, one can wonder when two different sets of linearly independent vectors generate the same lattice. The answer is given by the unimodular basis transformations.

Definition 5. Let $U \in \mathbb{Z}^{k\times k}$ be an integer square matrix. Then U is called a *unimodular matrix* if it has determinant $\det(U) = \pm 1$.

Two basis matrices B and C generate the same lattice $\Lambda(B) = \Lambda(C)$ if and only if $B = CU$ for a unimodular matrix U, see [46].

Next, we will introduce the *fundamental parallelepiped* of a lattice. Let $\Lambda \subset \mathbb{R}^n$ be a lattice with basis matrix $B = (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_k) \in \mathbb{R}^{n \times k}$. The fundamental parallelepiped of the lattice Λ associated with basis B is defined as

$$P(B) = \{B\boldsymbol{x} : \boldsymbol{x} \in \mathbb{R}^n, 0 \leq \boldsymbol{x}_i < 1\} .$$

It is worth pointing out that because the column vectors in B form a basis for Λ, it follows that the fundamental parallelepiped $\mathbb{P}(B)$ contains no other lattice points except the origin, i.e. $P(B) \cap \Lambda = \{\mathbf{0}\}$.

It is clear that the fundamental parallelepiped $P(B)$ depends on the basis B of the lattice Λ. See Figure 1.4.

Definition 6. The *determinant* of the lattice Λ with a basis matrix B is defined as

$$\det(\Lambda) = \sqrt{\det(B^T B)},$$

where $B^\top$ denotes the transpose of B.

In the special case when Λ is a full-dimensional lattice (that is $k = n$), the matrix B is a square matrix, and hence the determinant of the lattice is given by $\det(\Lambda) = |\det(B)| = \mathrm{vol}(P(B))$.

We will now show that the determinant is well defined, that is the value of the determinant does not depend on the choice of a lattice basis. Let the two bases $B_1, B_2 \in \mathbb{R}^{n \times k}$ generate the same lattice Λ. We know that for some unimodular matrix $U \in \mathbb{Z}^{k \times k}$ the equality $B_2 = B_1 U$ holds. Calculating the determinant $\det(\Lambda)$ related to the bases B_1 and B_2 yields that

$$\det(\Lambda) = \sqrt{\det\left(B_2^T B_2\right)} = \sqrt{\det\left(U^T B_1^T B_1 U\right)} = \sqrt{\det\left(B_1^T B_1\right)}$$

holds. A *sublattice* of a full-dimensional lattice $\Lambda \subset \mathbb{R}^n$ is defined as a lattice

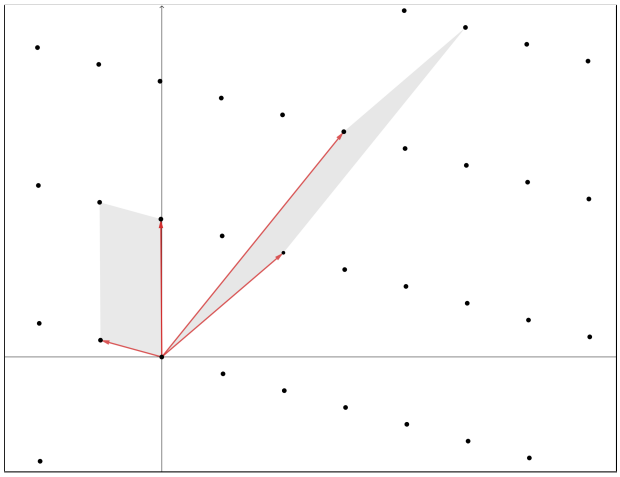


Figure 1.4: Different fundamental parallelepipeds dependent on different bases.

$\widetilde{\Lambda}$ such that $\widetilde{\Lambda} \subset \Lambda$. If $\boldsymbol{a}$ and $\bar{\boldsymbol{a}}$ are lattice points in Λ, and $\widetilde{\Lambda}$ is a sublattice of Λ, then we write

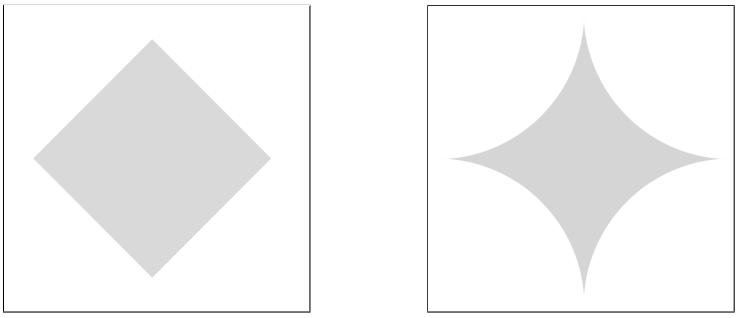
$$\boldsymbol{a} \equiv \bar{\boldsymbol{a}} \bmod \widetilde{\Lambda} \Leftrightarrow (\boldsymbol{a} - \bar{\boldsymbol{a}}) \in \widetilde{\Lambda}.$$

This means that $\boldsymbol{a}$ and $\bar{\boldsymbol{a}}$ belong to the same residue class of Λ with respect to $\widetilde{\Lambda}$. It is important to note that there are exactly $\det \widetilde{\Lambda} / \det \Lambda$ different residue classes of Λ with respect to $\widetilde{\Lambda}$.

1.3 Convex sets and convex bodies

Minkowski's Geometry of Numbers studies the interactions of lattices and convex sets. For a comprehensive introduction to convex sets, and to convex geometry in general, we refer the reader to [28].

Definition 7. A set $C \subset \mathbb{R}^n$ is called *convex* if for any $\boldsymbol{x}_1, \boldsymbol{x}_2 \in C$ and for any



Convex set. Non-convex set.

Figure 1.5: Examples of convex and non-convex sets.

$\theta \in [0,1]$, we have

$$\theta \boldsymbol{x}_1 + (1-\theta)\boldsymbol{x}_2 \in C.$$

In other words, one can move from any point in a convex set C to any other point via a line segment within the set. See Figure 1.5.

In what follows, we collect some basic properties that preserve convexity (see e.g. [10])

1. The empty set $\emptyset$ and the whole space $\mathbb{R}^n$ are both convex.

2. The intersection of convex sets is convex.

3. Convexity is preserved by scaling. If $C \subset \mathbb{R}^n$ is a convex set and $\alpha \in \mathbb{R}$, then the set $\alpha\, C = \{\alpha \boldsymbol{x} : \boldsymbol{x} \in C\}$ is convex.

4. Convexity is preserved by summation. The *Minkowski's sum* of two sets C_1 and C_2 is defined as

$$C_1 + C_2 = \{\boldsymbol{x} + \boldsymbol{y} : \boldsymbol{x} \in C_1,\ \boldsymbol{y} \in C_2\}.$$

If C_1 and C_2 are convex, then $C_1 + C_2$ is convex.

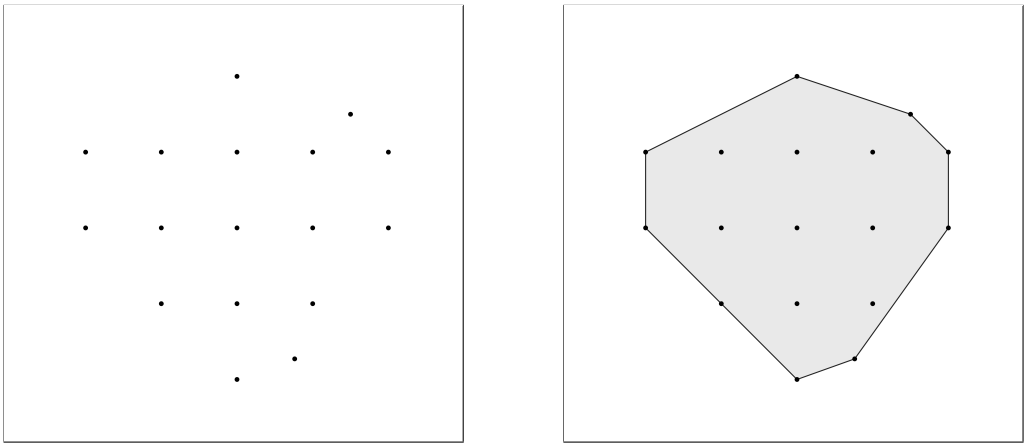


Figure 1.6: Visualisation of the set of points S (left) and its corresponding convex hull (right).

5. The image of a convex set under a linear affine transformation is also a convex set.

Given points $\boldsymbol{x_1}, \boldsymbol{x_2}, \ldots, \boldsymbol{x_t}$ in $\mathbb{R}^n$, a *convex combination* of these points is the point in the form

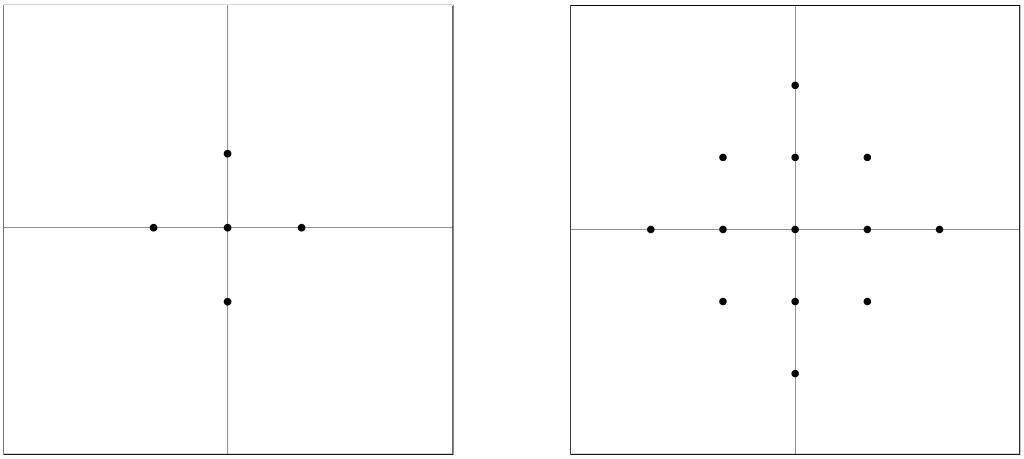
$$\theta_1 \boldsymbol{x_1} + \theta_2 \boldsymbol{x_2} + \cdots + \theta_t \boldsymbol{x_t},$$

where $\theta_1 + \theta_2 + \cdots + \theta_t = 1$ and $\theta_i \geq 0$ for $i = 1, 2, \ldots, t$.

Given a set C in $\mathbb{R}^n$, its *convex hull*, denoted $conv(C)$, is the smallest with respect to inclusions convex set that contains C. Equivalently, $conv(C)$ is the set of all convex combinations of points in C, See Figure 1.6.

Definition 8. A compact (that is closed and bounded) convex set $C \subset \mathbb{R}^n$ with nonempty interior is called a *convex body*.

We will denote the set of all convex bodies in $\mathbb{R}^n$ by $\mathscr{K}^n$, and the set of all $\mathbf{0}$-symmetric convex bodies by $\mathscr{K}_0^n$.



C $D(C)$

Figure 1.7: Example of Set of Points C (left) and its Difference Set $D(C)$ (right).

Definition 9. Given a set $C \in \mathbb{R}^n$, the *difference set of* C is defined as

$$D(C) = C - C = \{\boldsymbol{x} - \boldsymbol{y} : \boldsymbol{x}, \boldsymbol{y} \in C\}.$$

Clearly, $D(C)$ is $\mathbf{0}$-symmetric. If $C \in \mathscr{K}^n$, then $D(C) \in \mathscr{K}_0^n$, see for example Figure 1.7.

1.4 Minkowski's first fundamental theorem

The first Minkowski's fundamental theorem considers the following question: when does an origin-symmetric convex set contain a non-zero lattice point?

Theorem 1 (Minkowski's 1st fundamental theorem)**.** *Let $S \subset \mathbb{R}^n$ be an $\mathbf{0}$-symmetric convex set of volume* $\mathrm{vol}(S)$*, and let $L \subset \mathbb{R}^n$ be a lattice with determinant* $\det(L)$*. If* $\mathrm{vol}(S) > 2^n \det(L)$*, then S contains a nonzero point $\boldsymbol{u} \in L$.*

This remarkable result paved the way for many discoveries in number theory, as well as implications in combinatorics, computational complexity,

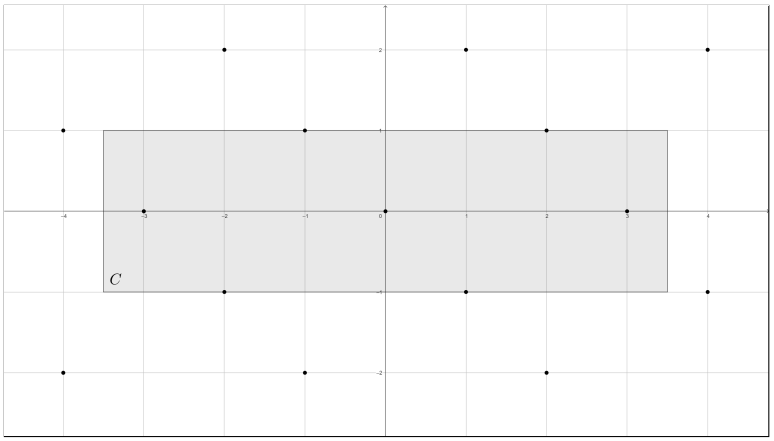


Figure 1.8: A two-dimensional lattice L and an $\mathbf{0}$-symmetric box C such that $\mathrm{vol}(C) > 4\det(L)$.

cryptography and other disciplines. Figure 1.8 provides a illustration for the Minkowski first fundamental theorem.

We will include in this thesis a proof of Theorem (1) based on the following beautiful result of Blichfeldt. We refer the reader to the classical book of Cassels [13] for a detailed introduction to the geometry of numbers.

Lemma 2 (Blichfeldt's Lemma)**.** *Let L be a lattice in $\mathbb{R}^n$ and $S \subset \mathbb{R}^n$ a set of volume* $\mathrm{vol}(S)$*. Suppose that* $\mathrm{vol}(S) > \det(L)$*, then there exist points $\boldsymbol{x}_1, \boldsymbol{x}_2 \in S$, $\boldsymbol{x}_1 \neq \boldsymbol{x}_2$, such that $\boldsymbol{x}_1 - \boldsymbol{x}_2 \in L$.*

Proof. Let $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ be any basis of the lattice L, and F be the corresponding fundamental paralleplepiped of L. It follows that $\mathrm{vol}(F) = \det(L)$. Furthermore, any point $\boldsymbol{x} \in \mathbb{R}^n$ can be expressed as $\boldsymbol{x} = \boldsymbol{u} + \boldsymbol{v}$, where $\boldsymbol{u} \in L$ and $\boldsymbol{v} \in F$. For each $\boldsymbol{u} \in L$ let $R(\boldsymbol{u})$ be the set of points $\boldsymbol{v}$ such that

$$\boldsymbol{v} \in F,\ \boldsymbol{u} + \boldsymbol{v} \in S.$$

Then

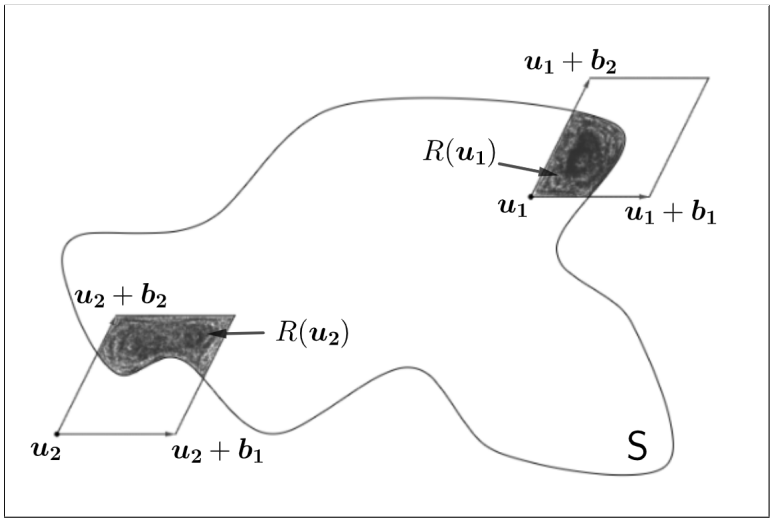


Figure 1.9: The sum of the volumes of the sets $R(\boldsymbol{u})$ for each $\boldsymbol{u}$ in L is equal to the volume of the set S.

$$\sum_{\boldsymbol{u}\in L} \text{vol}(R(\boldsymbol{u})) = \text{vol}(S).$$

Suppose that $\text{vol}(S) > \det(L)$ Then

$$\sum_{\boldsymbol{u}\in L} \text{vol}(R(\boldsymbol{u})) > \text{vol}(F).$$

Since $R(\boldsymbol{u})$ are all contained in F, see Figure 1.9, there must be at least one point $\boldsymbol{v}_0 \in F$ which belongs to at least two of the $R(\boldsymbol{u})$, say

$$\boldsymbol{v}_0 \in R(\boldsymbol{u}_1) \text{ and } \boldsymbol{v}_0 \in R(\boldsymbol{u}_2),$$

where $\boldsymbol{u}_1 \neq \boldsymbol{u}_2$. Then the points

$$\boldsymbol{x}_1 = \boldsymbol{v}_0 + \boldsymbol{u}_1,\ \boldsymbol{x}_2 = \boldsymbol{v}_0 + \boldsymbol{u}_2$$

are in S by definition of $R(\boldsymbol{u})$ and

$$\boldsymbol{x}_1 - \boldsymbol{x}_2 = \boldsymbol{u}_1 - \boldsymbol{u}_2 \in L\backslash\{\boldsymbol{0}\}.$$

The lemma is proved. □

We are now ready to prove the Minkowski's first fundamental theorem.

