SPRINGER BRIEFS IN MATHEMATICS

Sueli I.R. Costa
Frédérique Oggier
Antonio Campello
Jean-Claude Belfiore
Emanuele Viterbo

Lattices Applied to Coding for Reliable and Secure Communications

SBMAC
Sociedade Brasileira de Matemática Aplicada e Computacional

Springer

SpringerBriefs in Mathematics

SpringerBriefs in Mathematics showcases expositions in all areas of mathematics and applied mathematics. Manuscripts presenting new results or a single new result in a classical field, new field, or an emerging topic, applications, or bridges between new results and already published works, are encouraged. The series is intended for mathematicians and applied mathematicians.

More information about this series at http://www.springer.com/series/10030

SBMAC SpringerBriefs

The **SBMAC SpringerBriefs** series publishes relevant contributions in the fields of applied and computational mathematics, mathematics, scientific computing, and related areas. Featuring compact volumes of 50 to 125 pages, the series covers a range of content from professional to academic.

The Sociedade Brasileira de Matemática Aplicada e Computacional (Brazilian Society of Computational and Applied Mathematics, SBMAC) is a professional association focused on computational and industrial applied mathematics. The society is active in furthering the development of mathematics and its applications in scientific, technological, and industrial fields. The SBMAC has helped to develop the applications of mathematics in science, technology, and industry, to encourage the development and implementation of effective methods and mathematical techniques for the benefit of science and technology, and to promote the exchange of ideas and information between the diverse areas of application.

http://www.sbmac.org.br/

Sueli I.R. Costa • Frédérique Oggier
Antonio Campello • Jean-Claude Belfiore
Emanuele Viterbo

Lattices Applied to Coding for Reliable and Secure Communications

Springer

Sueli I.R. Costa
Institute of Mathematics,
Statistics and Computer Science
University of Campinas
Campinas, São Paulo, Brazil

Antonio Campello
Department of Electrical
and Electronic Engineering
Imperial College London
London, UK

Emanuele Viterbo
Department of Electrical and
Computer Systems Engineering
Monash University
Clayton, VIC, Australia

Frédérique Oggier
Division of Mathematical Sciences, School
of Physical and Mathematical Sciences
Nanyang Technological University
Singapore, Singapore

Jean-Claude Belfiore
Communications and Electronics
Department
Télécom ParisTech
Paris, France

ISSN 2191-8198 ISSN 2191-8201 (electronic)
SpringerBriefs in Mathematics
ISBN 978-3-319-67881-8 ISBN 978-3-319-67882-5 (eBook)
https://doi.org/10.1007/978-3-319-67882-5

Library of Congress Control Number: 2017959367

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Contents

Chapter 1
Introduction

Lattices are discrete sets of points in the n-dimensional Euclidean space $\mathbb{R}^n$, which are described as all integer linear combinations of independent vectors. They have been studied by mathematicians for their symmetries and other properties, who have also attempted partial characterizations of particularly well-structured lattices. They have also been studied by electrical and computer engineers, for their applications to communications, coding, and information theory, as well as cryptography.

To the variety of mathematical theories and applications that lattices have generated corresponds a very rich literature. As examples we may quote [26] for an encyclopedic reference, [33, 68] for mathematical theories, [112] for an information theoretic approach, and [73, 83] for a cryptography viewpoint, to name only a few.

The purpose of this book is to provide an introduction to lattices, which combines elementary lattice theory and some applications to coding theory and also cryptography. It is meant to be as self-contained as possible while assuming some familiarity with basic concepts of linear algebra. Numerous examples, computations, illustrations, and exercises are also provided to enhance the understanding, making this text hopefully accessible to both mathematicians who are interested in engineering applications of lattices and engineers who would like to strengthen their mathematical foundations on this topic.

In spite of being a classical subject, newcomers to lattice theory usually face some difficulty in finding details of fundamental concepts and properties. This is due in part to the lack of linear references suitable for a first contact with the theory. In this spirit, this book aims in no way to replace the classical literature nor to cover the topic exhaustively. The objective is to provide a comprehensible first approach to the fundamental concepts with some recent applications in communication areas.

Organization As must be, Chap. 2 starts with the elementary definitions of lattice, generator matrix, Gram matrix, volume, and fundamental regions. We then illustrate the use of lattices by discussing lattice packing and covering, with applications to coding for the Gaussian channel, quantization, and public-key cryptography.

S.I.R. Costa et al., *Lattices Applied to Coding for Reliable and Secure Communications*, SpringerBriefs in Mathematics,
https://doi.org/10.1007/978-3-319-67882-5_1

Relevant lattice properties needed for each of them are emphasized (e.g., packing density and "good basis"). Other concepts introduced and discussed include sublattices, nested lattices, and the Smith normal form of a lattice, whose applications will be seen in the upcoming chapters. This chapter also contains a list of important lattices and their relevant properties and parameters.

One natural way to construct new (or well known) lattices is by exploiting the connection between lattices and linear codes. This is the topic of Chap. 3, via one such construction called Construction A. Since one is usually interested in specific lattices, or at least lattices with specific parameters, it is also important to relate the linear code parameters to that of the obtained lattice. We discuss how linear code distances such as the Hamming distance or the Lee distance translate into norms of lattice vectors and the implications to decoding processes. Construction A is further used for wiretap coding, which is briefly explained.

Another way of constructing lattices (which can in fact be combined with Construction A, though we will only mention this) is by relying on the structure of ring of integers of a number field. We describe this construction in Chap. 4. To make the chapter accessible, we will restrict to the case of quadratic fields, which can be explained from scratch, without particular knowledge of algebraic number theory. A reader at ease with such theories can easily extend the lattice construction to an arbitrary number field. These lattices have, among others, applications to wireless communication. We then give a slightly different viewpoint on lattices coming from number fields, adopting that of cryptography. We briefly describe ideal lattices and list some of their usages to build cryptographic primitives.

The first three chapters establish the foundations of lattice theory and its main applications while paving the way for more advanced topics. In Chaps. 5 and 6, we provide a glimpse, in a survey-like style, of two selected topics: spherical codes and index coding. As a result, more technical terms may appear than in the previous chapters, not necessarily with a definition when this is not critical to the understanding, and no exercise is provided for these two chapters.

In Chap. 5, lattices are used to construct spherical codes either discrete or continuous, which can be used for transmission over AWGN (additive white Gaussian noise) channels. Those codes are highly homogeneous and have a special structure that allows a good performance in the coding and decoding processes. A review of recent papers in this matter is included in the discussion.

Whereas Chap. 4 discusses the role of lattices for wireless communication between a sender and a receiver, Chap. 6 considers a more complex wireless setting when one transmitter broadcasts messages to a set of receivers, each of them aided by the prior knowledge of a subset of messages. It presents a technique called index coding, which jointly encodes messages such as to simultaneously meet the demands of all the receivers in the most efficient manner by utilizing this prior knowledge at the receivers.

Foreword The geometry of lattices and packings has been intriguing famous mathematicians like Johannes Kepler, Isaac Newton, Carl Gauss, Joseph-Louis Lagrange, and Hermann Minkowski at least since the seventeenth century. This does not mean, however, in any way that the theory is outdated. To cite one recent example, the classification of universal quadratic forms concluded in [10] is heavily based on lattice reduction and genus theory and constitutes part of the works that granted Canadian-American mathematician Manjul Bhargava the Fields Medal in 2014.

Lattices have been used to approach problems in communications either for reliability (coding for reliable transmission) or security (cryptography) at least since the 1970s. The apparent simplicity of lattice that hides a number of symmetries makes them a very suitable framework for constructing structured codes for a number of communication systems, such as the Gaussian channel, fading channels, side-information problems, broadcast, interference alignment, source coding, etc. A huge number of works with lattice applications to these subfields have appeared in recent years.

Lattice-based cryptography which is the use of conjectured hard problems on lattices in $\mathbb{R}^n$ is the foundation for secure cryptographic systems. Over the past few years, it has been recognized as an important subarea of the so-called post-quantum cryptography [83] – a form of cryptography that can resist attacks by quantum computers. Certainly a big impulse in this field was the proof in the late 1990s that the most current used cryptographic schemes (RSA and Diffie-Hellman) will not be secure in an advent of quantum computers [95]. Lattice-based cryptography enjoys attractive properties [73], such as resistance to known quantum attacks, strong provable security guarantees, and flexibility for realizing powerful and high asymptotic efficiency.

The idea for this book was conceived after two tutorials ("On Codes and Lattices" and "Explicit Lattice Constructions: From Codes to Number Fields") presented by the authors on the occasion of the São Paulo Advanced School of Coding and Information (SPCODINGSCHOOL 2015), held at University of Campinas, Brazil.

Acknowledgment The authors wish to thank the reviewer for the interesting and pertinent suggestions presented and the important support provided by SBMAC (Brazilian Society of Computational and Applied Mathematics) and FAPESP foundation during the elaboration of this Springer Briefs book.

Chapter 2
Lattices and Applications

A lattice in $\mathbb{R}^n$ is a set of points (vectors) composed by all integer linear combinations of independent vectors.

Definition 2.1 Let $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_m$ be linearly independent vectors in $\mathbb{R}^n$. A *lattice* Λ with basis $\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_m\}$ is defined as

$$\Lambda = \{u_1\mathbf{b}_1 + \cdots + u_m\mathbf{b}_m : u_1, \ldots, u_m \in \mathbb{Z}\}. \tag{2.1}$$

The integer m is called the *rank* of Λ. If $m = n$, we say that Λ is *full rank*.
We may also consider the set $\{(0, \ldots, 0)\} \subset \mathbb{R}^n$ as a (degenerate) lattice of rank 0.

Definition 2.2 A *generator matrix* B for a lattice Λ is a matrix whose columns[1] are a basis for it, i.e.,

$$B = \begin{bmatrix} \mathbf{b}_1 & \mathbf{b}_2 & \ldots & \mathbf{b}_m \end{bmatrix}.$$

A vector $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{R}^n$ is in Λ if and only if it can be written as

$$\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} \mathbf{b}_1 & \mathbf{b}_2 & \ldots & \mathbf{b}_m \end{bmatrix} \begin{bmatrix} u_1 \\ \vdots \\ u_m \end{bmatrix}, u_1, \ldots u_m \in \mathbb{Z}. \tag{2.2}$$

In other words, $\Lambda = \{B\mathbf{u} : \mathbf{u} \in \mathbb{Z}^m\}$, where $\mathbb{Z}^m$ denotes the set of m-uples of integers. Note that in the above definition, B is a matrix of rank m and it is not unique, since a lattice, for $m \geq 2$, has infinitely many bases (as it will be seen next).

[1] Some authors use the row convention of considering basis vectors as rows of a generator matrix; we follow here the column convention.

S.I.R. Costa et al., *Lattices Applied to Coding for Reliable and Secure Communications*, SpringerBriefs in Mathematics,
https://doi.org/10.1007/978-3-319-67882-5_2

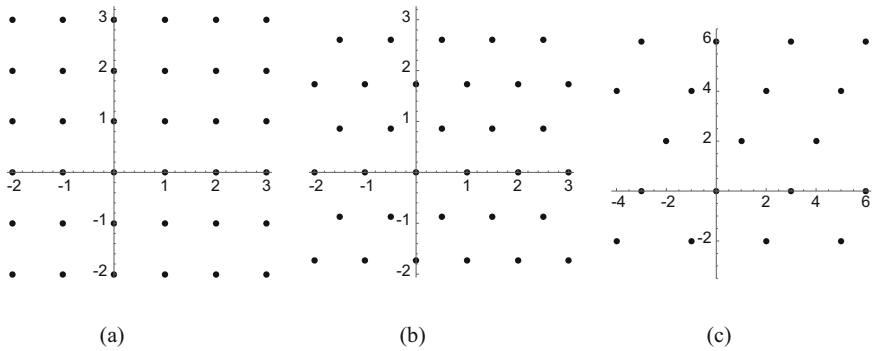


Fig. 2.1 Three lattices in $\mathbb{R}^2$. (**a**) The square lattice $\mathbb{Z}^2$. (**b**) The hexagonal lattice. (**c**) A lattice Λ with basis $\{(3,0),(1,2)\}$

Example 2.1 We start with three examples of rank 2 lattices in $\mathbb{R}^2$. In Fig. 2.1a the *square lattice* $\mathbb{Z}^2$ is displayed. A natural basis for it is $\{(1,0),(0,1)\}$. In Fig. 2.1b the so-called *hexagonal lattice* is displayed. One of its bases is $\left\{(1,0),(1/2,\sqrt{3}/2)\right\}$. A third lattice Λ is depicted in Fig. 2.1c, which has a natural basis given by $\{(3,0),(1,2)\}$.

Example 2.2 The *cubic lattice* $\mathbb{Z}^n \subset \mathbb{R}^n$ (also called the integer lattice) is the set of all n-uples of integers. A basis for $\mathbb{Z}^n$ is the canonical basis of $\mathbb{R}^n$, $\{\mathbf{e}_1,\ldots,\mathbf{e}_n\}$, where $\mathbf{e}_1 = (1,0,\ldots,0), \mathbf{e}_2 = (0,1,0\ldots,0),\ldots,\mathbf{e}_n = (0,0,\ldots,0,1)$. The first lattice $\mathbb{Z}^2$ of Example 2.1 is the particular case when $n = 2$.

Example 2.3 Consider the set A_2 of all vectors in $(x_1,x_2,x_3) \in \mathbb{Z}^3$ such that $x_1+x_2+x_3 = 0$. This set is parameterized by letting two coordinates be free and forcing the third one to be the negative sum of the two free coordinates (if we let say x_1, x_3 free, then $x_2 = -x_1-x_3$), showing that we can describe A_2 by integer linear combinations of two independent vectors. This is a rank 2 lattice in $\mathbb{R}^3$, since a generator matrix for it is

$$B = \begin{bmatrix} 1 & 0 \\ -1 & 1 \\ 0 & -1 \end{bmatrix}.$$

It turns out that the hexagonal lattices in Example 2.1 and A_2 are equivalent lattices, something that will be proven after Definition 2.11 (see Example 2.9). In a similar way, we can define the rank n lattice A_n in $\mathbb{R}^{n+1}$:

$$A_n = \left\{(x_1,x_2,\ldots,x_{n+1}) \in \mathbb{Z}^{n+1} : x_1 + x_2 + \cdots + x_{n+1} = 0\right\}. \tag{2.3}$$

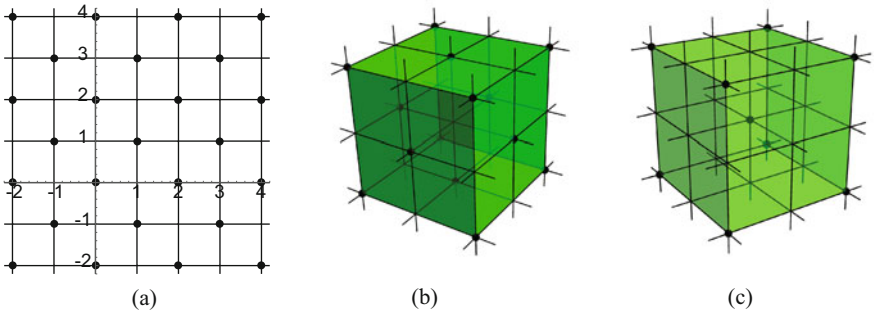


Fig. 2.2 The lattices D_2, D_3= FCC and BCC. (**a**) The D_2 lattice in $\mathbb{R}^2$. (**b**) The D_3 or FCC lattice (face-centered cubic lattice). (**c**) The BCC (body-centered cubic) lattice

Example 2.4 The full rank lattice $D_n \subset \mathbb{R}^n$, also called the checkerboard lattice, is defined as

$$D_n = \{(x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n : x_1 + x_2 + \cdots + x_n \text{ is even}\}. \tag{2.4}$$

The lattices D_2 and D_3, shown in Fig. 2.2a, b, have bases $\{(1,1),(-1,1)\}$ and $\{(2,0,0),(1,1,0),(1,0,1)\}$, respectively (see Exercise 2.1). The lattice D_3 is also known as the face-centered cubic lattice, FCC, since it can be spanned from the vertices and the face centers of a cube with sides of length 2 (Fig. 2.2b). Another lattice in $\mathbb{R}^3$ "constructed" from cubes is the body-centered cubic (BCC) lattice. For example, $\{(2,0,0),(0,2,0),(1,1,1)\}$ is a basis for the BCC lattice (Fig. 2.2c).

There is an alternative definition of lattice in terms of groups. We consider the natural group structure of $\mathbb{R}^n$ with respect to vector addition. Notice that any lattice $\Lambda \subset \mathbb{R}^n$ is a set of vectors satisfying

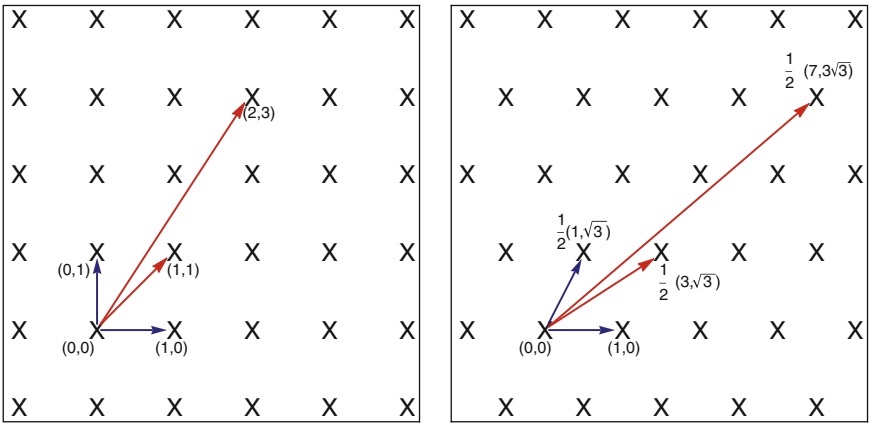
- closure: if $\mathbf{x}, \mathbf{y} \in \Lambda$, then $\mathbf{x} + \mathbf{y} \in \Lambda$,
- for every vector $\mathbf{x} \in \Lambda$, $-\mathbf{x} \in \Lambda$.

These two facts show that a lattice Λ is an *additive subgroup* of $\mathbb{R}^n$. Moreover, a lattice is also a *discrete subset* of $\mathbb{R}^n$. This means that there exists a radius r such that the balls in $\mathbb{R}^n$ centered at lattice points are disjoint. In fact, these two properties provide an equivalent definition of a lattice:

Theorem 2.1 ([20, p. 78]) *A subset of $\mathbb{R}^n$ is a lattice if and only if it is a discrete additive subgroup.*

Through the last proposition, we can see that a set composed by linear integer combinations of dependent vectors is not always a lattice. For instance, for $n = 1$, let A be the set of linear integer combinations of $v_1 = 1$ and $v_2 = \sqrt{2}$. This set is not a lattice, since it is not discrete.

As mentioned earlier, a lattice Λ has (infinitely) many bases for $m \geq 2$. Figure 2.3 illustrates different bases for the integer and for the hexagonal lattices in $\mathbb{R}^2$. The characterization of when distinct bases generate the same lattice is done next by



(a) (b)

Fig. 2.3 Examples of distinct bases for the same lattice. (**a**) $\mathbb{Z}^2$ lattice. (**b**) Hexagonal lattice

means of a special type of matrices, called unimodular. An $m \times m$ matrix U is said to be *unimodular* if it has integer entries and its determinant is 1 or -1. This is equivalent to saying that the integer matrix U has an inverse with integer entries, as stated in Exercise 2.2.

Theorem 2.2 *Two matrices B and $\overline{B}$ generate the same lattice if and only if there exists a unimodular matrix U such that $\overline{B} = BU$.*

Proof Let $\beta_1 = \{\mathbf{b}_1, \ldots, \mathbf{b}_m\}$ and $\beta_2 = \left\{\overline{\mathbf{b}}_1, \ldots, \overline{\mathbf{b}}_m\right\}$ be bases for Λ and $\overline{\Lambda}$, with associated generator matrices B and $\overline{B}$, respectively. Notice that $\overline{\Lambda} \subseteq \Lambda$ if and only if we can write all vectors of β_1 as integer linear combinations of β_2, i.e.,

$$\overline{\mathbf{b}}_j = \sum_{i=1}^{m} \mathbf{b}_i \alpha_{ij}, \text{ for } j = 1, \ldots m, \text{ and } \alpha_{ij} \in \mathbb{Z}.$$

In other words, $\overline{B} = BU$, where $U = (\alpha_{ij})$ is an integer matrix. Analogously, $\Lambda \subseteq \overline{\Lambda}$ if and only if $B = \overline{B}V$, for some integer matrix V. Combining both equations yields

$$\overline{B} = \overline{B}VU \Rightarrow \overline{B}(\mathbf{I} - VU) = \mathbf{0}$$

since every column of $\mathbf{I} - VU$ defines a linear equation in $\overline{\mathbf{b}}_1, \ldots, \overline{\mathbf{b}}_m$, and recalling that $\overline{\mathbf{b}}_1, \ldots, \overline{\mathbf{b}}_m$ are linearly independent, the corresponding coefficients must be all 0. Thus

$$VU = \mathbf{I} \Rightarrow \det(V)\det(U) = 1$$

which, together with the fact that U, V are matrices with integer coefficients, implies that $\det(U) = \det(V) = \pm 1$; therefore U is unimodular.

Conversely, if $\overline{B} = BU$, with U unimodular, then $\overline{\Lambda} \subseteq \Lambda$ and $B = \overline{B}U^{-1}$ where U^{-1} has integer entries, which implies that $\Lambda \subseteq \overline{\Lambda}$, concluding the proof.

Example 2.5 In Fig. 2.3 distinct bases for two lattices in the plane are illustrated. The generator matrices associated with the two different bases of the lattice $\mathbb{Z}^2$ exhibited in Fig. 2.3a are

$$B = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ and } \overline{B} = \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix}.$$

For the lattice of Fig. 2.3b, we have

$$B = \begin{bmatrix} 1 & 1/2 \\ 0 & \sqrt{3}/2 \end{bmatrix} \text{ and } \overline{B} = \begin{bmatrix} 3/2 & 7/2 \\ \sqrt{3}/2 & 3\sqrt{3}/2 \end{bmatrix} = \begin{bmatrix} 1 & 1/2 \\ 0 & \sqrt{3}/2 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix}.$$

In both cases, the unimodular matrix that takes a basis into the other is given by

$$U = \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix}.$$

Note that the above theorem provides a way to check if two full rank square matrices A and B generate the same lattice: this will happen if and only if $B^{-1}A$ is a unimodular matrix (see Exercise 2.3).

Definition 2.3 Given a generator matrix B for a lattice Λ, we define its associated *Gram matrix* by $G = B^T B$.

Each element G_{ij} is the inner product between the basis vectors $\mathbf{b}_i$ and $\mathbf{b}_j$, $G_{ij} = \langle \mathbf{b}_i, \mathbf{b}_j \rangle$. It follows from Theorem 2.2 that, for $m \geq 2$, a lattice has infinitely many Gram matrices; in fact, any $G' = U^T G U$, where U is unimodular, is also a Gram matrix for Λ. However the determinant of a Gram matrix is the same for all bases of Λ, since $|\det U| = 1$. We can then define the *determinant of* Λ as the determinant of any of its Gram matrices. Since this is always a positive number, we can define:

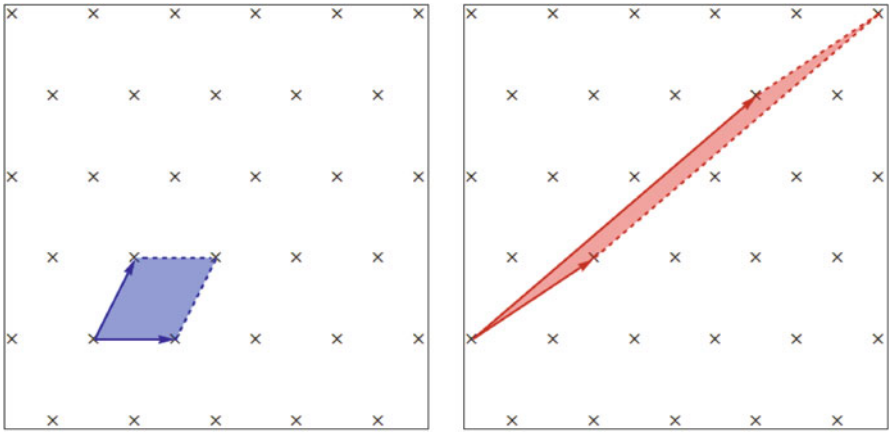
Definition 2.4 The *volume* of a lattice Λ, denoted by $V(\Lambda)$, is the (positive) square root of the determinant of a Gram matrix for Λ.

To give a geometric interpretation to the quantity $V(\Lambda)$, we define the *fundamental parallelotope* $\mathscr{P}(B)$ as

$$\mathscr{P}(B) = \{\alpha_1 \mathbf{b}_1 + \cdots + \alpha_m \mathbf{b}_m, 0 \leq \alpha_i < 1, i = 1, \ldots m\}. \tag{2.5}$$

$\mathscr{P}(B)$ is contained in the m-dimensional subspace of $\mathbb{R}^n$ generated by the set of vectors $\mathbf{b}_1, \ldots, \mathbf{b}_m$. The Euclidean *volume* of $\mathscr{P}(B)$ is

$$V(\Lambda) = \sqrt{\det B^T B} = |\det B|. \tag{2.6}$$



(a) (b)

Fig. 2.4 Distinct fundamental parallelotopes for the hexagonal lattice. (**a**) Parallelotope associated with the basis $\left\{(1,0),(1/2,\sqrt{3}/2)\right\}$. (**b**) Parallelotope associated with the basis $\left\{(3/2,\sqrt{3}/2),(7/2,3\sqrt{3}/2)\right\}$

Example 2.6 Continuing Example 2.5, the two distinct bases for the hexagonal lattice (Fig. 2.3b) produce different fundamental parallelotopes, illustrated in Fig. 2.4. The area of both parallelotopes is equal to $\sqrt{3}/2$, the volume of the hexagonal lattice.

Given a full rank lattice Λ, it is possible to check that the disjoint union of translates of $\mathscr{P}(B)$ by vectors of Λ is equal to the whole space $\mathbb{R}^n$. In other words, the fundamental parallelotope $\mathscr{P}(B)$ *tiles* $\mathbb{R}^n$ through translations by points of Λ, that is:

(i)

$$\text{If } \mathbf{x},\mathbf{y}\in\Lambda, \mathbf{x}\neq\mathbf{y}, \textit{then } (\mathbf{x}+\mathscr{P}(B))\bigcap(\mathbf{y}+\mathscr{P}(B))=\varnothing \text{ and}$$

(ii)

$$\bigcup_{\mathbf{x}\in\Lambda}(\mathbf{x}+\mathscr{P}(B))=\mathbb{R}^n. \tag{2.7}$$

From now on in this and in the next chapters, in order to simplify the statements, we *assume all lattices to be full rank*, unless stated otherwise.

Besides the fundamental parallelotope, other regions $A\subset\mathbb{R}^n$ may as well tile $\mathbb{R}^n$ through translations by elements of Λ. In fact, item (i) of the tiling condition above can be "relaxed" to (i') requiring that for $\mathbf{x},\mathbf{y}\in\Lambda$, $(\mathbf{x}+A)$ and $(\mathbf{y}+A)$ intersect at most on their boundaries. Any region $A\subset\mathbb{R}^n$ satisfying conditions

(i') and (ii) is called a *fundamental region* for Λ. Any fundamental region for Λ has volume $V(\Lambda)$ (see, e.g., [86, p.28, Thm. 1.6]). Another important fundamental region is the *Voronoi region*. Let $\|.\|$ denote the standard Euclidean norm of a vector $\mathbf{x} \in \mathbb{R}^n$,

$$\|\mathbf{x}\| = \sqrt{x_1^2 + x_2^2 + \ldots + x_n^2}.$$

Definition 2.5 The *Voronoi region*, also called Dirichlet region, $\mathcal{V}_\Lambda(\mathbf{x})$ at a point $\mathbf{x} \in \Lambda$ is the set of all points in $\mathbb{R}^n$ which are at least as close to $\mathbf{x}$ than to any other lattice point, i.e.:

$$\mathcal{V}_\Lambda(\mathbf{x}) = \{\mathbf{y} \in \mathbb{R}^n : \|\mathbf{x} - \mathbf{y}\| \leq \|\mathbf{z} - \mathbf{y}\|, \text{for all } \mathbf{z} \in \Lambda\}. \tag{2.8}$$

The Voronoi region at the origin,

$$\mathcal{V}_\Lambda(\mathbf{0}) = \mathcal{V}(\Lambda), \tag{2.9}$$

is called the Voronoi region of the lattice, and we have that $\mathcal{V}_\Lambda(\mathbf{x}) = \mathcal{V}(\Lambda) + \mathbf{x}$. It should be remarked that although the fundamental parallelotope depends on the choice of basis, the Voronoi region of a lattice is unique and intrinsic to the standard metric structure of $\mathbb{R}^n$. If a point is in the boundary of a Voronoi region, it is equidistant from at least two lattice points. Figures 2.5, 2.6, and 2.7 illustrate the tilings of three lattices by different fundamental regions including their Voronoi regions on part (b) (see also Exercise 2.4). The Voronoi regions of the lattices $\mathbb{Z}^3$ and FCC are a cube with sides of length one and a rhombic dodecahedron centered at the origin, respectively. The Voronoi region of a lattice is a convex set of $\mathbb{R}^n$ enclosed by hyperplanes which are equidistant from the origin and a relevant lattice point. It is usually very hard to determine, particularly in high dimensions. For special classes of lattices such as the so-called root lattices (which include A_n and D_n; see (2.4)), they have been determined [25, 26]. Algorithms for numerically determining the Voronoi region have been developed in several references. Those results are important in applications of lattices to communications such as the ones regarding quantizers and channel coding (see this chapter, Sect. 2.5.1, Chap. 6, and also [26, Chaps. 2 and 3].

2.1 Sphere Packing and Covering

One of the main subjects of research on lattices is their association with the hard problem of finding dense packings in the Euclidean space, which has many applications.

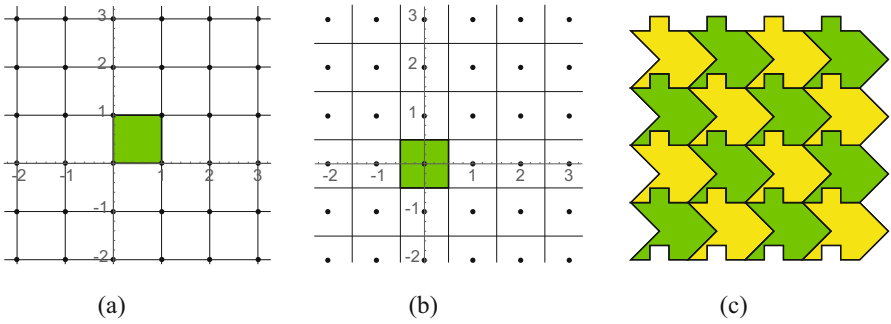


Fig. 2.5 Different fundamental regions and tilings of the plane by $\mathbb{Z}^2$. (**a**) The fundamental parallelotope of the lattice $\mathbb{Z}^2$ with basis $\{(1,0),(0,1)\}$ and associated plane tiling. (**b**) The Voronoi region of the lattice $\mathbb{Z}^2$ and its associated plane tiling. (**c**) A tiling of the plane though translations of another fundamental region of $\mathbb{Z}^2$

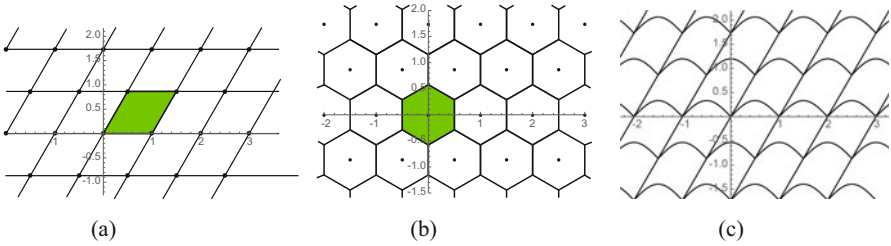


Fig. 2.6 Different fundamental regions and tilings of the plane by the hexagonal lattice A_2. (**a**) The fundamental parallelotope the hexagonal lattice for basis $\left\{(1,0),(1/2,\sqrt{3}/2)\right\}$ and associated plane tiling. (**b**) The Voronoi region of the hexagonal lattice and its associated plane tiling. (**c**) A tiling of the plane though translations of another fundamental region of the hexagonal lattice

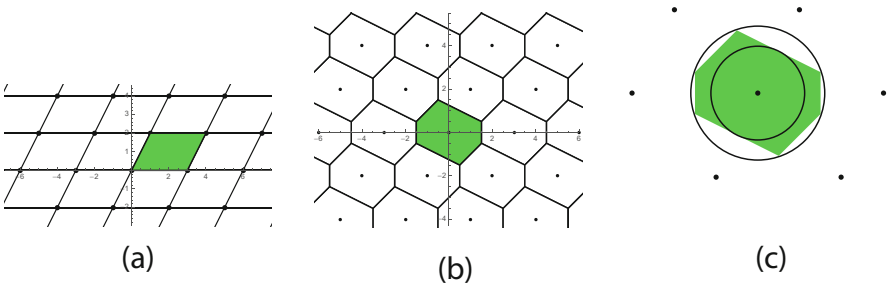


Fig. 2.7 The lattice Λ with basis $\{(3,0),(1,2)\}$: fundamental parallelotope, Voronoi region, and packing and covering balls. (**a**) The fundamental parallelotope of the lattice Λ with basis $\{(3,0),(1,2)\}$ and associated plane tiling. (**b**) The Voronoi region of the lattice Λ and its associated plane tiling. (**c**) The Voronoi region and the packing and the covering circles of Λ

The *minimum norm* (or minimum distance) of a lattice corresponds to the minimum among all norms of non-zero vectors in Λ, i.e.,[2]:

$$\lambda = \min_{\mathbf{0} \neq \mathbf{x} \in \Lambda} \|\mathbf{x}\| . \tag{2.10}$$

From the fact that a lattice is a discrete additive subgroup of $\mathbb{R}^n$ (Theorem 2.1), it can be shown that any lattice has a non-vanishing vector of minimum norm $\lambda > 0$.