Proof. The set

$$\frac{1}{2}S = \left\{\frac{1}{2}\boldsymbol{x} : \boldsymbol{x} \in S\right\},$$

has volume

$$\text{vol}\left(\frac{1}{2}S\right) = \frac{1}{2^n}\,\text{vol}(S).$$

Therefore, by the statement of the theorem

$$\text{vol}\left(\frac{1}{2}S\right) > \det(L),$$

This enables us to apply Lemma 2 to the set $(1/2)S$. In this case, we have

$$\boldsymbol{x}_1, \boldsymbol{x}_2 \in \frac{1}{2}S,\ \boldsymbol{x}_1 \neq \boldsymbol{x}_2, \tag{1.1}$$

such that

$$\boldsymbol{x}_1 - \boldsymbol{x}_2 \in L.$$

Obviously,

$$\boldsymbol{x}_1 = \frac{1}{2}\boldsymbol{u}_1,\ \boldsymbol{x}_2 = \frac{1}{2}\boldsymbol{u}_2,$$

where $\boldsymbol{u}_1, \boldsymbol{u}_2 \in S, \boldsymbol{u}_1 \neq \boldsymbol{u}_2$. We have by (1.1)

$$\frac{1}{2}\boldsymbol{u}_1 - \frac{1}{2}\boldsymbol{u}_2 = \frac{1}{2}\boldsymbol{u}_1 + \frac{1}{2}(-\boldsymbol{u}_2) \in L.$$

Given that S is symmetric with respect to the origin, we have $-\boldsymbol{u}_2 \in S$. Moreover, since S is convex, it follows that

$$\boldsymbol{0} \neq \frac{1}{2}\boldsymbol{u}_1 + \frac{1}{2}(-\boldsymbol{u}_2) \in S.$$

The geometry of this argument is illustrated by Figure 1.10. Therefore

$$\boldsymbol{0} \neq \frac{1}{2}\boldsymbol{u}_1 + \frac{1}{2}(-\boldsymbol{u}_2) \in S \cap L.$$

Theorem is proved. □

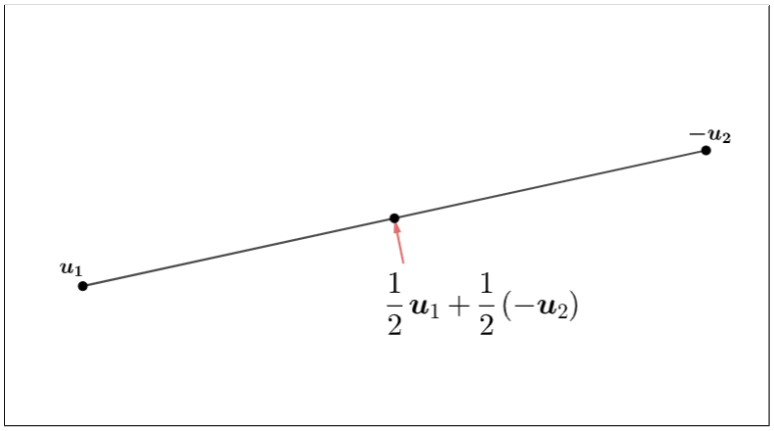


Figure 1.10: Midpoint of the line segment between $\boldsymbol{u}_1$ and $\boldsymbol{u}_2$.

1.5 Successive minima

Successive minima of convex bodies with respect to lattices were defined and investigated by Minkowski in the context of the geometry of numbers [35].

Definition 10. Let $C \in \mathscr{K}_0^n$ and $\Lambda \subset \mathbb{R}^n$ be a full-dimensional lattice. The ith *successive minimum* $\lambda_i(C,\Lambda)$, $1 \leq i \leq n$, of C with respect to the lattice Λ is defined by

$$\lambda_i(C,\Lambda) = \min\{\lambda > 0 : \dim(\lambda C \cap \Lambda) \geq i\},\ 1 \leq i \leq n.$$

In other words, the ith successive minimum is the smallest positive dilation factor λ such that λC contains at least i linearly independent points of the lattice Λ.

Clearly we have,

$$0 < \lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n.$$

Example 2. *Consider the cube* $C^2(1/2) = \{\boldsymbol{x} \in \mathbb{R}^2 : \|\boldsymbol{x}\|_\infty \leq 1/2\}$, *and the*

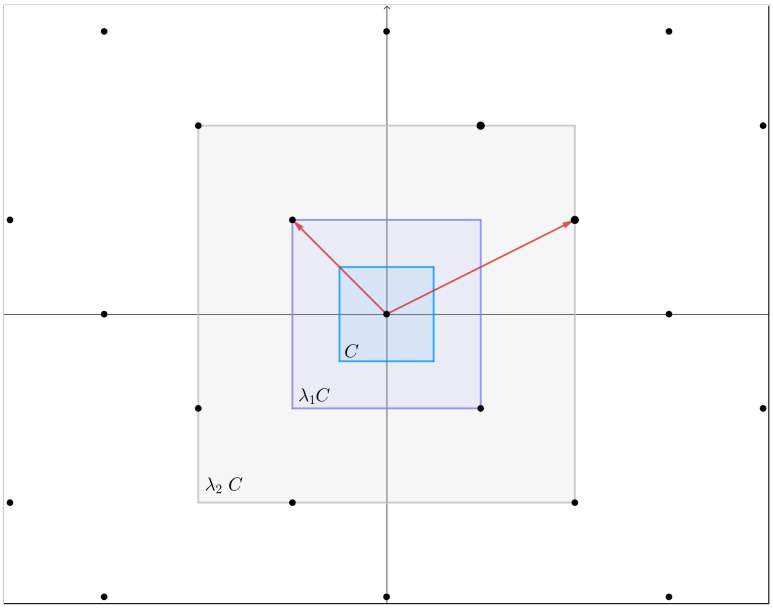


Figure 1.11: The first and second successive minima of convex body C with respect to the lattices $\Lambda(B)$.

lattice $\Lambda(B)$ *with basis matrix*

$$B = \begin{pmatrix} 2 & 1 \\ 1 & -1 \end{pmatrix}.$$

The first and second successive minima of $C^2(1/2)$ *with respect to* $\Lambda(B)$ *are* $\lambda_1 = 2$ *and* $\lambda_2 = 4$ *. See Figure 1.11.*

Any full-dimensional lattice Λ can be expressed as $\Lambda = A\mathbb{Z}^n$, where A is a non-singular $n \times n$ basis matrix. Consequently, we have $\lambda_i(C, \Lambda) = \lambda_i\left(A^{-1}C, \mathbb{Z}^n\right)$ and $|C \cap \Lambda| = \left|A^{-1}C \cap \mathbb{Z}^n\right|$.

Furthermore, there exists a basis $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ for Λ, such that the linear hull of any i of n linearly independent lattice points $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ is equal to the linear hull of $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_i$ for $1 \leq i \leq n$. This means that

$$\text{lin}\{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_i\} = \text{lin}\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_i\}.$$

In particular, if $\boldsymbol{z}_i \in \mathbb{Z}^n, 1 \leq i \leq n$, are n linearly independent lattice vectors that satisfy $\boldsymbol{z}_i \in \lambda_i(C, \mathbb{Z}^n)C$, then there exists a unimodular matrix $U \in \mathbb{Z}^{n\times n}$ such that

$$U\boldsymbol{z}_i \in (\lambda_i(UC, \mathbb{Z}^n)UC) \cap \operatorname{lin}\{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_i\}, \quad 1 \leq i \leq n, \tag{1.2}$$

where $\boldsymbol{e}_i \in \mathbb{R}^n$ denotes the i-th unit vector. Moreover, it can be observed that for n linearly independent lattice points $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ of a lattice Λ satisfying $\boldsymbol{a}_i \in \lambda_i(C, \Lambda)C$, the definition of the successive minima implies

$$\operatorname{int}(\lambda_i(C, \Lambda)C) \cap \Lambda \subset \operatorname{lin}\{\boldsymbol{0}, \boldsymbol{a}_1, \ldots, \boldsymbol{a}_{i-1}\} \cap \Lambda, \quad 1 \leq i \leq n, \tag{1.3}$$

where int denotes the interior.

1.6 Minkowski's theorem on successive minima

Minkowski's convex body theorem has many extensions and refinements. See for example Gruber and Lekkerkerker [29] and Lagarias [27]. An important refinement is the second fundamental theorem of Minkowski, also known as Minkowski's theorem on successive minima [28]. It gives optimal upper and lower bounds for the product of the successive minima of an origin-symmetric convex body with respect to a lattice.

Theorem 3 (Minkowski [35])**.** *Let $C \in \mathscr{K}_0^n$ and $\Lambda \subset \mathbb{R}^n$ be a full-dimensional lattice. Then we have,*

$$\frac{2^n}{n!} \det(\Lambda) \leq \prod_{i=1}^{n} \lambda_i(C, \Lambda) \operatorname{vol}(C) \leq 2^n \det(\Lambda) \ .$$

The difficult part of the proof is to show the right-hand inequality. The original proof of Minkowski [35] is rather involved. Alternative proofs were

found by Bambah, Woods and Zassenhaus [8] and others. Below we include an elegant proof due to Henk [31].

Proof. Without loss of generality, we will assume that $\Lambda = \mathbb{Z}^n$. For convenience, we denote $\lambda_i = \lambda_i(C, \mathbb{Z}^n)$, and set $C_i = \frac{\lambda_i}{2} C$. Moreover, we assume that $\boldsymbol{z}_1, \ldots, \boldsymbol{z}_n$ are n linearly independent lattice points such that $\boldsymbol{z}_i \in \lambda_i C \cap \mathbb{Z}^n$, and the linear space of $\boldsymbol{z}_1, \ldots, \boldsymbol{z}_i$ is equal to the linear space of $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_i$, where $1 \leq i \leq n$. For shortness, we denote the linear space $\operatorname{lin}\{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_i\}$ by L_i.

Let $M_q^n = \{\boldsymbol{z} \in \mathbb{Z}^n : |z_i| \leq q, 1 \leq i \leq n\}$ be a set of lattice points in $\mathbb{Z}^n$ where each coordinate is bounded by $q \in \mathbb{N}$. For $1 \leq j \leq n-1$, let $M_q^j = M_q^n \cap L_j$. Since C is a bounded set, there exists a constant γ, which depends only on C, such that

$$\operatorname{vol}\left(M_q^n + C_n\right) \leq (2q + \gamma)^n. \tag{1.4}$$

Using the definition of λ_1, for any two distinct lattice points $\boldsymbol{z}, \bar{\boldsymbol{z}} \in \mathbb{Z}^n$, the intersection of $(\boldsymbol{z} + \operatorname{int}(C_1))$ and $(\bar{\boldsymbol{z}} + \operatorname{int}(C_1))$ is empty. This is because otherwise, we would obtain a contradiction $\boldsymbol{z} - \bar{\boldsymbol{z}} \in (\operatorname{int}(C_1) - \operatorname{int}(C_1)) \cap \mathbb{Z}^n = \operatorname{int}(C_1 - C_1) \cap \mathbb{Z}^n = \operatorname{int}(\lambda_1 C) \cap \mathbb{Z}^n = \{0\}$. Therefore, we have the following

$$\operatorname{vol}\left(M_q^n + C_1\right) = (2q+1)^n \operatorname{vol}(C_1) = (2q+1)^n \left(\frac{\lambda_1}{2}\right)^n \operatorname{vol}(C). \tag{1.5}$$

We will now show that for $1 \leq i \leq n-1$, the following inequality holds

$$\operatorname{vol}\left(M_q^n + C_{i+1}\right) \geq \left(\frac{\lambda_{i+1}}{\lambda_i}\right)^{n-i} \operatorname{vol}\left(M_q^n + C_i\right). \tag{1.6}$$

Thus, we can assume that $\lambda_{i+1} > \lambda_i$ and consider two lattice points $\boldsymbol{z}$ and $\bar{\boldsymbol{z}}$ in $\mathbb{Z}^n$ that differ in the last $n-i$ coordinates, i.e., $(z_{i+1}, \ldots, z_n) \neq (\bar{z}_{i+1}, \ldots, \bar{z}_n)$. It follows that

$$[\boldsymbol{z} + \operatorname{int}(C_{i+1})] \cap [\bar{\boldsymbol{z}} + \operatorname{int}(C_{i+1})] = \emptyset. \tag{1.7}$$

If this is not the case, then the $i+1$ linearly independent lattice points $\boldsymbol{z} - \bar{\boldsymbol{z}}, \boldsymbol{z}_1, \ldots, \boldsymbol{z}_i$ would belong to the interior of $\lambda_{i+1}C$, contradicting the minimality of λ_{i+1}. Hence, from equation (1.7), we obtain

$$\begin{aligned}\operatorname{vol}\left(M_q^n + C_{i+1}\right) &= (2q+1)^{n-i} \operatorname{vol}\left(M_q^i + C_{i+1}\right),\\ \operatorname{vol}\left(M_q^n + C_i\right) &= (2q+1)^{n-i} \operatorname{vol}\left(M_q^i + C_i\right).\end{aligned}$$

To verify equation (1.6), it suffices to show

$$\operatorname{vol}\left(M_q^i + C_{i+1}\right) \geq \left(\frac{\lambda_{i+1}}{\lambda_i}\right)^{n-i} \operatorname{vol}\left(M_q^i + C_i\right). \tag{1.8}$$

Let f_1 and f_2 be linear maps from $\mathbb{R}^n$ to $\mathbb{R}^n$ defined as

$$\begin{aligned}f_1(\boldsymbol{x}) &= \left(\frac{\lambda_{i+1}}{\lambda_i}x_1, \ldots, \frac{\lambda_{i+1}}{\lambda_i}x_i, x_{i+1}, \ldots, x_n\right)^\top,\\ f_2(\boldsymbol{x}) &= \left(x_1, \ldots, x_i, \frac{\lambda_{i+1}}{\lambda_i}x_{i+1}, \ldots, \frac{\lambda_{i+1}}{\lambda_i}x_n\right)^\top.\end{aligned}$$

Using the fact that $M_q^i + C_{i+1} = f_2\left(M_q^i + f_1(C_i)\right)$, we have

$$\operatorname{vol}\left(M_q^i + C_{i+1}\right) = \left(\frac{\lambda_{i+1}}{\lambda_i}\right)^{n-i} \operatorname{vol}\left(M_q^i + f_1(C_i)\right).$$

To prove equation (1.8), we have to show

$$\operatorname{vol}\left(M_q^i + f_1(C_i)\right) \geq \operatorname{vol}\left(M_q^i + C_i\right). \tag{1.9}$$

Let $L_i^\perp$ be the $(n-i)$-dimensional orthogonal complement of L_i, and it is obvious that for any $\boldsymbol{x} \in L_i^\perp$, there exists a $t(\boldsymbol{x}) \in L_i$ such that $C_i \cap (\boldsymbol{x} + L_i) \subset (f_1(C_i) \cap (\boldsymbol{x} + L_i)) + t(\boldsymbol{x})$. Thus, we have

$$\left(M_q^i + C_i\right) \cap (\boldsymbol{x} + L_i) \subset \left[\left(M_q^i + f_1(C_i)\right) \cap (\boldsymbol{x} + L_i)\right] + t(\boldsymbol{x}).$$

From this, we obtain

$$\begin{aligned}\mathrm{vol}\left(M_q^i + C_i\right) &= \int_{\boldsymbol{x}\in L_i^\perp} \mathrm{vol}_i\left(\left(M_q^i + C_i\right)\cap(\boldsymbol{x}+L_i)\right)\mathrm{d}x \\ &\le \int_{\boldsymbol{x}\in L_i^\perp} \mathrm{vol}_i\left(\left(M_q^i + f_1(C_i)\right)\cap(\boldsymbol{x}+L_i)\right)\mathrm{d}x \\ &= \mathrm{vol}\left(M_q^i + f_1(C_i)\right),\end{aligned}$$

where $\mathrm{vol}_i(\cdot)$ denotes the i-dimensional volume. This implies (1.9), so we have proven (1.6). Finally, from (1.4), (1.5) and (1.6) we have

$$\begin{aligned}(2q+\gamma)^n &\ge \mathrm{vol}\left(M_q^n + C_n\right) \ge \left(\frac{\lambda_n}{\lambda_{n-1}}\right)\mathrm{vol}\left(M_q^n + C_{n-1}\right) \\ &\ge \left(\frac{\lambda_n}{\lambda_{n-1}}\right)\left(\frac{\lambda_{n-1}}{\lambda_{n-2}}\right)^2 \mathrm{vol}\left(M_q^n + C_{n-2}\right) \ge \cdots\cdots \\ &\ge \left(\frac{\lambda_n}{\lambda_{n-1}}\right)\cdot\left(\frac{\lambda_{n-1}}{\lambda_{n-2}}\right)^2 \cdot \ldots \cdot \left(\frac{\lambda_2}{\lambda_1}\right)^{n-1} \mathrm{vol}\left(M_q^n + C_1\right) \\ &= \lambda_n \cdot \ldots \cdot \lambda_1 \frac{\mathrm{vol}(C)}{2^n}(2q+1)^n\end{aligned}$$

and so

$$\lambda_1 \cdot \ldots \cdot \lambda_n \,\mathrm{vol}(C) \le 2^n \cdot \left(\frac{2q+\gamma}{2q+1}\right)^n.$$

Since this inequality holds for all $q \in \mathbb{N}$, the theorem is proven. □

1.7 Number of lattice points in a convex body and successive minima

Henk [31] used Minkowski's second theorem to give an upper bound on the number of lattice points in an origin symmetric convex body C in terms of the successive minima in the following way:

Theorem 4 (Henk [31]). *Let $n \geq 2$, $C \in \mathcal{K}_0^n$ and $\Lambda \subset \mathbb{R}^n$ be a full-dimensional lattice then*

$$|C \cap \Lambda| \leq 2^{n-1} \prod_{i=1}^{n} \left(\frac{2}{\lambda_i(C,\Lambda)} + 1 \right).$$

For completeness we include a proof of this result as given in [31].

Proof. Without loss of generality, let $\Lambda = \mathbb{Z}^n$, and we can assume that (cf. 1.2 and 1.3),

$$\operatorname{int}(\lambda_i(C,\mathbb{Z}^n)\,C) \cap \mathbb{Z}^n \subset \operatorname{lin}\{\mathbf{0}, \boldsymbol{e}_1, \ldots, \boldsymbol{e}_{i-1}\} \cap \mathbb{Z}^n, \quad 1 \leq i \leq n. \tag{1.10}$$

Let's denote $q_i = \left\lfloor \frac{2}{\lambda_i(C,\Lambda)} + 1 \right\rfloor$, where $1 \leq i \leq n$, for abbreviation. We need to determine n numbers $u_i \in \mathbb{N}$ such that

$$u_n = q_n, \quad q_i \leq u_i < 2q_i, \quad \text{and} \quad u_{i+1} \text{ divides } u_i, \quad 1 \leq i \leq n-1. \tag{1.11}$$

To determine u_k, we consider two cases, assuming that we have already found $u_n, \ldots, u_{k+1}$ with the properties mentioned earlier. If $u_{k+1} \geq q_k$, then we simply set $u_k = u_{k+1}$. This satisfies $q_k \leq u_k = u_{k+1} < 2q_{k+1} \leq 2q_k$, since $q_k \geq q_{k+1}$. Otherwise, if $u_{k+1} < q_k$. We can express q_k as $q_k = m \cdot u_{k+1} + r$, where $m \in \mathbb{N}$, $m \geq 1$, and $0 \leq r < u_{k+1}$. In this case, we set $u_k = q_k + u_{k+1} - r$, and it can be easily verified that u_k satisfies the requirements of (1.11). Let $\widetilde{\Lambda} \subset \mathbb{Z}^n$ be the lattice generated by the vectors $u_1\boldsymbol{e}_1, u_2\boldsymbol{e}_2, \ldots, u_n\boldsymbol{e}_n$. It follows that $\det\widetilde{\Lambda}/\det\Lambda = u_1 \cdot u_2 \cdot \ldots \cdot u_n$, and combining this with the upper bounds on the values of u_i as given in Lemma 2.1, in [31] we obtain

$$|C \cap \Lambda| \leq |2C \cap \widetilde{\Lambda}| \prod_{i=1}^{n} u_i < |2C \cap \widetilde{\Lambda}| 2^{n-1} \prod_{i=1}^{n} \left\lfloor \frac{2}{\lambda_i(C,\Lambda)} + 1 \right\rfloor.$$

To verify the theorem, it is sufficient to show that $2C \cap \widetilde{\Lambda} = \{\mathbf{0}\}$. Let's assume that there exists a non-zero element $\boldsymbol{g} \in 2C \cap \widetilde{\Lambda}$, and let k be the largest index

where $\boldsymbol{g}$ has a non-zero coordinate, i.e., $g_k \neq 0$, while $g_{k+1} = \cdots = g_n = 0$. Then we can express $\boldsymbol{g}$ as

$$\boldsymbol{g} = z_1(u_1\boldsymbol{e}_1) + z_2(u_2\boldsymbol{e}_2) + \cdots + z_k(u_k\boldsymbol{e}_k) \in 2C,$$

where $z_i \in \mathbb{Z}$. Since u_k is a divisor of $u_1, \ldots, u_{k-1}$, and we have $2/u_k < \lambda_k(C, \mathbb{Z}^n)$ (1.11), we can deduce that

$$\frac{1}{u_k}\boldsymbol{g} \in \left(\frac{2}{u_k}C\right) \cap \mathbb{Z}^n \subset \operatorname{int}(\lambda_k(C, \mathbb{Z}^n)\, C) \cap \mathbb{Z}^n.$$

However, this violates condition (1.10) since $g_k \neq 0$. Therefore, we conclude that $2C \cap \widetilde{\Lambda} = \{0\}$, proving the theorem. □

1.8 The generalised Hermite constant

The generalised Hermite constant $\gamma_{r,s}$, as defined by Rankin [39], is a positive real number defined as the infimum over all γ such that every lattice Λ of rank r in $\mathbb{R}^r$ has a sublattice Γ of rank s and determinant

$$\det(\Gamma) \leq \gamma^{1/2}(\det(\Lambda))^{s/r}. \tag{1.12}$$

In other words, $\gamma_{r,s}$ is the smallest constant for which this inequality holds for all lattices Λ of rank r and for all choices of sublattice Γ of rank s.

The generalised Hermite constant is an important constant in lattice theory and has applications in number theory, cryptography, and coding theory. The value of $\gamma_{r,s}$ is known exactly for some small values of r and s, but it is generally difficult to compute or estimate for larger values. We refer the reader to the papers [43, 50] for known results on the Rankin constant.

Note that in (1.12) $\gamma_{r,1} = \gamma_{r,r-1} = \gamma_r$ represents the ordinary Hermite constant [18].

Chapter 2

Compressed sensing for integer valued signals

2.1 Introduction

This chapter gives a brief introduction to the mathematical aspects of compressed sensing relevant to this thesis. It is based on the references [23, 24, 26, 33, 37, 42].

The main objective of compressed sensing is to design and efficiently solve underdetermined systems of linear equations

$$A\boldsymbol{x} = \boldsymbol{b}, \tag{2.1}$$

with $A \in \mathbb{R}^{m\times n}$ and $\boldsymbol{b} \in \mathbb{R}^m$, $m < n$, under an additional assumption that the solution $\boldsymbol{x} \in \mathbb{R}^n$ is "sparse". Here a solution vector $\boldsymbol{x}$ is "sparse" or, more specifically, *s-sparse* if the number of its non-zero elements is less than or equal to s. In other words, $\|\boldsymbol{x}\|_0 \leq s$.

The matrix A has been traditionally referred to as a *measurement matrix*, $\boldsymbol{b}$ as a vector of m *measurements* and a solution vector $\boldsymbol{x}$ as a *signal*. In a basic scenario, there is an unknown s-sparse signal $\boldsymbol{x}$ and we want to know what conditions for the measurement matrix A will allow us to uniquely and efficiently recover $\boldsymbol{x}$ from the measurements $\boldsymbol{b}$. That is, in particular, $\boldsymbol{x}$ must be the unique s-sparse solution to the system (2.1).

The feasibility of this problem in various practical settings is by now well-justified, and sparsity of data has been identified as a new paradigm in signal processing. Various sufficient conditions for precise recovery of the signal $\boldsymbol{x}$ have been found in terms of the properties of the measurement matrix A and the sparsity of $\boldsymbol{x}$. We refer the reader to [19] for an extensive survey. In the following section, we briefly discuss probably the most studied recovery approach.

2.2 Unique recovery using basis pursuit

A natural way to recover sparse signals from an underdetermined linear system would be to solve an ℓ_0-minimisation problem, that is the problem

$$\min \|\boldsymbol{x}\|_0 \quad \text{subject to} \quad A\boldsymbol{x} = \boldsymbol{b}\,. \tag{2.2}$$

This problem, however, is known to be NP-hard [36], which makes solving it unpractical. A popular and by now well-understood approach to avoid the NP-hardness barrier is to replace (2.2) with a convex optimisation problem

$$\min \|\boldsymbol{x}\|_1 \quad \text{subject to} \quad A\boldsymbol{x} = \boldsymbol{b}$$

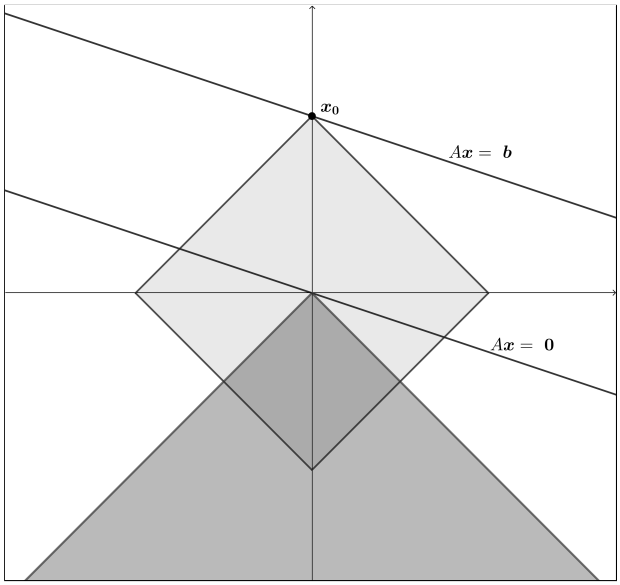


Figure 2.1: The 1-sparse vector $\boldsymbol{x_0}$ can be uniquely recovered via ℓ_1-minimisation since the null space of A intersects the cone only at the origin.

which is known as *basis pursuit* [16]. As this problem is convex, it can be solved efficiently using convex optimisation methods. A necessary and sufficient condition under which a signal $\boldsymbol{x}_0$ is uniquely recovered by basis pursuit is given as follows: The set of all feasible solutions, $\boldsymbol{x}_0 + \ker(A)$, intersects with the set $\left\{\boldsymbol{x} : \|\boldsymbol{x}\|_1 \leq \|\boldsymbol{x}_0\|_1\right\}$ exactly at $\boldsymbol{x}_0$. This condition provides a useful geometric intuition about properties of measurement matrices to ensure uniqueness of the solution. One of those properties is the so-called Null Space Property (NSP). To describe it we need to introduce a useful notation. Let $M \in \mathbb{R}^{m\times n}$ and let $\tau = \{i_1, \ldots, i_k\} \subseteq \{1, \ldots, n\}$ with $i_1 < i_2 < \cdots < i_k$. We will denote by M_τ the $m \times k$ submatrix of M with columns indexed by τ. In the same manner, given $\boldsymbol{x} \in \mathbb{R}^n$, we will denote by $\boldsymbol{x}_\tau$ the vector $(x_{i_1}, \ldots, x_{i_k})^\top$. The complement of τ in $\{1, \ldots, n\}$ will be denoted as $\bar{\tau}$.

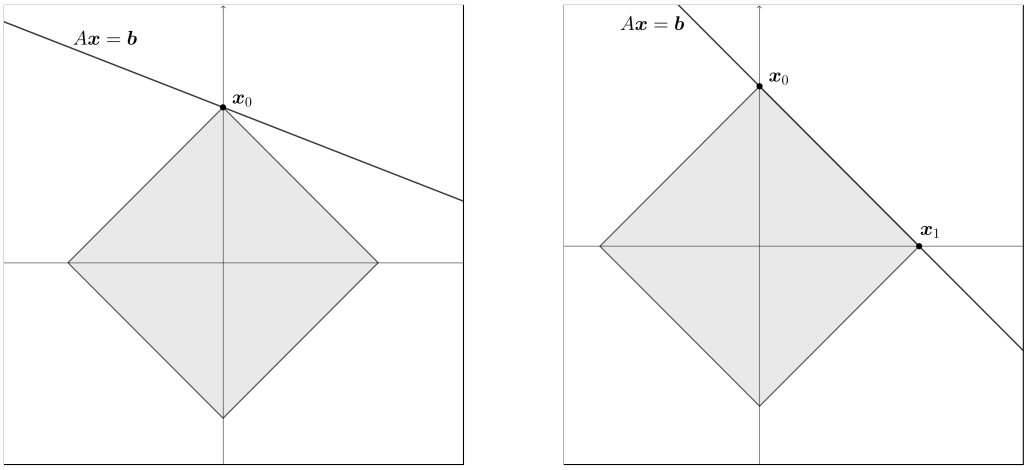


Figure 2.2: When the ℓ_1 ball intersects with the solution set of $A\boldsymbol{x} = \boldsymbol{b}$ in a single point (left), then ℓ_1 minimisation can provide the same solution as ℓ_0 minimisation.

Now the NSP is given by

$$\ker(A) \cap \left\{ w \in \mathbb{R}^n : \|w_\tau\|_1 \geq \|w_{\bar{\tau}}\|_1 \right\} = \{\mathbf{0}\},$$

where $\tau = \operatorname{supp}(\boldsymbol{x}_0)$. See Figure 2.1.