Let $\mathscr{B}^n(r)$ denote a Euclidean ball of radius r around the origin, i.e.:

$$\mathscr{B}^n(r) = \{\mathbf{x} \in \mathbb{R}^n : \|\mathbf{x}\| \leq r\} . \tag{2.11}$$

It is easy to see that $r = \lambda/2$ is the largest value for which the translates of the balls $\mathscr{B}^n(\rho)$ centered at $\mathbf{x} \in \Lambda$ have disjoint interiors. We call

$$\rho = \lambda/2 \tag{2.12}$$

the *packing radius* of Λ. Notice also that the ball $\mathscr{B}^n(\rho)$ is inside and touches the boundaries of the Voronoi region of Λ. We define a *lattice packing* as the union of translates of the ball $\mathscr{B}^n(\rho)$ by points of Λ.

The ratio $\text{vol}\, \mathscr{B}^n(\rho)/V(\Lambda)$ describes how much of the Voronoi region is occupied by $\mathscr{B}^n(\rho)$. Due to the lattice homogeneity, the percentage of the space $\mathbb{R}^n$ covered by translates of $\mathscr{B}^n(\rho)$ by lattice points is given by the same ratio.

Definition 2.6 The *packing density* of Λ is defined as

$$\Delta(\Lambda) = \frac{\text{vol}\, \mathscr{B}^n(\rho)}{V(\Lambda)}. \tag{2.13}$$

Example 2.7 In Fig. 2.8 we illustrate the lattices of Example 2.1, their packing balls and respective packing densities. The square and the hexagonal lattices both have packing radius equal to $1/2$ and packing densities $\Delta = 0.785$ and $\Delta = 0.906$, respectively. The lattice with basis $\{(3,0), (1,2)\}$ has packing radius equal to $\sqrt{5}/2$ and packing density $\Delta = 0.654$.

Notice that $\text{vol}\, \mathscr{B}^n(\rho) = \rho^n \text{vol}\, \mathscr{B}^n(1)$. The volume of the Euclidean ball $\mathscr{B}^n(1)$, of radius 1, is known [26]:

$$\text{vol}\, \mathscr{B}^n(1) = \begin{cases} \frac{\pi^{n/2}}{(n/2)!} & \text{if } n \text{ is even, and} \\ \frac{2^n \pi^{(n-1)/2}((n-1)/2)!}{n!} & \text{if } n \text{ is } \sout{\text{even}}\ \text{odd} \end{cases} \tag{2.14}$$

When $n = 2, 3$ we recover the area of the unit circle (π) and the volume of the unit sphere ($4\pi/3$), respectively.

[2] In several textbooks and papers, the minimum norm is defined as the square of this number.

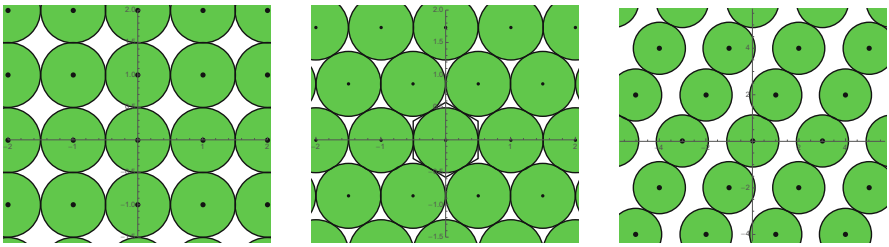


Fig. 2.8 Lattice packings. (**a**) The square lattice: ρ=1/2 and $\Delta(\mathbb{Z}^2) = 0.7854$. (**b**) The hexagonal lattice: ρ=1/2 and $\Delta(A_2) = 0.9069$. (**c**) The lattice Λ with basis $\{(3,0),(1,2)\}$: $\rho = \sqrt{5}/2$ and $\Delta(\Lambda) = 0.6545$

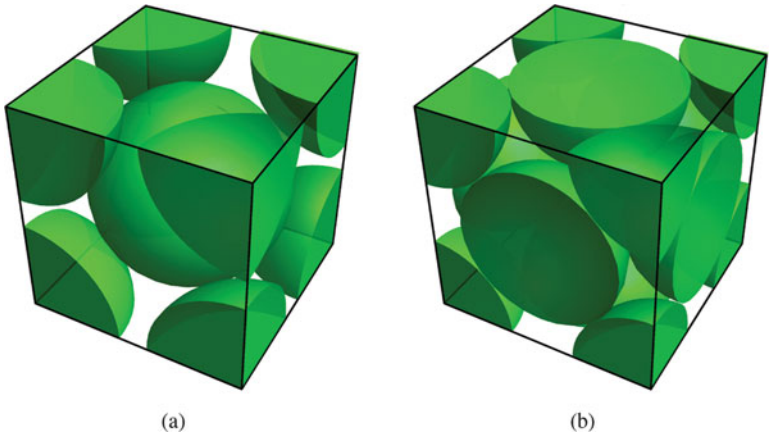


Fig. 2.9 The packing density of the BCC and the FCC lattices. (**a**) A view of the BCC packing density ($\rho = \sqrt{3}/2$, $\Delta = 0.6802$). (**b**) A view of the FCC packing density ($\rho = \sqrt{2}/2$, $\Delta = 0.7405$)

The packing densities of $\mathbb{Z}^3$ and of the lattices FCC and BCC are $\pi/6 = 0.5236$, $\pi/18 = 0.7405$, and $\pi\sqrt{3}/8 = 0.6802$, respectively (see Figs. 2.9 and 2.10).

Definition 2.7 The *center density* of a lattice is defined as $\delta(\Lambda) = \Delta(\Lambda)/\text{vol}\,\mathscr{B}^n(1) = \rho^n/V(\Lambda)$.
The center density provides a way of comparing lattices in the same dimension that avoids the complicated formula (2.14).

Attached to a sphere packing is the concept of kissing number.

Definition 2.8 The *kissing number* of a lattice is the number of packing balls that touch a fixed one, which corresponds to the number of lattice points having the minimum non-vanishing norm.
For our three lattices in Figs. 2.5, 2.6, and 2.7, this number is 4, 6, and 2, respectively.

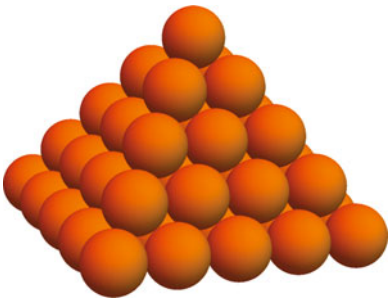


Fig. 2.10 The FCC lattice (the best packing in $\mathbb{R}^3$) represented as the centers of an orange pile

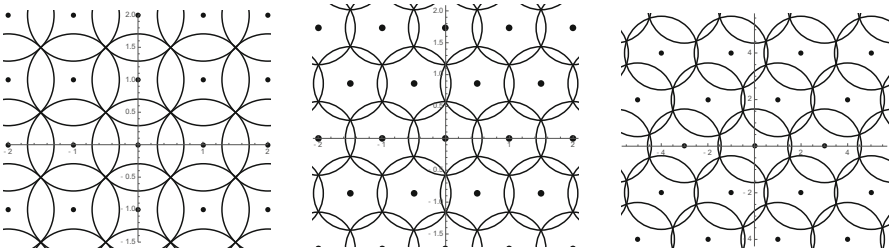


Fig. 2.11 Covering densities of three different lattices. (**a**) The square lattice: covering radius $\nu = \sqrt{2}/2$ and covering density $\theta(\mathbb{Z}^2) = 1.5708$. (**b**) The hexagonal lattice: covering radius $\mu = \sqrt{3}/3$, covering density $\Theta(A_2) = 1.2092$. (**c**) The lattice with basis $\{(3,0),(1,2)\}$: covering radius $\mu = \sqrt{10}/2$, covering density $\Theta(\Lambda) = 1.3088$

A "dual" concept to sphere packing is the one of *sphere covering* which also has several applications. In the covering problem, we ask for the thinnest possible arrangement of spheres that cover all points of $\mathbb{R}^n$. More formally:

Definition 2.9 The *covering radius* of a lattice is defined as the minimum μ such that the translates of the balls $\mathscr{B}^n(\mu)$ by points of Λ *cover* $\mathbb{R}^n$, i.e.:

$$\bigcup_{\mathbf{x}\in\Lambda} (\mathscr{B}^n(\mu) + \mathbf{x}) = \mathbb{R}^n.$$

If we consider the vertices of the Voronoi region of Λ (called holes), the covering radius is the biggest distance from one of the holes to the origin. (A hole which attains this distance is called a deep hole.) The n-dimensional covering ball $\mathscr{B}^n(\mu)$ circumscribes the Voronoi region of a lattice, whereas the packing ball is inscribed in it (see Figs. 2.11, 2.7 c).

Definition 2.10 The *covering density* is then defined as

$$\theta(\Lambda) = \frac{\text{vol}\,\mathscr{B}^n(\mu)}{V(\Lambda)}. \tag{2.15}$$

For $n \geq 2$, the covering density is always greater than 1, while the packing density is always smaller than 1. Figure 2.11 illustrates the covering density of our three different lattices in $\mathbb{R}^2$.

2.1.1 Equivalent Lattices

All lattice parameters discussed in this section remain unchanged under some transformations. For example, if we scale all lattice vectors by the same constant c, the lattice volume will be scaled by c^n and the (packing and covering) radii by c. Therefore, the packing and covering densities (as well as the kissing number) do not change. The same happens if we rotate all lattice points. Therefore, it makes sense to treat these lattices as equivalent. Equivalent lattices are obtained by rotating, reflecting, or scaling the original one. A formal definition is stated next. We recall that an $n \times n$ matrix Q is *orthogonal* if $Q^T Q = QQ^T = \mathbf{I}_n$, where $\mathbf{I}_n$ is the $n \times n$ identity matrix. Orthogonal matrices are associated with linear maps which preserve angles and lengths, defining rotations or reflections in $\mathbb{R}^n$.

Definition 2.11 Two lattices Λ_1 and Λ_2 contained in $\mathbb{R}^n$ are *equivalent* if there exist an orthogonal matrix Q, a real number c, and generator matrices B_1 and B_2 for Λ_1 and Λ_2, respectively, such that $B_1 = cQB_2$. In particular, Λ_1 and Λ_2 are called *congruent* if $|c| = 1$.
We write $\Lambda_1 \sim \Lambda_2$ for two equivalent lattices.

Remark 2.1 If we consider the Gram matrices G_1 and G_2 associated with the specific generator matrices B_1 and B_2 in the last definition, we have $G_1 = c^2 G_2$. Furthermore, it can be shown that two lattices which have Gram matrices related to specific bases satisfying $G_1 = c^2 G_2$ must be congruent, and therefore this can be taken as an alternative definition of equivalent lattices. Then congruent lattices must have identical Gram matrices related to some specific generator matrices.

Remark 2.2 Given Λ_1 and Λ_2 with arbitrary generator matrices B_1 and B_2, $\Lambda_1 \sim \Lambda_2$ if and only if there are matrices Q orthogonal and U unimodular such that $B_1 = cQB_2U$. Accordingly, two arbitrary Gram matrices G_1 and G_2 for equivalent lattices must satisfy $G_1 = c^2 U^t G_2 U$, with U unimodular.

Example 2.8 The lattice generated by

$$\begin{bmatrix} 1 & \frac{1}{2}\left(\sqrt{3}+1\right) \\ -1 & \frac{1}{2}\left(\sqrt{3}-1\right) \end{bmatrix}$$

is equivalent to the hexagonal lattice, since

$$\begin{bmatrix} 1 & \frac{1}{2}\left(\sqrt{3}+1\right) \\ -1 & \frac{1}{2}\left(\sqrt{3}-1\right) \end{bmatrix} = \sqrt{2}\begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix} \cdot \begin{bmatrix} 1 & \frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} \end{bmatrix}.$$

It is a clockwise rotation of 45° and an expansion of factor $\sqrt{2}$ of the hexagonal lattice.

Remark 2.3 The definition above can be extended to compare lattices which are originally contained in different dimensions by identifying a lattice in $\mathbb{R}^n$ with its natural inclusion in $\mathbb{R}^t$, $t > n$, which adds $(t - n)$ zeros in the coordinates of its vectors.

Example 2.9 View the hexagonal lattice of Example 2.1 as included in $\mathbb{R}^3$, generated by $\left\{(1,0,0),(1/2,\sqrt{3}/2,0)\right\}$. We can show that it is equivalent to the lattice A_2 given in Example 2.3. In fact, for the generator matrix B_1 associated with this basis and another generator matrix B_2 for the lattice A_2 associated with the basis $\{(1,-1,0),(0,-1,1)\}$, we can see that the Gram matrices of the two lattices related to these bases are multiples: $B_2^T B_2 = 2B_1^T B_1$, which implies their equivalence (Remark 2.1). We can also write explicitly the equivalence of these lattices as described in Remark 2.2 by starting from the generator matrix for A_2 as given in Example 2.3: $\begin{bmatrix} 1 & 0 \\ -1 & 1 \\ 0 & -1 \end{bmatrix} = \sqrt{2}Q \begin{bmatrix} 1 & \frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} \\ 0 & 0 \end{bmatrix} U$, where Q is the 3×3 orthogonal matrix having for its columns the vectors $(1/\sqrt{2}, -1/\sqrt{2}, 0)$, $(-1/\sqrt{6}, -1/\sqrt{6}, 2/\sqrt{6})$, and $(1/\sqrt{3}, 1/\sqrt{3}, 1/\sqrt{3})$, while U is the 2×2 unimodular matrix having for its columns the vectors $(1,0)$ and $(0,-1)$. You may use similar arguments in Exercise 2.7 to check another example of equivalent lattices.

2.2 Sublattices

Given lattices Λ' and Λ such that $\Lambda' \subseteq \Lambda$, Λ' is said to be a *sublattice* of Λ. A subset of a lattice is a sublattice if and only if it is an additive subgroup (i.e., for any $\mathbf{x}$ and $\mathbf{y}$ in Λ', $\mathbf{x} + \mathbf{y}$ and $-\mathbf{y}$ also are in Λ').

Let $\Lambda \subset \mathbb{R}^n$ be a full rank lattice with generator matrix B, and let M be an $n \times n$ integer matrix. If $\det(M) \neq 0$, then BM is a generator matrix of a full rank sublattice Λ' of Λ. Reciprocally any generator matrix A of a full rank sublattice Λ' of Λ can be written as BM for some integer matrix M: Λ and Λ' are said to form a *nested lattice pair*, where Λ is the fine lattice and Λ' is the coarse lattice.

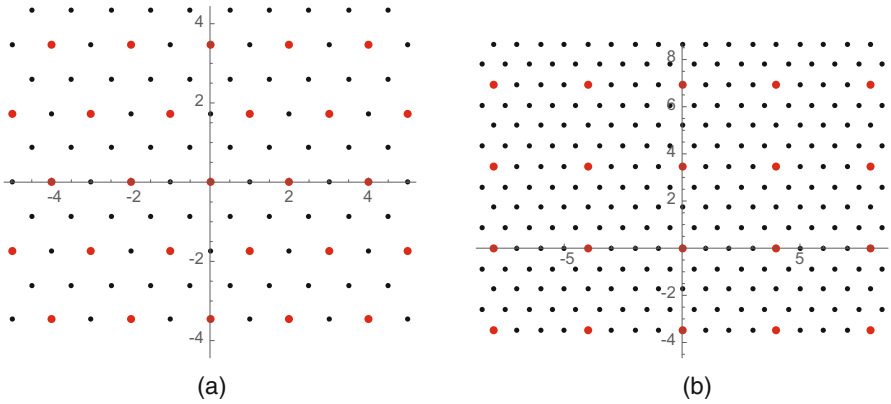


Fig. 2.12 Sublattices of the hexagonal lattice. (**a**) The hexagonal lattice and its sublattice Λ_1 with generator matrix BM_1. (**b**) The hexagonal lattice and its sublattice Λ_2 with generator matrix BM_2

Example 2.10 For the hexagonal lattice Λ with generator matrix

$$B = \begin{bmatrix} 1 & \frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} \end{bmatrix},$$

we may consider

$$M_1 = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} \text{ and } M_2 = \begin{bmatrix} 4 & -2 \\ 0 & 4 \end{bmatrix}$$

and the sublattices Λ_1 and Λ_2 generated by BM_1 and BM_2 (coarse lattice) illustrated in Fig. 2.12.

Example 2.11 The lattices D_n described in Sect. 2.4 are sublattices of the integer lattice $\mathbb{Z}^n$.

Nested lattices have been used in several applications. In this book, they appear in the construction of wiretap codes in Chap. 3, spherical codes in Chap. 5, and index codes in Chap. 6.

Since a sublattice $\Lambda' \subseteq \Lambda$ is a subgroup, Λ can be partitioned into a set of cosets of Λ' which form a finite quotient group $\frac{\Lambda}{\Lambda'}$ (or Λ/Λ'). Each of these cosets can be identified using a coset leader (or coset representative) in the fundamental parallelotope of the lattice Λ. Each leader also can be chosen in the Voronoi region of Λ, as it will be seen in Chap. 6. Let B be a generator matrix for Λ and $B' = BM$ be one for Λ'. The number of elements of $\frac{\Lambda}{\Lambda'}$ is given by:

$$\left|\frac{\Lambda}{\Lambda'}\right| = \frac{V(\Lambda')}{V(\Lambda)} = |\det(M)|.$$

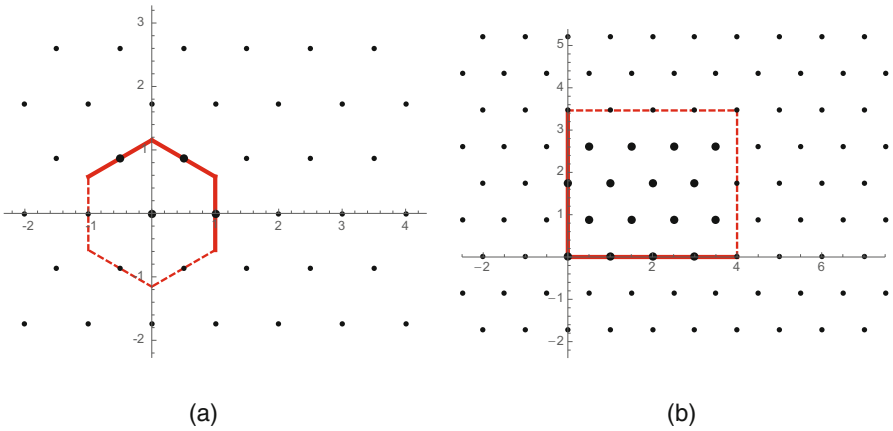


Fig. 2.13 Quotients of the hexagonal lattices. (**a**) The quotient $\frac{\Lambda}{\Lambda_1}$ represented by coset leaders inside the Voronoi set of Λ_1. (**b**) The quotient $\frac{\Lambda}{\Lambda_2}$ represented by coset leaders inside a fundamental polytope of Λ_2

In Example 2.10 above, we have $\left|\frac{\Lambda}{\Lambda'}\right| = 4$ and $\left|\frac{\Lambda}{\Lambda'}\right| = 16$ (see Fig. 2.13).

Any integer squared n-dimensional matrix M can be decomposed into the so-called *Smith normal form*: $M = UDW$ where U and W are unimodular matrices and $D = \{d_{i,j}\}$ is a diagonal matrix where $d_{j,j} \in \mathbb{N}$, $d_{i,i} | d_{i+1,i+1}$ [21, Sect. 2.4].

The Smith normal form can be used to extract special bases of a pair of nested full rank lattices.

Theorem 2.3 *Given a nested pair of full rank lattices $\Lambda' \subseteq \Lambda$, there exist special bases $\{\mathbf{w}_1, \ldots, \mathbf{w}_n\}$ of Λ' and $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ of Λ such that $\mathbf{w_i} = k_i \mathbf{v_i}$, for $i = 1, \ldots, n$, $k_i \in \mathbb{N}$.*

Proof Let B be a generator matrix of Λ and BM be a generator matrix of Λ'. Consider the Smith decomposition, $M = UDW$ where W, U are unimodular lattices. According to Theorem 2.2, $BMW^{-1} = (BU)D$ is also a generator matrix of Λ', and BU is a generator matrix of Λ, since U and W^{-1} are unimodular matrices. If we take $\{\mathbf{w}_1, \ldots, \mathbf{w}_n\}$ and $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ as the columns of the matrices BMW^{-1} and BU, respectively, we get $\mathbf{w}_i = d_{i,i}\mathbf{v}_i$. Take $k_i = d_{i,i}$.

Example 2.12 In the nested lattice pair $\Lambda_2 \subseteq \Lambda$ of Example 2.10, we have the following Smith decomposition for M:

$$M = UDW = \begin{bmatrix} -1 & -1 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} 2 & 0 \\ 0 & 8 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ -1 & 0 \end{bmatrix}.$$

After calculating $A = BMW^{-1} = (BU)D$ and BU, we get the basis $\{\mathbf{v}_1, \mathbf{v}_2\}$ of the hexagonal lattice, $\mathbf{v}_1 = (0, \sqrt{3})$, $\mathbf{v}_2 = (-\frac{1}{2}, \frac{\sqrt{3}}{2})$ and the basis $\{\mathbf{w}_1, \mathbf{w}_2\}$, $\mathbf{w}_1 = 2\mathbf{v}_1$, $\mathbf{w}_2 = 8\mathbf{v}_1$ for the lattice Λ_2.

For a nested pair $\Lambda' \subseteq \Lambda$ with generator matrices B and BM, the diagonal matrix of the Smith normal form of M also classifies the abelian quotient group $\frac{\Lambda}{\Lambda'}$, and this will be used in Chap. 5 to describe spherical codes.

2.3 The Dual of a Lattice

The dual of a lattice plays an important role in understanding its structure.

Definition 2.12 The *dual* lattice of a lattice Λ is by definition

$$\Lambda^* = \{\mathbf{y} \in \mathbb{R}^n \mid \langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z} \text{ for all } \mathbf{x} \in \Lambda\}. \tag{2.16}$$

Dual lattices are sometimes called *polar* or *reciprocal* and arise in areas as distinct as crystallography, cryptography, and harmonic analysis. To understand geometrically the notion of dual, let us start with a full rank lattice $\Lambda \subset \mathbb{R}^2$ generated by the vectors $(b_{11}, b_{21}), (b_{12}, b_{22})$. From the definition, the scalar product between any vector of the dual and the original lattice must be an integer. In fact, it is enough to ensure this for the basis vectors, since lattice points are obtained by integral linear combinations. Given $i \in \mathbb{Z}$, the set of vectors

$$H_1^{(i)} = \left\{(x_1, x_2) \in \mathbb{R}^2 \mid \langle (x_1, x_2), (b_{11}, b_{21}) \rangle = x_1 b_{11} + x_2 b_{21} = i\right\}.$$

is a straight line in $\mathbb{R}^2$. By changing $i \in \mathbb{Z}$, we obtain a set of parallel straight lines. Now imposing the same condition for the second basis vector, we have the set of parallel straight lines

$$H_2^{(j)} = \left\{(x_1, x_2) \in \mathbb{R}^2 \mid \langle (x_1, x_2), (b_{12}, b_{22}) \rangle = x_1 b_{12} + x_2 b_{22} = j\right\},$$

$j \in \mathbb{Z}$. Each straight line $H_1^{(i)}$ intersects $H_2^{(j)}$ in precisely one point. The union of all these points is Λ^* (see Fig. 2.14). The same interpretation holds in $\mathbb{R}^n$. For each basis vector $\mathbf{b}_k$, we have a set of parallel hyperplanes $H_k^{(j)}$, $j \in \mathbb{Z}$. The distance between each pair of consecutive hyperplanes H_k^j and H_k^{j+1} is $1/\|\mathbf{b}_k\|$. Indeed, if $\mathbf{x}$ belongs to H_k^j, then $\mathbf{x} + \mathbf{b}_k/\|\mathbf{b}_k\|^2$ belongs to H_k^{j+1}. The distance between these points is precisely the distance between the hyperplanes, namely, $1/\|\mathbf{b}_k\|$.

Example 2.13 The lattice $\mathbb{Z}^n$ is equal to its dual.

Example 2.14 Consider the hexagonal lattice, generated by $(1, 0), (1/2, \sqrt{3}/2)$. A point in its dual has to satisfy

$$\langle (x_1, x_2), (1, 0) \rangle = x_1 = l_1 \in \mathbb{Z} \text{ and}$$

$$\left\langle (x_1, x_2), \left(\tfrac{1}{2}, \tfrac{\sqrt{3}}{2}\right) \right\rangle = \frac{x_1}{2} + \frac{\sqrt{3}x_2}{2} = l_2 \in \mathbb{Z}.$$

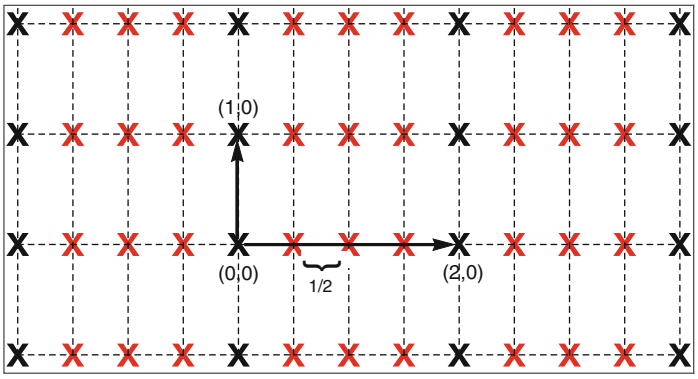


Fig. 2.14 A lattice with basis $\{\mathbf{b}_1, \mathbf{b}_2\} = \{(2,0),(0,1)\}$ and its dual, which has basis $\{\mathbf{b}_1^*, \mathbf{b}_2^*\} = \{(1/2,0),(0,1)\}$

Solving the equations for (x_1, x_2), we conclude that a point in the dual has the form $(x_1, x_2) = (l_1, (2l_2 - l_1)/\sqrt{3})$, $l_1, l_2 \in \mathbb{Z}$. In other words, the dual is a two-dimensional lattice generated by the vectors $(1, -1/\sqrt{3}), (0, 2/\sqrt{3})$. Notice that this lattice is equivalent to the hexagonal itself. See Exercise 2.10.

In general, calculating the dual lattice from the definition, as in Example 2.14, may not be worthwhile. In what follows, we summarize relations to get the parameters of Λ^* in a simple way (see [26, p.11] for (1)–(3) and Exercise 2.6 for (4)).

1 If B is a generator matrix for Λ, then $(B^T)^{-1}$ is a generator matrix for Λ^*.
2 In the same way, if G is a Gram matrix for Λ, G^{-1} is a Gram matrix for Λ^*.
3 $V(\Lambda^*) = V(\Lambda)^{-1}$.
4 If $\Lambda_1 \sim \Lambda_2$, then $\Lambda_1^* \sim \Lambda_2^*$.

Definition 2.13 We say that Λ is *integral* if it has a Gram matrix with integer entries. Note that this condition is equivalent to saying that the inner product between any two lattice vectors is an integer or that $\Lambda \subseteq \Lambda^*$.
In fact, for integer lattices we have $\Lambda \subseteq \Lambda^* \subseteq (\frac{1}{V(\Lambda)^2})\Lambda$.

Definition 2.14 If $\Lambda = \Lambda^*$, we say that Λ is *unimodular*, and this means that any of its Gram matrices is unimodular.

2.4 Important Lattices and Their Duals

Important lattices are lattices which have exceptional structures and typically are often encountered in the literature. This subsection provides a summarized description with parameters of well-known lattices, some of which will appear

Table 2.1 Relevant parameters for a lattice Λ in $\mathbb{R}^n$ with generator matrix B

Notation	Name	Reference
$\mathscr{P}(B)$	Fundamental parallelotope	(2.5)
$V(\Lambda) = \sqrt{\det(BB^T)}$	Volume	(2.6)
$\mathscr{V}(\Lambda)$	Voronoi region	(2.9)
$\mathscr{B}^n(1)$	Ball of radius 1 around the origin	(2.11)
$\lambda = \min_{\mathbf{x}\in\Lambda,\mathbf{x}\neq\mathbf{0}} \|\|\mathbf{x}\|\|$	Minimum norm (distance)	(2.10)
$\rho = \lambda/2$	Packing radius	(2.12)
$\Delta(\Lambda)$	Packing density	(2.13)
$\delta(\Lambda) = \rho^n/V(\Lambda)$	Center density	Def. 2.7
μ	Covering radius	Def. 2.9
$\theta(\Lambda)$	Covering density	(2.15)

in Table 2.4, which contains "record" lattices. Many more details regarding these lattices as well as other special types of lattices are found in [26, Chap. 4]. We recall the lattice parameters and related concepts that we have introduced so far in Table 2.1.

The Cubic Lattice $\mathbb{Z}^n$

This lattice is unimodular, $(\mathbb{Z}^n)^* = \mathbb{Z}^n$ It has minimum distance $\min_{\mathbf{x}\in\mathbb{Z}^n,\mathbf{x}\neq\mathbf{0}} ||\mathbf{x}|| = 1$, packing radius $\rho = 1/2$, covering radius $\sqrt{n}/2$ (a typical deep hole is $(1/2,\ldots,1/2)$) and kissing number $2n$. Its Voronoi region is a cube, its packing density is $\frac{\text{vol } \mathscr{B}^n(1)}{2^n}$, and its covering density $n^{\frac{n}{2}} \frac{\text{vol } \mathscr{B}^n(1)}{2^n}$.

The Lattice D_n

The checkerboard lattice D_n is defined in Example 2.4 as the full rank sublattice of $\mathbb{Z}^n$ where the sum of coordinates is even. As such, it has for basis $\{\mathbf{v}_1,\ldots,\mathbf{v}_n\}$ with $\mathbf{v}_1 = (-1,-1,0,\ldots,0)$, $\mathbf{v}_2 = (1,-1,0,\ldots,0)$, $\mathbf{v}_3 = (0,1,-1,0,\ldots,0)$, and $\ldots,\mathbf{v}_n = (0,0,\ldots,0,1,-1)$. Its minimum distance is $\sqrt{2}$, its volume is $V(D_n) = 2$ $(\det(D_n) = 4)$, its center density is $\delta(D_n) = 2^{-\frac{n}{2}-2}$, its kissing number is $2n(n-1)$, its covering radius is $\mu = 1$, for $n = 3$, and $\mu = \sqrt{\frac{n}{4}}$, for $n \geq 4$. As it can be seen in Table 2.4, D_n has the greatest lattice packing density in $\mathbb{R}^n$ for $n = 3$ (FCC), 4 and 5. The dual D_n^* has minimum distance $\frac{\sqrt{3}}{2}$, for $n = 3$, and 1, for $n \geq 4$.

The Lattice A_n

This lattice, defined in Example 2.3, is a rank-n sublattice of $\mathbb{Z}^{n+1}$ lying in the hyperplane H where the sum of the coordinates is zero $(A_n \subset D_{n+1} \subset \mathbb{Z}^{n+1})$. It has for basis $\{\mathbf{v}_1,\ldots,\mathbf{v}_n\}$ given by $\mathbf{v}_1 = (-1,1,0,\ldots,0)$, $\mathbf{v}_2 = (0,-1,1,0,\ldots,0)$, $\mathbf{v}_3 = (0,0,-1,1,0,\ldots,0),\ldots,\mathbf{v}_n = (0,0,\ldots,0,-1,1)$. If we consider the $(n+1)\times n$ generator matrix B whose columns are these basis vectors, we can see that its volume is $V(A_n) = (\det(B^TB))^{\frac{1}{2}} = n+1$. It has minimum distance $\sqrt{2}$ (minimum distance vectors are in fact given by permuting all the components of $\mathbf{v}_1$), center packing density $\delta = 2^{\frac{-n}{2}}(n+1)^{\frac{-1}{2}}$, kissing number $n(n+1)$, and covering radius $\mu = \frac{\sqrt{2}}{2}(\frac{2a(n+1-a)}{n+1})^{\frac{1}{2}}$, where $a = [(n+1)/2]$ is the integer part of $(n+1)/2$.

As mentioned in Example 2.9, A_2 is equivalent to the hexagonal lattice. Also A_3 is equivalent the lattice D_3 or the FCC lattice (see Exercise 2.7). Both A_2 and A_3 are the densest lattices in their dimensions. The dual lattice A_n^*, considered in the hyperplane H, has a very special Voronoi region given by the permutohedra with vertices being all the permutations of $\frac{1}{(n+1)}(-n, -n+2, -n+4, \ldots, n-2, n)$. As seen in Table 2.4, the lattices A_n^* have the smallest covering density known in several dimensions including dimensions $n = 3$ ($A_n^* = D_n^*$ =BCC), $n = 4, 5$, and $9 \leq n \leq 23$. For $n = 6,7$, and 8, the covering densities of A_n^* are 2.551, 3.060, and 3.666, respectively, and these densities were known to be the smallest in their dimensions until the results of [90] displayed in Table 2.4.

The Lattices E_6, E_7, and E_8

Also called the Gosset lattice after T. Gosset who was one of the first to study its geometry, the lattice E_8 is defined as

$$E_8 = \left\{ \mathbf{x} = (x_1, \ldots, x_8) \in \mathbb{Z}^8 : \mathbf{x} \in D_8 \text{ or } \mathbf{x} + \left(\frac{1}{2}, \ldots, \frac{1}{2}\right) \in D_8 \right\}. \tag{2.17}$$

A generator matrix for E_8 is given by

$$\begin{bmatrix} 2 & -1 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} \\ 0 & 1 & -1 & 0 & 0 & 0 & 0 & \frac{1}{2} \\ 0 & 0 & 1 & -1 & 0 & 0 & 0 & \frac{1}{2} \\ 0 & 0 & 0 & 1 & -1 & 0 & 0 & \frac{1}{2} \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & \frac{1}{2} \\ 0 & 0 & 0 & 0 & 0 & 1 & -1 & \frac{1}{2} \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & \frac{1}{2} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} \end{bmatrix}.$$

The lattice E_8 has minimum distance $\sqrt{2}$ and packing center density $\frac{1}{16}$ and is, up to congruence, the unique lattice in $\mathbb{R}^8$ with these minimum distance and density. It is a unimodular lattice, $E_8^* = E_8$. It is also known to be the unique (up to congruence) unimodular lattice in dimension 8 with even squared minimum distance. (In fact, up to dimension 8, the unique unimodular lattices, up to congruence, are $\mathbb{Z}^n$ and E_8 [26, Chap. 4].) The lattice E_8 has the greatest packing density in dimension 8 not only among lattices but for any *packing* [26, 98]. It has also the smallest known covering density in this dimension. Its name derives from its association with the E_8 root system (see [26, Chap. 4]).

The lattices E_7 and E_6 are lattices of ranks 7 and 6 naturally defined in $\mathbb{R}^8$ as

$$E_7 = \{\mathbf{x} = (x_1, \ldots, x_8) \in E_8 : x_1 = x_2\}, \tag{2.18}$$

$$E_6 = \{\mathbf{x} = (x_1, \ldots, x_8) \in E_8 : x_1 = x_2 = x_3\}. \tag{2.19}$$

Table 2.2 A generator matrix for the Barnes-Wall lattice

$$\left(\frac{1}{\sqrt{2}}\right)\begin{bmatrix}
4&2&2&2&2&2&2&2&2&2&2&1&0&0&0&1\\
0&2&0&0&0&0&0&0&0&0&0&1&1&0&0&1\\
0&0&2&0&0&0&0&0&0&0&0&1&1&1&0&1\\
0&0&0&2&0&0&0&0&0&0&0&1&1&1&1&1\\
0&0&0&0&2&0&0&0&0&0&0&1&1&1&1&1\\
0&0&0&0&0&2&0&0&0&0&0&1&0&1&1&1\\
0&0&0&0&0&0&2&0&0&0&0&1&0&1&1&1\\
0&0&0&0&0&0&0&2&0&0&0&1&0&1&0&1\\
0&0&0&0&0&0&0&0&2&0&0&1&1&0&1&1\\
0&0&0&0&0&0&0&0&0&2&0&0&1&1&0&1\\
0&0&0&0&0&0&0&0&0&0&2&0&0&1&1&1\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1
\end{bmatrix}$$

They can be considered as lattices in $\mathbb{R}^7$ and $\mathbb{R}^8$ and they are known to have the best lattice packing density in their dimensions.

The Barnes-Wall Lattice Λ_{16}

The so-called Barnes-Wall lattices BW_n defined in dimensions $n = 2^k$, k an integer greater than two, were introduced in [8] and have been constructed since then through several different methods, e.g., via the so-called Construction B from Reed-Muller codes [26]. They have some special properties (see [77]). $\Lambda_{16} = BW_{16}$ has the best known packing density in dimension 16. One of its generator matrices is given in Table 2.2.

The Leech Lattice Λ_{24}

The Leech lattice Λ_{24}, introduced by J. Leech in 1964, is a very special full rank lattice in $\mathbb{R}^{24}$. It is unimodular, $\Lambda_{24} = \Lambda_{24}^*$, has the greatest packing density in dimension 24, even considering non-lattice packings, and has the smallest known covering density in this dimension. Its kissing number is 196,560. There are many different constructions for this lattice (see [26, Chap. 24]). A generator matrix of the scaled version of the Leech lattice, $2\sqrt{2}\Lambda_{24}$, is given in Table 2.3.

2.4.1 Table of Record Lattices

In Table 2.4 below, the best known lattices (records) are found with respect to packing density, kissing number, and covering density, but also quantization (or more precisely, the normalized second moment (2.25)), to be approached in Sect. 2.5.1 [26, 90].

The marked boxes (†) display the lattices which were proved to be the best regarding the respective parameter among all the lattices in that dimension. The

Table 2.3 A generator for the Leech lattice Λ_{24} scaled by $2\sqrt{2}$

$$\begin{bmatrix}
8&4&4&4&4&4&4&2&4&4&4&2&4&2&2&2&4&2&2&2&0&0&0&-3\\
0&4&0&0&0&0&0&2&0&0&0&2&0&2&0&0&0&0&0&2&2&0&0&1\\
0&0&4&0&0&0&0&2&0&0&0&2&0&0&2&0&0&2&0&0&2&0&0&1\\
0&0&0&4&0&0&0&2&0&0&0&2&0&0&0&2&0&0&2&0&2&0&0&1\\
0&0&0&0&4&0&0&2&0&0&0&0&0&2&2&2&0&2&2&2&2&0&0&1\\
0&0&0&0&0&4&0&2&0&0&0&0&0&2&0&0&0&0&2&0&0&0&0&1\\
0&0&0&0&0&0&4&2&0&0&0&0&0&0&2&0&0&0&0&2&0&0&0&1\\
0&0&0&0&0&0&0&2&0&0&0&0&0&0&0&2&0&2&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&4&0&0&2&0&2&2&2&0&2&2&2&2&2&2&1\\
0&0&0&0&0&0&0&0&0&4&0&2&0&2&0&0&0&2&0&0&0&2&0&1\\
0&0&0&0&0&0&0&0&0&0&4&2&0&0&2&0&0&0&2&0&0&0&2&1\\
0&0&0&0&0&0&0&0&0&0&0&2&0&0&0&2&0&0&0&2&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&4&2&2&2&0&0&0&0&2&2&2&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&2&0&0&0&0&0&0&0&2&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&2&0&0&0&0&0&0&0&2&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&2&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&2&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&4&2&2&2&2&2&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&2&0&0&0&2&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&2&0&0&0&2&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&2&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&2&2&2&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&2&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&2&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1
\end{bmatrix}$$

lattices A_2, $A_3 \sim D_3 \sim FCC$, E_8, and Λ_{24} were proved to have the best packing density in their dimensions among all packings (not only lattice packings).

It was long believed that A_6^* was the best 6-dimensional covering. Recently, Schurmann and Vallentin [90] have found over 40 lattices with smaller covering density than A_6^* along with the record covering in dimensions 7, 8. We denote the best known lattice coverings presented in [90] in dimensions $n = 6, 7, 8$ by Q_n^1.

Asymptotically, a theorem by Minkowski and Hlawka (cf [20]) guarantees that there exist packings with density lower bounded by $\Delta \geq \zeta(n)/2^{n-1}$, where $\zeta(n) = 1 + 1/2^n + 1/3^n + \ldots$ is the *Riemman zeta function*. Improving this lower bound is still an active subject of research.

Remark 2.4 The classical notations for the lattices A_n, D_n, and E_n used here come from the fact that those lattices are associated with root systems in the context of the theory of Lie algebras which are known by the same symbols [1, 14]. These lattices are then called *root lattices*. The symbol Λ_n is used for a *laminated lattice* [26, Chap. 6] in dimension n. This concept was introduced in [24] to describe a lattice in dimension n constructed from layers of a suitable lattice in dimension $n-1$ in order to get the best possible density, starting from the one-dimensional lattice of

Table 2.4 Best known (record) lattices with respect to packing density, kissing number, covering density, and quantization

Dim	Packing density	Kissing number	Covering density	Quantization
1	$\mathbb{Z}$ $1^{(\dagger)}$	$\mathbb{Z}$ $2^{(\dagger)}$	$\mathbb{Z}$ $1^{(\dagger)}$	$\mathbb{Z}$ $0.0833^{(\dagger)}$
2	A_2 $0.9069^{(\dagger)}$	A_2 $6^{(\dagger)}$	A_2 $1.2092^{(\dagger)}$	A_2 $0.0802^{(\dagger)}$
3	$A_3 \sim D_3$ $0.7450^{(\dagger)}$	A_3 $12^{(\dagger)}$	$A_3^* \sim D_3^*$ $1.4635^{(\dagger)}$	$A_3^* \sim D_3^*$ 0.0785
4	D_4 $0.6169^{(\dagger)}$	D_4 $24^{(\dagger)}$	A_4^* $1.7655^{(\dagger)}$	D_4 0.0766
5	D_5 $0.4653^{(\dagger)}$	D_5 $40^{(\dagger)}$	A_5^* $2.1243^{(\dagger)}$	D_5^* 0.0756
6	E_6 $0.3730^{(\dagger)}$	E_6 $72^{(\dagger)}$	Q_6^1 2.4648*	E_6^* 0.0742
7	E_7 $0.2953^{(\dagger)}$	E_7 $126^{(\dagger)}$	Q_7^1 2.9000	E_7^* 0.0731
8	E_8 $0.2537^{(\dagger)}$	E_8 $240^{(\dagger)}$	Q_8^1 3.2013	E_8 0.0717
16	Λ_{16} 0.0147	Λ_{16} 4320	A_{16}^* 15.3109	Λ_{16} 0.0683
24	Λ_{24} $0.0019^{(\dagger)}$	Λ_{24} $196560^{(\dagger)}$	Λ_{24} $7.9035^{(\dagger)}$	Λ_{24} 0.0657

even integer points and keeping the same minimum norm. We have that $\Lambda_1 \sim \mathbb{Z}$, $\Lambda_2 \sim A_2$, $\Lambda_k \sim D_k$ for $3 \leq k \leq 5$ and $\Lambda_k \sim E_k$ for $6 \leq k \leq 8$. We also have that the Barnes-Wall lattice and the Leech lattice are the unique laminated lattices in dimensions 16 and 24, respectively [26, Chap. 6].

2.5 Applications

2.5.1 Coding

Consider the transmission of a vector $\mathbf{x}$ belonging to a discrete set of points $S \subset \mathbb{R}^n$ over an additive white Gaussian noise (AWGN) channel, meaning that the received signal $\mathbf{y}$ is of the form

$$\mathbf{y} = \mathbf{x} + \mathbf{n} \tag{2.20}$$

where $\mathbf{n}$ is a random vector whose components are independent Gaussian random variables with mean 0 and variance σ^2. The *Gaussian channel coding* problem

consists of figuring out (decoding) $\mathbf{x}$ from $\mathbf{y}$ despite the presence of the noise $\mathbf{n}$. Now if the transmitter had an infinite power at its disposal, given σ^2, it would be easy enough to solve this coding problem: just take the set S, and scale all its vectors enough so that they are well apart, meaning that the distance between any two vectors in S is much larger than $2\sigma^2$. Then choose for the decoded point the lattice point $\mathbf{x}$ which is closest to the received point $\mathbf{y}$. However we do want the transmitter not to waste too much power in transmitting $\mathbf{x}$, which is modeled by a power constraint that all the points of S lie within a sphere of radius $\sqrt{nP}$ around the origin (P thus defines a power constraint). Suppose now that S is a subset carved from a lattice Λ. The receiver will make a correct decision to choose the closest lattice point $\mathbf{x}$ from $\mathbf{y}$ as the decoded point exactly if the noise vector $\mathbf{n}$ falls in the Voronoi region $\mathcal{V}_\Lambda(\mathbf{x})$ of $\mathbf{x}$ (see Fig. 2.15), an event of probability

$$\frac{1}{(\sigma\sqrt{2\pi})^n}\int_{\mathcal{V}(\Lambda)} e^{-||\mathbf{x}||^2/2\sigma^2}\mathrm{d}\mathbf{x}.$$

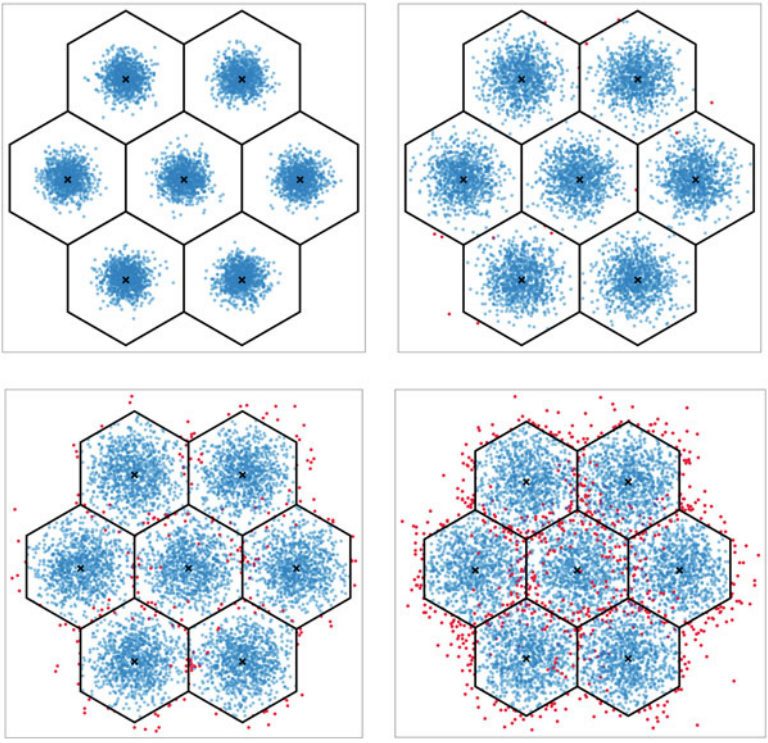


Fig. 2.15 Gaussian noise acting on a hexagonal lattice for $\sigma \in \{0.1, 0.15, 0.2, 0.25\}$. The blue (red) points correspond to received signals lying inside (outside) the Voronoi cell of the sent point

Thus if all points $\mathbf{x}$ are equally likely to be sent, the *error probability* P_e for S of decoding a lattice point $\hat{\mathbf{x}} \neq \mathbf{x}$ when $\mathbf{x}$ is sent is 1 minus the above probability. We thus want to find, given σ, the n-dimensional lattice of volume normalized to 1 for which the error probability P_e is minimized. Unfortunately, the above expression is hard to compute in a closed-form expression. It is thus usual to bound it using the so-called *union bound*.

For the sake of reasoning, suppose that the lattice Λ contains the vector $(1, 0, 0 \ldots, 0)$ and we want to decide whether $\mathbf{n}$ is closer to $(1, 0, \ldots, 0)$ than to the origin; this is equivalent to checking whether the first component of $\mathbf{n}$ is greater than $1/2$, an event that has probability

$$\frac{1}{\sigma\sqrt{2\pi}} \int_{1/2}^{\infty} e^{-x^2/2\sigma^2} \mathrm{d}x \leq \frac{1}{2} e^{-1/8\sigma^2}.$$

This reasoning generalizes to any lattice/lattice point. The probability that $\mathbf{n}$ is closer to some lattice point of norm m is bounded by (see Exercise 2.9) $(1/2)e^{-m^2/8\sigma^2}$. Therefore, the probability of an error event is given by

$$P(\mathbf{n} \text{ is closer to some } \mathbf{x} \in \Lambda \text{ than the origin}) \leq \frac{1}{2} \sum_{\mathbf{x} \in \Lambda \setminus \{0\}} e^{-\|\mathbf{x}\|^2/8\sigma^2}. \tag{2.21}$$

The dominant terms in the sum in the right-hand side of (2.21) are the ones corresponding to vectors with small norms. Therefore, dropping all terms except the ones of minimum norm, the upper bound can be approximated by

$$\frac{\kappa e^{-\rho^2/2}}{2}, \tag{2.22}$$

where we recall that ρ is the *packing radius* and κ denotes the *kissing number* of Λ. This expression is minimized if ρ is maximized (a "secondary" objective is that κ is minimized). Intuitively, we expect the number of points in S to be close to the ratio between the volume of a sphere of radius $\sqrt{nP}$ and the volume of Λ, i.e., $\mathrm{vol}\, \mathscr{B}^n(1)(nP)^n / V(\Lambda)$. Recalling the formula for the density and the approximation $|S| \approx \mathrm{vol}\, \mathscr{B}^n(\sqrt{n}P)/V(\Lambda)$, we can write expression (2.22) for the probability of error as

$$\frac{\kappa e^{-\Delta^{2/n}|S|^{-2/n}}}{2} \tag{2.23}$$

where Δ is the packing density. Therefore, for a fixed number of points, the objective of *minimizing the probability of error (or maximizing the probability of correct decision) can be achieved by maximizing the packing density of the underlying lattice*.

2.5.2 Quantization

Another important application where lattices play an important role is *quantization*. Suppose we want to represent the set of real numbers $\mathbb{R}$ by using finite precision arithmetics and a regular spaced grid. We can assume, up to scaling, that our approximation is going to be performed using the set of integers $\mathbb{Z}$. For each point $y \in \mathbb{R}$, the closest integer is denoted by $Q_{\mathbb{Z}}(y) = [y]$, and the squared error obtained in this approximation is $(Q_{\mathbb{Z}}(y) - y)^2$. Notice that for any point $y \in [-1/2, 1/2)$ (or $(-1/2, 1/2]$, depending on the rounding rule), $Q_{\mathbb{Z}}(y) = 0$ and the quantization error is y^2. Since the integers are regularly spaced, we define the *average* squared quantization error in the process by picking a point $y \in (-1/2, 1/2]$ uniformly at random and taking the average

$$\int_{-1/2}^{1/2} y^2 \mathrm{d}x = \frac{1}{12}.$$

This process can be extended by using extra dimensions to reduce the quantization error. Given a point $\mathbf{x} \in \mathbb{R}^n$ and a lattice $\Lambda \subset \mathbb{R}^n$, we define $Q_\Lambda(\mathbf{x})$ as the closest lattice point[3] to $\mathbf{y}$. Equivalently $Q_\Lambda(\mathbf{y}) = \mathbf{x}$ if and only if $\mathbf{y} \in \mathcal{V}_\Lambda(\mathbf{x})$.

Observe that $\mathbf{y} - Q_\Lambda(\mathbf{y})$ is closer to the origin than any non-zero lattice point, therefore $\mathbf{y} - Q_\Lambda(\mathbf{y}) \in \mathcal{V}_\Lambda(\mathbf{0})$ for any $\mathbf{y} \in \mathbb{R}^n$. Hence, subtracting the closest lattice point from $\mathbf{y}$ wraps the real vector $\mathbf{y}$ into the Voronoi region $\mathcal{V}_\Lambda(\mathbf{0})$ at the origin. This operation, called the *modulo-Λ* function, is denoted as

$$\mathbf{y} \bmod \Lambda = \mathbf{y} - Q_\Lambda(\mathbf{y}).$$

The modulo-Λ operation satisfies the property

$$(\mathbf{y}_1 + \mathbf{y}_2) \bmod \Lambda = (\mathbf{y}_1 \bmod \Lambda + \mathbf{y}_2) \bmod \Lambda \text{ for any } \mathbf{y}_1, \mathbf{y}_2 \in \mathbb{R}^n.$$

The modulo-Λ operation will be discussed more carefully and applied in Chap. 6. Analogous to the one-dimensional case, we define, for a point $\mathbf{x}$ drawn uniformly at random in the Voronoi cell of Λ, the average quantization error

$$E(\Lambda) = \frac{1}{V(\Lambda)} \int_{\mathcal{V}(\Lambda)} \|\mathbf{x}\|^2 \, \mathrm{d}\mathbf{x}, \tag{2.24}$$

[3] Strictly speaking, there might be more than one closest vector to $\mathbf{y}$, which might cause ambiguities. In order for $Q_\Lambda(\mathbf{y})$ to be well defined, one has to break the ties, i.e., to decide which "faces" of the Voronoi cell to use. In order to simplify notation, we will avoid such a technicality and consider that ties are broken according to some well-defined systematic rule. Considering this rule we will also, by abuse of notation, sometimes say "the" closest lattice point to $\mathbf{y}$. Notice that the faces of the Voronoi cell (i.e., the ambiguous points) have measure zero in $\mathbb{R}^n$.

where we use the subscript E_Λ to indicate that the expectation is with respect to a point uniformly distributed over the Voronoi region of Λ. Equation (2.24) gives the average mean squared quantization error, but is not the best choice to compare different lattices, since it does depend on the volume of Λ. For instance, for any scaling factor $\alpha\Lambda$, the quantization error is

$$E(\alpha\Lambda) = \alpha^2 E(\Lambda).$$

To allow a fair comparison between lattices with distinct volumes, we define the normalized second moment per dimension as

$$\mathscr{G}(\Lambda) = \frac{1}{nV(\Lambda)^{2/n+1}} \int_{\mathscr{V}(\Lambda)} \|\mathbf{x}\|^2 \, \mathrm{d}\mathbf{x}. \tag{2.25}$$

This quantity is independent of the volume and of the dimension (Exercise 2.13) but is fairly hard to calculate in general, as it involves an integration over the Voronoi cell of a lattice. Equation (2.25) was used to calculate the last column of Table 2.1.

Best Quantizers How small can the normalized second moment be? For a given volume $V(\Lambda) = V$, the integral in Eq. (2.25) is lower bounded by the integral over an n-dimensional ball of volume V. This gives the bound $\mathscr{G}(\Lambda) > 1/(2\pi e) \sim 0.059$ (e.g., [23]). The best lattices in terms of quantization are therefore, roughly speaking, the ones whose Voronoi cell resembles a ball.

Comparing with Table 2.1, it can be seen that, as the dimension increases, the best normalized second moment decreases. In fact, the ratio between the second moment of the one-dimensional lattice $\mathbb{Z}$ and the best possible quantizer is only[4] 1.42 and can be approached in very high dimensions. This ratio may be interpreted as the gain of using a good high-dimensional lattice over the simple quantizer that only rounds the coordinate of a vector in each dimension. Explicit constructions of lattices exhibiting the full gain are very challenging and not yet known.

2.5.3 Computational Problems and Cryptography

The parameters introduced so far, such as the minimum norm, the packing radius, or the center density, have a clean mathematical formulation, and lattices with record parameters according to them have been listed in Table 2.4 for dimensions up to 8, 16, and 24. Computing these parameters in higher dimensions becomes a computational problem. How easy is it algorithmically to compute, say the density of a given lattice? The answer is that it is usually hard. The main difficulty lies in the fact that calculating the density depends on knowing the packing radius (or

[4] Or approximately 1.53, in decibels. This number is sometimes referred to as the ultimate *shaping gain* of a lattice.

equivalently, the minimum norm (2.10)) of a lattice which, in turn, depends on the description of the given lattice Λ.

For a concrete example, let us consider the hexagonal lattice (Example 2.1). Consider the basis

$$B = \begin{bmatrix} 1 & 1/2 \\ 0 & \sqrt{3}/2 \end{bmatrix}.$$

Each vector in the lattice has the form $B\mathbf{u}$, $\mathbf{u} \in \mathbb{Z}^2$, and has norm $u_1^2 + u_1u_2 + u_2^2$. Since u_1, u_2 are integers, it follows that the minimum norm is 1, attained, for instance, by choosing $u_1 = 1, u_2 = 0$. However, if we are given instead the generator matrix

$$\overline{B} = \begin{bmatrix} 2401 & 96\sqrt{32} \\ 57649/2 & 2305\sqrt{3}/2 \end{bmatrix},$$

it is far from easy to compute that the minimum non-zero squared norm for $5792449u_1^2 + 139079089u_2u_1 + 834836569u_2^2$ is 1, attained by $u_1 = 2305$ and $u_2 = -192$. In fact, if we knew the unimodular transformation that takes B into $\overline{B}$, we could easily recover the minimum from the first basis. This tells us that, in some sense, it is easy to "hide" the minimum norm of a vector by transforming a "good" basis into a "bad one." This high-level idea is the starting point for the constructions of cryptographic primitives based on lattices (the case of public-key cryptography will be explained in more details below). The following problem is known as SVP (**S**hortest **V**ector **P**roblem):

Problem 2.1 (SVP) Given a matrix B, find the minimum norm of the lattice Λ generated by B.
A related problem is the following, known as CVP (**C**losest **V**ector **P**roblem).

Problem 2.2 (CVP) Given a generator matrix B for a lattice $\Lambda \subset \mathbb{R}^n$ and a vector $\mathbf{y} \in \mathbb{R}^n$, find the closest lattice point to $\mathbf{y}$.

This problem is relevant to coding theory, as it can be regarded as a "decoding problem," where $\mathbf{y}$ is a received signal for a message $\mathbf{x} \in \Lambda$ transmitted over a Gaussian channel, as in the previous section. CVP also depends critically on the given basis B. Suppose we start with the lattice $\mathbb{Z}^2$ and the matrix B associated with the canonical basis. Given a point $\mathbf{y} = (y_1, y_2)$, the closest point $\mathbf{x} = B\mathbf{u}$ to $\mathbf{y}$ is the one that minimizes

$$\|\mathbf{y} - \mathbf{x}\| = (y_1 - u_1)^2 + (y_2 - u_2)^2,$$

obtained by rounding the coordinates of $\mathbf{y}_1$, i.e., $u_1 = [y_1]$ and $u_2 = [y_2]$. One can think of a generalization of this algorithm for any generator matrix $\overline{B}$ as follows. First solve the system of equations $\mathbf{y} = \overline{B}\mathbf{u}$, and then round the solution, outputting the point $\mathbf{x} = \overline{B}[\mathbf{u}]$ (this is sometimes known as the Babai point, after the Hungarian mathematician Laszlo Babai). Unfortunately, even for the lattice $\mathbb{Z}^2$, depending on

the basis, this procedure may fall short of any reasonable estimate, as discussed in Exercise 2.12. In general finding the closest vector point to a given lattice basis is, in computational complexity language, an NP-hard problem [72]. This problem is closely related to the quantization problem in Sect. 2.5.1. In fact, in both cases we want to find the closest vector to a given lattice point. However the main difference lies in the fact that, from a complexity perspective, algorithms that solve CVP for *any* generator matrix (or for a large enough class) are sought, whereas from a coding theory perspective, we want to *design* a lattice with an easy CVP solver.

The two problems CVP and SVP, and their many variants, have been employed for cryptographic purposes since 1996 [3]. We provide next a general idea of how *public-key cryptography* can be performed using lattices. Suppose a user (usually called Alice in the cryptography literature) has access to a "good" generator matrix B for a high-dimensional lattice $\Lambda \subset \mathbb{R}^n$. From B, Alice generates a "bad" basis H and makes H publicly available while keeping B secret. Now anyone (say, Bob) with access to H can send an encrypted message $\mathbf{u} \in \mathbb{Z}^n$ as follows. Bob generates a noise vector $\mathbf{n}$ and sends the vector $\mathbf{y} = H\mathbf{u} + \mathbf{n}$ to Alice. Noticing that $\mathbf{x} = B\mathbf{u}$ is a lattice point, if $\mathbf{n}$ is "small" enough, Alice can recover $\mathbf{x}$ by finding the closest lattice point to $\mathbf{y}$. Roughly speaking, a "good" basis is one such that the (very efficient) rounding procedure explained in the previous paragraph will work, whereas for "bad" basis it is hard to guess the correct vector $\mathbf{x}$ (for instance, the rounding procedure will output a vector far from $\mathbf{x}$, as in Exercise 2.12). Therefore, an intruder that intercepts $\mathbf{y}$ and has access to H is not expected to efficiently guess the sent message $\mathbf{x}$.

Of course the above high-level description depends critically on how to choose the noise vector, the "good" and the "bad" basis or, in other words, the private-key B and the public-key H. For further information on this and on other applications of lattices to cryptography, the reader is referred to [73]. We close this section with a word on two relevant notions: special bases and bounds on the shortest vector.

Special Bases The rounding procedure described in this section is not sufficient to solve the closest vector problem and, depending on the chosen basis, may produce very crude estimates. To overcome this problem, we might want to preprocess the basis given to us before trying to find the closest lattice point $\mathbf{x}$ to a given point $\mathbf{y} \in \mathbb{R}^n$. For example, the best possible basis for the integer lattice $\mathbb{Z}^n$ in terms of complexity of finding the closest vector is the canonical basis. However not all lattices possess such a neat basis. Intuitively, a good basis for a lattice Λ is as close as possible from being "orthogonal," with small norm vectors. This notion has been quantified and formalized in several different ways. We present below the notion of Minkowski-reduced basis, arguably the most intuitive way of defining a "good" basis.

We say that a set of vectors $\{\mathbf{b}_1, \ldots, \mathbf{b}_i\} \subset \Lambda$ is *primitive* if it can be extended to a basis of Λ, i.e., if there exist $\{\mathbf{b}_{i+1}, \ldots, \mathbf{b}_n\}$ such that $\{\mathbf{b}_1, \ldots, \mathbf{b}_i, \mathbf{b}_{i+1}, \ldots, \mathbf{b}_n\}$ is a basis for Λ.

Definition 2.15 (Minkowski-Reduced Basis) A basis $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ for a lattice Λ is said to be *Minkowski-reduced if*:

(i) $\mathbf{b}_1$ *is a shortest vector in* Λ *and*

(ii) for any $i = 1, \ldots, n-1$, $\mathbf{b}_{i+1}$ *is a shortest vector in* Λ *such that* $\{\mathbf{b}_1, \ldots, \mathbf{b}_i, \mathbf{b}_{i+1}\}$ *is primitive.*

Given a basis $\alpha = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$, the above conditions (i) and (ii) will imply inequalities to be satisfied by its associated Gram matrix $G = \{b_{ij}\} = \langle \mathbf{b}_i, \mathbf{b}_j \rangle$ for this basis to be Minkowski-reduced. Some of these inequalities are [26, Chap. 15, 10.1]:

(A) $0 < b_{11} \leq b_{22} \leq \ldots \leq b_{nn}$
If $\mathbf{v} = \mathbf{b}_t - \sum_{s \in S} \epsilon_s \mathbf{b}_s$ (for some set S of subscripts $s < t$ and $\epsilon_s = \pm 1$), the inequality $\|\mathbf{b}_t\| \leq \|\mathbf{v}\|$ becomes

(B) $$2 \left| \sum_{s \in S} \epsilon_s b_{st} - \sum_{r,s \in S} \epsilon_r \epsilon_s b_{rs} \right| \leq \sum_{s \in S} b_{ss}.$$

For the cases $S = \{i\}$, $S = \{i, j\}$, and $S = \{i, j, k\}$, the above condition B can be written as:

(B1) $2 \left| b_{ij} \right| \leq b_{ii}$, $(i < j)$;
(B2) $2 \left| b_{ij} \pm b_{ik} \pm b_{jk} \right| \leq b_{ii} + b_{jj}$, $(i < j < k)$; and
(B3) $2 \left| \epsilon_1 b_{ir} + \epsilon_2 b_{jr} + \epsilon_3 b_{kr} - \epsilon_1 \epsilon_2 b_{ij} - \epsilon_1 \epsilon_3 b_{ik} - \epsilon_2 \epsilon_3 b_{jk} \right| \leq b_{ii} + b_{jj} + b_{kk}$, $(i < j < k < r)$

For $n = 2$, $n = 3$, and $n = 4$, the simultaneous conditions A and B1; A, B1, and B2; and A, B1, B2, and B3, respectively, are also sufficient to assure that the basis is Minkowski-reduced [26]. These characterizations can be used in Exercises 2.3 and 2.8. Note that condition B is related to the "more orthogonal" characteristic required for such bases. As it can be shown in Exercise 2.3, $\{(1, 1, 0), (1, 0, 1), (0, 1, 1)\}$ is a basis for the FCC lattice composed by vectors of minimum norm, but it is not Minkowski-reduced since condition B2 is not verified.