It is well-known that, if A fulfills the NSP with respect to some subset $\tau \subset [n]$, every signal $\boldsymbol{x}_0$ supported on τ is the unique minimiser of (2.2) with $\boldsymbol{b} = A\boldsymbol{x}_0$ (cf. [17, 20, 21, 22, 24]). Figure 2.2 illustrates this concept.

By using random matrices A such as a matrix with independent and identically distributed Gaussian entries, it is possible to achieve a very high probability of A having the NSP and therefore of (2.2) to succeed, given that the number of measurements satisfies $m \geq Cs\log(n)$, where s is the sparsity of the signal $\boldsymbol{x}_0$ and C some positive constant not depending on s and n [11].

2.3 Unique recovery of integer signals

In some applications, additional information on the signal $\boldsymbol{x}$ is known and one can say that the signal belongs to a certain *signal space* S that possesses certain additional structure. Hence, we face a natural question: how the structure of S can be exploited to improve recovery guarantees? In this thesis, we will focus on the integer-valued signals, which appear, for instance, in MIMO systems [41], wideband spectrum sensing [7] and error correcting codes [12]. We will work in the setting introduced by Fukshansky, Needell, and Sudakov [26].

Further, in this thesis we will consider the signals with bounded entries. We will focus on the conditions that guarantee the uniqueness of the solution.

Let us fix a set $S \subset \mathbb{Z}^n$ which will be our *signal space*. Fukshansky, Needell, and Sudakov [26] introduced and studied the problem of unique recovery of a signal $\boldsymbol{x}_0 \in S$ from a relatively small number of noisy linear integer measurements. Specifically, given a number of measurements m with $m < n$, we aim to construct an integer measurement matrix $A \in \mathbb{Z}^{m\times n}$ such that any signal $\boldsymbol{x}_0 \in S$ can be uniquely recovered from m measurements represented by the vector $\boldsymbol{b} \in \mathbb{R}^m$ of the form

$$\boldsymbol{b} = A\boldsymbol{x}_0 + \boldsymbol{e} \tag{2.3}$$

with an unknown *noise vector* $\boldsymbol{e} \in \mathbb{R}^m$. To allow unique recovery we assume that

$$\|\boldsymbol{e}\|_2 < c\,,$$

where $\|\cdot\|_2$ denotes the ℓ_2-norm and c is a suitably chosen constant. Note that, the number of measurements m is independent of the choice of the constant c.

Based on [26], we will use the following recovery approach. For a set $Q \subset \mathbb{Z}^n$ we denote by $\mathscr{R}(Q)$ the set of all integer matrices A such that

$$\|A\boldsymbol{y}\|_2 \geq 1 \text{ for any nonzero } \boldsymbol{y} \in Q\,. \tag{2.4}$$

Recall that the *difference set* $D(X)$ of a set $X \in \mathbb{R}^n$ consists of all points $\boldsymbol{x} - \boldsymbol{y}$ with $\boldsymbol{x}, \boldsymbol{y} \in X$. We set $c = 1/2$ and consider measurement matrices $A \in \mathscr{R}(Q)$ with $Q = D(S)$. In this case, for any $\boldsymbol{e} \in \mathbb{R}^m$ with $\|\boldsymbol{e}\|_2 < c = 1/2$, the signal $\boldsymbol{x}_0$ is the unique point of S satisfying the bound

$$\|A\boldsymbol{x} - \boldsymbol{b}\|_2 \leq \frac{1}{2}\,. \tag{2.5}$$

Indeed, for any $\boldsymbol{x} \in S$, $\boldsymbol{x} \neq \boldsymbol{x}_0$, satisfying (2.5), we would have

$$\begin{aligned}\|A(\boldsymbol{x} - \boldsymbol{x}_0)\|_2 &= \|A\boldsymbol{x} - \boldsymbol{b} - (A\boldsymbol{x}_0 - \boldsymbol{b})\|_2 \\ &= \|A\boldsymbol{x} - \boldsymbol{b} + \boldsymbol{e}\|_2 \\ &\leq \|A\boldsymbol{x} - \boldsymbol{b}\|_2 + \|\boldsymbol{e}\|_2 < 1\,,\end{aligned}$$

contradicting (2.4). Therefore, $\boldsymbol{x}_0$ can be recovered by any algorithm that, given input $\boldsymbol{b} \in \mathbb{R}^m$ computes a vector $\boldsymbol{x} \in S$ satisfying (2.5).

By $\mathbb{Z}^n_l$ we will denote the set of l-sparse n-dimensional integer vectors:

$$\mathbb{Z}^n_l = \{\boldsymbol{z} \in \mathbb{Z}^n : \|\boldsymbol{z}\|_0 \leq l\}\,.$$

Given positive integers n, r, we denote by $C^n(r)$ the n-dimensional cube defined as $C^n(r) = \{\boldsymbol{x} \in \mathbb{R}^n : \|\boldsymbol{x}\|_\infty \leq r\}$.

We will be interested in unique recovery of l-sparse signals with entries from a finite integer alphabet $[-r, r] \cap \mathbb{Z}$. Specifically, we will work with the signal space

$$S^n_l(r) = C^n(r) \cap \mathbb{Z}^n_l\,,$$

where $2l < n$.

The space $S_l^n(r)$ is finite and hence allows using a single measurement for unique recovery of its signals. From the computational and error-correcting perspectives (see [26] for more details), the measurement should have as small as possible absolute integer entries. Hence, given $l, n \in \mathbb{Z}$ with $1 \leq l < n/2$, $r \in \mathbb{Z}_{>0}$ and letting $Q = D(S_l^n(r))$, we face the optimisation problem

$$\min\{\|H\|_\infty : H \in \mathbb{Z}^{1\times n},\ H \in \mathscr{R}(Q)\}\,. \tag{2.6}$$

In Chapter 4 we obtain general estimates for the minimum in (2.6).

2.4 Recent results on unique recovery over $\mathbb{Z}_l^n$

The papers [26, 25, 33, 32] consider the problem of unique recovery over the signal space $\mathbb{Z}_l^n$, where l is a positive integer with $2l < n$. In this setting, the difference set $D(\mathbb{Z}_l^n)$ consists of $2l$-sparse integer vectors, $D(\mathbb{Z}_l^n) = \mathbb{Z}_{2l}^n$. The unique recovery of signals from $\mathbb{Z}_l^n$ involves constructing matrices $A \in \mathbb{Z}^{m\times n}$ with $m = 2l$ and as large as possible n, that belong to $\mathscr{R}(\mathbb{Z}_m^n)$. From the computational and error-correcting perspectives (see [26] for more details), it is also desirable to fix or bound the maximum absolute entry $\|A\|_\infty$ of the matrix A.

Konyagin [32, Theorem 3] proved the following theorem.

Theorem 5. *For integers $k, m \geq 2$, and integer n with*

$$m < n \leq \frac{c^{-m} k^{m/(m-1)}}{\log(k)}$$

there exists an integer $m \times n$ matrix $A \in \mathscr{R}(\mathbb{Z}_m^n)$ such that $\|A\|_\infty = k$, where c is an absolute constant.

The proof of Theorem 5 employs probabilistic arguments to show existence of the desired measurement matrices. Subsequently, Konyagin and Sudakov [33, Theorem 1.3] (see also Ryutin [42]) proved the following result using an explicit and easily computable construction.

Theorem 6. *Let $k \in \mathbb{Z}_{>0}$, $m \in \mathbb{Z}_{>0}$, $m \geq 2$, and*

$$m < n \leq \max(k+1, k^{m/(m-1)}/2)\,. \tag{2.7}$$

Then there exists an $m \times n$ integer matrix $A \in \mathscr{R}(\mathbb{Z}_m^n)$ such that $\|A\|_\infty \leq k$.

Theorem 6 implies the following result.

Corollary 7. *For any given $m, n \in \mathbb{Z}_{>0}$, $2 \leq m < n$ there exists an $m \times n$ integer matrix $A \in \mathscr{R}(\mathbb{Z}_m^n)$ with*

$$\|A\|_\infty \leq \Delta(m,n) = \min(n-1, (2n)^{(m-1)/m})\,.$$

We will use Corollary 7 in the proofs of our results given in Chapter 4.

Chapter 3

Main tools: consolidation of linear Diophantine equations and Siegel's lemma

3.1 Consolidation/aggregation of linear Diophantine equations

The proof of one of the main results of this thesis (see Theorem 18) is based on consolidation/aggregation of linear Diophantine equations. This topic has been extensively studied in the literature. We refer the reader to the papers [38, 40].

Let $D \subset \mathbb{Z}^n$ be a set of integer points, $A \in \mathbb{Z}^{m\times n}$, $2 \leq m < n$, be a matrix of rank $\operatorname{rank}(A) = m$, and $\boldsymbol{b} \in \mathbb{Z}^m$.

Let $B \in \mathbb{Z}^{l\times m}$, $l < m$, be a matrix of rank l such that

$$\{\boldsymbol{x} \in D : (BA)\boldsymbol{x} - B\boldsymbol{b} = \boldsymbol{0}\} = \{\boldsymbol{x} \in D : A\boldsymbol{x} - \boldsymbol{b} = \boldsymbol{0}\}.$$

Following [40], we will call B an *m-into-l consolidating matrix* and $(BA)\boldsymbol{x} - B\boldsymbol{b} = \boldsymbol{0}$ an *m-into-l consolidation* of $A\boldsymbol{x} - \boldsymbol{b} = \boldsymbol{0}$ with respect to the set D.

Let further $C \in \mathbb{Z}^{m\times(m-l)}$ be an integer matrix of $\operatorname{rank}(C) = m-l$ such that, for some consolidating matrix B, the columns of C span the *kernel* $\ker(B) = \{\boldsymbol{x} \in \mathbb{R}^m : B\boldsymbol{x} = \boldsymbol{0}\}$. That is, denoting by $\operatorname{span}_{\mathbb{R}}(C)$ the subspace spanned by the columns of C, we have $\operatorname{span}_{\mathbb{R}}(C) = \ker(B)$. We will call C an *aggregating matrix* for $A\boldsymbol{x} - \boldsymbol{b} = \boldsymbol{0}$ with respect to the set D.

We will write

$$F(\boldsymbol{x}) = A\boldsymbol{x} - \boldsymbol{b},$$

and denote by $F_i(\boldsymbol{x})$ the ith entry of the vector $F(\boldsymbol{x})$, that is

$$F(\boldsymbol{x}) = (F_1(\boldsymbol{x}), \ldots, F_m(\boldsymbol{x}))^\top.$$

Consider the set

$$F^o = \{F(\boldsymbol{x}) : \boldsymbol{x} \in D\} = \{A\boldsymbol{x} : \boldsymbol{x} \in D\} - \boldsymbol{b}.$$

This is the image of D under the linear mapping determined by the matrix A translated by the vector $-\boldsymbol{b}$. The following well-known lemma describes very important properties of the consolidation/aggregation.

Lemma 8. *Let $B \in \mathbb{Z}^{l\times m}$, $l < m$, be a matrix of rank l and $C \in \mathbb{Z}^{m\times(m-l)}$ be a matrix of rank $m-l$. Then*

(i) B an m-into-l consolidating matrix for $A\boldsymbol{x} - \boldsymbol{b} = \boldsymbol{0}$ if and only if $F^o \cap \ker(B) \subset \{\boldsymbol{0}\}$.

(ii) C *is an aggregating matrix of* $A\boldsymbol{x}-\boldsymbol{b}=\boldsymbol{0}$ *if and only if* $F^o \cap \operatorname{span}_{\mathbb{R}}(C) \subset \{\boldsymbol{0}\}$.

We will need the following lemma, given in [6, Theorem 6]. For completeness, we include a proof of this result as given in [40, Example 4.1].

Lemma 9. *Assume that* $q_i \in \mathbb{Z}$ *satisfy* $|F_i(\boldsymbol{x})| < q_i$ *for every* $\boldsymbol{x} \in D$ *such that* $F_i(\boldsymbol{x}) = \cdots = F_{i-1}(\boldsymbol{x}) = 0$, $i = 1, \ldots, m-1$. *Then* $F_1(\boldsymbol{x}) + q_1F_2(\boldsymbol{x}) + q_1q_2F_3(\boldsymbol{x}) + \cdots + q_1 \cdots q_{m-1}F_m(\boldsymbol{x}) = 0$ *is an* m*-into-*1 *consolidation of* $F(\boldsymbol{x}) = \boldsymbol{0}$.

Proof. We have to show that $B = (1, q_1, \ldots, q_1 \cdots q_{m-1})$ is an m-into-1 consolidating matrix for $F(\boldsymbol{x}) = \boldsymbol{0}$. Let $C = (c_{ij}) \in \mathbb{Z}^{m\times(m-1)}$ be defined by $c_{1,k} = q_1\delta_{1,k}$ for $k = 1, \ldots, m-1$ and $c_{ij} = q_i\delta_{i,j} - \delta_{i-1,j}$ for $i = 2, \ldots, m$, $j = 1, \ldots, m-1$. Here $\delta_{i,j}$ stands for the Kronecker delta. That is

$$C = \begin{pmatrix} q_1 & 0 & \cdots & 0 & 0 \\ -1 & q_2 & \cdots & 0 & 0 \\ 0 & -1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & -1 & q_{m-1} \\ 0 & 0 & \cdots & 0 & -1 \end{pmatrix}.$$

We will show that C is an aggregating matrix for $F(\boldsymbol{x}) = \boldsymbol{0}$. It is sufficient to check that the inclusion $F^o \cap \operatorname{span}_{\mathbb{R}}(C) \subset \{\boldsymbol{0}\}$ in the part (ii) of Lemma 8 holds. Suppose

$$C\boldsymbol{v} = F(\boldsymbol{x}) \tag{3.1}$$

for some $\boldsymbol{v} \in \mathbb{R}^{m-1}$ and $\boldsymbol{x} \in D$.

Observe that the greatest common divisor of $m \times m$ subdeterminants of C is equal to one. It follows that the columns of C form a basis of the lattice

$\mathrm{span}_{\mathbb{R}}(C)\cap\mathbb{Z}^m$. Next, by (3.1) we have $C\boldsymbol{v}\in\mathbb{Z}^m$. Therefore, $\boldsymbol{v}\in\mathbb{Z}^{m-1}$. The first coordinate of $C\boldsymbol{v}$ is q_1v_1, hence $|q_1v_1|=|F_1(\boldsymbol{x})|<|q_1|$ implies $v_1=F_1(\boldsymbol{x})=0$. The second coordinate of $C\boldsymbol{v}$ is $q_2v_2-v_1=q_2v_2=F_2(\boldsymbol{x})$. Now by definition of q_2 we have $|q_2v_2|=|F_2(\boldsymbol{x})|<|q_2|$ and, consequently, $v_2=0$. Proceeding in this way we get $\boldsymbol{v}=\mathbf{0}$.

Finally, it is easy to see that the columns of C span $\ker(B)$. Hence B is an m-into-1 consolidating matrix for $F(\boldsymbol{x})=\mathbf{0}$. □

3.2 Siegel's lemma

Consider a system of homogeneous linear equations

$$\begin{cases} a_{11}x_1 \ +\cdots+\ a_{1n}x_n \ =0\,, \\ \quad\vdots \\ a_{m1}x_1 \ +\cdots+\ a_{mn}x_n \ =0\,. \end{cases} \tag{3.2}$$

Let $A=(a_{ij})\in\mathbb{Z}^{m\times n}$, $m<n$. We can write the system (3.2) in the form:

$$A\boldsymbol{x}=\mathbf{0}\,. \tag{3.3}$$

Since $m<n$, the system (3.3) must have a non–trivial solution in integers. If the entries of A are small integers, then one can expect that there will be a solution in relatively small integers. This idea was applied by Thue in [49] to Diophantine approximations. Subsequently, Siegel [47, Bd. I, p. 213, Hilfssatz] was the first to state this principle formally.

Recall that we denote by $\|A\|_\infty$ the maximum absolute value of an entry of A, that is $\|A\|_\infty=\max_{ij}|a_{ij}|$. In what follows, without loss of generality we may assume that A has rank m. Following Siegel's work, Schmidt [45] states the following result.

Theorem 10 (Siegel's Lemma)**.** *The system* (3.3) *has a solution* $\boldsymbol{x} \in \mathbb{Z}^n$ *with*

$$0 < \|\boldsymbol{x}\|_\infty < 1 + (n\|A\|_\infty)^{m/(n-m)}. \tag{3.4}$$

The exponent $m/(n-m)$ on the right hand side of (3.4) is optimal.

In general, Siegel's lemma refers to a family of results that link the properties of lattice points in the kernel space of the matrix A and the characteristics of the matrix, such as its maximum absolute entry or certain functions of its subdeterminants.

Bombieri and Vaaler [9] proved, by using geometry of numbers, the following version of Siegel's lemma which involves $n-m$ solutions to the system (3.3).

Theorem 11 (Bombieri and Vaaler [9])**.** *The system* (3.3) *has* $n-m$ *linearly independent integer solutions* $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{n-m} \in \mathbb{Z}^n$*, with*

$$\prod_{i=1}^{n-m} \|\boldsymbol{x}_i\|_\infty \leq \frac{\sqrt{\det(AA^T)}}{\gcd(A)},$$

where $\gcd(A)$ *is the greatest common divisor of all* $m \times m$ *subdeterminants of* A*.*

In this thesis, Siegel's lemma in the form of Theorem 11 plays an important role in the proof of Theorem 19. In what follows we will give a short overview of selected results related to Siegel's lemma in line with a recent paper [4].

Recall that $C^n(1) = [-1,1]^n$ and let $\ker(A) = \{\boldsymbol{x} \in \mathbb{R}^n : A\boldsymbol{x} = \boldsymbol{0}\}$. Consider the section $S(A) = C^n(1) \cap \ker(A)$ of the cube $C^n(1)$ and the lattice $\Lambda(A) = \mathbb{Z}^n \cap \ker(A)$. The lattice $\Lambda(A)$ has determinant $\det(\Lambda(A)) = \sqrt{\det(AA^T)}/\gcd(A)$. The $(n-m)$-dimensional subspace $\ker(A)$ can be considered as a usual Euclidean $(n-m)$-dimensional space. This immediately extends the definition of

successive minima to o-symmetric bounded convex sets with nonempty relative interior in $\ker(A)$ and $(n-m)$-dimensional lattices in $\ker(A)$. Theorem 11 is an immediate corollary of the following result.

Theorem 12. *Let $A \in \mathbb{Z}^{m\times n}$, $m < n$, be an integral matrix of rank m. Then the inequality*

$$\prod_{i=1}^{n-m} \lambda_i(S(A), \Lambda(A)) \le \det(\Lambda(A)) \tag{3.5}$$

holds.

Proof of Theorem 12: Using a result of Vaaler [51], we have $\mathrm{vol}_{n-m}(S(A)) \ge 2^{n-m}$. Hence, Minkowski's theorem on successive minima gives

$$\prod_{i=1}^{n-m} \lambda_i(S(A), \Lambda(A)) \le \frac{2^{n-m}\det(\Lambda(A))}{\mathrm{vol}_{n-m}(S(A))} \le \det(\Lambda(A)).$$

□

In what follows, we will discuss the special case $m = 1$, that is when A is just an n-dimensional nonzero row vector. Refinements for this case imply a slight improvement of the bound (4.13).

Theorem 11 implies that for every nonzero vector $\boldsymbol{a}$ in $\mathbb{Z}^n$, $n \ge 2$, there exists a vector $\boldsymbol{x}$ in $\mathbb{Z}^n$, such that

$$\boldsymbol{a}\cdot\boldsymbol{x} = 0, \quad 0 < \|\boldsymbol{x}\|_\infty^{n-1} \le \sqrt{n}\|\boldsymbol{a}\|_\infty . \tag{3.6}$$

The exponent $n-1$ in the latter bound is optimal. Let us define

$$c(n) = \sup_{\boldsymbol{a}\in\mathbb{Z}^n\setminus\{0\}} \inf_{\substack{\boldsymbol{x}\in\mathbb{Z}^n\setminus\{0\} \\ \boldsymbol{a}\cdot\boldsymbol{x}=0}} \frac{\|\boldsymbol{x}\|_\infty^{n-1}}{\|\boldsymbol{a}\|_\infty}.$$

That is $c(n)$ is the optimal constant in the bound (3.6).

It is easy to see that $c(2) = 1$. Further, the equality $c(3) = 4/3$ is implicit in [15]. Namely, the inequality $c(3) \leq 4/3$ is contained in [15, Lemma 4], while the inequality $c(3) \geq 4/3$ is a consequence of [15, Lemma 7]. We have also $c(4) = 27/19$. The inequality $c(4) \geq 27/19$ was proved by Chaladus in [14] and its counterpart $c(4) \leq 27/19$ was obtained in [2] (see also [44]). For $n > 4$, the exact values of the constants $c(n)$ remain unknown.

A general result that gives a geometric interpretation for the constant $c(n)$ was given by Schinzel [44]. Given an origin-symmetric convex body K we denote by $\Delta(K)$ its critical determinant.

Theorem 13 (Schinzel [44])**.** *For $n \geq 3$*

$$c(n) = \sup \Delta(H_{\alpha_1,\ldots,\alpha_{n-3}})^{-1},$$

where $H_{\alpha_1,\ldots,\alpha_{n-3}}$ is a generalised hexagon given by

$$H_{\alpha_1,\ldots,\alpha_{n-3}} = \left\{ \boldsymbol{x} \in \mathbb{R}^{n-1} : \|\boldsymbol{x}\|_\infty \leq 1, \left| \sum_{i=1}^{n-3} \alpha_i x_i + x_{n-2} + x_{n-1} \right| \leq 1 \right\}$$

and the supremum is taken over all rational numbers $\alpha_1, \ldots, \alpha_{n-3}$ in the interval $(0, 1]$.

Based on the values of $c(n)$ for $n \leq 4$, the following conjecture was proposed in [2].

Conjecture 14. *The equality*

$$c(n) = \Delta(H_{1,\ldots,1})^{-1}$$

holds. Here $H_{1,\ldots,1}$ is a generalised hexagon in $\mathbb{R}^{n-1}$.

The bound in Theorem (11) immediately implies

$$c(n) \leq \sqrt{n}\,. \tag{3.7}$$

In [2], the constant $c(n)$ was estimated as

$$c(n) \leq \sigma_n^{-1}\,, \tag{3.8}$$

where σ_n is the sinc integral

$$\sigma_n = \frac{2}{\pi}\int_0^\infty \left(\frac{\sin t}{t}\right)^n dt\,.$$

The bound (3.8) asymptotically improves on (3.7) with factor $\sqrt{\pi/6}$. The numbers σ_n are rational, the sequences of numerators and denominators of $\sigma_n/2$ can be found in [48] (sequences A049330 and A049331).

Chapter 4

Unique recovery of finite-valued integer signals

This chapter presents the main results of the thesis, published in [1].

4.1 Unique recovery of sparse bounded integer signals

In this thesis, we will obtain general estimates for the minimum in (2.6). Using condition (2.4), to get an upper bound for (2.6), it is sufficient to find an $1 \times n$ measurement matrix H such that its kernel space does not share any nonzero integer points with the convex hull of $D(S_l^n(r))$. This straightforward approach, however, results in the estimate

$$\|H\|_\infty = O(r^{n-1}), \tag{4.1}$$

where the implicit constant depends on l and n.

The first result of this thesis shows that the exponent $n-1$ in (4.1) can be replaced with $2l-1$. Let

$$p_{m,n}(r) = (m\Delta(m,n)r+1)^{m-1} + \Delta(m,n)\sum_{i=0}^{m-2}(m\Delta(m,n)r+1)^i,$$

where $\Delta(m,n) = \min(n-1, (2n)^{(m-1)/m})$.

Theorem 15. *For any $l, n \in \mathbb{Z}$ with $1 \le l < n/2$ and $r \in \mathbb{Z}_{>0}$ there exists an $1 \times n$ integer matrix H such that $H \in \mathscr{R}(Q)$ with $Q = D(S_l^n(r))$ and*

$$\|H\|_\infty < p_{2l,n}(2r). \tag{4.2}$$

The proof of Theorem 15 is constructive. To obtain the bound (4.2) we combine known results on unique recovery over $\mathbb{Z}_l^n$, outlined in Section 2.4, with aggregation techniques, outlined in Section 3.1.

The second result gives a lower bound for the minimum in (2.6). Notably, it shows that the polynomial $p_{2l,n}(2r)$ in (4.2) cannot be replaced by a polynomial in r with degree smaller than $2l-1$.

Theorem 16. *For any $l, n \in \mathbb{Z}$ with $1 \le l < n/2$, $r \in \mathbb{Z}_{>0}$ and $1 \times n$ integer matrix $H \in \mathscr{R}(Q)$ with $Q = D(S_l^n(r))$ the bound*

$$\|H\|_\infty > \frac{r^{2l-1}}{\sqrt{2l}} \tag{4.3}$$

holds.

Based on Theorems 15 and 16 we pose the following question. Let us fix the sparsity level l and dimension n. In this setting, it would be interesting to find optimal upper bounds for minimal $\|H\|_\infty / r^{2l-1}$ when r tends to infinity. Specifically, given $l, n \in \mathbb{Z}_{>0}$ with $1 \le l < n/2$, to estimate

$$c_1(l,n) = \limsup \inf \frac{\|H\|_\infty}{r^{2l-1}}, \tag{4.4}$$

where the supremum limit is taken over all positive integers r and the infimum is taken over all $1 \times n$ integer matrices $H \in \mathscr{R}(Q)$ with $Q = D(S_l^n(r))$. Theorems 15 and 16 give a large interval for values of this quantity

$$\frac{1}{\sqrt{2l}} \leq c_1(l,n) \leq (4l\Delta(2l,n))^{2l-1}.$$

Although for finite signal spaces a single measurement is sufficient for unique recovery, one can ask whether allowing extra measurements would result in reducing measurements' entries. In this vein, we obtain the following general result. Let $Q \subset \mathbb{Z}^n$ be an arbitrary set. Suppose that we have an $1 \times n$ matrix $H \in \mathscr{R}(Q)$. We show that, for any integer m with $1 < m < n$, there exists an $m \times n$ matrix $A = (a_{ij})$ such that $A \in \mathscr{R}(Q)$ and the maximum absolute entry $\|A\|_\infty = \max_{i,j} |a_{ij}|$ is sub-linear in $\|H\|_\infty$.

Recall that $\gamma_{r,s}$ denotes the generalised Hermite constant, introduced in Section 1.8.

Theorem 17. *Let $Q \subset \mathbb{Z}^n$ and let H be an $1 \times n$ matrix such that $H \in \mathscr{R}(Q)$. For any integer m with $1 < m < n$, there exists an $m \times n$ matrix A such that $A \in \mathscr{R}(Q)$ and*

$$\|A\|_\infty \leq c_2(m,n)\|H\|_\infty^{\frac{n-m}{n-1}}, \tag{4.5}$$

where $c_2(m,n) = \gamma_{n-1,n-m}^{1/2} n^{(n-m)/(2(n-1))}$.

The proof of Theorem 17 makes use of results on rational subspaces obtained in [5]. Note that (4.5) improves the immediate bound $\|A\|_\infty \leq \|H\|_\infty$ when $\|H\|_\infty > c_2(m,n)^{(n-1)/(m-1)}$.

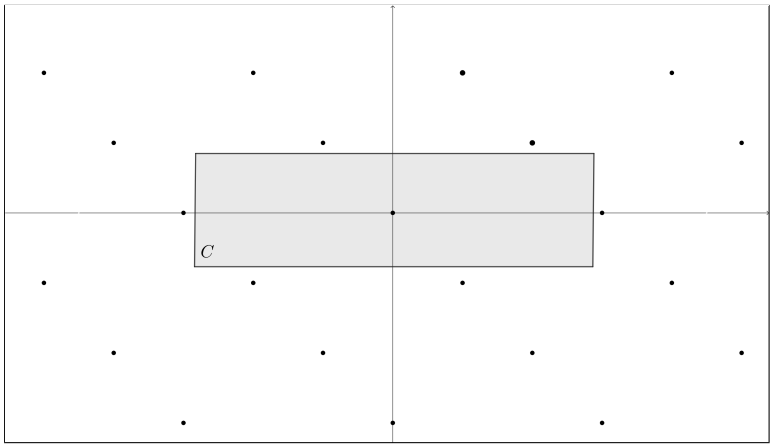


Figure 4.1: The lattice Λ does not intersect with the $\mathbf{0}$-symmetric convex body C in any non-zero points. This means that the lattice Λ is admissible for C.

4.2 Admissible lattices of m-sparse n-cubes

By a *rational subspace* of $\mathbb{R}^n$ we understand a subspace generated by integer vectors. A rational hyperplane can be written as $P = \{\boldsymbol{x} \in \mathbb{R}^n : H\boldsymbol{x} = 0\}$, where $H = (H_{11}, \ldots, H_{1n})$ is an $1 \times n$ integer matrix with $\gcd(H) := \gcd(H_{11}, \ldots, H_{1n}) = 1$. We say that P has *height* $h(P) = \|H\|_\infty$.

A lattice $\Lambda \subset \mathbb{R}^d$ is *(strictly) admissible* for a set $X \subset \mathbb{R}^d$ if $\Lambda \cap X = \{\mathbf{0}\}$. See, for example, Figure 4.1. For a comprehensive introduction to the theory of lattices we refer the reader to [13, 29].

Let r be a positive integer and m be a positive integer with $1 < m < n$. We will consider an m-sparse n-dimensional cube

$$C_m^n(r) = \{\boldsymbol{x} \in C^n(r) : \|\boldsymbol{x}\|_0 \leq m\}.$$

An example of this m-sparse n-dimensional cube can be seen in Figure 4.2.

Constructing single measurements for unique recovery of sparse integer signals is closely linked to constructing admissible $(n-1)$-dimensional lattices for $C_m^n(r)$. From the unique recovery perspective, it is desirable to find a

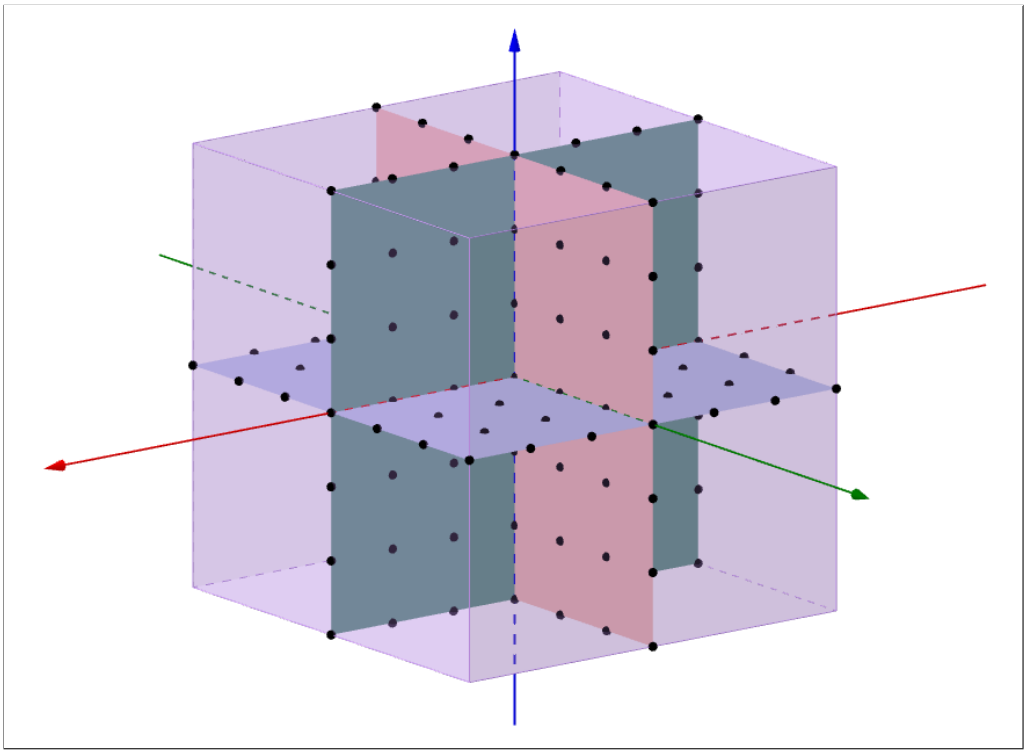


Figure 4.2: The set of all 2-sparse signal S_2^3 inside a three dimensional cube $C^3(3) = \{\boldsymbol{x} \in \mathbb{R}^3 : |x_i| \leq 3 \text{ where } 1 \leq i \leq 3\}$.

rational hyperplane P of smallest possible height such that the lattice $P \cap \mathbb{Z}^n$ is admissible for $C_m^n(r)$. Similarly to (2.6), we consider the following optimisation problem. Given $m, n \in \mathbb{Z}$ with $1 < m < n$ and $r \in \mathbb{Z}_{>0}$, find

$$\min\{h(P) : P \text{ is a rational hyperplane in } \mathbb{R}^n \text{ and the lattice } P \cap \mathbb{Z}^n \text{ is admissible for } C_m^n(r))\}. \tag{4.6}$$

The proofs of Theorems 15 and 16 will be based on the following estimates for the minimum in (4.6) that are of independent interest.