Any lattice has a Minkowski-reduced basis, but unfortunately, for high dimensions, there is no simple characterization, and producing such a basis is computationally hard. It entails, for instance, calculating the shortest vector and, therefore, should be at least as hard as solving SVP [2]. One widely used relaxation in the literature is the definition of LLL-reduced basis [73], which provides relatively small vectors and can be computed with fast algorithms. For a thorough formal complexity discussion on reduced bases and other computational aspects, the reader is referred to [73].

Minkowski Theorem If we were to search the shortest lattice vector to solve Problem 2.1 by looking at all points inside a ball, how large should the radius of this ball be? The following fundamental bound due to Minkowski gives a first approach to this question.

Theorem 2.4 *The minimum norm* λ *of a full rank lattice* $\Lambda \subset \mathbb{R}^n$ *satisfies*

$$\lambda \leq \sqrt{n} V(\Lambda)^{1/n}. \tag{2.26}$$

Before proving the theorem, we perform a quick sanity check. If Λ is scaled by $\alpha > 0$, then its minimum norm is also scaled by $\alpha > 0$, while its volume is scaled by α^n. The term $V(\alpha\Lambda)^{1/n} = \alpha V(\Lambda)^{1/n}$ then guarantees that the bound scales appropriately.

Proof From the expression for the density of Λ (2.13), we have

$$\Delta(\Lambda) = \frac{\text{vol}\,\mathscr{B}^n(\rho)}{V(\Lambda)} = \left(\frac{\lambda}{2}\right)^n \frac{\text{vol}\,\mathscr{B}^n(1)}{V(\Lambda)} \leq 1 \Rightarrow$$

$$\lambda \leq 2V(\Lambda)^{1/n}/\text{vol}\,\mathscr{B}^n(1)^{1/n}.$$

To finish the proof, we have to bound the volume of a unit ball. Notice that a maximal inscribed cube in the ball $\mathscr{B}^n(1)$ has diagonal length 2 and side length $2/\sqrt{n}$ (Exercise 2.11). In particular, we have the inclusion $[-1/\sqrt{n}, 1/\sqrt{n}]^n \subset \mathscr{B}^n(1)$, which implies the inequality

$$\text{vol}\,\mathscr{B}^n(1) \geq (2/\sqrt{n})^n.$$

□

A slightly tighter upper bound can be obtained by noticing that

$$(\text{vol}\,\mathscr{B}^n(1))^{1/n} \sim \sqrt{\frac{2\pi e}{n}} \tag{2.27}$$

in high dimensions (this follows from (2.14) and from Stirling's approximation for the factorial, e.g., [26]). The upper bound (2.26) can be far from tight, even for the simplest example $\Lambda = \mathbb{Z}^n$. However, the Minkowski-Hlawka *lower* bound briefly mentioned in Sect. 2.4.1, combined with (2.27), implies that there exist lattices with minimum norm at least $\sim V(\Lambda)^{1/n}\sqrt{n/2\pi e}$.

Remark 2.5 The ratio $\lambda^2/V(\Lambda)^{2/n}$ is called the Hermite parameter of Λ (and is of course, closely related to the packing density). The previous discussions show that the Hermite parameter of the densest n-dimensional lattice should grow linearly with n.

For the closest vector Problem 2.2, bounds of the same nature as that of Theorem 2.26 for the SVP are far more complicated. From the definition of the covering radius μ, the distance from any point to a closest lattice point should not exceed μ. However, there is no simple way of bounding μ. A very useful (nontrivial) bound is $\mu\lambda^* \leq n/2$; here λ^* is the minimum norm of Λ^*. A proof for this result is out of the scope of the book and can be found in [6].

Exercises

Exercise 2.1 Verify that the sets $\{(1,1),(-1,1)\}$ and $\{\{(2,0,0),(1,1,0),(1,0,1)\}$ in Example 2.4 are bases for D_2 and D_3, according to the definition of D_n.

Exercise 2.2 Show that an $m \times m$ matrix is unimodular (has integer entries and determinant 1 or -1) if and only if it has integer entries and is invertible and its inverse matrix has also integer entries. (Hint: Recall determinant properties and the expression for the inverse of a matrix in terms of its cofactors.)

Exercise 2.3 Show as a direct consequence of Theorem 1.2 that two full rank square matrices A and B generate the same lattice if and only if $B^{-1}A$ is a unimodular matrix and use this result to check if the sets $\alpha = \{(-1,-1,0),(1,-1,0),(0,1,-1)\}$ and $\beta = \{(1,1,0),(1,0,1),(0,1,1)\}$ are bases for the FCC lattice and if the set $\gamma = \{(1,-1,1),(1,1,-1),(1,1,1)\}$ is a basis for the BCC lattice (see Example 2.4). Show also (checking the conditions A, B1, and B2 just after Definition 2.15) that α and γ are Minkowski-reduced bases for these lattices but β is not.

Exercise 2.4

(a) Determine the Voronoi regions of the lattices in Examples 2.1, 2.2, and 2.5, and check with Fig. 2.5.
(b) Design the Voronoi region of the BCC and FCC lattices (Examples 2.3 and 2.4).

Exercise 2.5 Consider a full rank lattice Λ. Prove that a fundamental parallelotope $\mathscr{P}(B)$ of Λ tiles $\mathbb{R}^n$ by verifying (i) and (ii) (Eq. (2.7)).

Exercise 2.6 Prove that if $\Lambda_1 \sim \Lambda_2$, then $\Lambda_1^* \sim \Lambda_2^*$.

Exercise 2.7 Show that the lattice A_3 introduced in Example 2.3 is equivalent to the lattice D_3 from Example 2.4 (which is also the lattice *FCC*). You may use the technique of Example 2.9.

Exercise 2.8 This exercise explores several lattice concepts in dimension 2. Consider the lattice Λ in $\mathbb{R}^2$ generated by $\{(1,11),(2,18)\}$.

(a) Look for a "good" basis and find the minimum distance of the lattice. Is your basis a Minkowski-reduced one?
(b) Describe a fundamental parallelotope of your choice, the Voronoi region and another fundamental region.
(c) Find the packing and the covering radii, the kissing number, and the packing and covering densities of Λ.
(d) Find a rectangular sublattice Λ' of Λ and the coset classes of $\frac{\Lambda}{\Lambda'}$.
(e) Determine the dual lattice, Λ^*, and its relevant parameters.
(f) Illustrate the relation $\Lambda \subseteq \Lambda^* \subseteq (\frac{1}{V(\Lambda)^2})\Lambda$ (since Λ is an integer lattice). What lattice do you think is "better," in some sense, Λ or Λ'?

Exercise 2.9 Prove that the probability that $\mathbf{n}$ is closer to a point of norm m than to the origin is upper bounded by $(1/2)e^{-m^2/8\sigma^2}$.
(*Hint:* First show that the inner product $\langle \mathbf{n}, \mathbf{x} \rangle$ has normal distribution with variance $\|\mathbf{x}\|^2 \sigma^2$.)

Exercise 2.10 Show that the dual of the hexagonal lattice is equivalent to itself. Identify the associated rotation and scaling factor.

Exercise 2.11 A rectangle $\mathscr{R} \subset \mathbb{R}^n$ is a set of the form

$$\mathscr{R} = \{\mathbf{x} \in \mathbb{R}^n : x_i \in [a_i, b_i], i = 1, \ldots, n\} = [a_1, b_1] \times \ldots \times [a_n, b_n],$$

for integers $a_i < b_i$. The volume of a rectangle is $(b_1 - a_1) \times (b_2 - a_2) \times (b_n - a_n)$. Show that the rectangle with the smallest volume contained in $\mathscr{B}^n(1)$ is a *cube* with $a_i = -1/\sqrt{n}$ and $b_i = 1/\sqrt{n}$ (or any of its rotations).

Exercise 2.12 Let B be the matrix

$$\begin{bmatrix} 4390 & 133 \\ 439033 & 13301 \end{bmatrix}$$

and $\mathbf{y} = (1.3, -1.9)$.

(a) Using the matrix B and the rounding procedure described in Sect. 2.5.1, find an estimate for the closest point to the lattice generated by Λ.
(b) Check that the lattice generated by B is equal to $\mathbb{Z}^2$. Compare the solution to a) with the actual closest lattice point.

Exercise 2.13 The *cartesian product* between two full rank lattices $\Lambda_1 \subset \mathbb{R}^{n_1}$ and $\Lambda_2 \subset \mathbb{R}^{n_2}$ is defined as

$$\Lambda_1 \times \Lambda_2 = \{(x_1, \ldots, x_{n_1}, y_1, \ldots, y_{n_2}) \in \mathbb{R}^n : (x_1, \ldots, x_{n_1}) \in \Lambda_1 \text{ and } (y_1, \ldots, y_{n_2}) \in \Lambda_2\},$$

where $n = n_1 + n_2$. For instance, $\mathbb{Z} \times \mathbb{Z} = \mathbb{Z}^2$. Show that, for any lattice $\Lambda \subset \mathbb{R}^n$:

a) The normalized second moment (2.25) of $\Lambda \times \Lambda$ equals $\mathscr{G}(\Lambda)$
b) For any lattice Λ, $\mathscr{G}(\alpha\Lambda) = \mathscr{G}(\Lambda)$.

Exercise 2.14 (*) Calculate $\mathscr{G}(A_2)$.
(*Hint:* Use the Voronoi cell computation of Exercise 2.4.)

Chapter 3
Lattices from Codes

3.1 Construction A

A natural way of constructing lattices is from error-correcting codes, using the so-called Construction A. It associates a lattice in $\mathbb{R}^n$ to a linear code in $\mathbb{Z}_q^n$ (the set $\mathbb{Z}_q$ of integers modulo q will be introduced next). Such lattices are also called q-ary lattices (or modulo-q lattices) and have several applications in information theory and cryptography. Lattice-based cryptographic schemes are usually built on q-ary lattices and are linked to the computational difficulty of the shortest and closest vector problems (SVP and CVP, defined respectively in Problems 2.1 and 2.2) in this class [73]. Regarding applications to information theory, Construction A is employed, for instance, in the development of good (capacity-achieving) codes for the Gaussian channel, for some channels with side information [111], as well as for wiretap coding.

The theory of error-correcting codes has been extensively developed (see, e.g., comprehensive books such as [53] and [66]). We will focus here on q-ary codes, that is, codes which have $\mathbb{Z}_q$ as their "alphabet," and provide a self-contained elementary introduction.

For $q \geq 2$ a positive integer, consider the set $\mathbb{Z}_q = \{0, 1, \ldots, q-1\}$ of integers modulo q, where $a \pmod q$ means for a given $a \in \mathbb{Z}$, the set of integers $a + bq$, $b \in \mathbb{Z}$, and by convention a is typically chosen to be between 0 and $q-1$. In this set, addition and multiplication modulo q are well defined. For example, in $\mathbb{Z}_5$, $3+4 = 2, 2\cdot 3 = 1$, and $-3 = 2$. There is a significant structural difference between $\mathbb{Z}_q$, where q is a composite number, and $\mathbb{Z}_p$, where p is a prime number. When q is a composite number, say $q = m_1 m_2$, $m_1, m_2 \neq 0$, then $\mathbb{Z}_q$ contains non-zero elements which are not invertible with respect to multiplication. For instance, m_1, m_2 are such elements. Indeed, if m_1 were invertible, then there would exist an element $a \in \mathbb{Z}_q$ such that $m_1 a = 1$, but then $m_2 m_1 a = m_2 = qa = 0$, a contradiction.When p

S.I.R. Costa et al., *Lattices Applied to Coding for Reliable and Secure Communications*, SpringerBriefs in Mathematics,
https://doi.org/10.1007/978-3-319-67882-5_3

is a prime, such a behavior cannot happen and $\mathbb{Z}_p$ has a field structure, which $\mathbb{Z}_q$, $q = m_2 m_1$ does not have, and for this reason, we will use also the notation $\mathbb{F}_p$ to denote $\mathbb{Z}_p$ and emphasize this difference.

In the Cartesian product $\mathbb{Z}_q^n$, we consider the component-wise sum and multiplication modulo q. If $q = p$ is prime $\mathbb{Z}_p^n = \mathbb{F}_p^n$ is a vector space over the field $\mathbb{Z}_p = \mathbb{F}_p$, which does not hold if q is composite number. A linear code C in $\mathbb{Z}_q^n$ is by definition a subset which is an additive subgroup of $\mathbb{Z}_q^n$. Vectors in C are called codewords. Note that $\mathbf{0} \in C$, since it is the identity element of the group, that $\mathbf{a}, \mathbf{b} \in C$ implies $\mathbf{a} + \mathbf{b} \in C$ (this is the closure property for a group) and that $c\mathbf{a} \in C$ for $\mathbf{a} \in C$ and c any element of $\mathbb{Z}_q$: this is also a consequence of the closure property: $\underbrace{\mathbf{a} + \mathbf{a} + \ldots + \mathbf{a}}_{c \text{ times}} = c\mathbf{a} \in C$. As an example, $C = \{a(1,2), a \in \mathbb{Z}_5\} = \{(0,0), (1,2), (2,4), (3,1), (4,3)\}$ is a linear code in $\mathbb{Z}_5^2$. If $q = p$ is prime, a linear code is a subspace of dimension k of the vector space $\mathbb{Z}_p^n = \mathbb{F}_p^n$ (called an (n,k) code). In this last example, the code C is the subspace of $\mathbb{Z}_5^2$ of dimension 1 generated by the vector $(1,2)$, and we use the notation $C = \langle (1,2) \rangle$.

Next we establish a connection between linear codes in $\mathbb{Z}_q^n$ and lattices. Let

$$\rho : \mathbb{Z} \to \mathbb{Z}_q = \{0, 1, \ldots, q-1\},\ x \mapsto x \ (\mathrm{mod} q),$$

be the map of reduction modulo q. Given $a \pmod q$, its pre-image $\rho^{-1}(a)$ is the set of integers that are mapped to a by ρ (see Fig. 3.1a), that is $\rho^{-1}(a) = \{a + bq,\ b \in \mathbb{Z}\}$.

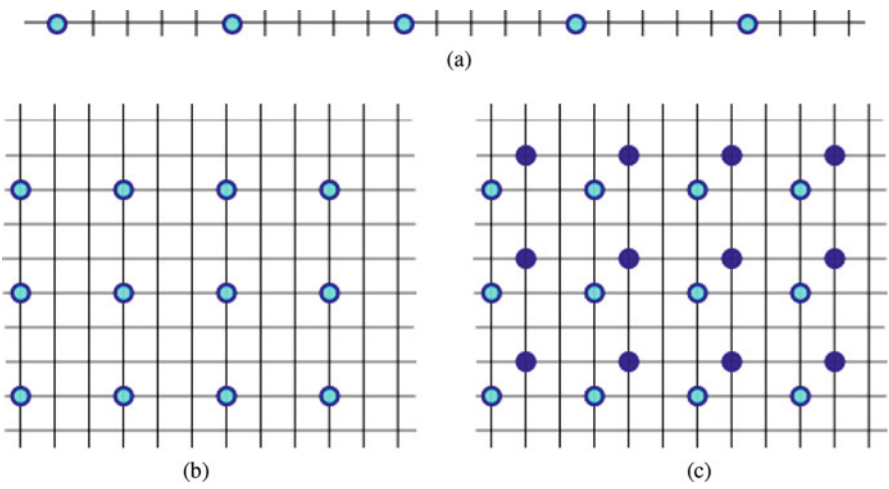


Fig. 3.1 Preimages $\rho^{-1}(S)$ for different sets S. (**a**) The pre-image $\rho^{-1}(a) \subset \mathbb{Z}$ of $a \pmod 5$. (**b**) The pre-image $\rho^{-1}((a_1, a_2)) \subset \mathbb{Z}^2$ of $(a_1 \pmod 3, a_2 \pmod 3)$. (**c**) The pre-image $\rho^{-1}(S) \subset \mathbb{Z}^2$ of $S = \{(a_1 \pmod 3, a_2 \pmod 3), (a_1 + 1 \pmod 3, a_2 + 1 \pmod 3)\}$

Now consider the Cartesian product of integers modulo q, namely, $\mathbb{Z}_q \times \mathbb{Z}_q$. An element in this set is a *two*-dimensional vector (a_1, a_2) of integers modulo q. Let

$$\rho : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}_q \times \mathbb{Z}_q, \ (x_1, x_2) \mapsto (x_1 \ (\mathrm{mod} q), x_2 \ (\mathrm{mod} q)),$$

be the map of reduction modulo m component-wise. The pre-image $\rho^{-1}((a_1, a_2))$ is now the set of 2-dimensional vectors with integer entries that is mapped to a_1, a_2 by ρ (see Fig. 3.1b).

One could alternatively consider a set $S \subset \mathbb{Z}_q \times \mathbb{Z}_q$ and $\rho^{-1}(S)$, which is again the set of 2-dimensional vectors which are mapped to elements in S by ρ (see Fig. 3.1c for an example). Geometrically this inverse image spreads the set S from the inside of the $[0, q) \times [0, q)$ box into the plane.

The map ρ can be defined component-wise over an arbitrary number n of copies of $\mathbb{Z}_q$:

$$\rho : \mathbb{Z}^n \to \mathbb{Z}_q^n, \ \mathbf{x} \mapsto \rho(\mathbf{x})$$

by taking the reduction modulo q component-wise, over the n components of $\mathbf{x}$. Now one may take any arbitrary subset S of $\mathbb{Z}_q^n$ and compute $\rho^{-1}(S)$, but it is more interesting to start with S a subset that has a structure and to understand how this structure is carried over to $\rho^{-1}(S)$. We are next interested in $\rho^{-1}(S)$ where $S \subset \mathbb{Z}_q^n$ is a linear code.

We start with a result which relies on the additive group structure of $C \subset \mathbb{Z}_q^n$ and thus holds for any q.

Proposition 3.1 *Given a subset $S \subset \mathbb{Z}_q^n$, then $\rho^{-1}(S)$ is a lattice in $\mathbb{R}^n$ if and only if S is a linear code in $\mathbb{Z}_q^n$.*

Proof Suppose $S \subset \mathbb{Z}_q^n$ is a linear code. We need to check that $\rho^{-1}(C)$ is a discrete additive subgroup of $\mathbb{R}^n$ (Theorem 2.1). Since $\rho^{-1}(C) \subset \mathbb{Z}^n$, it is a discrete subset of $\mathbb{R}^n$. We next show that it is an additive subgroup.

Take $\mathbf{x}, \mathbf{y}$ two arbitrary vectors in $\rho^{-1}(C)$. To ensure closure under addition, their sum must belong to $\rho^{-1}(C)$. But $\mathbf{x} + \mathbf{y} \in \rho^{-1}(C)$ is equivalent to say that $\rho(\mathbf{x} + \mathbf{y})$ is a codeword in C. Now (in what follows q could be either prime or composite)

$$\begin{aligned} \rho(\mathbf{x} + \mathbf{y}) &= (x_1 + y_1 \ (\mathrm{mod}\ q), \ldots, x_n + y_n \ (\mathrm{mod}\ q)) \\ &= (x_1 \ (\mathrm{mod}\ q), \ldots, x_n \ (\mathrm{mod}\ q)) + (y_1 \ (\mathrm{mod}\ q), \ldots, y_n \ (\mathrm{mod}\ q)) \\ &= \rho(\mathbf{x}) + \rho(\mathbf{y}). \end{aligned}$$

Since $\mathbf{x}$ and $\mathbf{y}$ were chosen in $\rho^{-1}(C)$, this means that $\rho(\mathbf{x})$ and $\rho(\mathbf{y})$ are codewords, and since a code C is closed under addition, $\rho(\mathbf{x}) + \rho(\mathbf{y}) \in C$, thus $\rho(\mathbf{x} + \mathbf{y}) \in C$ as needed.

Since $\mathbf{0} \in C \in \mathbb{Z}_q^n$, $\mathbf{0} \in \rho^{-1}(C) \in \mathbb{Z}^n$.

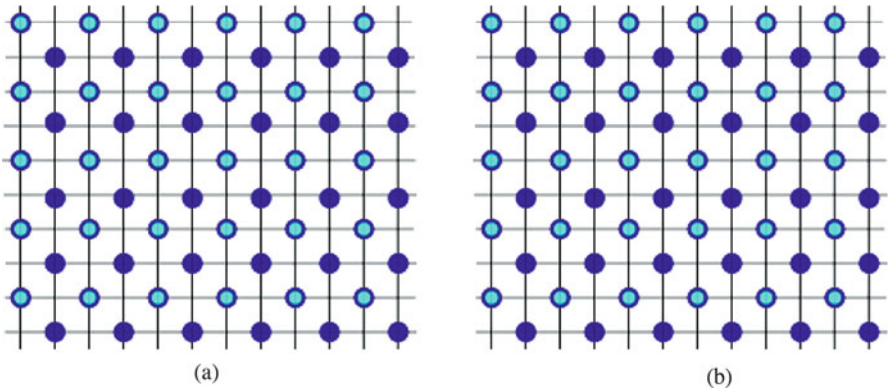


Fig. 3.2 Preimages $\rho^{-1}(S)$ for different sets S. (**a**) The pre-image $\rho^{-1}(S) \subset \mathbb{Z}^2$ of $S = \{(a_1 \pmod 3), a_2 \pmod 3), (a_1 + 1 \pmod 3), a_2 + 1 \pmod 3))\}$. (**b**) The pre-image $\rho^{-1}(C) \subset \mathbb{Z}^2$ of the linear binary code $C = \{(0,0),(1,1)\}$

We are left to check that $-\mathbf{x} \in \rho^{-1}(C)$ whenever $\mathbf{x} \in \rho^{-1}(C)$ or equivalently $\rho(-\mathbf{x}) \in C$ whenever $\rho(\mathbf{x}) \in C$. But

$$\rho(-\mathbf{x}) = (-x_1 \pmod q, \ldots, -x_n \pmod q) = -\rho(\mathbf{x}),$$

and it belongs to C since $c\mathbf{a} \in C$ for any scalar c (here $c = -1 \pmod q$).

The converse is left as an exercise (see Exercise 3.1), namely, to show that for $S \subset \mathbb{Z}_q^n$, if $\rho^{-1}(S)$ is a lattice in $\mathbb{R}^n$, then S is a linear code.

This proposition is illustrated in Fig. 3.2b. Take $C = \{(0,0),(1,1)\}$ over $\mathbb{F}_2 = \mathbb{Z}_2$. It is a linear code, because $(0,0) + (0,0)$, $(0,0) + (1,1)$, and $(1,1) + (1,1)$ all belong to C, using vector addition modulo 2. Also $(0,0) \in C$ and since the only two scalars are $0, 1$, $c(0,0)$ and $c(1,1)$ are both in C, for $c \in \{0,1\}$. As a linear code, it has dimension 1 and basis given by $(1,1)$. We can appreciate the nice lattice structure of $\rho^{-1}(C)$ in the illustration. On the other hand, take $S = \{(0,0),(1,1)\}$ but this time modulo 3. Then $(1,1) + (1,1)$ does not belong to S, so S is not a linear code, and $\rho^{-1}(S)$ is not a lattice either, as is clear from Fig. 3.2a.

Definition 3.1 Let C be a linear code in $\mathbb{Z}_q^n$, the integers modulo a positive integer $q \geq 2$, where q is either prime or composite. Let $\rho : \mathbb{Z}^n \to \mathbb{Z}_q^n$ be the component-wise reduction modulo q. Then the lattice $\Lambda_C = \rho^{-1}(C)$ is said to have been obtained via *Construction A*.

The lattice Λ_C is also known as a q-ary lattice or modulo q lattice. Note that, since $0 \in C$, $q\mathbf{e}_i \in \Lambda_C$, for all canonical vectors $\mathbf{e}_i$, hence we have that $q\mathbb{Z}^n$ is a sublattice of Λ_C and the lattice inclusions $q\mathbb{Z}^n \subset \Lambda_C \subset \mathbb{Z}_q^n$. On the other hand, any lattice Λ in $\mathbb{R}^n$ satisfying $q\mathbb{Z}^n \subset \Lambda \subset \mathbb{Z}_q^n$ is obtained from the code $C = \rho(\Lambda)$ via Construction A, and so this is an equivalent definition of q-ary lattice as it is used in lattice-based cryptography [73]. Other straightforward properties of Construction A lattices are described next:

Proposition 3.2

a) If Λ_C is the q-ary lattice associated to the code $C \subseteq \mathbb{Z}_q^n$, then: $\left|\frac{\Lambda_C}{q\mathbb{Z}^n}\right| = \frac{q^n}{V(\Lambda_C)} = |C|$, *where $|C|$ is the number of codewords of C.*

b) Any full rank integer lattice $\Lambda \subseteq \mathbb{Z}^n$ is q-ary for $q = V(\Lambda)$.

Proof The first property is direct, due to the isomorphism between $\Lambda_C/q\mathbb{Z}^n$ and C. The second one comes from the fact that since $\Lambda \subset \mathbb{Z}^n$, it follows that its volume $V(\Lambda) \in \mathbb{Z}$. Taking a generator matrix B for Λ and $q = V(\Lambda) = |det(B)|$, the linear system $B\mathbf{x} = q\mathbf{z}$ has an integer solution for any $\mathbf{z} \in \mathbb{Z}^n$, and therefore $q\mathbb{Z}^n \subset \Lambda$ (Λ is a q-ary lattice).

If q is prime, a code C is a subspace of dimension $k \leq n$ of $\mathbb{Z}_q^n = \mathbb{F}_q^n$ and hence has q^k codewords. From the last proposition, we have that $V(\Lambda_C) = q^{n-k}$.

A generator matrix (Definition 2.2) is a convenient explicit way to describe a lattice, especially for computations and applications. A generator matrix of the lattice $\rho^{-1}(C)$ can be obtained from that of C. Let us thus see how to obtain such a generator matrix, for both $\mathbb{F}_p$ and $\mathbb{Z}_q$.

If p is prime, the linear (n, k) code C over $\mathbb{Z}_p = \mathbb{F}_p$ is a subspace and has a basis, formed by k vectors. These k vectors can be stacked in a matrix, either as row or column vectors, depending on the convention, to form a generator matrix. Using the column convention adopted here, we get an $n \times k$ matrix M with elements in $\mathbb{Z}_p$ such that any codeword of C can be written as $M\mathbf{y}$, where $\mathbf{y}$ is a column vector of $\mathbb{Z}_p^k$. Note also that in this case, up to coordinate permutation, any code has a generator matrix in the reduced systematic form,

$$\begin{bmatrix} \mathbf{I}_k \\ A \end{bmatrix}$$

where $\mathbf{I}_k$ is the k-dimensional identity matrix, and A is an $(n-k) \times n$ matrix.

For C a linear code in $\mathbb{Z}_q^n$, where q is a composite number, we also have a generator matrix, which contains vectors that generate C as its columns; however, these vectors do not always form a basis, and we may not have a generator matrix in systematic form. We will illustrate and explain why next.

Example 3.1 Consider the linear codes

$$C_1 = \{(2a, 2b, a+b),\ a, b \in \mathbb{F}_3\},\ C_2 = \{(2a, 2b, a+b),\ a, b \in \mathbb{Z}_4\}.$$

The code over $\mathbb{F}_3$ has dimension 2, length $n = 3$, and contains 9 codewords

$$(0,0,0), (0,2,1), (0,1,2), (2,0,1), (2,2,2), (2,1,0), (1,0,2), (1,0,2), (1,1,1).$$

A generator matrix is

$$M = \begin{bmatrix} 2 & 0 \\ 0 & 2 \\ 1 & 1 \end{bmatrix}$$

since a codeword in the column form is this matrix multiplied by $\begin{bmatrix} a & b \end{bmatrix}^T$. Another generator matrix of C_1 is the reduced echelon form of M, obtained by multiplying both columns by 2:

$$R = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 2 & 2 \end{bmatrix}.$$

The code C_2 over $\mathbb{Z}_4$ has length $n = 3$ and contains 8 codewords:

$$(0,0,0), (2,0,1), (0,0,2), (2,0,3), (0,2,1), (2,2,2), (0,2,3), (2,2,0).$$

The above matrix M is again a generator matrix for C_2; only this time, it is not possible to multiply or combine its columns to obtain $(1,0)$ and $(0,1)$ as first two rows. The vectors $(2,0,1)$ and $(0,2,1)$ do not form a basis, because a basis needs to satisfy linear independence. Here

$$\lambda_1(2,0,1) + \lambda_2(0,2,1) = 0$$

does not imply $\lambda_1 = \lambda_2 = 0$ since it could also be $\lambda_1 = \lambda_2 = 2$.
Now that we know what generator matrices are for linear codes, let us go back to generator matrices for the lattices obtained via Construction A.

Since C is a linear code, we saw above that each codeword $\mathbf{a} \in C$ can be written using a set of generators, say $\mathbf{a} = \sum_{i=1}^{l} a_i \mathbf{v}_i$, $\mathbf{v}_i = (v_{i1}, \ldots, v_{in})$ for $i = 1, \ldots, l$ (and $l = k$ for the case of a linear (n,k) code over $\mathbb{F}_p$). Now

$$\mathbf{a} = \sum_{i=1}^{l} a_i \mathbf{v}_i \in C \iff \rho^{-1}(\mathbf{a}) = \sum_{i=1}^{l} a_i \mathbf{v}_i + \sum_{i=1}^{n} q h_i \mathbf{e}_i \in \mathbb{R}^n$$

where $0 \leq a_i, v_{ij} \leq m-1$ for all i, j, $\mathbf{e}_i$, $i = 1, \ldots, n$ form the canonical basis of $\mathbb{R}^n$ and $h_1, \ldots, h_n \in \mathbb{Z}$. In words, $\rho^{-1}(\mathbf{a})$ is an integral linear combination of $\mathbf{v}_1, \ldots, \mathbf{v}_l, q\mathbf{e}_1, \ldots, q\mathbf{e}_n$. An expanded generator matrix B can thus be obtained as follows: stack all the column vectors in an $n \times (n+l)$ matrix. Now we would like to obtain a row echelon form for this matrix, except that because we are working with a lattice, only $\mathbb{Z}$-linear combinations are allowed, and we can only perform elementary operations on the columns which consist of additions and subtractions (divisions are not allowed, unlike for the echelon form). The notion of reduced echelon form is,

over $\mathbb{Z}$, formally replaced by that of *Hermite normal norm (HNF)* . We say that an integer matrix of full row rank is in (column) Hermite normal form if it is of the form $[H\ \mathbf{0}]$ with $H = (h_{ij})$ a square matrix and

1. $h_{ij} = 0$ for $i < j$, which means the matrix H will be lower triangular.
2. $0 \leq h_{ij} < h_{ii}$ for $i > j$, that is entries are nonnegative, and each row has a maximum entry on the diagonal.

Note that any matrix B with integer entries can be reduced to a column Hermite normal form, $B = [H\ \mathbf{0}]U$, where U is a square unimodular matrix. If B is full row rank as it is the case of the expanded generator matrix of Λ_C above, then H is also full rank. For algorithms that compute the HNF, see, e.g., [21, p. 67, 68; algorithm included]. Mathematical software packages such as Mathematica, Maple, MATLAB, Scilab, and Sage also have implemented algorithms. Usually those algorithms appear in the Hermite row form, so for the column form used here, it should be adapted via transposed matrices.

Proposition 3.3 *Let $\mathbf{v}_1, \ldots, \mathbf{v}_l$ be generators for the linear code C over $\mathbb{Z}_q$ and $\mathbf{e}_1, \ldots, \mathbf{e}_n$ be the canonical basis of $\mathbb{R}^n$. Then a generator matrix for the lattice $\rho^{-1}(C)$ is given by the $n \times n$ full rank matrix H obtained by computing the Hermite normal form $[H\ \mathbf{0}]$ of $[\mathbf{v}_1, \ldots, \mathbf{v}_l, q\mathbf{e}_1, \ldots, q\mathbf{e}_n]$. If the generator matrix of C can be put in systematic form*

$$\begin{bmatrix} \mathbf{I}_l \\ A \end{bmatrix},$$

(which, up to coordinate permutation, is always the case for $\mathbb{Z}_p = \mathbb{F}_p$ (and $l = k$) and may or may not be possible otherwise), then a generator matrix of Λ_C is

$$\begin{bmatrix} \mathbf{I}_l & \mathbf{0}_{l\times(n-l)} \\ A & q\mathbf{I}_{n-l} \end{bmatrix}.$$

Proof We already know from above that $\mathbf{v}_1, \ldots, \mathbf{v}_l, q\mathbf{e}_1, \ldots, q\mathbf{e}_n$ generate the lattice, we just need to extract a basis by computing the Hermite normal form out of the $n \times (n + l)$ matrix

$$\left[\mathbf{v_1}, \ldots, \mathbf{v}_l, q\mathbf{e}_1, \ldots, q\mathbf{e}_n\right],$$

which looks like $[H\ \mathbf{0}]$, and H clearly contains a basis. In the case C has a generator matrix in systematic form, then we need to compute a Hermite normal form out of

$$\begin{bmatrix} \mathbf{I}_l & q\mathbf{I}_l & \mathbf{0}_{l\times(n-l)} \\ A & \mathbf{0}_{(n-l)\times l} & q\mathbf{I}_{n-l} \end{bmatrix}.$$

Multiplying the first l columns by $-q$ and adding them to the next l columns give

$$\begin{bmatrix} \mathbf{I}_l & \mathbf{0}_l & \mathbf{0}_{l\times(n-l)} \\ A & -qA & q\mathbf{I}_{n-l} \end{bmatrix}.$$

Then multiplying the column containing the ith 1 of $\mathbf{I}_{n-l}$ in turn by a_{ij}, for $j = 1, \ldots, n-l$ and adding it to the corresponding column in $-qA$ will give the desired result.