Theorem 18. *For any $m, n \in \mathbb{Z}$ with $1 < m < n$ and $r \in \mathbb{Z}_{>0}$ there exists a rational hyperplane P in $\mathbb{R}^n$ such that the lattice $P \cap \mathbb{Z}^n$ is admissible for $C_m^n(r)$ and*

$$h(P) < p_{m,n}(r). \tag{4.7}$$

To prove Theorem 18 we combine constructions from the proof of Theorem 6 with aggregation techniques outlined in Section 3.1. The next result shows that the polynomial $p_{m,n}(r)$ in (4.7) cannot be replaced by a polynomial in r of degree smaller than $m-1$.

Theorem 19. *For any $m, n \in \mathbb{Z}$ with $1 < m < n$, any $r \in \mathbb{Z}_{>0}$ and any rational hyperplane P in $\mathbb{R}^n$ such that the lattice $P \cap \mathbb{Z}^n$ is admissible for $C_m^n(r)$ we have*

$$h(P) > \frac{r^{m-1}}{\sqrt{m}} \tag{4.8}$$

holds.

Similarly to (4.4), for $m, n \in \mathbb{Z}$ with $1 < m < n$, it would be interesting to estimate

$$c_3(m,n) = \limsup \inf \frac{h(P)}{r^{m-1}}, \tag{4.9}$$

where the supremum limit is taken over all positive integers r and the infimum is taken over rational hyperplanes P in $\mathbb{R}^n$ such that $P \cap \mathbb{Z}^n$ is admissible for $C_m^n(r)$. Theorems 18 and 19 imply the bounds

$$\frac{1}{\sqrt{m}} \le c_3(m,n) \le (m\Delta(m,n))^{m-1}.$$

4.3 Proofs of Theorem 18 and Theorem 15

We will begin with proving Theorem 18. The proof of Theorem 6 (Konyagin and Sudakov [33, Theorem 1.3]) gives two explicit constructions that can be used to obtain matrices $A \in \mathscr{R}(\mathbb{Z}_m^n)$ that satisfy conditions of Corollary 7. For completeness, we will outline these constructions here.

Proof of Theorem 18

Observe first that $A \in \mathscr{R}(\mathbb{Z}_m^n)$ if and only if all $m \times m$ subdeterminants of A are nonzero. Therefore, if for some d satisfying $m < n < d$ there exists an $m \times d$ matrix $A \in \mathscr{R}(\mathbb{Z}_m^d)$, then an $m \times n$ matrix in $\mathscr{R}(\mathbb{Z}_m^n)$ can be obtained by removing any $d-n$ columns from A. Set first $k = n-1$. The first construction gives $A = (a_{ij}) \in \mathscr{R}(\mathbb{Z}_m^d)$ with $d \geq k+1$. The dimension d is chosen as an odd prime number satisfying $k+1 \leq d \leq 2k+1$. Subsequently, the entries of the matrix A are defined as $a_{ij} \equiv j^{i-1} (\mathrm{mod}\ d)$ with $|a_{ij}| \leq (d-1)/2 \leq k$. In particular, for all j we have $a_{1j} = 1$. Next, set $k = (2n)^{(m-1)/m}$. The second construction gives $A = (a_{ij}) \in \mathscr{R}(\mathbb{Z}_m^d)$ with $d \geq k^{m/(m-1)}/2$. One can assume that $k^{m/(m-1)}/2 > k+1$ and, in particular, $k \geq 3$. The dimension d is now chosen as a prime number with $k^{m/(m-1)}/2 \leq d \leq k^{m/(m-1)}$. The entries of the matrix A satisfy $a_{ij} \equiv l_{ij} j^{i-1} (\mathrm{\ mod\ } d)$, where l_{ij} are certain integers not divisible by d chosen in a such way that $|a_{ij}| \leq k$. In particular, for all j one can take $l_{1j} = 1$, so that $a_{1j} = 1$.

In both constructions above, renumbering the rows of A, we may assume that $a_{mj} = 1$ for all j. Set $k = \Delta(m,n)$ and for $s = m\,k\,r + 1$ take

$$B = (1, s, \ldots, s^{m-1})$$

and

$$H = BA.$$

We will show that the hyperplane $P = \ker(H)$ satisfies the conditions of Theorem 18.

Let $F(\boldsymbol{x}) = A\boldsymbol{x}$ and let $F_i(\boldsymbol{x})$ denote the ith entry of $F(\boldsymbol{x})$, that is

$$\begin{aligned} F_1(\boldsymbol{x}) &= a_{11}x_1 + \cdots + a_{1n}x_n\,, \\ &\vdots \\ F_m(\boldsymbol{x}) &= a_{m1}x_1 + \cdots + a_{mn}x_n\,. \end{aligned}$$

For any $\boldsymbol{x} \in C_m^n(r)$ and any $i \in \{1,\ldots,m\}$, we have

$$F_i(\boldsymbol{x}) \le \|\boldsymbol{x}\|_0 \|A\|_\infty r \le m\,k\,r < s\,.$$

Lemma 9, applied with $D = C_m^n(r) \cap \mathbb{Z}^n$ and $q_i = s$ for $i = 1,\ldots,m-1$, implies that

$$\{\boldsymbol{x} \in C_m^n(r) \cap \mathbb{Z}^n : H\boldsymbol{x} = \boldsymbol{0}\} = \{\boldsymbol{x} \in C_m^n(r) \cap \mathbb{Z}^n : A\boldsymbol{x} = \boldsymbol{0}\}\,. \tag{4.10}$$

Since $A \in \mathscr{R}(\mathbb{Z}_m^n)$ we have

$$\{\boldsymbol{x} \in C_m^n(r) \cap \mathbb{Z}^n : A\boldsymbol{x} = \boldsymbol{0}\} = \{\boldsymbol{0}\}\,. \tag{4.11}$$

Consequently, combining (4.10) and (4.11), the lattice $P \cap \mathbb{Z}^n$ is admissible for $C_m^n(r)$.

Finally, we obtain the bound

$$h(P) \le \|H\|_\infty \le s^{m-1} + k\sum_{i=0}^{m-2} s^i$$

that implies (4.7).

Remark 1: For given sparsity level m, dimension n and cube size r the set $\{F(\boldsymbol{x}) : \boldsymbol{x} \in D\}$ constructed in the proof will likely allow a more accurate choice of parameters q_i in Lemma 9, resulting in an improvement on the bound (4.7). Further, aggregation techniques can be also applied to the matrices in $\mathscr{R}(\mathbb{Z}_m^n)$ obtained using a probabilistic approach from the proof of Theorem 5 (Konyagin [32, Theorem 3]).

Proof of Theorem 15

Let $m = 2l$ and let P be a rational hyperplane in $\mathbb{R}^n$ such that the lattice $P \cap \mathbb{Z}^n$ is admissible for $C_m^n(2r) \cap \mathbb{Z}^n$. We can write $P = \ker(H)$ for an $1 \times n$ integer matrix H with $h(P) = \|H\|_\infty$.

The inclusion

$$D(S_l^n(r)) \subset S_m^n(2r) = C_m^n(2r) \cap \mathbb{Z}^n$$

implies the condition (2.4) with $Q = D(S_l^n(r))$. Hence $H \in \mathscr{R}(Q)$. Finally, the bound (4.2) immediately follows from (4.7).

4.4 Examples of measurement matrices

In this section, we compute examples of $m \times n$ integer matrix A using the method outlined in the proof of Theorem 15. Specifically, we set the maximum absolute entry of A to $k = n-1$ and $k = \lceil (2n)^{(m-1)/m} \rceil$. Subsequently, we verify that all $m \times m$ square submatrices of A were nonsingular. Next, we fix a positive integer r and set $s = m\ k\ r + 1$. Then we construct a one-row matrix B which has powers of s as its entries, and multiply it by A to generate the measurement matrix H. Afterwards, we used a Python program to recover the signal $\boldsymbol{x}$ by solving the equation $H\boldsymbol{x} = \boldsymbol{b}$, where $\boldsymbol{b}$ is a measurement vector.

We tested two measurement matrices under different scenarios by modifying the sparsity level and the bound on entries of the signal $\boldsymbol{x}$. In Examples 3 and 4, the Python program successfully recovered a unique signal $\boldsymbol{x}$ that satisfied Theorem 1.

Example 3. *Let $n = 10$ and $m = 4$. Using the method in the proof of Theorem 18, we construct a matrix A as follows:*

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & -1 \\ 1 & 4 & 9 & 5 & 3 & 3 & 5 & 9 & 4 & 1 \\ 1 & 8 & 5 & 9 & 4 & 7 & 2 & 6 & 3 & -1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

The maximum absolute value is $k = 9$. Every $m \times m$ submatrix of A is non-singular.

Next, we set $r = 2$, $s = mkr + 1 =$ and compute 1×4 matrix B as :

$$B = \begin{pmatrix} 1 & s & s^2 & s^3 \end{pmatrix} = \begin{pmatrix} 1 & 73 & 5329 & 389017 \end{pmatrix}.$$

We now create a sensing matrix H by multiplying A by B, which gives us:

$$H = \begin{pmatrix} 394420 & 431943 & 416322 & 437347 & 410557 & 426545 & 400047 \\ 421656 & 405305 & 383760 \end{pmatrix}.$$

Note that H satisfied (4.2).

Finally, we use the sensing matrix H to recover a signal

$$\boldsymbol{x}_0 = (-1, 0, 1, 0, 0, 0, 0, 0, 0, 0)^\top.$$

by solving the system $H\boldsymbol{x} = \boldsymbol{b}$, where $\boldsymbol{b} = H\boldsymbol{x}_0 = 21902$. Notice that $\|\boldsymbol{x}_0\|_0 = 2$ and the absolute values of its entries are bounded by one. Using a Python program we checked that $\boldsymbol{x}_0$ is the unique solution over the signal space set $S_2^{10}(2)$. Thus, we have successfully recovered the sparse signal $\boldsymbol{x}$ using the measurement matrix H and the set of linear equations $H\boldsymbol{x} = \boldsymbol{b}$.

Interestingly, only replacing $S_2^{10}(2)$ *with a substantially larger set* $S_4^{10}(3)$ *we obtain one extra solution to* $H\boldsymbol{x} = 21902$*:*

$$\boldsymbol{x}_1 = (0,0,0,3,-2,-3,0,0,2,0)^\top.$$

In this situation $H \notin \mathscr{R}(D(S_4^{10}(3)))$.

Example 4. *Next we construct an integer* $m \times n$ *matrix* A *with* $m = 4$ *and* $n = 12$*, with maximum absolute value* $k = \lceil (2n)^{(m-1)/m} \rceil = 11$*, such that all* $m \times m$ *submatrix are non-singular:*

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & -1 \\ 1 & 4 & 9 & 3 & -1 & 10 & 10 & -1 & 3 & 9 & 4 & 1 \\ 1 & 8 & 1 & -1 & 8 & 8 & 5 & 5 & 1 & -1 & 5 & -1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

We set $r = 2$*,* $s = mkr+1 =$ *and compute a* 1×4 *matrix* $B = \begin{pmatrix} 1 & s & s^2 & s^3 \end{pmatrix}$*, where* $s = 89$*. We then obtain the sensing matrix* H *by multiplying* A *by* B*:*

$$H = \begin{pmatrix} 712980 & 768695 & 713694 & 697319 & 768253 & 769233 & 745471 \\ 744493 & 713166 & 697859 & 744941 & 697136 \end{pmatrix}.$$

One can verify that (4.2) *is satisfied. We take*

$$\boldsymbol{x}_0 = (0,0,0,-1,0,1,0,0,0,0,0,0)^\top.$$

and solve the system $H\boldsymbol{x} = \boldsymbol{b}$*, where* $\boldsymbol{b} = H\boldsymbol{x}_0 = 71914$*, to recover the sparse signal* $\boldsymbol{x}$*. A Python program was used to verify the uniqueness of the solution over* $S_2^{12}(2)$*.*

Interestingly, replacing $S_2^{12}(2)$ *by* $S_4^{12}(4)$ *gives extra solutions to* $H\boldsymbol{x} = 71914$*:*

$$\boldsymbol{x}_1 = (0,3,0,-2,-4,0,0,3,0,0,0,0)^\top,$$

and

$$\boldsymbol{x}_2 = (0,-3,0,0,4,2,0,-3,0,0,0,0)^\top .$$

Clearly, by changing the signal space the unique recovery is no longer guaranteed. In this situation $H \notin \mathscr{R}(D(S_4^{12}(4)))$.

4.5 Proofs of Theorem 19 and Theorem 16

We will first prove Theorem 19.

Proof of Theorem 19

Let $A \in \mathbb{Z}^{m\times n}$, $m < n$, and let $\tau = \{i_1,\dots,i_k\} \subseteq \{1,\dots,n\}$ with $i_1 < i_2 < \cdots < i_k$. Recall that we denote by A_τ the $m \times k$ submatrix of A with columns indexed by τ. In the same manner, given $\boldsymbol{x} \in \mathbb{R}^n$, we denote by $\boldsymbol{x}_\tau$ the vector $(x_{i_1},\dots,x_{i_k})^\top$. The complement of τ in $\{1,\dots,n\}$ is denoted as $\bar{\tau}$. For matrices A of rank m, the notation $\gcd(A)$ will be used for the greatest common divisor of all $m \times m$ subdeterminants of A.

The proof makes use of Theorem 11, which is a version of Siegel's Lemma obtained by Bombieri and Vaaler [9, Theorem 2].

Suppose, to derive a contradiction, that Theorem 19 does not hold. Then for some $m,n \in \mathbb{Z}_{>0}$ with $1 < m < n$, and $r \in \mathbb{Z}_{>0}$ there exists a rational hyperplane P in $\mathbb{R}^n$ such that $P \cap \mathbb{Z}^n$ is admissible for $C_m^n(r)$ and

$$h(P) \le \frac{r^{m-1}}{\sqrt{m}}. \tag{4.12}$$

There exists an $1\times n$ integer matrix H such that $P = \ker(H)$ and $h(P) = \|H\|_\infty$. Take $\tau = \{1,\dots,m\}$. Observe that H cannot have zero entries, as otherwise

its kernel P would contain the corresponding standard basis vectors. Hence, $H_\tau \neq \mathbf{0}$. By Theorem 11, applied with $M = H_\tau$, there exists an integer vector $\boldsymbol{x}_\tau \in \ker(H_\tau)$ such that

$$0 < \|\boldsymbol{x}_\tau\|_\infty^{m-1} \leq \frac{\|H_\tau\|_2}{\gcd(H_\tau)} \leq \sqrt{m}\|H_\tau\|_\infty \leq \sqrt{m}\, h(P)\,. \tag{4.13}$$

By the upper bound (4.12) we have

$$\|\boldsymbol{x}_\tau\|_\infty \leq r\,.$$

Consequently, the lifted vector

$$\begin{pmatrix} \boldsymbol{x}_\tau \\ \mathbf{0}_{\bar{\tau}} \end{pmatrix} \in C_m^n(r) \cap P \cap \mathbb{Z}^n,$$

contradicting the assumption that $P \cap \mathbb{Z}^n$ is admissible for $C_m^n(r)$. The obtained contradiction completes the proof of Theorem 19.

Remark 2: A minor improvement of (4.13) can be obtained using a refinement of Siegel's lemma proved in [3]. The latter refinement is also discussed for completeness in Section of this thesis; see the bound (3.8). Further, the last inequality in (4.13) can be slightly strengthened using the following observation. Since $P \cap \mathbb{Z}^n$ is admissible for $C_m^n(1)$ and $m \geq 2$, we may assume that $H_{11} < H_{12} < \cdots < H_{1n}$. This allows choosing H_τ with $\|H_\tau\| \leq \|H\|_\infty - n + m$.

Proof of Theorem 16

Take any $l, n \in \mathbb{Z}_{>0}$ with $1 \leq l < n/2$, $r \in \mathbb{Z}_{>0}$ and any $1 \times n$ integer matrix $H \in \mathscr{R}(Q)$ with $Q = D(S_l^n(r))$. Consider the hyperplane $P = \ker(H)$. Set $m = 2l$ and observe that

$$C_m^n(r) \cap \mathbb{Z}^n \subset Q\,.$$

Therefore, the lattice $P \cap \mathbb{Z}^n$ is admissible for $C_m^n(r)$ and (4.8) implies (4.3).

4.6 Proof of Theorem 17

The proof of Theorem 17 is based on the following result, which is a special case of Proposition 1 (ii) in [5].

Theorem 20. *Let S be an one-dimensional rational subspace of $\mathbb{R}^n$. When $1 < m < n$, there is a rational subspace $T \supset S$ of dimension m in $\mathbb{R}^n$ with*

$$\det(T \cap \mathbb{Z}^n) \leq \gamma_{n-1,n-m}^{1/2} \det(S \cap \mathbb{Z}^n)^{(n-m)/(n-1)}. \tag{4.14}$$

The constant $\gamma_{n-1,n-m}^{1/2}$ here is best possible.

Take any $Q \subset \mathbb{Z}^n$ and suppose that we are given an integer $1 \times n$ matrix $H \in \mathscr{R}(Q)$. Let m be an integer with $1 < m < n$ and let T be the subspace from Theorem 20, applied to the rational subspace S of $\mathbb{R}^n$ spanned by the row vector H.

By Theorem 11, applied with any $(n-m) \times n$ integer matrix M with $T = \ker(M)$, there exist m linearly independent integer vectors $\boldsymbol{g}_1, \ldots, \boldsymbol{g}_m \in T$ such that

$$\|\boldsymbol{g}_1\|_\infty \cdots \|\boldsymbol{g}_m\|_\infty \leq \frac{\sqrt{\det(MM^T)}}{\gcd(M)} = \det(T \cap \mathbb{Z}^n). \tag{4.15}$$

For a proof of the last equality in (4.15) we refer the reader to [45, Corollaries 5I-J]. Now we can form a matrix A with rows $\boldsymbol{g}_1^\top, \ldots, \boldsymbol{g}_m^\top$, so that $S \subset \operatorname{span}_{\mathbb{R}}(A^\top)$. Observe that $\ker(A) \subset \ker(H)$ and hence, $A \in \mathscr{R}(E)$.

Finally, combining (4.15), (4.14) and the bound $\det(S \cap \mathbb{Z}^n) \leq \sqrt{n}\|H\|_\infty$, we get the estimate (4.5):

$$\|A\|_\infty \leq \gamma_{n-1,n-m}^{1/2} n^{(n-m)/(2(n-1))} \|H\|_\infty^{(n-m)/(n-1)}.$$

Chapter 5

Probability of uniqueness of sparse solutions with integer bounded entries

In this chapter, we consider the uniqueness of sparse integer solutions of underdetermined linear systems from a probabilistic point of view. In the case of unbounded solutions, Konyagin [32] proved the following two theorems.

Theorem 21 (Konyagin [32])**.** *Consider an $m \times m$ random matrix M with independent elements, each of which takes any integer value from $-k$ to k with probability $1/(2k+1)$. Then the probability of the determinant of M being zero is at most $C^{m^2} k^{-m} (\log k + 1)^{m-1}$, where $C > 0$ is an absolute constant.*

This result is linked to sparse solutions of a system $A\boldsymbol{x} = \boldsymbol{b}$ with $A \in \mathbb{Z}^{m \times n}$, $m < n$, since any l-sparse solution with $l \leq m$ of the latter system corresponds to a singular $m \times m$ submatrix M of A. Theorem 21 was subsequently used to prove Theorem 5, which we recall here for convenience of the reader.

Theorem 5 [Konyagin [32]]

For integers $k, m \geq 2$, and integer n with

$$m < n \leq \frac{c^{-m} k^{m/(m-1)}}{\log(k)}$$

there exists an integer $m \times n$ matrix $A \in \mathscr{R}(\mathbb{Z}_m^n)$ such that $\|A\|_\infty = k$, where c is an absolute constant.

The assertions of Theorem 21 and 5 are nontrivial if k is sufficiently large and $m \leq c \log k$, $c > 0$.

Our goal is to obtain a result similar to Theorem 21 which utilises the boundedness of the integer signals and apply it to estimate the probability of uniqueness of bounded integer sparse signals (see Theorem 25). A future direction of work is to use Theorem 25 to obtain an analog of Theorem 5 in the bounded setting.

The proofs of Theorems 24 and 25 below are based on the proof of Theorem 21. We will start with developing auxiliary tools required for dealing with bounded integer signals. Given $A \in \mathbb{Z}^{m \times n}$ and $\boldsymbol{b} \in \mathbb{Z}^m$, we will denote by $\Gamma(A, \boldsymbol{b})$ the set of integer points in the affine subspace

$$H(A, \boldsymbol{b}) = \{\boldsymbol{x} \in \mathbb{R}^n : A\boldsymbol{x} = \boldsymbol{b}\},$$

that is

$$\Gamma(A, \boldsymbol{b}) = H(A, \boldsymbol{b}) \cap \mathbb{Z}^n.$$

The set $\Gamma(A, \boldsymbol{b})$ is either empty or an affine lattice of the form $\Gamma(A, \boldsymbol{b}) = \boldsymbol{r} + \Gamma(A)$, where $\boldsymbol{r}$ is any integer vector with $A\boldsymbol{r} = \boldsymbol{b}$ and $\Gamma(A) = \Gamma(A, \boldsymbol{0})$ is the lattice formed by all integer points in the kernel $\ker(A) = \{\boldsymbol{x} \in \mathbb{R}^n : A\boldsymbol{x} = \boldsymbol{0}\}$ of the matrix A.

Lemma 22. *Let $n > m \geq 2l$, and $A \in \mathbb{Z}^{m\times n}$. If for any $m \times 2l$ submatrix M of A*

$$\Gamma(M) \cap D(S_l^n(r)) = \{\mathbf{0}\} \tag{5.1}$$

then any $\boldsymbol{x}_0 \in S_l^n(r)$ is the unique solution to the system $A\boldsymbol{x} = A\boldsymbol{x}_0$ over $S_l^n(r)$.

Proof. Take any $\boldsymbol{x}_0 \in S_l^n(r)$. Suppose, to derive a contradiction, that there exists a vector $\boldsymbol{x}_1 \in S_l^n(r)$ such that $\boldsymbol{x}_0 \neq \boldsymbol{x}_1$ and $A\boldsymbol{x}_0 = A\boldsymbol{x}_1$. Set $\boldsymbol{y} = \boldsymbol{x}_0 - \boldsymbol{x}_1 \neq \mathbf{0}$ and $\tau = \operatorname{supp}(\boldsymbol{y})$. Take any set of indices $\sigma \subset [n]$ such that $|\sigma| = 2l$ and $\tau \subset \sigma$. Then

$$\boldsymbol{y}_\sigma \in \Gamma(A_\sigma) \cap D(S_l^n(r)),$$

contradicting (5.1).

□

In what follows, we will consider the case $m = 2l < n$. Given $U \in \mathbb{Z}^{m\times m}$ with rows $\boldsymbol{u}_1^T, \ldots, \boldsymbol{u}_m^T$ and rank $d \leq m-1$, we will denote by $\Sigma(U)$ the lattice formed by all integer points in the subspace $\operatorname{span}_{\mathbb{R}}(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_m)$ spanned by $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_m$. That is

$$\Sigma(U) = \operatorname{span}_{\mathbb{R}}(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_m) \cap \mathbb{Z}^m.$$

Let $\lambda_i(\Sigma(U)) = \lambda_i(C^m(1), \Sigma(U))$ be the ith successive minimum of the cube $C^m(1)$ with respect to $\Sigma(U)$. Note that $1 \leq \lambda_1(\Sigma(U)) \leq \cdots \leq \lambda_d(\Sigma(U))$.

Lemma 23. *Suppose that* $\operatorname{rank}(U) = m-1$ *and*

$$\lambda_1(\Sigma(U)) > R = (2r\sqrt{m})^{1/(m-1)}.$$

Then for $K = S_m^n(r)$ we have

$$\Gamma(U) \cap D(K) = \{\mathbf{0}\}.$$

Proof. Since $\lambda_1(\Sigma(U)) > R$, the lattice $\Sigma(U)$ is admissible for the cube section $S = C^m(R) \cap \text{span}_{\mathbb{R}}(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_m)$. Therefore,

$$\det(\Sigma(U)) > \Delta(S), \tag{5.2}$$

where $\Delta(S)$ is the critical determinant of the set S. Further, by Theorem 5 in Section 17.3 of [29],

$$\Delta(S) \geq \frac{\text{vol}(S)}{2^{m-1}}. \tag{5.3}$$

The cube-slicing inequality of Vaaler [51] implies that $\text{vol}(S) \geq (2R)^{m-1}$. Therefore, by (5.2) and (5.3),

$$\det(\Sigma(U)) > R^{m-1}. \tag{5.4}$$

Note that $\Sigma(U) = \Gamma(U)^{\perp} := \{\boldsymbol{x} \in \mathbb{Z}^m : \boldsymbol{x}^{\top}\boldsymbol{y} = 0 \text{ for all } \boldsymbol{y} \in \Gamma(U)\}$. Hence, by [34], $\det(\Sigma(U)) = \det(\Gamma(U))$ and, using (5.4), we have

$$\det(\Gamma(U)) > R^{m-1}. \tag{5.5}$$

Therefore, the one-dimensional lattice $\Gamma(U)$ is generated by a basis vector $\boldsymbol{v}$ with $\|\boldsymbol{v}\|_2 > R^{m-1} = 2r\sqrt{m}$. Since $D(K) \subset C^m(2r)$, we have $\Gamma(U) \cap D(K) = \{\boldsymbol{0}\}$.

□

Theorem 24. *Fix $R \in \mathbb{R}_{>1}$, $k \in \mathbb{Z}_{>0}$ and consider a random matrix $M = (a_{ij}) \in \mathbb{Z}^{m\times m}$ with independent entries that take integer values from $-k$ to k with probability $(2k+1)^{-1}$. Then the probability that M is a singular matrix with $\lambda_1(\Sigma(M)) \leq R$ is at most*

$$\frac{15^{m^2-m} R(\log(k)+1)^{m-2}}{k^m}. \tag{5.6}$$

Proof. Consider the set

$$\mathscr{M} = \{M \in \mathbb{Z}^{m\times m} : \operatorname{rank}(M) \le m-1, \|M\|_\infty \le k, \lambda_1(\Sigma(M)) \le R\}.$$

We will obtain an upper bound for $|\mathscr{M}|$ using the following strategy. Let $\mathscr{P}$ be the set of primitive $m-1$ dimensional lattices $\Omega \subset \mathbb{Z}^m$ with $\lambda_1(C^m(1),\Omega) \le R$ and $\lambda_{m-1}(C^m(1),\Omega) \le k$. First, we will construct a function $\phi : \mathscr{M} \to \mathscr{P}$. Second, we split $\mathscr{P}$ into subsets of lattices $\mathscr{P}_{\lambda_1,\dots,\lambda_{m-1}}$ that correspond to the fixed values of successive minima $\lambda_1,\dots,\lambda_{m-1}$ and write

$$\mathscr{P} = \bigcup_{\substack{1\le\lambda_1\le R\\ 1\le\lambda_2,\dots,\lambda_{m-1}\le k}} \mathscr{P}_{\lambda_1,\dots,\lambda_{m-1}}.$$

Then we use the estimate

$$|\mathscr{M}| \le \sum_{\substack{1\le\lambda_1\le R\\ 1\le\lambda_2,\dots,\lambda_{m-1}\le k}} |\mathscr{P}_{\lambda_1,\dots,\lambda_{m-1}}| \cdot L_{\lambda_1,\dots,\lambda_{m-1}}, \tag{5.7}$$

where $L_{\lambda_1,\dots,\lambda_{m-1}} = \max_{\Omega\in\mathscr{P}_{\lambda_1,\dots,\lambda_{m-1}}} |\phi^{-1}(\Omega)|$. The desired bound is then obtained by estimating $|\mathscr{P}_{\lambda_1,\dots,\lambda_{m-1}}|$ and $L_{\lambda_1,\dots,\lambda_{m-1}}$.

Given $M \in \mathscr{M}$, we construct the lattice $\phi(M)$ as follows. If $\operatorname{rank}(M) = m-1$, we set $\phi(M) = \Sigma(M)$. Suppose now that $\operatorname{rank}(M) < m-1$ and take any basis $\boldsymbol{b}_1,\dots,\boldsymbol{b}_l$ of the lattice $\Sigma(M)$. There exist the standard basis vectors $\boldsymbol{e}_{i_1},\dots,\boldsymbol{e}_{i_{m-1-l}}$ such that the linear subspace S spanned by $\boldsymbol{b}_1,\dots,\boldsymbol{b}_l,\boldsymbol{e}_{i_1},\dots,\boldsymbol{e}_{i_{m-1-l}}$ has dimension $m-1$. We set $\phi(M) = S \cap \mathbb{Z}^m$. Note that $\phi(M) \in \mathscr{P}$ as in this case $\lambda_1(C^m(1),\phi(M)) = 1$ and $\lambda_{m-1}(C^m(1),\phi(M)) \le k$.

Let us now fix the values $\lambda_1,\dots,\lambda_{m-1}$ and estimate the size of the set $\mathscr{P}_{\lambda_1,\dots,\lambda_{m-1}}$. Given a lattice $\Omega \in \mathscr{P}_{\lambda_1,\dots,\lambda_{m-1}}$, there exist linearly independent vec-

tors $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{m-1} \in \Omega$ such that

$$\|\boldsymbol{x}_i\|_\infty = \lambda_i(C^m(1), \Omega). \tag{5.8}$$

The lattice Ω is the intersection of the $m-1$ dimensional subspace S of $\mathbb{R}^m$ spanned by $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{m-1}$ and $\mathbb{Z}^m$. Consequently, Ω is uniquely determined by $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{m-1}$.