Note that a generator matrix for Λ_C is obtained from $B = [\mathbf{v}_1, \ldots, \mathbf{v}_l, q\mathbf{e}_1, \ldots, q\mathbf{e}_n]$ when it is reduced to the form $[H\ \mathbf{0}]$ even if H does not satisfy all the requirements of the Hermite normal form, but the latter has a kind of canonical format similar to the reduced echelon form.

Example 3.2 For the codes C_1 and C_2 in Example 3.1, generator matrices for the lattices Λ_{C_1} and Λ_{C_2} can be obtained by considering the Hermite normal form of the matrices

$$B_1 = \begin{bmatrix} 2&0&3&0&0 \\ 0&2&0&3&0 \\ 1&1&0&0&3 \end{bmatrix} \text{ and } B_2 = \begin{bmatrix} 2&0&4&0&0 \\ 0&2&0&4&0 \\ 1&1&0&0&4 \end{bmatrix},$$

respectively, which are

$$H_1 = \begin{bmatrix} 1&0&0 \\ 0&1&0 \\ 2&2&3 \end{bmatrix} \text{ and } H_2 = \begin{bmatrix} 2&0&0 \\ 0&2&0 \\ 1&1&2 \end{bmatrix}.$$

Note also that H_1 is built from the generator matrix of the code C_1 in systematic form as described in the last proposition. As another example, consider the code C_3 in $\mathbb{Z}_6^3$ generated by the codeword $(1, 2, 3)$. Since it has a generator matrix in systematic form, $\begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}$, a generator matrix of the lattice Λ_{C_3} in $\mathbb{R}^3$ is $\begin{bmatrix} 1&0&0 \\ 2&6&0 \\ 3&0&6 \end{bmatrix}$.

Example 3.3 Proposition 3.3 always provides a basis and a generator matrix for the lattice Λ_C associated with a code C. In some cases, other generator matrices can be derived from the Hermite matrices to better describe the lattice. For example, consider the code C over $\mathbb{Z}_5$ generated by $(1, 2)$, namely,

$$C = \langle (1,2) \rangle = \{(0,0), (1,2), (2,4), (3,1), (4,3)\} \subset \mathbb{Z}_5^2.$$

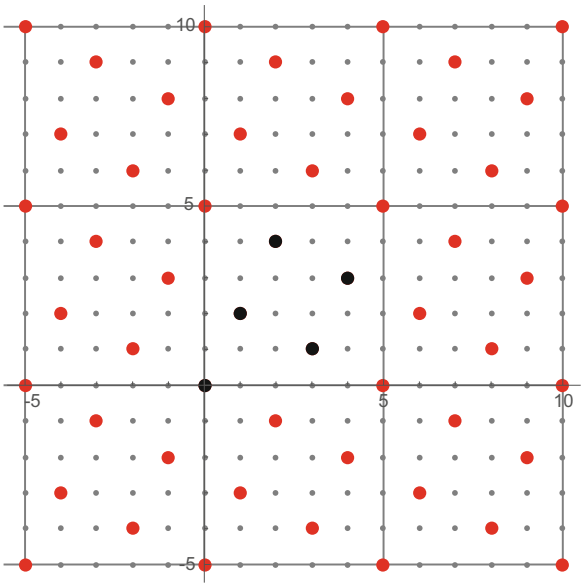


Fig. 3.3 The lattice constructed from the code $\langle(1,2)\rangle \subset \mathbb{Z}_5^2$

According to the above proposition, a basis for Λ_C is $\begin{bmatrix} 1 & 0 \\ 2 & 5 \end{bmatrix}$. One can verify using Theorem 2.2 that $\begin{bmatrix} 1 & -2 \\ 2 & 1 \end{bmatrix}$ is also a generator matrix for this lattice, whose basis is Minkowski reduced (see Definition 2.15), geometrically revealing a square shape (see Fig. 3.3).

Example 3.4 Consider the linear code $C = \{(a_1, \ldots, a_{n-1}, \sum_{i=1}^{n-1} a_i),\ a_1, \ldots, a_{n-1} \in \mathbb{F}_2\}$ over $\mathbb{F}_2$. It has length n and dimension $n-1$. A systematic generator is

$$\begin{bmatrix} \mathbf{I}_{n-1} \\ 1 \ldots 1 \end{bmatrix}.$$

A generator matrix for Λ_C is thus

$$\begin{bmatrix} \mathbf{I}_{n-1} & \mathbf{0}_{(n-1)\times 1} \\ 1 \ldots 1 & 2 \end{bmatrix}.$$

This means that every vector $\mathbf{x} \in \rho^{-1}(C)$ is of the form $\mathbf{x} = (x_1, \ldots, x_{n-1}, \sum_{i=1}^{n-1} x_i + 2x_n)$, $x_i \in \mathbb{Z}$ for all i. This describes every vector which satisfies that the sum of its entries is even. Indeed, a constraint on the sum means that there are $n-1$ degrees of freedom in the first $n-1$ entries (they can be chosen to be anything), and to force the sum to be even no matter what is the choice of $x_1, \ldots, x_{n-1}$, the last component must contain $\sum_{i=1}^{n-1} x_i$. But then our constraint is just that the sum is even, so the

entry should be able to be anything as long as it is even; thus it is of the form $\sum_{i=1}^{n-1} x_i + 2x_n$ where x_n can take any value and $2x_n$ means any even value. This shows that we have just constructed the lattices

$$D_n = \{(x_1, \ldots, x_n), \ \sum_{i=1}^{n} x_i \text{ is even}\}$$

presented in Example 2.4.

3.2 Relevant Distances in Codes and Lattices

Since we are studying lattices with interesting parameters, one may wonder how distances defined over codes translate into parameters for lattices via Construction A. Distances are used in linear codes to characterize their error correction capability. We will consider here the widely used Hamming distance and the ℓ_p distances , $1 \leq p \leq \infty$, also called p-Lee distances. For $p = 1$, $p = 2$, and $p = \infty$, these are the well-known Lee, Euclidean, and the maximum or Chebyshev distances which are used in applications such as constrained and relay channels [38, 88, 101] ($p = 1$), physical layer networks [39] ($p = 2$), rank modulation, and flash memory [94] ($p = \infty$). General d_p distances $1 \leq p \leq \infty$ are considered in [19, 32, 45, 57, 85] and appear while studying the complexity of computational lattice problems [2, 82].

We recall the mathematical definition of a distance.

Definition 3.2 A *distance* or *metric* in a set A is a map $d : A \times A \to \mathbb{R}$ which satisfies the following three conditions :

i) $d(x, y) \geq 0$ and $d(x, y) = 0$ if and only if $x = y$.
ii) $d(x, y) = d(y, x)$, and
iii) $d(x, z) \leq d(x, y) + d(y, z)$, for every x, y, z in A.

In what follows, we treat the Hamming, Lee and p-distances for codes and lattices, and related concepts such as the minimum distance of a set and closed balls

$$B_d(x, R) = \{y \in A; d(y, x) \leq R\} \tag{3.1}$$

in these distances.

The Hamming Distance For $A = \mathbb{Z}_q^n$, particularly for $q = 2$, corresponding to binary codes, the commonly used distance is the *Hamming distance* d_H which counts the number of coordinates in which two codewords differ. For $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ and $\mathbf{y} = (y_1, y_2, \ldots, y_n)$,

$$d_H(\mathbf{x}, \mathbf{y}) = |\{i; x_i \neq y_i\}|.$$

For example, in $\mathbb{Z}_2^4$,

$$d_H((1,0,1,1),(0,1,0,1)) = 3$$

and in $\mathbb{Z}_5^3$,

$$d_H((1,0,3),(1,2,0)) = 2.$$

The Minimum Hamming Distance For a linear code C in $\mathbb{Z}_q^n$, it is defined as the minimum of all distances between two different vectors in the code. Since $d_H(\mathbf{x},\mathbf{y}) = d_H(\mathbf{x}+\mathbf{k},\mathbf{y}+\mathbf{k})$, for every $\mathbf{x},\mathbf{y},\mathbf{k} \in \mathbb{Z}_q^n$, the minimum Hamming distance is the minimum of $d_H(\mathbf{x},\mathbf{0})$, $(\mathbf{x} \in C, \mathbf{x} \neq \mathbf{0})$, that is the minimum weight of a non-zero codeword.

For binary linear codes $C \subset \mathbb{Z}_2^n$, the minimum Hamming distance $d_H(C)$ is linked to the error correction capability. A code with minimum distance $d_H(C)$ can correct $R = \left\lfloor \frac{d_H(C)-1}{2} \right\rfloor$ errors. Geometrically this means that the Hamming balls of radius R centered at codewords do not intersect. Hence, any received vector in $\mathbb{Z}_2^n$ with no more than r different coordinates (errors) from that of a codeword will be located in just one of these balls and will be decoded as its center.

Definition 3.3 A binary linear code is *R-perfect* in the Hamming metric if the union of those balls centered in its codewords with the radius R is $\mathbb{Z}_2^n$.
The Hamming codes introduced by R.W. Hamming in 1950 and used in several applications are 1-perfect. In $\mathbb{Z}_2^7$, a 1-perfect code can be described as $C = \{(a_1,a_2,a_3,a_4,a_2+a_3+a_4,a_1+a_3+a_4,a_1+a_2+a_4), a_i \in \mathbb{Z}_2\}$.

The relation between the minimum Hamming distance of a code $C \subset \mathbb{Z}_2^n$ and the minimum norm (Euclidean distance) of its associated Construction A lattice Λ_C is described in the next proposition [60].

Proposition 3.4 *Let C be a linear binary code with minimum distance $d_H(C)$ and λ be the minimum norm (see (2.10)) of its associated lattice Λ_C. Then:*

i) If $d_H(C) < 4$, $\lambda = \sqrt{d}$ and the set of minimum norm vectors of Λ_C is composed by the codewords of C with weight d and the vectors obtained from these codewords by replacing one or more coordinates set to 1 by -1.
ii) If $d_H(C) = 4$, $\lambda = 2$ and the set of minimum norm vectors of Λ_C is composed by the codewords of C with weight equal to 4, the vectors obtained from these codewords by replacing one or more coordinates set to 1 by -1 and the vector which have ± 2 for their unique non-zero coordinate.
iii) If $d_H(C) > 4$, $\lambda = 2$ and the minimum norm vectors of Λ_C are the ones which have ± 2 for their unique non-zero coordinate.

This result is useful to detect the set of minimum norm vectors of special lattices which may be difficult to find in general. For example, consider the lattice E_8 (see Chap. 2). A lattice congruent to E_8 can be obtained via Construction A from the extended Hamming code in $\mathbb{Z}_2^8$ given by

$$C = \{(a_1,a_2,a_3,a_4,a_2+a_3+a_4,a_1+a_3+a_4,a_1+a_2+a_4,a_1+a_2+a_3), a_i \in \mathbb{Z}_2\}$$

(see [98, Chap. 5, 2.1]). The code C has minimum Hamming distance 4 and 14 of its codewords have this minimum distance (see Exercise 3.2). By the above proposition, considering all 2^4 possibilities of sign changes in each codeword of minimum distance plus the lattice vectors on the edges, we get that E_8 must have $14 \cdot 2^4 + 16 = 240$ vectors of minimum norm. This number (the kissing number of E_8) appears also in the theta series of this lattice (see the following section).

The Lee and the ℓ_p Distances Another distance used for $q-$ary codes is the Lee distance in $\mathbb{Z}_q^n$, introduced in [61] for non-binary codes. We consider here the set of integers modulo q in its typical representation, $\mathbb{Z}_q = \{0, 1, \ldots, q-1\}$. For a and b in $\mathbb{Z}_q$, it is the "circular" graph distance (see Fig. 3.4), defined by

$$d_{\text{Lee}}(a, b) = min\{|a - b|, q - |a - b|\}.$$

In the Cartesian product $\mathbb{Z}_q^n$, the Lee distance between $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ and $\mathbf{b} = (b_1, b_2, \ldots, b_n)$ is defined as

$$d_{\text{Lee}}(\mathbf{a}, \mathbf{b}) = \sum_{i=1}^{n} d_{\text{Lee}}(a_i, b_i).$$

We remark (see Exercise 3.3) that for $q = 2$ and $q = 3$, the Lee and the Hamming distances in $\mathbb{Z}_q^n$ are the same for all pairs of vectors and these are the only values of

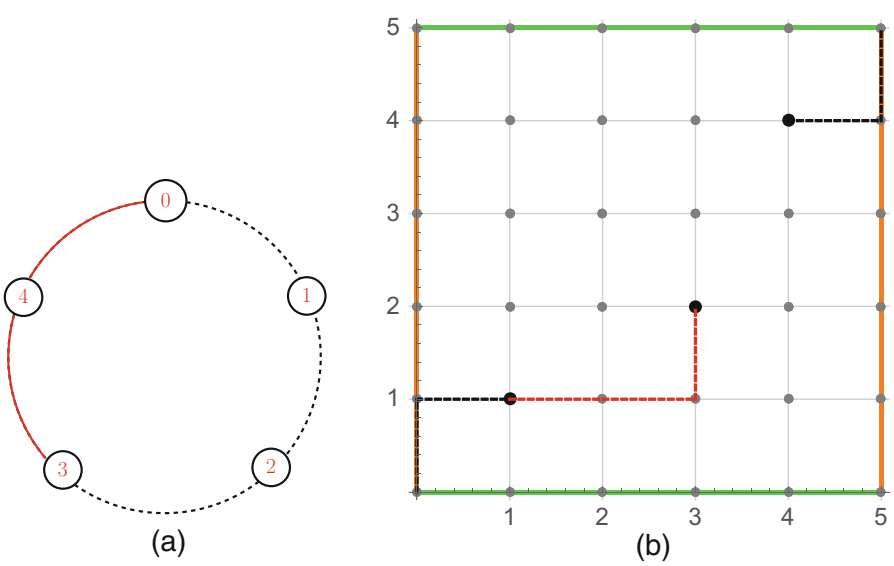


Fig. 3.4 (**a**) Lee distance in $\mathbb{Z}_5$: the smallest number of edges in the circular graph on the left (e.g., $d_{\text{Lee}}(0, 3) = 2$). (**b**) Lee distance in $\mathbb{Z}_5^2$: in the integer grid with the parallel board sides identified (flat torus), it is again the graph distance, that is the smallest number of edges connecting two pairs (e.g., $d_{\text{Lee}}((1, 1), (3, 2)) = 3$ (red path), $d_{\text{Lee}}((1, 1), (4, 4)) = 4$ (black path)

q for which both metrics coincide. For instance, in $\mathbb{Z}_5^3$ $d_{\text{Lee}}((1,0,3),(1,2,0)) = 5$ and $d_H((1,0,3),(1,2,0)) = 2$, as we have seen.

The Lee distance in $\mathbb{Z}_q^n$ can be seen as induced by the l_1 or Manhattan distance in $\mathbb{Z}^n$, $d_1(\mathbf{a},\mathbf{b}) = \sum_{i=1}^n |a_i - b_i|$, into the quotient $\mathbb{Z}^n/q\mathbb{Z}^n \simeq \mathbb{Z}_q^n$. We can also consider distances either in $\mathbb{Z}^n$ or in $\mathbb{Z}_q^n$ as the ones induced by the well-known l_p metrics in $\mathbb{R}^n$, which are defined for $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ and $\mathbf{b} = (b_1, b_2, \ldots, b_n)$ in $\mathbb{Z}^n$ and $p \in \mathbb{N}$, $p \geqslant 1$,as

$$d_p(\mathbf{a},\mathbf{b}) = \left(\sum_{i=1}^n |a_i - b_i|^p\right)^{\frac{1}{p}}$$

and $d_\infty(\boldsymbol{a},\mathbf{b}) := \max\{|a_i - b_i|;\ i = 1,\ldots,n\}$. Note that for $p = 1$ and $p = 2$, we have the Lee distance and the standard Euclidean distance, respectively, whereas for $p = \infty$, this distance is also known as the maximum or Chebyshev metric. The correspondent induced ℓ_p- distance for $\mathbf{a}$ and $\mathbf{b}$ in $\mathbb{Z}^n/q\mathbb{Z}^n \simeq \mathbb{Z}_q^n$ (also called p-Lee distance) is given by [19]

$$d_p(\mathbf{a},\mathbf{b}) = \left(\sum_{i=1}^n (d_{\text{Lee}}(a_i,b_i))^p\right)^{\frac{1}{p}} \text{ for } p \in \mathbb{N}, p \geqslant 1,$$

and

$$d_\infty(\boldsymbol{a},\mathbf{b}) := \max\{d_{\text{Lee}}(a_i,b_i), i = 1,\ldots,n\}.$$

Example 3.5 For $\mathbf{a} = (1,1)$ and $\mathbf{b} = (4,4)$ in $\mathbb{Z}^2$, we have

$$d_1(\mathbf{a},\mathbf{b}) = 6,\ d_2(\mathbf{a},\mathbf{b}) = 6\sqrt{2},\ d_\infty(\mathbf{a},\mathbf{b}) = 3,$$

whereas for $\mathbf{a} = (1,1)$, $\mathbf{b} = (4,4)$ now considered in $\mathbb{Z}_5^2$,

$$d_1(\mathbf{a},\mathbf{b}) = d_{\text{Lee}}(\mathbf{a},\mathbf{b}) = 4,\ d_2(\mathbf{a},\mathbf{b}) = 4\sqrt{2},\ d_\infty(\mathbf{a},\mathbf{b}) = 2.$$

Like the Hamming distance, all the p-Lee distances in $\mathbb{Z}^n$ or $\mathbb{Z}_q^n$ are invariant by translations (Exercise 3.4):

$$d(\mathbf{a},\mathbf{b}) = d(\mathbf{a}+\mathbf{c},\mathbf{b}+\mathbf{c}).$$

As functions we have (see Exercise 3.5) that $d_1 \geq d_2 \geq \ldots \geq d_\infty$, which implies the inclusion reversal order for the closed balls of a fixed radius. For $p = 1$ (Lee) and $p = \infty$, the p-distances in $\mathbb{Z}^n$ or in $\mathbb{Z}_q^n$ are always integers, and there are closed form expressions for the number of points $\mu_p(n,R)$ in the closed balls of radius R in $\mathbb{Z}^n$, given by

$$\mu_1(n,R) = \sum_{i=0}^{\min\{n,R\}} 2^i \binom{n}{i}\binom{R}{i} \tag{3.2}$$

$$\mu_\infty(n,R) = (2R+1)^n. \tag{3.3}$$

Note also that, for $2R+1 \leq q$, the number of points in a closed ball of radius R in $\mathbb{Z}_q^n$ either in the Lee or in the infinity metric in $\mathbb{Z}_q^n$ is the same as in the ball in $\mathbb{Z}^n$ with the same radius.

Example 3.6 For $n=2$, we have from the expressions above that $\mu_1(n,R) = R^2 + (R+1)^2$ and $\mu_\infty(n,R) = (2R+1)^2$. Thus a closed ball of radius 2 in the d_1 (Lee) distance either in $\mathbb{Z}^2$ or in $\mathbb{Z}_7^2$ has 13 points, whereas in the distance d_∞ a ball with the same radius has 25 points, since $2R+1 \leq q$. For the distance d_1, the closed balls with $R=4$ in $\mathbb{Z}^2$ and in $\mathbb{Z}_7^2$ have 41 and 37 points, respectively. The balls of radius 4 for the distance d_∞ in $\mathbb{Z}^2$ and in $\mathbb{Z}_7^2$ have 81 and 49 points (since $d_\infty(\boldsymbol{a},\mathbf{b}) \leq 3$, for all $\mathbf{a},\mathbf{b} \in \mathbb{Z}_7^2$), respectively.

The Minimum Distance $d_p(C)$ For a linear code C in $\mathbb{Z}_q^n$ or a lattice Λ in $\mathbb{Z}^n$, it is defined as the minimum of the ℓ_p distances between two different vectors in the code or in the lattice which, due to invariance under translation, is the same as the minimum ℓ_p−distance from a non-zero vector to the null vector (*minimum ℓ_p-norm*).

It should be remarked that for a large enough alphabet size, a code and its associated lattice via Construction A have the same minimum ℓ_p-distance [56, 89], since

$$d_p(\Lambda_C) = \min\left\{d_p(C), q\right\}. \tag{3.4}$$

Like in the Hamming metric, we may use the closest neighbor criterion under the p-distance for decoding by considering disjoint p-balls centered at codewords. We define the *d_p-packing radius* R of a code $C \subset \mathbb{Z}_q^n$ ($\Lambda \subset \mathbb{Z}^n$) as the greatest R such that the closed balls of radius R in the d_p metric centered at the distinct points of C are disjoint and there is at least one point of $\mathbb{Z}_q^n$ ($\mathbb{Z}^n$) at the boundary of these closed balls. Hence any received vector which is inside these balls will be univocally decoded as the codeword center of its ball.

For $p=1$ and $p=\infty$, the packing radius of a linear code $C \subset \mathbb{Z}_q^n$ ($\Lambda \subset \mathbb{Z}^n$) is an integer given by the expression $R = \left\lfloor \frac{d_p(C)-1}{2} \right\rfloor$. For $1 < p < \infty$, a similar expression is not valid [19].

Similarly to the binary case with Hamming distance (recall Definition 3.3), we can consider closed balls (3.1) in $\mathbb{Z}_q^n$ or $\mathbb{Z}^n$ with respect to the ℓ_p metric and define:

Definition 3.4 If the union of disjoint closed balls of packing radius R in a p-metric covers $\mathbb{Z}_q^n$ (or $\mathbb{Z}^n$), we say that C (or Λ) is *R-perfect in this metric*.

For $R < \frac{q}{2}$, a necessary condition for a code to be R-perfect in the ℓ_p metric is that $|C|\,\mu_p(n,R) = q^n$. We may use the closed form expression for the number of closed ball points $\mu_p(n,R)$ in the cases $p=1$ (3.2) and $p=\infty$ (3.3).

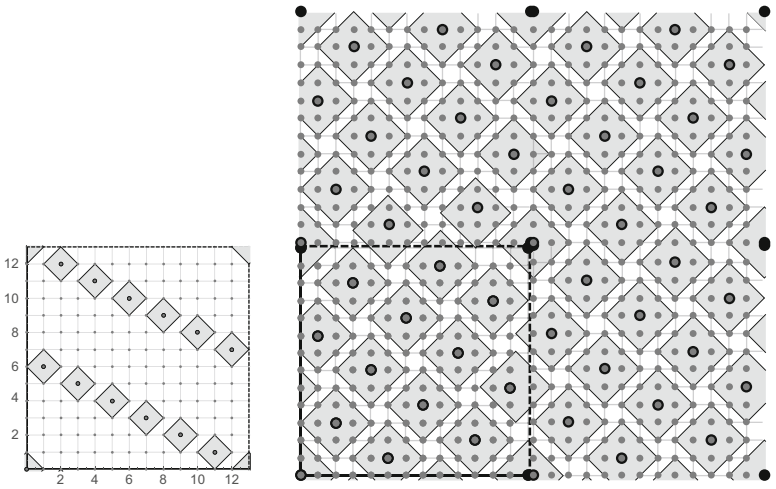


Fig. 3.5 Codes in $\mathbb{Z}_{13}^2$ with the Lee distance. On the left the code $C_1 = \langle(1,6)\rangle$ with its packing balls, on the right the perfect code $C_2 = \langle(2,3)\rangle$ represented inside its associated lattice Λ_{C_2}

Example 3.7 Consider the linear codes $C_1 = \langle(1,6)\rangle$ and $C_2 = \langle(2,3)\rangle$ in $\mathbb{Z}_{13}^2$ generated by the vectors $(2,3)$ and $(1,6)$, respectively. Both codes have 13 codewords, minimum distances in the Lee metric which are $d_1(C_1) = 3$ and $d_1(C_2) = 5$, and hence their packing radii are 1 and 2, respectively. The code C_2 is 2-perfect in the Lee distance since balls of radius 2 centered at its codewords are disjoint and cover $\mathbb{Z}_{13}^2$, whereas C_1 is not. Note also that, taking into account the above Example 3.6, the lattice Λ_{C_2} is also 2-perfect with respect to the l_1 distance (see Fig. 3.5). This relation between perfect codes and associated perfect lattices can be extended to all d_p distances.

Proposition 3.5 ([19]) *If $C \subset \mathbb{Z}_q^n$ is a perfect linear code in the ℓ_p-metric with packing radius $R < \frac{q}{2}$, then the lattice Λ_C is also perfect in this metric with the same radius.*

Example 3.8 Consider the perfect code given by $C_k = \langle(k, k+1)\rangle \subset \mathbb{Z}_h^2$, where $h = k^2 + (k+1)^2$, in the Lee metric with radius $R = k$ (see Exercise 3.6). Since $k < \frac{h}{2}$, the associated lattice Λ_C is also perfect in $\mathbb{Z}^2$. This provides, for $n = 2$, examples of perfect Lee lattices of any radius.

The result of the last example cannot be extended to dimension 3. This is a consequence of the so-called Golomb-Welch conjecture. Introduced in [46], it states that for $n \geq 3$, the unique Lee perfect lattices are the ones with radius $R = 1$. This long-standing conjecture is, up to now, only proved in particular cases and for $n \leq 11$ (see [50] and references therein). It is important to note that the condition $R < \frac{q}{2}$ in the last proposition cannot be removed. A counterexample

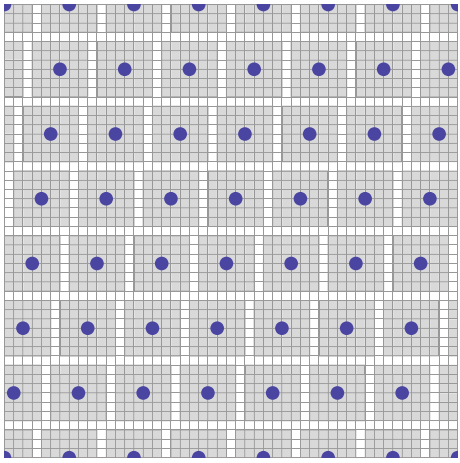


Fig. 3.6 The code $C = \langle (1, 7) \rangle \subset \mathbb{Z}_{49}^2$, which is perfect in the ℓ_∞ distance with its packing balls

can be given by the perfect binary code C with radius 7 in the Lee metric, $C = \{(0, 0, 0, 0, 0, 0, 0), (1, 1, 1, 1, 1, 1, 1)\} \subset \mathbb{Z}_2^7$ since Λ_C is not perfect in $\mathbb{Z}^7$ (see Exercise 3.7).

Note that the trivial codes $C = \{\mathbf{0}\}$ and $C = \mathbb{Z}_q^n$ may be considered perfect for any d_p distance. For $p = \infty$, the existence of perfect codes is fully characterized next.

Proposition 3.6 ([32]) *There are nontrivial perfect codes $C \subset \mathbb{Z}_q^n$ in the ℓ_∞ metric if and only if $q = bm$ with $b > 1$ an odd integer and $m > 1$ an integer.*

Example 3.9 Simple examples of perfect codes of packing radius R in the ℓ_∞ metric are, for $b = 2R + 1$, the Cartesian codes, $C = \sum_{i=1}^{n} \alpha_j b \mathbf{e_i}, \subset \mathbb{Z}_{bm}^n$, $(\alpha_j = 0, 1, \ldots, m)$. An example of a non-Cartesian perfect code in the d_∞ metric is $C = \langle (1, 7) \rangle \subset \mathbb{Z}_{49}^2$ (see Fig. 3.6). Its packing radius is 3.

The next proposition shows that for each perfect code in the ℓ_∞ metric, there exists $p^* \geq 1$ such that this code is also perfect in the p-Lee metric for all $p \geq p^*$.

Proposition 3.7 ([32]) *Let $C \subseteq \mathbb{Z}_q^n$ be a perfect code in the ℓ_∞ metric with packing radius R. If $p > \frac{\ln(n)}{\ln\left(1+\frac{1}{R}\right)}$, then C is perfect in the ℓ_p metric, with radius $R_p = Rn^{1/p}$.*

Note that according to the above proposition the ℓ_∞-perfect code with packing radius 3, $C = \langle (1, 7) \rangle \subset \mathbb{Z}_{49}^2$, from Example 3.7 (Fig. 3.6) is also ℓ_p-perfect with packing radius $3.2^{\frac{1}{p}}$ for any $p \geq 3$.

It may be worth noting that the lattice distances discussed in this chapter were all related to the underlying code distances. Other distances may of course be of interest, e.g., the *p*roduct distance, discussed in the next chapter.

3.2.1 *q-ary Lattice Decoding*

We have discussed so far many connections between distances on codes and distances on their associated lattice via Construction A. We next give applications of these connections, in particular to the problem of lattice decoding. We recall (see also Chap. 2) that given a vector in $\mathbb{R}^n$ (obtained through transmission via for example a Gaussian channel), lattice decoding consists of finding a lattice vector which is closest to it. Without the setting of transmission via a communication channel, this becomes the closest vector problem (see Problem 2.2). The case of communication via a Gaussian channel corresponds to the Euclidean distance ($p = 2$). There is a huge amount of literature on this problem (e.g., [49, 109]). On the other hand, lattice-based cryptographic schemes are usually built upon q-ary lattices and are linked to the computational difficulty of the shortest (see Problem 2.1) and closest vector problems (Problem 2.2). While both problems are difficult in general, for q-ary lattices obtained from codes via Construction A, it is possible to solve them more efficiently by decoding the code.

In the next proposition and example, we denote by $\bar{\mathbf{x}}$ a codeword of a linear code $C \subset \mathbb{Z}_q^n$ and by $\mathbf{x}$ an associated vector in Λ_C. Since there is an isomorphism $\Lambda_C/q\mathbb{Z}^n \simeq C$, we do not distinguish elements of $\Lambda_C/q\mathbb{Z}^n \subseteq \mathbb{R}^n/q\mathbb{Z}^n$ from the codewords of C.

Proposition 3.8 ([32, 57]) *Let Λ_C be a q-ary lattice and $\boldsymbol{r} = (r_1, \ldots, r_n) \in \mathbb{R}^n$. Let $\bar{\boldsymbol{r}} \in \mathbb{R}^n/q\mathbb{Z}^n$ and $\bar{\boldsymbol{c}} \in C, \boldsymbol{c} = (c_1, \ldots, c_n)$, $0 \leq c_i < q$, a closest codeword to $\bar{\boldsymbol{r}}$ considering the d_p distance in $\mathbb{R}^n/q\mathbb{Z}^n$. An element $\boldsymbol{z} \in \Lambda_C$ which is closest to $\boldsymbol{r}$ considering the ℓ_p metric in $\mathbb{R}^n$ is $\boldsymbol{z} = (z_1, \cdots, z_n)$, where $z_i = c_i + qw_i$ and $w_i = \left\lceil \dfrac{r_i - x_i}{q} \right\rfloor$, for each $i = 1, \ldots, n$.*

Example 3.10 Consider the code $C = \langle(\bar{2}, \bar{3})\rangle \subset \mathbb{Z}_{13}^2$ and its associated lattice Λ_C. For the received vector $\mathbf{r} = (0, -6) \in \mathbb{R}^2$, the closest codeword from $\bar{\mathbf{r}} = (\bar{0}, \bar{7})$ is $\bar{\mathbf{x}} = (\overline{12}, \bar{8})$. The closest lattice point to $\mathbf{r}$ in the distance d_1 is $\mathbf{z} = (-1, -5)$.

3.3 Wiretap Coding and Theta Series

Let us look again at the lattice $\Lambda_C = \rho^{-1}(C)$ obtained from a linear code $C \subset \mathbb{Z}_q^n$ via Construction A geometrically. It is obtained by considering the lattice $q\mathbb{Z}^n$ and its translations by the codewords of C. As a first example, in Fig. 3.2b, $\rho^{-1}(C)$ is the union of $2\mathbb{Z}^2$ and $2\mathbb{Z}^2 + (1, 1)$. Also, for $C = \langle(1, 2)\rangle \subset \mathbb{Z}_5^2$ (Fig. 3.3), the lattice Λ_C is the union of $\Lambda = 5\mathbb{Z}^2$ with the four translations of Λ by the nonvanishing codewords of C, $(1, 2)$, $(2, 4)$, $(3, 1)$ and $(4, 3)$ (called gluing vectors). In other words, $\rho^{-1}(C)$ is the union of cosets of $q\mathbb{Z}^n$, and codewords of C form coset representatives. This makes Construction A particularly suitable for a coding strategy called *coset coding*, which we will explain next in the context of wiretap coding.

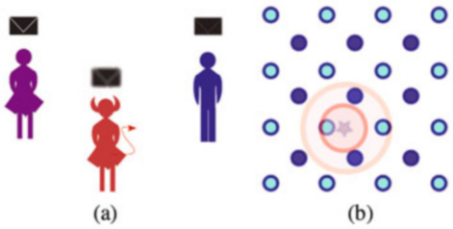


Fig. 3.7 Gaussian wiretap channel: channel and intuition. (**a**) A wiretap channel, where Alice and Bob want to exchange a confidential message in the presence of an eavesdropper Eve. (**b**) Bob's noise is such that it can decode the point transmitted via coset coding normally. Eve's noise is such that two points from the first coset and two points from the second coset are equally possible, and thus she has to decode one of the two at random

Let us consider Gaussian wiretap coding, and recall from (2.20) that transmission of a vector $\mathbf{x}$ over a Gaussian channel is of the form $\mathbf{y}_B = \mathbf{x} + \mathbf{n}_B$ where $\mathbf{n}_B$ is a random vector whose components are independent Gaussian random variables with mean 0 and variance σ_B^2. Suppose now that an eavesdropper (wiretapper) is listening to this transmission (see Fig. 3.7a). Then the eavesdropper will receive $\mathbf{y}_E = \mathbf{x} + \mathbf{n}_E$, where the noise $\mathbf{n}_E$ has variance σ_E^2. The subscripts B and E refer to Bob and Eve, the standard names of players when security is involved in a protocol. Now the Gaussian wiretap coding problem asks for reliability between the legitimate transmitter (Alice) and receiver (Bob), which is the Gaussian channel coding problem discussed in Chap. 2, but also confidentiality despite the presence of the eavesdropper Eve [62]. This is done via the introduction of randomness at the transmitter, and coset coding gives a practical way to handle this randomness. The secret information is encoded into cosets, while $\mathbf{x}$ is then chosen randomly within this coset. If we consider again the code $\{(0,0),(1,1)\} \subset \mathbb{Z}_2^2$ of Fig. 3.2b, one bit of secret can be transmitted using coset coding: to send 0, choose the coset $2\mathbb{Z}^2$, and to send 1, choose the coset $2\mathbb{Z}^2 + (1,1)$.

The idea behind wiretap coding is probably best understood in the scenario, called *wiretap II* [81], where Alice and Bob have a noiseless channel, and Eve receives μ symbols out of the n sent by Alice. Alice knows μ, but she does not know which μ positions are known to Eve. In the simplest case, say Alice sends $n = 2$ bits, and $\mu = 1$. Then Alice can achieve perfect confidentiality by sending $(b + r, r)$ where b is her secret bit, and r is a random bit, chosen uniformly at random. In the Gaussian case, the introduction of random bits is mimicked, but the intuition is different. Since Eve is supposed to have a stronger noise than Bob (as was already assumed in the wiretap II case since Bob has a noiseless channel), the geometric intuition is that when Bob receives a noisy codeword, his channel is such that in the radius around his received point, only the codeword that was sent is present, while Eve will find in her radius points from different cosets, such that each coset is equally likely to have been sent. This is illustrated in Fig. 3.7b. A practical example of the effect of coset coding is shown in Fig. 3.8, where an image has been transmitted, over a USRP testbed [65], using coset coding: on the right,

Fig. 3.8 The cameraman image transmitted by Alice and received by an eavesdropper: on the left, with no coset coding, in the middle with one bit of randomness, and on the right with two bits of randomness

one secret bit is mapped to a coset in $\mathbb{Z}_2$ ($\mathbb{Z}$ is partitioned into two cosets), and the coset representative is chosen with 2 bits of randomness. The technical settings of the experiments are found in [65].

Coset encoding uses two nested lattices $\Lambda_E \subset \Lambda_B$, where Λ_B is the lattice from which a signal constellation is carved for transmission to Bob, while Λ_E is the sublattice used to partition Λ_B. In the right picture of Fig. 3.8, $\Lambda_B = 2\mathbb{Z}$ and $\Lambda_E = \mathbb{Z}$. For a general Construction A, as explained above, Λ_B is partitioned using $\Lambda_E = q\mathbb{Z}^n$. This suggests two questions:

- Can we apply Construction A with other pairs of nested lattices? The answer is yes, and there are plenty of works and constructions following the same principle: instead of n copies of $\mathbb{Z}$, take n copies of some commutative ring R, and instead of $q\mathbb{Z}$, take an ideal I of this ring (see the introduction of the next chapter for a definition). Then use a linear code C which is a subset of $(R/I)^n$. See, e.g., [33, 59] and references therein.
- Would another choice of nested pairs of lattices $\Lambda_E \subseteq \Lambda_B$ bring more confidentiality, and what would be a design criterion for such a lattice? We will be discussing this criterion next.

As explained above, in wiretap coset coding, one message corresponds to one coset, here of a lattice, instead of one lattice point. Thus, mimicking the probability analysis of Chap. 2, the probability $P_{c,E}$ that Eve correctly decodes her received message is

$$P_{c,E} \leq \frac{1}{(\sqrt{2\pi}\sigma_E)^n} \sum_{\mathbf{t}\in\Lambda_E} \int_{\mathcal{V}_{\Lambda_B}(\mathbf{0})} e^{-\|\mathbf{u}+\mathbf{t}\|^2/2\sigma_E^2} \mathrm{d}\mathbf{u}.$$

It was shown in [80] that $P_{c,E}$ is bounded by

$$P_{c,E} \leq \frac{V(\Lambda_B)}{(\sqrt{2\pi}\sigma_E)^n} \sum_{\mathbf{t}\in\Lambda_E} e^{-||\mathbf{t}||^2/2\sigma_E^2} = \frac{V(\Lambda_B)}{(\sqrt{2\pi}\sigma_E)^n} \Theta_{\Lambda_E}\left(\frac{1}{2\pi\sigma_E^2}\right)$$

where we recall that $V(\Lambda_B)$ is the volume of Λ and Θ_Λ is the *theta series* of Λ [26] defined by

$$\Theta_\Lambda(z) = \sum_{\mathbf{x}\in\Lambda} q^{\|\mathbf{x}\|^2},\ q = e^{i\pi z}, \mathrm{Im}(z) > 0. \tag{3.5}$$

In the above upper bound, we set $y = -iz$ and thus consider $\Theta_\Lambda(y)$, for $y > 0$. In what follows, we will write $\Theta_\Lambda(q)$ whenever it does not matter whether we consider z or y. The theta series of an integral lattice keeps track of the different norms of lattice points. The coefficient $N(m)$ of q^m in this series tells how many points in the lattice are at squared distance m from the origin. This series always starts with 1, corresponding to the zero vector. The second term corresponds to the squared minimum norm λ^2 (see (2.10)), and thus the coefficient $N(\lambda^2)$ of q^{λ^2} is the kissing number of the lattice. The theta series of a general lattice is hard to compute, but in special cases, it can be expressed in terms of Jacobi theta functions [26, Chap. 4.1]. For example, it can be easily checked geometrically for $\mathbb{Z}^2$ that the first terms of its series are $\Theta_{\mathbb{Z}^2}(q) = 1 + 4q + 4q^2 + 4q^4 + 8q^5 + \ldots$. But it is not straightforward to see the coefficient attached to q^m, for big m in this series. A computation (that actually uses a Jacobi theta function) is shown in Example 3.11.

In Table 3.1 (extracted from [26]), the first non-zero coefficients of the theta series of the lattices $\mathbb{Z}^2$, A_2^*, $\mathbb{Z}^3$, FCC, BCC, and E_8 are given. Here A_2^* is the scaled version of the lattice A_2 (see Example 2.3), with minimum norm one, which is identified to the hexagonal lattice (Example 2.1).

Example 3.11 Let us compute the theta series of the lattice $\mathbb{Z}^n$:

$$\Theta_{\mathbb{Z}^n}(q) = \sum_{\mathbf{x}\in\mathbb{Z}^n} q^{||\mathbf{x}||^2} = \sum_{x_1\in\mathbb{Z}} q^{x_1^2} \cdots \sum_{x_n\in\mathbb{Z}} q^{x_n^2} = \left(\sum_{m\in\mathbb{Z}} q^{m^2}\right)^n$$

Table 3.1 First non-zero coefficients $N(m)$ of the Θ-series of some lattices studied in Chap. 2 [26, chap. 4]

$\mathbb{Z}^2$	m	0	1	2	4	5	8	9	10	13	16	17	18	20	25	26	29	32
	$N(m)$	1	4	4	4	8	4	4	8	8	4	8	4	8	12	8	8	4
A_2^*	m	0	1	3	4	7	9	12	13	16	19	21	25	27	28	31	36	37
	$N(m)$	1	6	6	6	12	6	6	12	6	12	12	6	6	12	12	6	12
$\mathbb{Z}^3$	m	0	1	2	3	4	5	6	8	9	10	11	12	13	14	16	17	18
	$N(m)$	1	6	12	8	6	24	24	12	30	24	24	8	24	48	6	48	36
FCC	m	0	2	4	6	8	10	12	14	16	18	20	22	24	26	30	32	34
	$N(m)$	1	12	6	24	12	24	8	28	6	36	24	24	24	72	48	12	48
BCC	m	0	3	4	8	11	12	16	18	19	24	27	31	35	36	40	43	44
	$N(m)$	1	8	6	12	24	8	6	24	24	24	32	12	48	30	24	24	24
E_8	m	0		2		4		6		8		10		12		14		16
	$N(m)$	1		240		2160		6720		17520		30240		60480		82560		140400

$$= (1 + 2q + 2q^4 + 2q^9 + \ldots)^n = \Theta_{\mathbb{Z}}(q)^n.$$

To evaluate the benefit of using a specific lattice Λ_E with respect to using $\Lambda_E = \nu\mathbb{Z}^n$ (ν is a scaling factor so that $\mathbb{Z}^n$ scaled to the same volume), we compare the behavior of the theta series of $\nu\mathbb{Z}^n$ with that of Λ_E and consequently define the notion of secrecy gain. This idea of defining a gain (here in terms of secrecy) by comparing the lattice $\mathbb{Z}^n$ and another lattice is fairly standard. In fact, we already mentioned it in the context of quantization (see the discussion on best quantizers at the end of Sect. 2.5.1).

Definition 3.5 The *(strong) secrecy gain* $\chi_{\Lambda,\text{strong}}$ of an n-dimensional lattice Λ is defined by

$$\chi_{\Lambda,\text{strong}} = \sup_{y>0} \frac{\Theta_{\nu\mathbb{Z}^n}(y)}{\Theta_{\Lambda}(y)}$$

defined for $y > 0$.
The role of the theta series Θ_{Λ_E} at the point $y = \frac{1}{2\pi\sigma_E^2}$ has been independently confirmed in [63], where it was shown for the mod-Λ Gaussian channel that the mutual information $I(\mathbf{S};\mathbf{Z})$, an information theoretic measure of the amount of information that Eve gets about the secret message $\mathbf{S}$ by receiving $\mathbf{Z}$, is bounded by a function that depends of the channel parameters and of $\Theta_{\Lambda_E}\left(\frac{1}{2\pi\sigma_E^2}\right)$.

The adjective "strong" in the definition of secrecy gain is motivated by the fact that the above quantity is hard to compute, while for unimodular lattices, the secrecy gain seems to correspond to a multiplicative symmetry point of the function $\frac{\Theta_{\nu\mathbb{Z}^n}(y)}{\Theta_{\Lambda}(y)}$, as illustrated in Fig. 3.9 (in log scale) for the E_8 lattice. The shape of the function is typical of that of a unimodular lattice. The "weak" secrecy gain thus corresponds to this symmetric point, conjectured to be the maximum of the function and thus the secrecy gain. As of now, this conjecture is still under investigation.

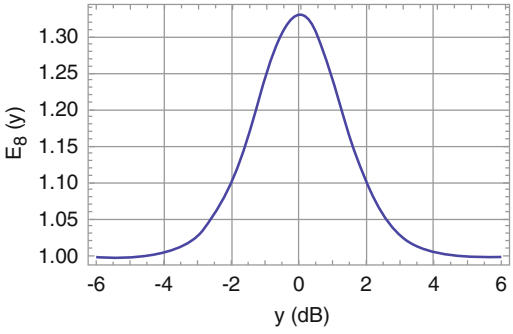


Fig. 3.9 The secrecy gain of the 8-dimensional unimodular lattice E_8 where the x-axis is in decibels ($10\log_{10}(y)$)

Exercises

Exercise 3.1 Show that for $S \subset \mathbb{Z}_q^n$, if $\rho^{-1}(S)$ is a lattice in $\mathbb{R}^n$, then S is a linear code.

Exercise 3.2 Show that the extended Hamming code in $\mathbb{Z}_2^8$ has minimum Hamming distance 4 and that 14 of its codewords have this minimum distance.

Exercise 3.3 Show that for $q = 2, 3$, the Lee distance is the same distance as the Hamming distance.

Exercise 3.4 Prove that the Hamming distance and the p-Lee distances are invariant by translation.

Exercise 3.5 Prove that for the Lee distances d_p, $d_1 \geq d_2 \geq \ldots \geq d_\infty$.

Exercise 3.6 As you can see in Figs. 3.3 and 3.5, the codes $\langle(1,2)\rangle \subset \mathbb{Z}_5^2$ and $\langle(2,3)\rangle \subset \mathbb{Z}_{13}^2$ are perfect in the Lee Metric. Prove that this result can be extended: Any code $C_k = \langle(k, k+1)\rangle \subset \mathbb{Z}_h^2$, where $h = k^2 + (k+1)^2$, is a perfect code in the Lee metric with packing radius $R = k$.

Exercise 3.7 Show that the condition $R < \frac{q}{2}$ in Proposition 3.5 cannot be removed by proving that $C = \{(0,0,0,0,0,0,0), (1,1,1,1,1,1,1)\} \subset \mathbb{Z}_2^7$ is perfect with radius 3 in the Lee metric but Λ_C is not perfect in $\mathbb{Z}^7$.

Chapter 4
Ideal Lattices

In Chap. 2, interesting lattices together with their parameters and applications were presented. In Chap. 3, one method to build such lattices was discussed, which consists of obtaining lattices from linear codes. This chapter presents two other methods to construct lattices, both called ideal lattices, because they both rely on the structure of ideals in rings. We recall that given a commutative ring R, an *ideal* of R is an additive subgroup of R which is also closed under multiplication by elements of R. The same terminology is used for two different viewpoints on lattices because of the communities that studied them. We will explain the first method using quadratic fields and refer to [79] for general number field constructions. We note that such a lattice construction from number fields can in turn be combined with Construction A to obtain further lattices, e.g., [59] and references therein. In the second method, "ideal lattices" refer to a family of lattices recently used in cryptography.

4.1 Ideal Lattices from Quadratic Fields

For $d > 1$ a squarefree integer, consider the field

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d},\ a, b \in \mathbb{Q}\}$$

which is called *quadratic* because it has dimension 2 as a vector space over $\mathbb{Q}$ (elements in $\mathbb{Q}(\sqrt{d})$ can be written as vectors (a, b), fixing, for example, $\{1, \sqrt{d}\}$ as a basis).

Since $d > 1$, $\mathbb{Q}(\sqrt{d}) \subset \mathbb{R}$. It is clear that we have this field inclusion, but what is maybe less clear is that there are actually two meaningful ways of embedding $\mathbb{Q}(\sqrt{d})$ into $\mathbb{R}$:

S.I.R. Costa et al., *Lattices Applied to Coding for Reliable and Secure Communications*, SpringerBriefs in Mathematics,
https://doi.org/10.1007/978-3-319-67882-5_4

$$\sigma_1 : a + b\sqrt{d} \mapsto a + b\sqrt{d}$$
$$\sigma_2 : a + b\sqrt{d} \mapsto a - b\sqrt{d}$$

The first one, the identity map, is probably the one that everyone thinks of. However, the second one is just as "meaningful," in the sense that σ_2, just as σ_1, includes $\mathbb{Q}(\sqrt{d})$ into $\mathbb{R}$ while preserving (1) its ring structure ($\sigma_2(x+y) = \sigma_2(x) + \sigma_2(y)$ and $\sigma_2(xy) = \sigma_2(x)\sigma_2(y)$ for all $x, y \in \mathbb{Q}(\sqrt{d})$) (2) its vector space structure ($\sigma_2(a) = a$ for any $a \in \mathbb{Q}$). In fact, σ_1, σ_2 are the only two maps that satisfy the above (2) conditions. Suppose τ satisfies both of them, then:

$$\tau\left((\sqrt{d})^2\right) = \begin{cases} \tau(d) = d \\ \tau(\sqrt{d})^2 \end{cases}$$

and thus $\tau(\sqrt{d})$ must satisfy

$$\tau(\sqrt{d})^2 - d = 0$$

showing that $\tau(\sqrt{d}) = \pm\sqrt{d}$. As a consequence $\sigma = (\sigma_1, \sigma_2)$ gives an embedding of $\mathbb{Q}(\sqrt{d})$ into $\mathbb{R}^2$.

4.1.1 Lattice Constructions

Now our purpose is to obtain lattices, which are discrete structures. The above embedding suggests it may be possible to obtain 2-dimensional lattices, if we start from a discrete structure within $\mathbb{Q}(\sqrt{d})$. A natural candidate for this is

$$\mathbb{Z}[\sqrt{d}] = \left\{a + b\sqrt{d}, a, b, \in \mathbb{Z}\right\}.$$

Now $\mathbb{Z}[\sqrt{d}]$ is not a vector space, but it has a basis, given, for example, by $\{1, \sqrt{d}\}$. Embedding this basis using σ gives,

$$B = \begin{bmatrix} 1 & \sigma_1(\sqrt{d}) \\ 1 & \sigma_2(\sqrt{d}) \end{bmatrix} = \begin{bmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{bmatrix}$$

and integer linear combinations of rows of B do define a lattice (since the two rows are linearly independent). Note that

$$Bu = \begin{bmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{bmatrix} \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} = \begin{bmatrix} u_1 + u_2\sqrt{d} \\ u_1 - u_2\sqrt{d} \end{bmatrix} = \begin{bmatrix} \sigma_1(x) \\ \sigma_2(x) \end{bmatrix}, \; x = u_1 + u_2\sqrt{d} \tag{4.1}$$

which gives a nice geometric interpretation of how an element $x \in \mathbb{Z}[\sqrt{d}]$ is embedded in the lattice $\sigma(\mathbb{Z}[\sqrt{d}])$.

The lattice construction proposed above only relies on having a "discrete structure"[1] in $\mathbb{Q}(\sqrt{d})$ with a $\mathbb{Z}$-basis. If $d \equiv 1 (\mathrm{mod} 4)$, it is possible for example to take $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. Let us give some examples, before discussing the meaning of the condition $d \equiv 1 (\mathrm{mod} 4)$.

Example 4.1 The ring $\mathbb{Z}[\frac{1+\sqrt{5}}{2}] = \{a + b\frac{1+\sqrt{5}}{2},\ a, b \in \mathbb{Z}\}$ is a subset of the field $\mathbb{Q}(\sqrt{5}) = \{a + b\sqrt{5},\ a, b \in \mathbb{Q}\}$. The two ways of embedding $\mathbb{Q}(\sqrt{5})$ into $\mathbb{R}$ are:

$$\sigma_1 : \sqrt{5} \mapsto \sqrt{5},\ \sigma_2 : \sqrt{5} \mapsto -\sqrt{5}.$$

We then embed $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ into $\mathbb{R}^2$ using $\sigma = (\sigma_1, \sigma_2)$, to get a generator matrix

$$B = \begin{bmatrix} 1 & \sigma_1(\frac{1+\sqrt{5}}{2}) \\ 1 & \sigma_2(\frac{1+\sqrt{5}}{2}) \end{bmatrix}.$$

This lattice is shown in Fig. 4.2. Its corresponding Gram matrix is

$$G = B^T B = \begin{bmatrix} 1 & 1 \\ \sigma_1(\frac{1+\sqrt{5}}{2}) & \sigma_2(\frac{1+\sqrt{5}}{2}) \end{bmatrix} \begin{bmatrix} 1 & \sigma_1(\frac{1+\sqrt{5}}{2}) \\ 1 & \sigma_2(\frac{1+\sqrt{5}}{2}) \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 3 \end{bmatrix}.$$

To compare, a Gram matrix for the lattice $\sigma(\mathbb{Z}[\sqrt{5}])$, shown in Fig. 4.1, is

$$\begin{bmatrix} 1 & 1 \\ \sigma_1(\sqrt{5}) & \sigma_2(\sqrt{5}) \end{bmatrix} \begin{bmatrix} 1 & \sigma_1(\sqrt{5}) \\ 1 & \sigma_2(\sqrt{5}) \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 0 & 10 \end{bmatrix}.$$

Let us now consider $d \not\equiv 1 (\mathrm{mod} 4)$.

Example 4.2 The two ways of embedding $\mathbb{Q}(\sqrt{2})$ into $\mathbb{R}$ are:

$$\sigma_1 : \sqrt{2} \mapsto \sqrt{2},\ \sigma_2 : \sqrt{2} \mapsto -\sqrt{2}.$$

We then embed $\mathbb{Z}[\frac{1+\sqrt{2}}{2}]$ into $\mathbb{R}^2$ using $\sigma = (\sigma_1, \sigma_2)$, to get as Gram matrix

$$\begin{bmatrix} 1 & 1 \\ \sigma_1(\frac{1+\sqrt{2}}{2}) & \sigma_2(\frac{1+\sqrt{2}}{2}) \end{bmatrix} \begin{bmatrix} 1 & \sigma_1(\frac{1+\sqrt{2}}{2}) \\ 1 & \sigma_2(\frac{1+\sqrt{2}}{2}) \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 3/2 \end{bmatrix},$$

[1] Such suitable structures are orders (rings with a $\mathbb{Z}$-basis) and their ideals, which explains the terminology *ideal lattice*.

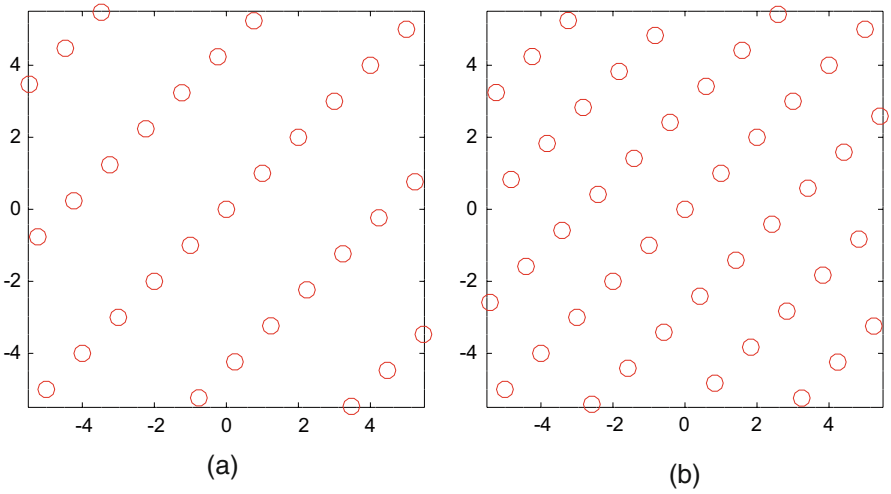


Fig. 4.1 Lattices from the quadratic fields $\mathbb{Z}[\sqrt{5}]$ and $\mathbb{Z}[\sqrt{2}]$, respectively. (**a**) The lattice obtained from $\{1, \sqrt{5}\}$. (**b**) The lattice obtained from $\{1, \sqrt{2}\}$

while a Gram matrix for the lattice $\sigma(\mathbb{Z}[\sqrt{2}])$ is

$$\begin{bmatrix} 1 & 1 \\ \sigma_1(\sqrt{2}) & \sigma_2(\sqrt{2}) \end{bmatrix} \begin{bmatrix} 1 & \sigma_1(\sqrt{2}) \\ 1 & \sigma_2(\sqrt{2}) \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 0 & 4 \end{bmatrix}.$$

This lattice is shown in Fig. 4.1.

The difference between the first example and the second is that in the first example, both Gram matrices have integer coefficients (the lattice is integral; see Definition 2.13), while in the second example, this is not the case.

The reason behind this is that the ring $\mathbb{Z}[\sqrt{d}]$ turns out to contain elements from $\mathbb{Q}(\sqrt{d})$ which all have the property of being the root of some monic polynomial whose coefficients live in $\mathbb{Z}$ (we recall that a polynomial $p(X)$ is monic if the coefficient of its leading term is equal to one). Now when $d \not\equiv 1 (\mathrm{mod} 4)$, it turns out (see Exercise 4.1) that $\mathbb{Z}[\sqrt{d}]$ is exactly the set of elements from $\mathbb{Q}(\sqrt{d})$ which are roots of monic polynomials with coefficients in $\mathbb{Z}$, while when $d \equiv 1 (\mathrm{mod} 4)$, this set is $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ and $\mathbb{Z}[\sqrt{d}] \subset \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$.

Now for a $\mathbb{Z}$-basis $\{\theta_1, \theta_2\}$ (of, respectively, $\mathbb{Z}[\sqrt{d}]$ or $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ depending on the congruence of $d (\mathrm{mod} 4)$ or of (an ideal of) an order of these two rings), a Gram matrix is of the form

$$\begin{aligned} &\begin{bmatrix} \sigma_1(\theta_1) & \sigma_2(\theta_1) \\ \sigma_1(\theta_2) & \sigma_2(\theta_2) \end{bmatrix} \begin{bmatrix} \sigma_1(\theta_1) & \sigma_1(\theta_2) \\ \sigma_2(\theta_1) & \sigma_2(\theta_2) \end{bmatrix} \\ &= \begin{bmatrix} \sigma_1(\theta_1)^2 + \sigma_2(\theta_1)^2 & \sigma_1(\theta_1)\sigma_1(\theta_2) + \sigma_2(\theta_1)\sigma_2(\theta_2) \\ \sigma_1(\theta_1)\sigma_1(\theta_2) + \sigma_2(\theta_1)\sigma_2(\theta_2) & \sigma_1(\theta_2)^2 + \sigma_2(\theta_2)^2 \end{bmatrix} \\ &= \begin{bmatrix} \sigma_1(\theta_1^2) + \sigma_2(\theta_1^2) & \sigma_1(\theta_1\theta_2) + \sigma_2(\theta_1\theta_2) \\ \sigma_1(\theta_1\theta_2) + \sigma_2(\theta_1\theta_2) & \sigma_1(\theta_2^2) + \sigma_2(\theta_2^2) \end{bmatrix}. \end{aligned}$$

If we observe the coefficients of this matrix, they all are of the form

$$\sigma_1(a + b\sqrt{d}) + \sigma_2(a + b\sqrt{d}) = 2a$$

for some $a, b \in \mathbb{Q}$, which explains why the Gram matrix coefficients are in $\mathbb{Q}$.

Now $\sigma_1(a + b\sqrt{d}), \sigma_2(a + b\sqrt{d})$ and thus $\sigma_1(a + b\sqrt{d}) + \sigma_2(a + b\sqrt{d})$ belong to the intersection of $\mathbb{Z}[\sqrt{d}]$ (or $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ depending on $d(\mathrm{mod}4)$) and $\mathbb{Q}$. We claim that this intersection is $\mathbb{Z}$, and therefore the Gram matrix has integer coefficients.

To prove that the intersection is $\mathbb{Z}$, recall that we are looking at elements in $\mathbb{Q}$, thus of the form u/v, $v \neq 0$, $u, v \in \mathbb{Z}$, and we can assume $\gcd(u, v) = 1$, which are roots of some monic polynomial $p(X)$ with coefficients in $\mathbb{Z}$. This means

$$p(u/v) = p_0 + p_1(u/v) + p_2(u/v)^2 + \cdots + p_{n-1}(u/v)^{n-1} + (u/v)^n = 0$$

which implies

$$v^n p_0 + p_1 u v^{n-1} + p_2 u^2 v^{n-2} + \cdots + p_{n-1} u^{n-1} v + u^n = 0.$$

Now it must be that

$$v^n p_0 + p_1 u v^{n-1} + p_2 u^2 v^{n-2} + \cdots + p_{n-1} u^{n-1} v = -u^n$$

but the left-hand side is divisible by v, while the right-hand side is not, a contradiction, apart for $v = 1$.

Canonical $\mathbb{Z}$-bases are $\{1, \sqrt{d}\}$ and $\{1, \frac{1+\sqrt{d}}{2}\}$ depending on d. A variety of interesting lattices can be obtained by introducing a "twisting" element α such that $\sigma_1(\alpha) > 0$ and $\sigma_2(\alpha) > 0$ as follows. Let θ denote $\sqrt{d}$ or $\frac{1+\sqrt{d}}{2}$ depending on $d(\mathrm{mod}4)$. A generator matrix of a lattice using a twisting element α is given by

$$B = \begin{bmatrix} \sqrt{\sigma_1(\alpha)} & \sqrt{\sigma_1(\alpha)}\sigma_1(\theta) \\ \sqrt{\sigma_2(\alpha)} & \sqrt{\sigma_2(\alpha)}\sigma_2(\theta) \end{bmatrix} = \begin{bmatrix} \sqrt{\sigma_1(\alpha)} & 0 \\ 0 & \sqrt{\sigma_2(\alpha)} \end{bmatrix} \begin{bmatrix} \sigma_1(1) & \sigma_1(\theta) \\ \sigma_2(1) & \sigma_2(\theta) \end{bmatrix}$$

and a Gram matrix by

$$B^T B = \begin{bmatrix} \sigma_1(\alpha) + \sigma_2(\alpha) & \sigma_1(\alpha\theta) + \sigma_2(\alpha\theta) \\ \sigma_1(\alpha\theta) + \sigma_2(\alpha\theta) & \sigma_1(\alpha\theta^2) + \sigma_2(\alpha\theta^2) \end{bmatrix}.$$

Note that the conditions $\sigma_1(\alpha) > 0$ and $\sigma_2(\alpha) > 0$ ensure that the lattice remains real (and no complex value is introduced when taking the square root). Furthermore, by taking α in $\mathbb{Z}[\theta]$, the lattice will remain an integral lattice, even though $\sqrt{\alpha}$ typically has no reason to be in $\mathbb{Z}[\theta]$. By Definition 2.4, the volume of the lattice[2] $\sigma(\sqrt{\alpha}\mathbb{Z}[\theta])$ is given by the square root of

[2]Writing $\sigma(\sqrt{\alpha}\mathbb{Z}[\theta])$ is a slight abuse of notation, since σ cannot really be applied to $\sqrt{\alpha}$ when it does not belong to $\mathbb{Z}[\theta]$.

$$\left(\det\begin{bmatrix}\sigma_1(1) & \sigma_2(1)\\ \sigma_1(\theta) & \sigma_2(\theta)\end{bmatrix}\right)^2 \left(\det\begin{bmatrix}\sqrt{\sigma_1(\alpha)} & 0\\ 0 & \sqrt{\sigma_2(\alpha)}\end{bmatrix}\right)^2 = \sigma_1(\alpha)\sigma_2(\alpha)(\sigma_2(\theta)-\sigma_1(\theta))^2,$$

thus

$$V(\sigma(\sqrt{\alpha}\mathbb{Z}[\theta])) = \sqrt{|\sigma_1(\alpha)\sigma_2(\alpha)|}|\sigma_2(\theta)-\sigma_1(\theta)|.$$

We continue Example 4.1.