The number of vectors $\boldsymbol{x} \in \mathbb{Z}^m$ with $\|\boldsymbol{x}\|_\infty = \lambda$ is

$$(2\lambda+1)^m - (2\lambda-1)^m < 2m(2\lambda+1)^{m-1} < 3^m m\lambda^{m-1} < 5^m \lambda^{m-1}.$$

Therefore,

$$|\mathscr{P}_{\lambda_1,\ldots,\lambda_{m-1}}| \leq 5^{m^2-m} \prod_{i=1}^{m-1} \lambda_i^{m-1}.$$

Further,

$$\begin{aligned}
|\mathscr{P}| &\leq 5^{m^2-m} \sum_{\lambda_1=1}^{R} \sum_{\lambda_2=1}^{k} \cdots \sum_{\lambda_{m-1}=1}^{k} \prod_{i=1}^{m-1} \lambda_i^{m-1} \\
&\leq 5^{m^2-m} \sum_{\lambda_2=1}^{k} \cdots \sum_{\lambda_{m-1}=1}^{k} \left(\sum_{\lambda_1=1}^{R} \prod_{i=1}^{m-1} \lambda_i^{m-1} \right) \\
&\leq 5^{m^2-m} R^m \sum_{\lambda_2=1}^{k} \cdots \sum_{\lambda_{m-1}=1}^{k} \prod_{i=2}^{m-1} \lambda_i^{m-1}.
\end{aligned}$$

Next, for fixed values $\lambda_1, \ldots, \lambda_{m-1}$, we will estimate $L_{\lambda_1,\ldots,\lambda_{m-1}}$. For a lattice $\Omega \in \mathscr{P}_{\lambda_1,\ldots,\lambda_{m-1}}$ and, consequently, for vectors $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{m-1}$ satisfying (5.8), $|\phi^{-1}(\Omega)|$ is the number of matrices $M \in \mathscr{M}$ with $\Omega = \phi(M)$. Observe that the number of possible jth rows of such a matrix M is bounded from above by $|\Omega \cap C^m(k)|$.

Let $\mu_i = \lambda_i(C^m(k), \Omega)$, so that

$$\mu_i = \frac{\lambda_i}{k}.$$

By Theorem 4 ([31, Theorem 1.5]), we have

$$|\Omega \cap C^m(k)| \leq 2^{m-2} \prod_{i=1}^{m-1} \left(\frac{2}{\mu_i} + 1 \right).$$

Hence

$$|\Omega \cap C^m(k)| \leq 6^{m-1} \prod_{i=1}^{m-1} \frac{1}{\mu_i} = 6^{m-1} k^{m-1} \prod_{i=1}^{m-1} \lambda_i^{-1}.$$

Therefore, the number of matrices $M \in \mathscr{M}$ with $\Omega = \phi(M)$ is at most

$$|\Omega \cap C^m(k)|^m \leq 6^{m^2-m} k^{m^2-m} \prod_{i=1}^{m-1} \lambda_i^{-m}.$$

Using (5.7), we get the bound

$$\begin{aligned} |\mathscr{M}| &\leq 30^{m^2-m} k^{m^2-m} \sum_{\lambda_1=1}^{R} \sum_{\lambda_2=1}^{k} \cdots \sum_{\lambda_{m-1}=1}^{k} \prod_{i=1}^{m-1} \lambda_i^{-1} \\ &\leq 30^{m^2-m} k^{m^2-m} R \sum_{\lambda_2=1}^{k} \cdots \sum_{\lambda_{m-1}=1}^{k} \prod_{i=2}^{m-1} \lambda_i^{-1}. \end{aligned}$$

Next,

$$\sum_{\lambda_2=1}^{k} \cdots \sum_{\lambda_{m-1}=1}^{k} \prod_{i=2}^{m-1} \lambda_i^{-1} = \left(\sum_{\lambda=1}^{k} \lambda^{-1} \right)^{m-2} \leq (\log(k)+1)^{m-2}.$$

It is now sufficient to observe that the number of matrices $M \in \mathbb{Z}^{m \times m}$ with $|M| \leq k$ is $(2k+1)^{m^2}$. Therefore, the required probability is

$$\begin{aligned} &\leq 30^{m^2-m} k^{m^2-m} R (\log(k)+1)^{m-2} (2k+1)^{-m^2} \\ &\leq 15^{m^2-m} k^{-m} R (\log(k)+1)^{m-2}. \end{aligned}$$

□

The bound (5.6) is smaller than the bound for the unbounded case in Theorem 21 provided that $R < \log(k) + 1$.

Theorem 25. *Consider a random matrix $A = (a_{ij}) \in \mathbb{Z}^{m \times n}$, $m = 2s < n$ with independent entries that take integer values from $-k$ to k with probability* $(2k+$

$1)^{-1}$. *Then the probability that any* $\boldsymbol{x}_0 \in S_m^n(r)$ *is the unique solution to the system* $A\boldsymbol{x} = A\boldsymbol{x}_0$ *over* $S_m^n(r)$ *is at least*

$$1 - \frac{\binom{n}{m} \cdot 15^{m^2-m} R(\log(k)+1)^{m-2}}{k^m}, \tag{5.9}$$

where $R = (2r\sqrt{m})^{1/(m-1)}$.

Proof. By Theorem 24 and the union bound, the probability that there exists a singular submatrix M of A with $\lambda_1(\Omega(M)) \leq R = (2r\sqrt{m})^{1/(m-1)}$ is at most

$$\binom{n}{m} \cdot 15^{m^2-m} k^{-m} R(\log(k)+1)^{m-2},$$

Therefore, by Lemma 23, with probability at least (6.1) the matrix A satisfies condition (5.1). The result now follows by Lemma 22. □

Chapter 6

Conclusions

In this final chapter, we give a brief overview of the contributions obtained in this thesis and, additionally, outline possible directions for future research.

6.1 Conclusions

The main results of the thesis are included in Chapter 4. Firstly, for integer bounded l-sparse n-dimensional signals, we obtained general estimates for the minimum size of a measurement matrix that corresponds to the minimum in (2.6). A straightforward approach, based on constructing admissible lattices for convex hulls of the sparse sets, would only show existence of a measurement $1 \times n$ matrix H with

$$\|H\|_\infty = O(r^{n-1}),$$

where r is the entry size and the implicit constant depends on the sparsity level l and dimension n. Here $2l < n$. We showed that the exponent $n-1$ in (4.1) can be replaced with $2l-1$. Specifically, for a polynomial $p_{2l,n}(r)$ of

degree $2l-1$, Theorem 15 gives the bound

$$\|H\|_\infty < p_{2l,n}(2r)\,.$$

Secondly, we give a lower bound for the minimum in (2.6). Roughly speaking, for any measurement matrix H in our setting, Theorem 16 shows that

$$\|H\|_\infty > \frac{r^{2l-1}}{\sqrt{2l}}$$

This implies that the polynomial $p_{2l,n}(2r)$ above cannot be replaced by a polynomial in r with degree smaller than $2l-1$.

Although for finite signal spaces a single measurement is sufficient for unique recovery, it is interesting to know whether allowing extra measurements would result in reducing measurements' entries. We indeed confirmed that such a reduction possible.

Avoiding technical details, given any $1 \times n$ measurement matrix H, Theorem 17 states existence of $m \times n$ measurement matrices A with entries sublinear in $\|H\|_\infty$:

$$\|A\|_\infty \leq c_2(m,n)\|H\|_\infty^{\frac{n-m}{n-1}},$$

where $c_2(m,n)$ is a constant.

Another group of our results considers admissible lattices of m-sparse n-cubes $C_m^n(r)$. In fact, constructing single measurements for unique recovery of sparse integer signals is directly linked to constructing admissible $(n-1)$-dimensional lattices for $C_m^n(r)$. Such lattices can be described in terms of rational hyperplanes. Then the height of a hyperplane P, denoted in the thesis by $h(P)$ corresponds to the maximum absolute entry of a measurement matrix associated with P.

Theorem 18 shows existence of an admissible lattice determined by a rational subspace P of a relatively small height. Specifically,

$$h(P) < p_{m,n}(r)\,.$$

As its counterpart, Theorem 19 shows that the polynomial $p_{m,n}(r)$ in the latter bound cannot be replaced by a polynomial in r of degree smaller than $m-1$:

$$h(P) > \frac{r^{m-1}}{\sqrt{m}}$$

holds.

Additionally, in Chapter 5, we consider the uniqueness of sparse integer solutions of underdetermined linear systems from a probabilistic perspective. Our main contribution here gives a result, similar to Theorem 21, which utilises the boundedness of the integer signals. Avoiding technical details, Theorem 25 gives a lower bound for the probability of obtaining a measurement matrix for integer signals from m-sparse hypercubes. This probability is at least

$$1 - \frac{\binom{m}{n} \cdot 15^{m^2-m} R(\log(k)+1)^{m-2}}{k^m}\,,$$

where r is the cube size, k bounds measurement matrix absolute entries and $R = (2r\sqrt{m})^{1/(m-1)}$. Hence, as k grows, the probability of unique recovery rapidly tends to one.

Bibliography

[1] A. Alasmari and I. Aliev. On unique recovery of finite-valued integer signals and admissible lattices of sparse hypercubes. *Optim. Lett.*, 17(3):739–751, 2023.

[2] I. Aliev. *On decomposition of integer vectors*. PhD thesis, Institute of Mathematics PAN, Warsaw, 2001.

[3] I. Aliev. Siegel's lemma and sum-distinct sets. *Discrete Comput. Geom.*, 39(1-3):59–66, 2008.

[4] I. Aliev and M. Henk. Minkowski's successive minima in convex and discrete geometry. *Commun. Math.*, 31:35–59, 2023.

[5] I. Aliev, A. Schinzel, and W. Schmidt. On vectors whose span contains a given linear subspace. *Monatsh. Math.*, 144(3):177–191, 2005.

[6] J. Anthonisse. A note on equivalent systems of linear Diophantine equations. *Z. Operations Res. Ser. A-B*, 17:A167–A177, 1973.

[7] E. Axell, G. Leus, E. Larsson, and H. Poor. Spectrum sensing for cognitive radio: State-of-the-art and recent advances. *IEEE Signal Process. Mag.*, 29(3):101–116, 2012.

[8] R. Bambah, A. Woods, and H. Zassenhaus. Three proofs of minkowski's second inequality in the geometry of numbers. *J. Aust. Math. Soc.*, 5(4):453–462, 1965.

[9] E. Bombieri and J. Vaaler. On Siegel's lemma. *Invent. Math.*, 73(1):11–32, 1983.

[10] S. Boyd and L. Vandenberghe. *Convex Optimization*. Cambridge University Press, 2004.

[11] E. Candes, J. Romberg, and T. Tao. Stable signal recovery from incomplete and inaccurate measurements. *Commun. Pure Appl. Math.*, 59(8):1207–1223, 2006.

[12] E. Candes, M. Rudelson, T. Tao, and R. Vershynin. Error correction via linear programming. In *proceedings of the 46th Annual IEEE Symposium on Foundations of Computer Science (FOCS'05)*, pages 668–681. IEEE, 2005.

[13] J. Cassels. *An introduction to the geometry of numbers*. Springer-Verlag, Berlin-New York, 1971.

[14] S. Chaładus. On the densest lattice packing of centrally symmetric octahedra. *Math. Comput.*, 58(197):341–345, 1992.

[15] S. Chaladus and A. Schinzel. A decomposition of integer vectors. II. *PLISKA Studia mathematica bulgarica*, 11(1):15–23, 1991.

[16] S. Chen, D. Donoho, and M. Saunders. Atomic decomposition by basis pursuit. *SIAM review*, 43(1):129–159, 2001.

[17] A. Cohen, W. Dahmen, and R. DeVore. Compressed sensing and best k-term approximation. *J. Am. Math. Soc.*, 22(1):211–231, 2009.

[18] J. Conway and N. Sloane. *Sphere packings, lattices and groups*. Grundlehren der mathematischen Wissenschaften. Springer New York, 2013.

[19] M. Davenport, M. Duarte, Y. Eldar, and G. Kutyniok. Introduction to compressed sensing, 2012.

[20] D. Donoho and M. Elad. Optimally sparse representations in general dictionaries by ℓ_1 minimization. Technical report, Statistics Department, Stanford University, 2002.

[21] D. Donoho, X. Huo, et al. Uncertainty principles and ideal atomic decomposition. *IEEE Trans. Inf. Theory*, 47(7):2845–2862, 2001.

[22] M. Elad and A. Bruckstein. A generalized uncertainty principle and sparse representation in pairs of bases. *IEEE Trans. Inf. Theory*, 48(9):2558–2567, 2002.

[23] Y. Eldar and G. Kutyniok. *Compressed sensing: theory and applications*. Cambridge university press, 2012.

[24] S. Foucart and H. Rauhut. *A mathematical introduction to compressive sensing*. Birkhäuser Basel, 2013.

[25] L. Fukshansky and A. Hsu. Covering point-sets with parallel hyperplanes and sparse signal recovery. *Discrete Comput. Geom.*, 2022.

[26] L. Fukshansky, D. Needell, and B. Sudakov. An algebraic perspective on integer sparse recovery. *Appl. Math. Comput.*, 340:31–42, 2019.

[27] R. Graham, M. Grötschel, and L. Lovász. *Handbook of Combinatorics*. Elsevier, 1995.

[28] P. Gruber. *Convex and discrete geometry*. Springer, 2007.

[29] P. Gruber and C. Lekkerkerker. *Geometry of numbers*. North-Holland Publishing Co., Amsterdam, second edition, 1987.

[30] P. Gruber and J. Wills. *Handbook of Convex Geometry*. Elsevier Science, 1993.

[31] M. Henk. Successive minima and lattice points. *arXiv preprint math/0204158*, 2002.

[32] S. Konyagin. On the recovery of an integer vector from linear measurements. *Mat. Zametki*, 104(6):863–871, 2018.

[33] S. Konyagin and B. Sudakov. An extremal problem for integer sparse recovery. *Linear Algebra Appl.*, 586:1–6, 2020.

[34] P. McMullen. Determinants of lattices induced by rational subspaces. *Bull. London Math. Soc.*, 16(3):275–277, 1984.

[35] H. Minkowski. *Geometrie der Zahlen*. B. G. Teubner, 1968.

[36] B. Natarajan. Sparse approximate solutions to linear systems. *SIAM J. Comput.*, 24(2):227–234, 1995.

[37] D. Needell. *Topics in compressed sensing*. University of California, Davis, 2009.

[38] P. Poirion. Optimal constraints aggregation method for ILP. *Discrete Appl. Math.*, 262:148–157, 2019.

[39] R. Rankin. On positive definite quadratic forms. *J. London Math. Soc.*, 28:309–314, 1953.

[40] I. Rosenberg. Aggregation of equations in integer programming. *Discrete Math.*, 10:325–341, 1974.

[41] M. Rossi, A. Haimovich, and Y. Eldar. Spatial compressive sensing for mimo radar. *IEEE Trans. Signal Process.*, 62(2):419–430, 2013.

[42] K. Ryutin. Recovering sparse integer vectors from linear measurements. *Uspekhi Mat. Nauk*, 74(6(450)):167–168, 2019.

[43] K. Sawatani, T. Watanabe, and K. Okuda. A note on the Hermite-Rankin constant. *J. Théor. Nombres Bordeaux*, 22(1):209–217, 2010.

[44] A. Schinzel. A property of polynomials with an applicationto Siegel's lemma. *Monatshefte für Mathematik*, 137:239–251, 2002.

[45] W. Schmidt. *Diophantine approximations and Diophantine equations*. Lecture Notes in Mathematics. Springer-Verlag, 1991.

[46] A. Schrijver. *Theory of linear and integer programming*. Wiley Series in Discrete Mathematics & Optimization. Wiley, 1998.

[47] C. Siegel. Über einige anwendungen diophantischer approximationen. In *On some applications of Diophantine approximations*, Quad./Monogr., pages 81–138. Ed. Norm., Pisa, 2014.

[48] N. Sloane. The on-line encyclopedia of integer sequences, 2003.

[49] A. Thue. Über annäherungswerte algebraischer zahlen. *Journal für die reine und angewandte Mathematik*, 135:284–305, 1909.

[50] J. Thunder. Higher-dimensional analogs of Hermite's constant. *Michigan Math. J.*, 45(2):301–314, 1998.

[51] J. Vaaler. A geometric inequality with applications to linear forms. *Pacific J. Math.*, 83(2):543–553, 1979.