Example 4.3 Take

$$\alpha = 3-\tfrac{1+\sqrt{5}}{2},\ \alpha\theta = -1+2\tfrac{1+\sqrt{5}}{2},\ \alpha\theta^2 = 2+\tfrac{1+\sqrt{5}}{2}.$$

Then a generator matrix of $\sigma(\sqrt{\alpha}\mathbb{Z}[\frac{1+\sqrt{5}}{2}])$, illustrated in Fig. 4.2 is

$$B = \begin{bmatrix}\sqrt{\alpha} & \sqrt{\alpha}\frac{1+\sqrt{5}}{2}\\ \sqrt{\sigma_2(\alpha)} & \sqrt{\sigma_2(\alpha)}\frac{1-\sqrt{5}}{2}\end{bmatrix}$$

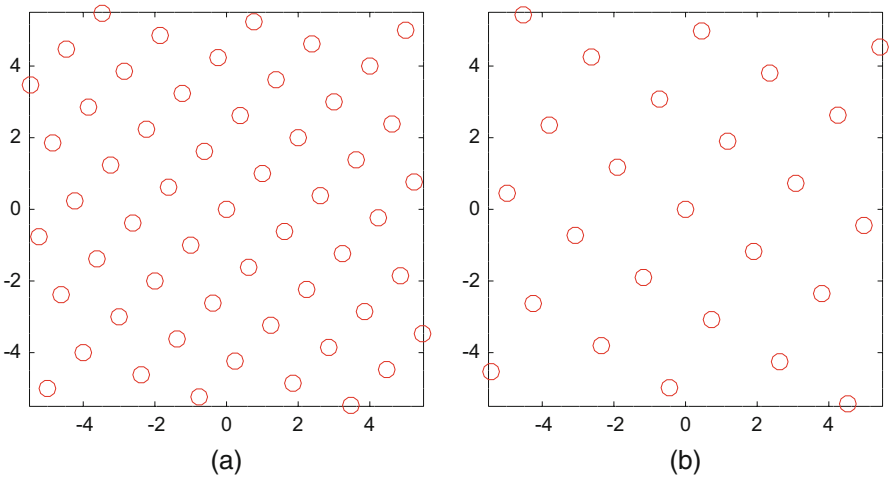


Fig. 4.2 Lattices from the quadratic field $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ with and without twisting. (**a**) The lattice obtained from $\{1, \frac{1+\sqrt{5}}{2}\}$. (**b**) The lattice obtained from $\{1, \frac{1+\sqrt{5}}{2}\}$ using a twisting element $\alpha = 3-\frac{1+\sqrt{5}}{2}$

with corresponding Gram matrix

$$G = \begin{bmatrix} \sigma_1(3-\frac{1+\sqrt{5}}{2})+\sigma_2(3-\frac{1+\sqrt{5}}{2}) & \sigma_1(-1+2\frac{1+\sqrt{5}}{2})+\sigma_2(-1+2\frac{1+\sqrt{5}}{2}) \\ \sigma_1(-1+2\frac{1+\sqrt{5}}{2})+\sigma_2(-1+2\frac{1+\sqrt{5}}{2}) & \sigma_1(2+\frac{1+\sqrt{5}}{2})+\sigma_2(2+\frac{1+\sqrt{5}}{2}) \end{bmatrix}$$
$$= \begin{bmatrix} 5 & 0 \\ 0 & 5 \end{bmatrix}$$

and volume

$$V(\sigma(\sqrt{\alpha}\mathbb{Z}[\tfrac{1+\sqrt{5}}{2}])) = \sqrt{|\sigma_1(\alpha)\sigma_2(\alpha)|}|\sigma_2(\theta)-\sigma_1(\theta)|$$
$$= \sqrt{5}|\sqrt{5}| = 5.$$

This lattice is equivalent to (a scaled version of) $\mathbb{Z}^2$ (see Exercise 4.3).

4.1.2 Some Sublattices

Consider two lattices $\sigma(\beta\mathbb{Z}[\sqrt{d}])$ and $\sigma(\alpha\mathbb{Z}[\sqrt{d}])$, or $\sigma(\beta\mathbb{Z}[\frac{1+\sqrt{d}}{2}])$ and $\sigma(\alpha\mathbb{Z}[\frac{1+\sqrt{d}}{2}])$, with $\beta = \alpha\sigma(\alpha)$, $\alpha \neq \sigma(\alpha)$. Then $\sigma(\beta\mathbb{Z}[\sqrt{d}])$ is a sublattice of $\sigma(\alpha\mathbb{Z}[\sqrt{d}])$, or in the other case, $\sigma(\beta\mathbb{Z}[\frac{1+\sqrt{d}}{2}])$ is a sublattice $\sigma(\alpha\mathbb{Z}[\frac{1+\sqrt{d}}{2}])$. Indeed, consider, for the former case, the sets $I_1 = \{\alpha a + \alpha b\sqrt{d},\ a, b \in \mathbb{Z}\}$, $I_2 = \{\sigma(\alpha)a + \sigma(\alpha)b\sqrt{d},\ a, b \in \mathbb{Z}\}$, and $I = \{\beta a + \beta b\sqrt{d},\ a, b \in \mathbb{Z}\}$. Define the sets I, I_1, I_2 accordingly for the latter case, and the following argument also hold by replacing $\sqrt{d}$ by $\frac{1+\sqrt{d}}{2}$. Then $I_1 + I_2 = 1$, from which it follows that $I_1 I_2 = I_1 \cap I_2$ (see Exercise 4.4), and $I_1 I_2 = I$, where $I_1 I_2$ is the set formed by finite sums of terms of the form $i_1 i_2$, $i_1 \in I_1$, $i_2 \in I_2$. Take the lattice point

$$\begin{bmatrix} \sigma_1(\beta x) \\ \sigma_2(\beta x) \end{bmatrix}$$

in $\sigma(\beta\mathbb{Z}[\sqrt{d}])$. It is obtained by embedding $\beta x \in I$, with $I = I_1 I_2 = I_1 \cap I_2$. Thus βx also belongs to I_1, so its embedding will appear in the embedding of I_1, which yields $\sigma(\alpha\mathbb{Z}[\sqrt{d}])$. This is illustrated in Fig. 4.3.

4.1.3 Coding Applications

Recall from (4.1) that points in lattices obtained from quadratic fields are of the form

$$\begin{bmatrix} \sigma_1(x) \\ \sigma_2(x) \end{bmatrix}, \text{ or } \begin{bmatrix} \sqrt{\sigma_1(\alpha)}\sigma_1(x) \\ \sqrt{\sigma_2(\alpha)}\sigma_2(x) \end{bmatrix}$$

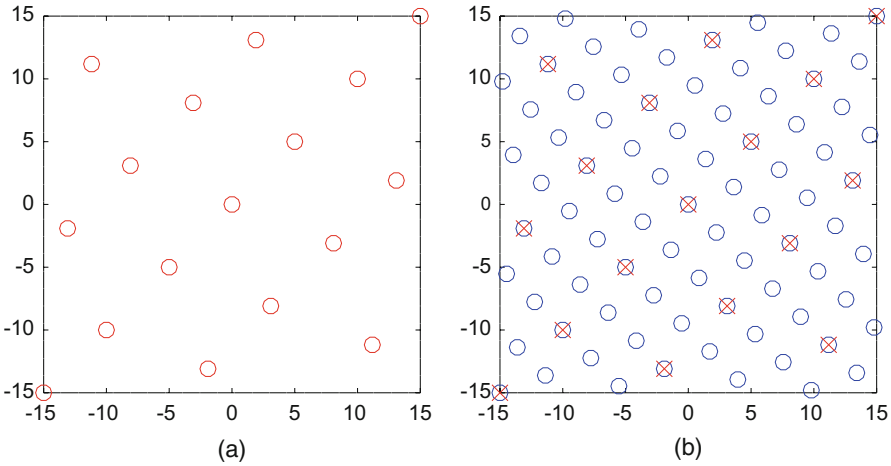


Fig. 4.3 The lattice $\sigma(5\mathbb{Z}[\frac{1+\sqrt{5}}{2}])$ and a sublattice. (**a**) The lattice obtained from $\{5, 5\frac{1+\sqrt{5}}{2}\}$. (**b**) The sublattice obtained from $\{\alpha, \alpha\frac{1+\sqrt{5}}{2}\}$, $\alpha = 3 - \frac{1+\sqrt{5}}{2}$

for $x = u_1 + u_2\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, depending on the presence or not of a twisting element α. Such pairs of points satisfy the property that

$$\sigma_1(x) \neq 0,\ \sigma_2(x) \neq 0$$

for all $x \neq 0$, since $\sigma_1(x) = u_1 + u_2\sqrt{d} = 0$ if and only if $x = 0$, and similarly $\sigma_2(x) = u_1 - u_2\sqrt{d} = 0$ if and only if $x = 0$. Now take any two arbitrary distinct lattice points

$$\begin{bmatrix}\sigma_1(x)\\ \sigma_2(x)\end{bmatrix},\ \begin{bmatrix}\sigma_1(y)\\ \sigma_2(y)\end{bmatrix},\ \text{or}\ \begin{bmatrix}\sqrt{\sigma_1(\alpha)}\sigma_1(x)\\ \sqrt{\sigma_2(\alpha)}\sigma_2(x)\end{bmatrix},\ \begin{bmatrix}\sqrt{\sigma_1(\alpha)}\sigma_1(y)\\ \sqrt{\sigma_2(\alpha)}\sigma_2(y)\end{bmatrix},$$

then their difference belongs to the lattice and

$$\begin{aligned}\sqrt{\sigma_1(\alpha)}\sigma_1(x) - \sqrt{\sigma_1(\alpha)}\sigma_1(y) &= \sqrt{\sigma_1(\alpha)}\sigma_1(x-y) \neq 0,\\ \sqrt{\sigma_2(\alpha)}\sigma_2(x) - \sqrt{\sigma_2(\alpha)}\sigma_2(y) &= \sqrt{\sigma_2(\alpha)}\sigma_2(x-y) \neq 0.\end{aligned}$$

Geometrically, this means that given any two distinct lattice points, they will always differ on both their components, as can be observed on the different earlier figures of this chapter.

This is meaningful when lattice points are used for transmission over fast-fading channels. We have already seen in Chap. 2 how lattice points are used for transmission over Gaussian channels. Over a fast-fading channel, communication is modeled by

$$\mathbf{y} = H\mathbf{x} + \mathbf{n},\ H = \begin{bmatrix} h_1 & 0 \\ 0 & h_2 \end{bmatrix}$$

where $\mathbf{n}$ is a random vector whose components are independent Gaussian random variables with mean 0 and variance σ^2, and h_1, h_2 are independently Rayleigh distributed. We notice that the model is very similar to (2.20), except for the matrix H which takes into account fading in a wireless environment. Assuming the receiver knows H (this is called a *coherent* channel), he is facing a channel similar to a Gaussian channel, only the lattice constellation transmitted is now twisted by the fading H. If $\mathbf{x}$ is a lattice point of the form $B\mathbf{u}$, then it is as if the lattice used for transmission had in fact generator matrix HB, and

$$H\mathbf{x} = \begin{bmatrix} h_1 & 0 \\ 0 & h_2 \end{bmatrix} \begin{bmatrix} \sigma_1(x) \\ \sigma_2(x) \end{bmatrix} = \begin{bmatrix} h_1\sigma_1(x) \\ h_2\sigma_2(x) \end{bmatrix}.$$

A lattice constellation for a Gaussian channel will make sure that lattice points are separated enough to resist the channel noise. However, even if $\sigma_j(x)$ and $\sigma_j(y)$ are designed to be apart, $h_j\sigma_j(x)$ and $h_j\sigma_j(y)$ could be arbitrarily close, depending on h_j, $j = 1, 2$.

The relevant distance in this case is the so-called *product distance*, which is the minimum of the absolute value of the product of the coordinates of non-zero vectors in the lattice. We may check (see Exercise 4.5) that the product distance, despite its name, is actually not a distance, as per Definition 3.2. It was shown that constellations in lattices with greater minimum product distance are associated to smaller error probability when used in signal transmission over Rayleigh fading channels [15]. The intuition is that the product distance captures the number of components in which lattice points (and therefore differences of lattice points) differ, guaranteeing that if the fading affects some components, the lattice points will still be distinguishable on their other non-zero components. Therefore lattices Λ in $\mathbb{R}^n$ with full diversity n are preferred, that is, lattices such that any of their vectors $\mathbf{x} = (x_1, x_2, \ldots, x_n)$, have $x_i \neq 0$, for any i. For a general lattice, it is computationally hard to determine its minimum product distance, which makes the interest of algebraic constructions of the type presented above; see, e.g., [9, 58]. Furthermore, since for a lattice in dimension n, its diversity is at most n, it can be increased by augmenting n, the dimension in which the lattice lives. One technique to do so is by considering tensor products, as explained next.

4.1.4 High-Dimensional Lattices

Consider two generator matrices

$$B_1 = \begin{bmatrix} \sigma_1(\theta_1) & \sigma_1(\theta_2) \\ \sigma_2(\theta_1) & \sigma_2(\theta_2) \end{bmatrix},\ B_2 = \begin{bmatrix} \tau_1(\nu_1) & \tau_1(\nu_2) \\ \tau_2(\nu_1) & \tau_2(\nu_2) \end{bmatrix}$$

and their Kronecker (tensor) product

$$B_1 \otimes B_2 = \begin{bmatrix} \sigma_1(\theta_1)B_2 & \sigma_1(\theta_2)B_2 \\ \sigma_2(\theta_1)B_2 & \sigma_2(\theta_2)B_2. \end{bmatrix}$$

Surely this defines the generator matrix of a 4-dimensional lattice, since the columns of this matrix are linearly independent: the determinant of the generator matrix is the product of the determinants of B_1 and B_2. Now in terms of diversity, it is harder to say something in general, though there is one case where we can easily show that the property of diversity is inherited from B_1 and B_2. Suppose that $\tau_i(\theta_j) = \theta_j$ and $\sigma_i(\nu_j) = \nu_j$, and we place ourselves in a large enough field[3] which contains θ_j, ν_j, and for which τ_i, σ_i are embeddings. Then

$$B_1 \otimes B_2 = \begin{bmatrix} \sigma_1\tau_1(\theta_1\nu_1) & \sigma_1\tau_1(\theta_1\nu_2) & \sigma_1\tau_1(\theta_2\nu_1) & \sigma_1\tau_1(\theta_2\nu_2) \\ \sigma_1\tau_2(\theta_1\nu_1) & \sigma_1\tau_2(\theta_1\nu_2) & \sigma_1\tau_2(\theta_2\nu_1) & \sigma_1\tau_2(\theta_2\nu_2) \\ \sigma_2\tau_1(\theta_1\nu_1) & \sigma_2\tau_1(\theta_1\nu_2) & \sigma_2\tau_1(\theta_2\nu_1) & \sigma_2\tau_1(\theta_2\nu_2) \\ \sigma_2\tau_2(\theta_1\nu_1) & \sigma_2\tau_2(\theta_1\nu_2) & \sigma_2\tau_2(\theta_2\nu_1) & \sigma_2\tau_2(\theta_2\nu_2) \end{bmatrix}$$

which is now the generator matrix of a lattice of dimension 4 and diversity 4. This process can be iterated to obtain lattices in dimensions which are powers of 2 (see Exercise 4.6).

Example 4.4 Take

$$B_1 = \begin{bmatrix} 1 & \sigma_1(\frac{1+\sqrt{5}}{2}) \\ 1 & \sigma_2(\frac{1+\sqrt{5}}{2}) \end{bmatrix}, \; B_2 = \begin{bmatrix} 1 & \tau_1(\sqrt{2}) \\ 1 & \tau_2(\sqrt{2}) \end{bmatrix}.$$

We place ourselves in $\mathbb{Q}(\sqrt{2}, \sqrt{5}) = \{a_0 + a_1\sqrt{5} + a_2\sqrt{2} + a_3\sqrt{5}\sqrt{2},\ a_0, a_1, a_2, a_3 \in \mathbb{Q}\}$, so that $\sigma(\sqrt{2}) = \sqrt{2}$ and $\tau(\sqrt{5}) = \sqrt{5}$. Then $B_1 \otimes B_2$ is a 4-dimensional lattice with diversity 4.

4.2 Ideal Lattices for Cryptography

Consider a lattice Λ of dimension n living in $\mathbb{Z}^n$ instead of $\mathbb{R}^n$, meaning that all lattice points have integer coordinates. Now we ask for the following further *cyclic* property that for every $\mathbf{x} = (x_1, \ldots, x_n) \in \Lambda$, it must be that $(x_n, x_1, \ldots, x_{n-1})$ also belongs to Λ. Note that since the cyclic property is asked for every lattice point, it means that $(x_{n-1}, x_n, x_1, \ldots, x_{n-2}) \in \Lambda$ and, iteratively, all shifts of $\mathbf{x} = (x_1, \ldots, x_n)$ must be in Λ.

[3] We voluntarily skip the definition of compositum of two fields with coprime discriminants here, which would be the proper way to describe the suitable field extension.

Example 4.5 The lattice $\mathbb{Z}^2$ is cyclic. Indeed, if $(x_1, x_2) \in \mathbb{Z}^2$, this means that x_1, x_2 are integers, and (x_2, x_1) also belongs to $\mathbb{Z}^2$.

One way to obtain cyclic lattices is to use the following lemma.[4]

Lemma 4.1 *A lattice Λ in $\mathbb{Z}^n$ is a cyclic lattice if Λ is an ideal of $\mathbb{Z}[X]/(X^n - 1)$.*

Proof Given a lattice point $\mathbf{a} = (a_1, \cdots, a_n) \in \Lambda$, associate the polynomial in $\mathbb{Z}[X]$ given by $a_1 + a_2X + a_3X^2 + \ldots a_nX^{n-1}$. We notice that this polynomial belongs to $\mathbb{Z}[X]/(X^n - 1)$ since its degree is less than n. By definition of ideal, Λ is an ideal of $\mathbb{Z}[X]/(X^n - 1)$ means that it is closed under multiplication, that is, if we multiply $a_1 + a_2X + a_3X^2 + \ldots a_nX^{n-1}$ by X (and iteratively by powers of X), the result remains in Λ. But if we compute

$$(a_1 + a_2X + a_3X^2 + \ldots a_nX^{n-1})X = a_1X + a_2X^2 + a_3X^3 + \cdots a_nX^n,$$

we obtain $a_1X + a_2X^2 + a_3X^3 + \ldots a_n$ since $X^n \equiv 1$ in $\mathbb{Z}[X]/(X^n - 1)$. This shows that $(a_n, a_1, \ldots, a_{n_1}) \in \Lambda$ as desired.

Example 4.6 Consider $\mathbb{Z}[X]/(X^2 - 1)$, which is the set of polynomials $a_1 + a_2X$, $a_1, a_2 \in \mathbb{Z}$. Take the polynomial $g(X) = 2 + X \in \mathbb{Z}[X]/(X^2 - 1)$ and the ideal $(g(X))$ which is the set of all polynomials in $\mathbb{Z}[X]/(X^2 - 1)$ which are multiples of $g(X)$. It is indeed an ideal since it is closed under addition:

$$g(X)(a_1 + a_2X) + g(X)(a_1' + a_2'X)$$

is a multiple of $g(X)$. It is also clearly closed under multiplication: a multiple of $g(X)$ multiplied by any polynomial will remain a multiple of $g(X)$. Furthermore:

$$(2 + X)(a_1 + a_2X) = 2a_1 + 2a_2X + a_1X + a_2 = (a_2 + 2a_1) + (2a_2 + a_1)X.$$

This gives a set of vectors of the form $(a_2 + 2a_1, 2a_2 + a_1)$ corresponding to a generator matrix:

$$\begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}.$$

One may check explicitly (see Exercise 4.7) that this lattice is indeed cyclic.

Remark 4.1 The quotient $\mathbb{Z}[X]/(X^n - 1)$ does not have a field structure, therefore the underlying multiplicative structure of this construction is different from that of the previous "ideal lattices."

One interest in this construction of lattices is its succinct representation, since an n-dimensional lattice can be encoded with one vector. Furthermore, fast arithmetic

[4] A reader familiar with the theory of cyclic codes will notice the analogy between cyclic codes and cyclic lattices and their characterization.

is enabled using the fast Fourier transform (FFT). Yet unlike the q-ary lattices of Sect. 3.2.1, ideal lattices come with some guarantee in terms of complexity, e.g., the worst-case hardness of the SVP (see Problem 2.1) in cyclic lattices was analyzed in [71], to build one-way functions. Thus cyclic ideal lattices have been considered to build efficient cryptographic primitives and homomorphic encryption schemes. However, such lattice exhibit some weaknesses; see, e.g., [73, p.11], due to the fact that $X^n - 1$ is reducible over the rationals.

A natural generalization is to consider a polynomial[5] $p(X) \in \mathbb{Z}[X]$ other than $X^n - 1$, such as $X^n + 1$, for example, (in particular, the factor $X - 1$ of $X^n - 1$ is not present, and thus $X^n + 1$ tends to be preferred to $X^n - 1$). If $p(X)$ is instead a monic irreducible polynomial ($X^n - 1$ is not), then the quotient $\mathbb{Z}[X]/(p(X))$ becomes a field. A family of polynomials that has been considered in the literature is that of cyclotomic polynomials. The *m-th cyclotomic polynomial* $\phi_m(X)$ is by definition

$$\phi_m(X) = \prod_{k,\gcd(k,m)=1} (X - e^{\frac{2ik\pi}{m}}).$$

If m is prime, then $\phi_m(X) = \frac{X^m-1}{X-1}$. If m is a power of 2, then $\phi_m(X) = X^{m/2} + 1$ (see Exercise 4.8). We use the notation $\zeta_m = e^{\frac{2ik\pi}{m}}$. In that case, we have

$$\mathbb{Z}[X]/(\phi_m(X)) \simeq \mathbb{Z}[\zeta_m] \subset \mathbb{Q}(\zeta_m) \simeq \mathbb{Q}(X)/(\phi_m(X))$$

and $\mathbb{Q}(\zeta_m) = \{a_1 + a_2\zeta_m + \cdots + a_{d-1}\zeta_m^{d-1},\ a_1, \ldots, a_{d-1} \in \mathbb{Q}\}$ and $d = \varphi(n)$ is the Euler totient of n. The reason for considering cyclotomic polynomials is that they have been well studied.

Remark 4.2 Unlike for the quotient $\mathbb{Z}[X]/(X^n - 1)$, in this case of cyclotomic polynomials, both notions of "ideal lattices" coincide.

Thus to a vector, $(a_1, \ldots, a_{d-1})$ corresponds a polynomial $a_1 + a_2X + \cdots + a_{d-1}X^{d-1}$ in $\mathbb{Z}[X]/\phi_m(X)$, which in turn corresponds to an element $a_1 + a_2\zeta_m + \cdots + a_{d-1}X^{d-1} \in \mathbb{Q}(\zeta_m)$. The corresponding lattice is now obtained by embedding $\mathbb{Q}(\zeta_m)$ into $\mathbb{C}^n$. We illustrate this for the case $m = 4$, corresponding to the cyclotomic polynomial $\phi_4(X) = X^2 + 1$. Then $\mathbb{Q}(X)/(X^2 + 1) \simeq \mathbb{Q}(i)$.There are two embeddings (see the previous ideal construction):

$$\sigma_1 : i \mapsto i,\ \sigma_2 : i \mapsto -i.$$

A generator matrix is given by

$$\begin{bmatrix} 1 & i \\ 1 & -i \end{bmatrix}.$$

[5]For linear codes, we would call these pseudo-cyclic codes.

There is a similar problem to that of the shortest vector problem (see Problem 2.1) for ideal (see [102], [84], Sec. 4.3.4. and the references therein). Consider $\sigma = (\sigma_1, \ldots, \sigma_d)$ the vector of embeddings of a degree-d number field K.

Problem 4.1 Given an ideal I of $\mathcal{O}_K$, where K is a number field, find a non-zero element $b \in I$ which minimizes $\|\sigma(b)\|$.

The complexity of ideal lattice problems are summarized in [102], together with applications.

Exercises

Exercise 4.1 Show that the set of elements from $\mathbb{Q}(\sqrt{d})$ which are roots of monic polynomials with coefficients in $\mathbb{Z}$ is $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ when $d \equiv 1 (\mathrm{mod} 4)$ and $\mathbb{Z}[\sqrt{d}]$ when $d \not\equiv 1 (\mathrm{mod} 4)$.

Exercise 4.2 Construct a 2-dimensional lattice from $\mathbb{Z}[\sqrt{3}]$.

Exercise 4.3 Show that the lattice $\sigma(\sqrt{\alpha}\mathbb{Z}[(1 + \sqrt{5})/2])$ in Example 4.3 is equivalent to $\mathbb{Z}^2$. Exhibit the explicit orthogonal transformation matrix and scaling factor.

Exercise 4.4 Show that the sets $I_1 = \{\alpha a + \alpha b\sqrt{d},\ a, b \in \mathbb{Z}\}$, $I_2 = \{\sigma(\alpha)a + \sigma(\alpha)b\sqrt{d},\ a, b \in \mathbb{Z}\}$ and $I = \{\beta a + \beta b\sqrt{d},\ a, b \in \mathbb{Z}\}$ with $\beta = \alpha\sigma(\alpha), \alpha \neq \sigma(\alpha)$ satisfy $I_1 I_2 = I_1 \cap I_2$. Discuss what happens if $\alpha = \sigma(\alpha)$.

Exercise 4.5 Show that the product distance is not a mathematical distance.

Exercise 4.6 Construct an 8-dimensional lattice by tensor product.

Exercise 4.7 Show that the lattice with generator matrix

$$\begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$$

is cyclic.

Exercise 4.8 Prove that for m a power of 2, the cyclotomic polynomial is $\phi_m(X) = X^{m/2} + 1$.

Chapter 5
Lattices and Spherical Codes

Lattices in $\mathbb{R}^n$ with sublattices which have an orthogonal basis are associated with spherical codes in $\mathbb{R}^{2n}$ generated by a finite commutative group of orthogonal matrices. They also can be used to construct homogeneous spherical curves for transmitting a continuous alphabet source over an AWGN channel. In both cases, the performance of the decoding process is related to the packing density of the lattices (see (2.13)). In the continuous case, the packing density of these curves relies on the search for projection lattices with good packing density. We present here a survey on this topic mainly based on [18, 31, 96, 105].

5.1 Spherical and Geometrically Uniform Codes

Consider the sphere of radius a in $\mathbb{R}^n$, $S^{n-1}(a) = \{\mathbf{x} \in \mathbb{R}^n; \|\mathbf{x}\| = a \geq 0\}$. A *spherical code* is a finite set of M points on this sphere. Usually we consider only spherical codes on the sphere of radius one, $S^{n-1} = S^{n-1}(1)$, and all the conclusions will be extended by similarity to a sphere of radius a. Two dual optimization (packing) problems regarding spherical codes, which have several applications in physics, chemistry, architecture, and signal processing, can be stated as:

Problem 1 Given a dimension n and an integer number $M > 0$, find a spherical code with M points such that the minimum distance between two points in the code is the largest possible.

Problem 2 Given a dimension n and a minimum distance $d > 0$, find a spherical code with the biggest number M of points such that each two of them are at distance at least d.

Codes which are solutions for one of these problems are called optimal spherical codes. In dimension 2, codes which are vertices of regular polygons inscribed in S^1 provide solutions for both problems. The solution of Problem 1 in dimension 3

S.I.R. Costa et al., *Lattices Applied to Coding for Reliable and Secure Communications*, SpringerBriefs in Mathematics,
https://doi.org/10.1007/978-3-319-67882-5_5

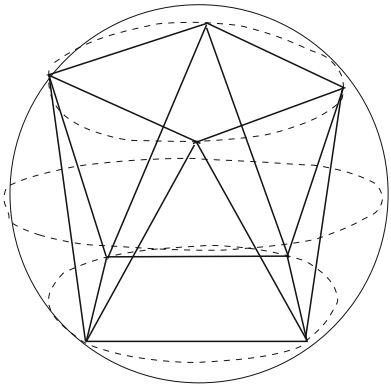


Fig. 5.1 Antiprism with eight vertices

is only known up to now for $1 \leq M \leq 12$ and for $M = 24$ [37]. As examples, for $M = 2$, 3, and 4, the optimal spherical codes in $\mathbb{R}^3$ are two antipodal points, the vertices of an equilateral triangle inscribed on an "equator" and the vertices of an inscribed regular tetrahedron in $S^2 \subset \mathbb{R}^3$, respectively. For $M = 8$ the optimal spherical code in $\mathbb{R}^3$ is given by the vertices, not of a cube as one could have possibly expected, but of a regular (with same length edges) antiprism with *eight* vertices (Fig. 5.1).

Other spherical codes known to be optimal for their minimum distances are the biorthogonal codes of $2n$ points in $\mathbb{R}^n$, obtained as all coordinate permutations of the vectors $(0, 0, \ldots, 0, \pm 1)$, and the simplex code which is the n-dimensional version of the triangle and tetrahedron vertices. It has $M = n+1$ points and can be described in the unit sphere in $\mathbb{R}^{n+1}$ as all permutations of the vector $\frac{1}{\sqrt{n+n^2}}(1, 1, \ldots, 1, -n)$. The distance between any two distinct points in this code is $\sqrt{\frac{2(n+1)}{n}}$.

Group codes as introduced by Slepian [97] and developed in subsequent articles [11, 16, 54, 64] are defined as finite sets on an n-dimensional sphere generated by the action of a group of orthogonal matrices. Geometrically uniform codes introduced by Forney [42] generalize this concept by considering also infinite sets of points in the Euclidean space having a transitive symmetry group. We consider this concept in the context of metric spaces [29]: for X a metric space, a signal set $S \subset X$ is a geometrically uniform code if and only if for s, t in S, there is an isometry f (depending on s, t) in X such that $f(s) = t$ and $f(S) = S$. Geometrically uniform codes capture the highly desirable properties that come from homogeneity: the same distance profile, congruent Voronoi regions in the same sense as defined for lattices, and the same error transmission probability for each codeword. One recurrent metric space considered here is the n-dimensional flat torus, obtained by identifying the opposite sides of an n-dimensional box and which can be defined as a quotient $T = \mathbb{R}^n/\Lambda$ where Λ is the group of translations generated by the n independent vectors which define this box (Λ is a lattice).

5.2 Flat Tori

A 2-dimensional flat torus can be visualized as a standard torus in the 3-dimensional space (Fig. 5.2), but it can be distinguished from the latter by being locally like a piece of plane (flat). One flat surface in $\mathbb{R}^3$ is a cylinder, obtained by identifying the boundaries of a rectangle. The flat torus can only be realized isometrically as a 2-dimensional surface in $\mathbb{R}^4$, and it is contained in a 3-dimensional sphere. For $\mathbf{c} = (c_1, c_2)$ with c_1, c_2 positive numbers such that $c_1^2 + c_2^2 = 1$, consider the map $\Phi_{\mathbf{c}} : \mathbb{R}^2 \to \mathbb{R}^4$, defined as $\Phi_{\mathbf{c}}(u_1, u_2) = (c_1 \cos(\frac{u_1}{c_1}), c_1 \sin(\frac{u_1}{c_1}), c_2 \cos(\frac{u_2}{c_2}), c_2 \sin(\frac{u_2}{c_2}))$. Observe that this map is doubly periodic, having identical images in the translates of the rectangle $[0, 2\pi c_1) \times [0, 2\pi c_2)$ by vectors $(k_1 2\pi c_1, k_2 2\pi c_2)$, k_i integers, and that its image is contained in a sphere of radius one in $\mathbb{R}^4$.

The parallel boundaries of each of these rectangles will be "glued" together and form a 2-dimensional surface with zero curvature – *the flat torus* $T_{\mathbf{c}}$. For each pair $\mathbf{c}$ under the above condition, we have a flat torus, and the sphere S^3 in $\mathbb{R}^4$ can be obtained as the union (foliation) of these tori. In Fig. 5.3 we can see for $\mathbf{c} = (0.8, 0.6)$, the tessellation of the plane given by the associated torus map. Note also that $\Phi_{\mathbf{c}}^{-1}(c_1, 0, c_2, 0)$ is the lattice given by the vertices of the rectangles. Spherical codes in $\mathbb{R}^4$ which are the image through a torus map of lattices in $\mathbb{R}^2$ with rectangular sublattices, as the one in the example of Fig. 5.3, present special homogeneous properties to be discussed in the next sections.

We next describe how any sphere in even dimensions $n = 2L$ can be considered as foliated by L-dimensional flat tori. Inequalities relating the distances on a flat torus in $\mathbb{R}^{2L}$ and on its associated hyperbox in $\mathbb{R}^L$ to be used in the next sections are also presented.

The unit sphere $S^{2L-1} \subset \mathbb{R}^{2L}$ can be foliated by flat tori (also called Clifford tori) as follows. For each unit vector $\mathbf{c} = (c_1, c_2, ..., c_L) \in S^{L-1}, c_i > 0, \sum_{i=1}^{L} c_i^2 = 1$, and $\mathbf{u} = (u_1, u_2, \ldots, u_L) \in \mathbb{R}^L$, let $\Phi_{\mathbf{c}} : \mathbb{R}^L \to \mathbb{R}^{2L}$ be defined as

$$\Phi_{\mathbf{c}}(\mathbf{u}) = \left(c_1 \cos\left(\frac{u_1}{c_1}\right), c_1 \sin\left(\frac{u_1}{c_1}\right), \ldots, c_L \cos\left(\frac{u_L}{c_L}\right), c_L \sin\left(\frac{u_L}{c_L}\right) \right). \tag{5.1}$$

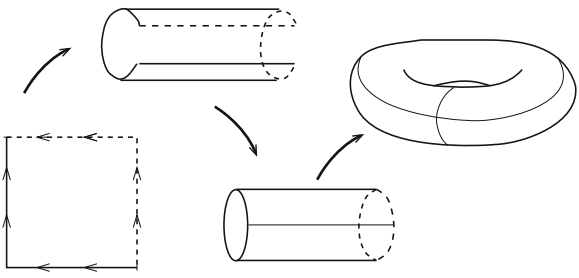


Fig. 5.2 A view of the 2-dimensional flat torus which only can be realized in $\mathbb{R}^4$

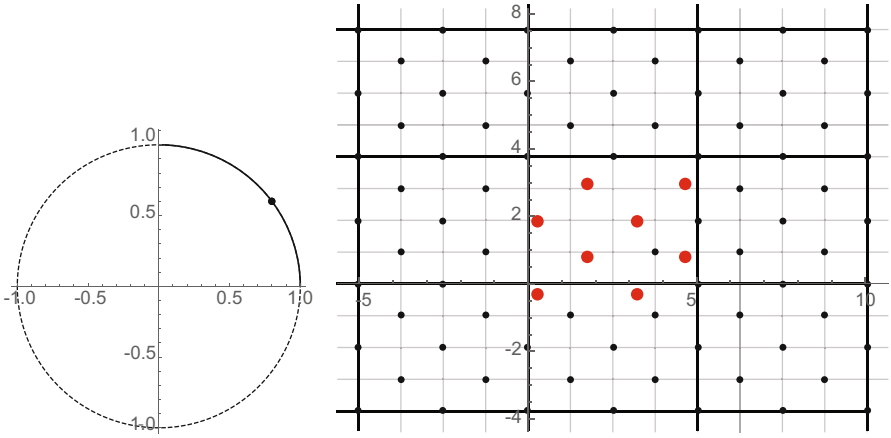


Fig. 5.3 The tessellation of the plane associated to $\mathbf{c} = (0.8, 0.6) \in S^1$, and a lattice Λ (black dots) which contains $2\pi c_1\mathbb{Z} \times 2\pi c_2\mathbb{Z}$ as a rectangular sublattice. In this case $\phi_{\mathbf{c}}(\Lambda)$ is a spherical code with $M = 8$

The image of this periodic map $\Phi_{\mathbf{c}}$ is the torus $T_{\mathbf{c}}$, a flat L-dimensional surface contained in the unit sphere S^{2L-1}, and $T_{\mathbf{c}}$ is also the image of an L-dimensional box $\mathscr{P}_{\mathbf{c}}$,

$$\mathscr{P}_{\mathbf{c}} = \{\mathbf{u} \in \mathbb{R}^L; 0 \leq u_i < 2\pi c_i, \;\; 1 \leq i \leq L\}. \tag{5.2}$$

The restriction of $\Phi_{\mathbf{c}}$ to $\mathscr{P}_{\mathbf{c}}$ is injective.

For $\mathbf{c} \in S^{L-1}$ and $c_i \geq 0$, if $c_i = 0$ for some $1 \leq i \leq L$, we may replace in (5.1) the coordinates related to c_i by 0 and obtain a degenerated flat torus $T_{\mathbf{c}}$, which is an embedding of a $(L-k)$-dimensional box in $\mathbb{R}^{2L}$, where k is the number of zero coordinates of $\mathbf{c}$.

The Gaussian curvature of a torus $T_{\mathbf{c}}$ is zero, and $T_{\mathbf{c}}$ can be cut and flattened into the box, $\mathscr{P}_{\mathbf{c}}$, just as a cylinder in $\mathbb{R}^3$ can be cut and flattened into a 2-dimensional rectangle [103]. Since the inner product $\langle \partial\Phi_{\mathbf{c}}/\partial u_i, \partial\Phi_{\mathbf{c}}/\partial u_j\rangle = \delta_{ij}$, where δ_{ij} is the Kronecker delta function, the application $\Phi_{\mathbf{c}}$ is a local isometry, which means that any measure of length, area, and volume up to dimension $L-k$ on $T_{\mathbf{c}}$ is the same of the corresponding pre-image in the box $\mathscr{P}_{\mathbf{c}}$.

We say that the family of flat tori $T_{\mathbf{c}}$ and their degenerations, with $\mathbf{c} = (c_1, c_2, ..., c_L)$, $\|\mathbf{c}\| = 1$, $c_i \geq 0$, defined above is a foliation on the unit sphere of $S^{2L-1} \subset \mathbb{R}^{2L}$. This means that any vector of S^{2L-1} belongs to one and only one of these flat tori.

The following results [105, 107] allow to relate the distances between two points in $\mathbb{R}^L$ and their spherical image on a flat tori in $\mathbb{R}^{2L}$.

Proposition 5.1 *[[105, 107]] Let $T_{\mathbf{b}}$ and $T_{\mathbf{c}}$ be two flat tori, defined by unit vectors* $\mathbf{b}$ *and* $\mathbf{c}$ *with nonnegative coordinates. The minimum distance $d(T_{\mathbf{c}}, T_{\mathbf{b}})$ between two points $\Phi_{\mathbf{c}}(\mathbf{u})$ and $\Phi_{\mathbf{c}}(\mathbf{v})$ on these flat tori is*

$$d(T_{\mathbf{c}}, T_{\mathbf{b}}) = \|\mathbf{c} - \mathbf{b}\| = \left(\sum_{i=1}^{L} (c_i - b_i)^2 \right)^{1/2}. \tag{5.3}$$

The distance between two points $\Phi_{\mathbf{c}}(\mathbf{u})$ and $\Phi_{\mathbf{c}}(\mathbf{v})$ on the same torus $T_{\mathbf{c}}$, defined by a vector $\mathbf{c} = (c_1, \cdots, c_L)$, is given by

$$||\Phi_{\mathbf{c}}(\mathbf{u}) - \Phi_{\mathbf{c}}(\mathbf{v})|| = 2\sqrt{\sum c_i^2 \sin^2\left(\frac{u_i - v_i}{2c_i}\right)} \tag{5.4}$$

and it is bounded according to the next proposition [105].

Proposition 5.2 ([106]) *Let* $\mathbf{c} = (c_1, c_2, ..., c_L) \in S^{2L-1}$, $c_i > 0$, $c_\xi = \min_{1 \le i \le L} c_i \neq 0$, $\Delta = \|\mathbf{u} - \mathbf{v}\|$ *for* $\mathbf{u}, \mathbf{v} \in \mathscr{P}_c$. *Suppose* $0 < \Delta \le c_\xi$, *then*

$$\frac{2\Delta}{\pi} \le \sin\left(\frac{\Delta}{2c_\xi}\right) 2c_\xi \le \|\Phi_{\mathbf{c}}(\mathbf{u}) - \Phi_{\mathbf{c}}(\mathbf{v})\| \le 2 \sin\frac{\delta}{2} \le \Delta.$$

Note that this last proposition shows that, for small values, the distance in $\mathbb{R}^{2L}$ between two points in a flat torus can be approached by the distance of the original points in the box $\mathscr{P}_c$ in half of the dimension.

The upcoming Sect. 5.3 is a strongly geometrical approach to commutative group codes presenting their connections with flat tori and quotient of lattices which allows the establishment of specific upper bounds on the number of points of those codes. Some results on constructions which may approach those bounds for optimal commutative group codes are discussed. Remarks on commutative group codes considered on graphs are also included. Section 5.4.1 summarizes a construction of spherical codes on layers of flat tori with some comparisons with well-known spherical codes. In Sect. 5.4.2 the homogeneous structure of flat tori and lattices come together again now in a coding scheme for transmitting continuous alphabet source over an AWGN channel. The search for projection lattices with good packing density plays a crucial role in this case.

5.3 Commutative Group Codes, Flat Tori, and Lattices

5.3.1 Commutative Group Codes

Let $\mathscr{O}_n$ be the multiplicative group of orthogonal $n \times n$ matrices and $\mathscr{G}_n(M)$ be the set of all order M commutative subgroups in $\mathscr{O}_n$.

A spherical *commutative group code* $\mathscr{C}$ is a set of M vectors which is the orbit of an initial vector $\mathbf{u}$ on the unit sphere $S^{n-1} \subset \mathbb{R}^n$ by a given finite group $G \in \mathscr{G}_n(M)$, i.e., $\mathscr{C} := G\mathbf{u} = \{g\mathbf{u}, g \in G\}$. Recalling the definition of *orthogonal matrix* in Sect. 2.1.1, one can see that starting from a vector in the sphere, all elements of $\mathscr{C}$ will be also in the sphere, and therefore $\mathscr{C}$ is indeed a spherical code.

The *minimum distance* in $\mathscr{C}$ is:

$$d := \min_{\substack{\mathbf{x},\mathbf{y} \in \mathscr{C} \\ \mathbf{x} \neq \mathbf{y}}} ||\mathbf{x} - \mathbf{y}|| = \min_{g_i \neq \mathbf{I} \in G} ||g_i\mathbf{x} - \mathbf{x}||,$$

where $||.||$ denotes the standard Euclidean norm.

A canonical form for a commutative group $G \in \mathscr{G}_n(M)$ can be obtained from the following result.

Proposition 5.3 ([43, p. 292]) *All the matrices O_i of a commutative group $\mathscr{O} = \{O_i\}_{i=1}^M$ of $n \times n$ orthogonal real matrices can simultaneously be put into a diagonal block canonical form through an orthogonal matrix Q:*

$$Q^T O_i Q = \left[\mathrm{Rot}\left(\frac{2\pi b_{i1}}{M}\right), \ldots, \mathrm{Rot}\left(\frac{2\pi b_{iq}}{M}\right), \mu_{2q+1}(i), \ldots, \mu_n(i) \right], \tag{5.5}$$

where b_{ij} are integers, the blocks $Rot(a)$ are the ones associated with 2-dimensional rotations by an angle of a radians:

$$\mathrm{Rot}(a) = \begin{bmatrix} \cos(a) & -\sin(a) \\ \sin(a) & \cos(a) \end{bmatrix},$$

and $\mu_l(i) = \pm 1$ with $l = 2q + 1, \ldots, n$.

The next proposition [28, 96] describes the geometric locus of a commutative group code. For even dimension this locus is always contained in a flat torus.

Proposition 5.4 *Every commutative group code of order M is, up to isometry, equal to a spherical code $\mathscr{X}$ whose initial vector is $\mathbf{u} = (u_1, \ldots, u_n)$, and its points have the form*

$$(\mathrm{Rot}(a_{i1})(u_1, u_2), \ldots, \mathrm{Rot}(a_{iq})(u_{2q-1}, u_{2q}), \mu_{2q+1}(i)u_{2q+1}, \ldots, \mu_n(i)u_n),$$

where $a_{ij} = \dfrac{2\pi b_{ij}}{M}$. Moreover,

1. *If $n = 2L$, $\mathscr{X}$ is contained in the flat torus $T_{\mathbf{c}}$, $\mathbf{c} = (c_1, \ldots, c_L)$ where $\mathbf{c}_i^2 = u_{2i-1}^2 + u_{2i}^2$.*
2. *If $n = 2L + 1$ and $\mathscr{X}$ is not contained in a hyperplane, $\mathscr{X} = \mathscr{X}_1 \cup \mathscr{X}_2$, where $\mathscr{X}_i$ is contained in the plane $\mathscr{P}_i = \{(x_1, \ldots, x_{2L+1}) \in \mathbb{R}^{2L+1}; x_{2L+1} = (-1)^i u_n\}$. Also, $\mathscr{X}_i$ is contained in the torus $T_{\mathbf{c}}$ of a sphere in $\mathbb{R}^{2L}$ with radius $(1 - u_n^2)^{1/2}$, where $\mathbf{c}_i^2 = u_{2i-1}^2 + u_{2i}^2$.*

5.3.2 *Lattice Connections*

We say that a $2L$-dimensional commutative group code is free from reflection blocks if its generator matrix group, considered as Proposition 5.3, satisfies $2L = 2q = n$. By reflection blocks, we refer to the 2-dimensional blocks

$$\pm \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix},$$

which appear in the canonical form when $2q < n$. Commutative group codes in even dimension, whose generator matrices are free from reflections blocks, are directly related to lattices.

For such commutative group codes $\mathscr{C} = G\mathbf{u}$, we may consider without loss of generality the initial vector as $\mathbf{u} = (c_1, 0, c_2, 0, \ldots, c_L, 0)$ where $\mathbf{c} = (c_1, c_2, ..., c_L)$ is a unit vector. We also will consider here $c_i > 0$, that is, codes that are not contained in a hyperplane of $\mathbb{R}^{2L}$. For the rotation angles $a_{ij} = (2\pi b_{ij})/M$, where $1 \leq i \leq M$, $1 \leq j \leq L$ as in Proposition 5.4, let $\mathbf{v}_i = (a_{i1}, \ldots a_{iL})$, $1 \leq i \leq M$ and the lattice Λ defined as the set of all integer combinations of $\mathbf{v}_i$. Note that Λ contains the rectangular lattice

$$\Lambda_{\mathbf{c}} = (2\pi c_1)\mathbb{Z} \times (2\pi c_1)\mathbb{Z} \times \cdots \times (2\pi c_L)\mathbb{Z}.$$

as a sublattice. The connection between these two lattices and the group code $\mathscr{C} = G\mathbf{u}$ is given next [96].

Proposition 5.5 *Let $\mathscr{C} = G\mathbf{u}$ with $\mathbf{u} = (c_1, 0, c_2, 0, \ldots, c_L, 0)$, $\mathbf{c} = (c_1, c_2, ..., c_L)$, $||c|| = 1$, $c_i > 0$ be a commutative group code in $\mathbb{R}^{2L}$, free from reflection blocks. The inverse image $\Phi_{\mathbf{c}}^{-1}$ by the torus mapping (5.1) is the lattice Λ defined as above. Moreover, the quotient of lattices $\dfrac{\Lambda}{\Lambda_{\mathbf{c}}}$ is isomorphic to the generator group G.*

Example 5.1 Let us consider the commutative group code $\mathscr{C}$ in $\mathbb{R}^4$ having G generated by the 4×4 matrix M with rotation blocks $[R(\frac{2\pi.1}{5}), R(\frac{2\pi.2}{5})]$ and initial vector $\mathbf{w} = (1/\sqrt{2}, 0, 1/\sqrt{2}, 0)$. Note that in this case we have $M = 5$ and a cyclic group of matrices, $G = \{\mathbf{I}, M, M^2, M^3, M^4\} \approxeq \mathbb{Z}_5$. In the notation of Proposition 5.3 $b_{i1} = i/5$, $b_{i2} = 2i/5$, and the code $\mathscr{C}$ of 5 words is obtained by multiplying $M^i\mathbf{w}$ ($\mathbf{w}$ in the column format). Then, for $\mathbf{c} = (c_1, c_2) = (1/\sqrt{2}, 1/\sqrt{2})$, the inverse image of the torus map $\Phi_{\mathbf{c}}$ of this code is the lattice $\Lambda \in \mathbb{R}^2$ generated by the vectors $\mathbf{v_1} = ((1/5)(2\pi c_1), (2/5)(2\pi c_2)$, $\mathbf{v_2} = ((-2/5)2\pi c_1, (1/5)2\pi c_2)$. Note also that if we consider the rectangular (square) sublattice $\Lambda_{\mathbf{c}}$ generated by $\mathbf{w_1} = (2\pi c_1, 0)$ and $\mathbf{w_1} = (0, 2\pi c_2)$, the quotient of lattices $\Lambda/\Lambda_{\mathbf{c}} \cong \mathbb{Z}_5$ and it is generated by $\bar{\mathbf{v}}_1$ (Fig. 5.4). It is interesting to note that this spherical code $\mathscr{C}$ is in fact the (optimal) simplex code in $\mathbb{R}^4$: any two of its five points are at a distance $\sqrt{5/2}$.

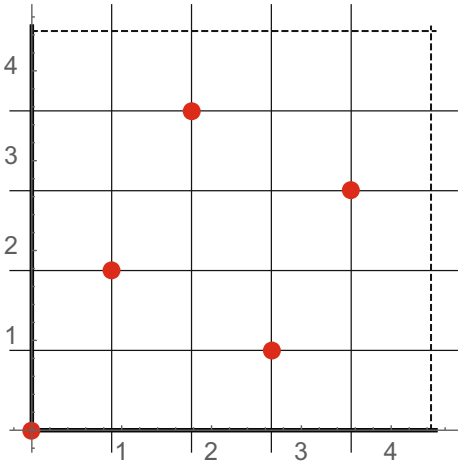


Fig. 5.4 The quotient of lattices linked to the simplex code in $\mathbb{R}^4$ with initial vector $(1/\sqrt{2}, 0, 1/\sqrt{2}, 0)$ and group of matrices generated by $[\mathrm{Rot}(\frac{2\pi.1}{5}), \mathrm{Rot}(\frac{2\pi.2}{5})]$

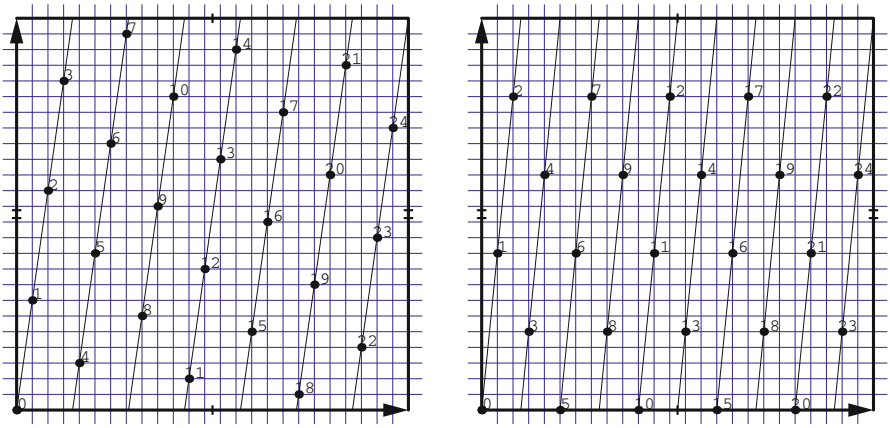


Fig. 5.5 Pre-images $\Phi_{\mathbf{c}}^{-1}$ of two cyclic group codes $\mathscr{C} = G\mathbf{u}$ of order $M = 25$ in $\mathbb{R}^4$. On the left, $G = \langle[\mathrm{Rot}(\frac{2\pi}{25}), Rot(\frac{2\pi 7}{25}]\rangle$, and the initial vector is $\mathbf{u} = (1/\sqrt{2}, 0, 1/\sqrt{2}, 0)$. On the right side, $G = \langle[\mathrm{Rot}(\frac{2\pi}{25}), \mathrm{Rot}(\frac{2\pi 10}{25}]\rangle$, and the initial vector is $\mathbf{u} = (\sqrt{0.54915}, 0, \sqrt{0.45085}, 0)$, which provides the best commutative group code of this order in $\mathbf{R}^4$[96]

Example 5.2 Figure 5.5 shows the inverse image of two commutative group codes. In both the group is cyclic ($\cong \mathbb{Z}_{25}$). Note that the lattice associated with the code on the left is equivalent to the square lattice with basis $\{(4, 3), (-3, 4)\}$ which is less dense than the lattice associated with the optimum code [106] on the right.

Proposition 5.6 ([96]) *Every commutative group code $\mathscr{C} = G\mathbf{u}$ of order M in $\mathbb{R}^{2L}$ free from 2×2 reflection blocks with initial vector $u = (u_1, \ldots, u_{2L})$ and minimum distance d satisfies*

$$M \leq \frac{\pi^L \Pi_{i=1}^{L} (u_{2i-1}^2 + u_{2i}^2)^{1/2} \Delta_{G\mathbf{u}}}{(\arcsin \frac{d}{4})^L} \leq \Delta_L \left(\frac{\pi}{(\arcsin \frac{d}{4}).L^{1/2}} \right)^L,$$

where $\Delta_{G\mathbf{u}}$ is the center density of the lattice Λ associated to the code and Δ_L is the maximum center density of a lattice packing in $\mathbb{R}^L$.

Remark 5.1 The inverse image through the torus mapping $\Phi_{\mathbf{c}}$ of a commutative group code of order M generated by matrices which may contain 2×2 reflection blocks ($2q < n$ in Proposition 5.4) not always is a quotient of lattices. However, from the L-periodicity of $\Phi_{\mathbf{c}}$ in $\mathbb{R}^L$,we can assert that for $\mathbf{u} = (u_1, \ldots, u_{2L})$, it is a periodic distribution of M points in the hyperbox $\mathscr{P}_{\mathbf{c}} \subset \mathbb{R}^L$, $c_i = \sqrt{u_{2i-1}^2 + u_{2i}^2}$ spanned by the lattice associated to this box. Therefore, for general commutative group in $\mathbb{R}^{2L}$, the lattice packing density in the last proposition can be replaced by the best periodical packing density in $\mathbb{R}^L$. Since any packing density in $\mathbb{R}^L$ can be approached by periodical packing densities as remarked in [22], we can also replace Δ_L in the last proposition for D_L, by the best center packing density in $\mathbb{R}^L$ [96]. Here it should be pointed out that for a general spherical code (not a group code), we have much bigger upper bounds and the codes may approach the packing density of $\mathbb{R}^{2L-1}$. The great advantages of commutative group codes are their homogeneity, easiness, and low cost of the encoding and decoding processes on flat tori [107]. Bounds for commutative group codes in odd dimensions, $n = 2L + 1$, can also be obtained [96] by observing that those codes must lie on two parallel hyperplanes and are formed by two equivalent copies of commutative group codes in $\mathbb{R}^{2L}$. Examples of such codes in $\mathbb{R}^3$ are the antiprisms. An interesting exercise is to describe the best spherical code of 8 points in $\mathbb{R}^3$, which is an antiprism with same size edges (Fig. 5.1), as a commutative group code described in Proposition 5.4.

The torus bounds given in the Proposition 5.6 and Remark 5.1 are tight in the following sense. Consider, for instance, the dual inequality of Proposition 5.2,

$$d \leq 2 \sin \left(\prod_{i=1}^{L} c_i D_L / M \right).$$

For big M the distance d must be small (from Proposition 5.2), and the inverse image of the ball of radius d in $\mathbb{R}^{2L}$ centered in a point of $T_{\mathbf{c}}$ will be arbitrarily close to the ball of same radius in $\mathbb{R}^L$. This means that the best packing in the flat torus will be approached by the best packing in its pre-image in the box $\mathscr{P}_{\mathbf{c}}$ and then the upper bounds of the above proposition and remark will be approached.

5.3.3 Approaching the Bound: Good and Optimum Commutative Group Codes

For small distances d or big M, good commutative group codes may be found on the search for orthogonal sublattices $\tilde{\Lambda}$ of a lattice Λ with good packing density. For each such sublattice, $\tilde{\Lambda}$ let $b_1, b_2, ..., b_n$ be length of the orthogonal basis vectors, $b = \left(\sum_{i=1}^{L} b_i^2 \right)^{\frac{1}{2}}$ the rescaled lattices $(1/b)\Lambda$ and $(1/b)\tilde{\Lambda}$. The commutative group

code $\mathscr{C}$ associated to the quotient $\frac{(1/b)\Lambda}{(1/b)\tilde{\Lambda}}$ on a flat torus $T_{\mathbf{c}}$ is a possible choice for a good code, particularly if Λ has the best packing density in its dimension.

The next proposition describes the spherical code in $\mathbb{R}^{2L}$ attached to a nested pair of lattices $\tilde{\Lambda} \subset \Lambda \subset \mathbb{R}^L$, $\tilde{\Lambda}$ orthogonal.

Proposition 5.7 *Let $\alpha = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$ and $\beta = \{\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_n\}$ bases of lattices Λ_α and Λ_β, $\Lambda_\beta \subset \Lambda_\alpha$, and the associated generator matrices A_α, A_β. Then $A_\beta = A_\alpha H$, where H is an integer matrix. Suppose that β is composed by orthogonal vectors, and consider the frame in $\mathbb{R}^n$ given by the normalizations of these vectors. Let $b_i = \|\mathbf{w}_i\|$, $b=\left(\sum_{j=1}^n \left\|\mathbf{w}_j\right\|^2\right)^{\frac{1}{2}}$, $c_i = \frac{b_i}{b}$, $\mathbf{c} = (c_1, c_2, \ldots, c_n)$ and $\phi_{\mathbf{c}}$ the torus map regarding in this frame. Then the normalized nested pair $(1/b)\Lambda_\beta \subset (1/b)\Lambda_\alpha$ of lattices is associated with a spherical code in $\mathbb{R}^{2n}$ with initial vector $(c_1, 0, c_2, 0, \ldots, c_n, 0)$ and generator group of matrices determined by the Smith normal decomposition of H.*

Proof As pointed out in Chap. 2, 2.2, by considering the Smith decomposition, $H = PDQ$, where P and Q are unimodular and D is the diagonal matrix with diagonal terms d_i, we have $A_\beta Q^{-1} = A_\alpha PD$, which implies that the columns $\mathbf{h}_i$ of the generator matrix $B_\beta = A_\beta Q^{-1}$ of Λ_β must be multiples of the columns $\mathbf{y}_i$ of the generator matrix of $B_\alpha = A_\alpha P$ of Λ_α, $\mathbf{h}_i = d_i \mathbf{y}_i$, and $i = 1, \ldots, n$. Since the expression $\mathbf{y}_i$ in terms of the original basis α is given by the matrix P, we have that for each $d_i \neq 1$, $\mathbf{y}_i$ represents a generator of the quotient of lattices with order d_j in terms of α, which implies that $\Lambda_\alpha/\Lambda_\beta \cong \mathbb{Z}_{\hat{d}_i} \oplus \ldots \oplus \mathbb{Z}_{\hat{d}_k}$, $\hat{d}_j \neq 1$. Then for each $d_j \neq 1$, it is associated the generator matrix $O_j = [Rot[2\pi p_{j1}/d_j], \ldots, Rot[2\pi p_{jn}/d_j]]$, where $M = |det(H)| = d_1 \ldots d_n$. The commutative group G composed by $M = |det(H)| = d_1 \ldots d_n$ orthogonal matrices will be the one generated by O_j, $j = 1, \ldots, k$. So in the Smith decomposition of H, the matrix D provides the group structure and the matrix P the rotation matrices involved.

Example 5.3 In the example of Fig. 5.3, we have, according to the notation used in the above proposition, $\alpha = \{\mathbf{v}_1, \mathbf{v}_2\}$, $\beta = \{\mathbf{w}_1, \mathbf{w}_2\}$, with $\mathbf{v}_1 = ((0.8)2\pi/4, 0)$, $\mathbf{v}_2 = ((0.8)2\pi/2, (0.6)2\pi/4)$,$\mathbf{w}_1 = ((0.8)2\pi, 0)$,$\mathbf{w}_2 = (0, (0.6)2\pi)$. Note this is an already normalized pair of lattices ($b = 1$). Since $\mathbf{w}_1 = 2\mathbf{v}_1$ and $\mathbf{w}_2 = 4\mathbf{v}_2 - 2\mathbf{v}_1$, we have:

$$H = \begin{bmatrix} 2 & -2 \\ 0 & 4 \end{bmatrix} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 2 & 0 \\ 0 & 4 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \Longrightarrow \Lambda_\alpha/\Lambda_\beta = \mathbb{Z}_2 \oplus \mathbb{Z}_4.$$

Besides, the two generators of the quotient of lattices are the classes $\bar{\mathbf{v}}_1$ of order 2 and $\bar{\mathbf{v}}_1 - \bar{\mathbf{v}}_2$ of order 4 (note that in this case we could also choose $\bar{\mathbf{v}}_2$ as a generator of order 4 – see Fig. 5.3). The associated spherical code in $\mathbb{R}^4$ will have $(0.8, 0, 0.6, 0)$ for initial vector, as expected, and the group composed by eight matrices. $G = \{A^r.B^s, 0 \leq r \leq 1, 0 \leq s \leq 3$, where $A = [\text{Rot}[2\pi(1/2)], \text{Identity}]$ and $B = [\text{Rot}[2\pi(-1/4)], \text{Rot}[2\pi(1/4)]]$.

Table 5.1 Examples of commutative group codes in $\mathbb{R}^n$, $n = 4, 6, 8, 16$, constructed through the quotient of A_2, D_3, D_4, E_8 by "rectangular" sublattices

n	M	$d_{\min}$	Upper bound	Group
4	141,180	0.012706	0.0127061	$\mathbb{Z}_{141180}$
4	423,540	0.00733585	0.00733588	$\mathbb{Z}_{423540}$
6	32	1.1547	1.26069	$\mathbb{Z}_2 \oplus \mathbb{Z}_4^2$
6	2048	0.318581	0.320294	$\mathbb{Z}_8 \oplus \mathbb{Z}_{16}^2$
8	648	0.707107	0.736258	$\mathbb{Z}_3 \oplus \mathbb{Z}_6^3$
8	10,368	0.366025	0.369712	$\mathbb{Z}_6 \oplus \mathbb{Z}_{12}^3$
16	65,536	0.707107	0.780361	$\mathbb{Z}_2 \oplus \mathbb{Z}_4^6 \oplus \mathbb{Z}_8$
16	16777,216	0.382683	0.392069	$\mathbb{Z}_4 \oplus \mathbb{Z}_8^6 \oplus \mathbb{Z}_{16}$

Their minimum distances approach the upper bound Proposition 5.6

In [4] it is studied the existence of orthogonal sublattices of A_2, D_3,D_4, E_8, which (Chap. 2, 2.3) are the densest lattices in dimensions 2, 3, 4, and 8, and it is obtained the spherical codes in the double of these dimensions which approaches the bound of Proposition 5.3 particularly when M increases (Table 5.1).

In what follows, $\mathscr{C}(M, n, d)$ denotes a commutative group code $\mathscr{C}$ in $\mathbb{R}^n$ with M points and minimum distance equal to d. A $\mathscr{C}(M, n, d)$ is said to be *optimum* if d is the largest minimum distance for a fixed M and n.

As it is well-known, the minimum distance of a group code $\mathscr{C}$, generated by a finite group G, may vary significantly depending on the choice of the initial vector u. This problem still does not have a general solution, but have been studied in some important special cases, including reflection group codes [84] and permutation group codes [37]. Biglieri and Elia have shown in [11] that, for a fixed cyclic group code, the problem can be formulated as a linear programming problem. They also discussed the efficiency of some of these codes and remarked on the hardness of obtaining the best cyclic group code for a given cardinality M and dimension n.

In the search for the best commutative group code $\mathscr{C}(M, n, d)$, for fixed values of M and n, we must first find the set $G_n(M)$ of all commutative groups in $\mathscr{O}_n$ of order M and then the best initial vector for each one of those groups. An optimum code will be one which has the largest minimum distance in this set. The total number of $G_n(M)$ is related with the Euler number of divisors of M and is of order $\binom{M/2}{n/2}$. It is worth to remark that even isomorphic groups must be considered, since the resulting minimum distance may vary depending on which representation in $\mathscr{O}_n$ is taken for each group, i.e., two isomorphic groups may generate two non-isometric spherical codes, as illustrated in Fig. 5.5.

An approach to this problem is based on the association between commutative group codes and lattices described here. An important step of the algorithm derived in [106] is to reduce the number of cases to be analyzed by discarding isometric codes. This is done via the following proposition which consider generator matrices in the Hermite normal form (Chap. 3, 3.2).

Table 5.2 Some best commutative group codes of order M in $\mathbb{R}^6$ with $50 \leq M \leq 1000$, initial vector $\mathbf{c} = (c_1, 0, c_2, 0, c_3)$, generators (Gen) given by rotation blocks where b_{i1}, b_{i2}, b_{i3} as in Proposition 5.3 and bound from Proposition 5.6

M	$d_{\min}$	c_1	c_2	c_3	Group	Gen	Bound
50	0.9763	0.604	0.506	0.615	$\mathbb{Z}_{50}$	(7,6, 34)	1.091
250	0.6180	0.525	0.625	0.668	$\mathbb{Z}_5^2 \oplus \mathbb{Z}_{10}$	(50, 0, 0), (50, 50, 0), (25,25,25)	0.436
500	0.5046	0.577	0.577	0.577	$\mathbb{Z}_5 \oplus \mathbb{Z}_{10}^2$	(100, 0, 0), (50, 50, 0), (50, 0, 50)	0.5116
750	0.4367	0.587	0.549	0.594	$\mathbb{Z}_{750}$	(187,229,560)	0.5116
1000	0.3979	0.560	0.632	0.535	$\mathbb{Z}_{1000}$	(319,694,45)	0.4065

Proposition 5.8 ([106]) *Every commutative group code $\mathscr{C}(M, 2L, d)$, generated by a group $G \in \mathscr{O}_{2L}$ free of 2×2 reflection blocks, is isometric to a code obtained as image by $\Phi_{\mathbf{c}}$ of a lattice $\Lambda_G(\mathbf{c})$ which generator matrix T satisfies the following conditions:*

1. *T is in the Hermite Normal Form.*
2. $\det(T) = M^{L-1}$.
3. *There is a matrix W, with integer elements satisfying $WT = MI_L$, where I_L is the $L \times L$ identity matrix.*
4. *The elements of the diagonal of T satisfy $T(i,i) = \dfrac{M}{a_i}$ where a_i is a divisor of M and $(a_i)^i \cdot (a_{i+1} \cdots a_L) \leqslant M$, $\forall i = 1, \ldots, L$.*

As an example of application of the proposition above, let us consider $M = 128$. There are, up to isomorphism, only 4 abstract commutative groups or order 128: $\{Z_{128}, Z_2 \times Z_{64}, Z_4 \times Z_{32}, Z_8 \times Z_{16}\}$. However, for $n = 2L = \{4, 6, 8\}$, there are $\{2016, 41664, 635376\}$ distinct representations of them in $\mathscr{O}_n$. After discarding isometric codes by using Proposition 5.8, we must consider just $\{71, 2539, 55789\}$ representations, respectively [106]. Then the initial vector problem can be solved only for those cases.

In Table 5.2, it is shown some best commutative group codes in $\mathbb{R}^6$ [106].

5.3.4 Commutative Group Codes and Codes on Graphs

Commutative group codes can also be viewed as a graph or a coset code [40] on a flat torus with the graph distance (minimum number of edges from one vertex to another). They are also geometrically uniform in this context. This is the approach presented in [30]. As an example, consider the codes presented in Fig. 5.5 where each edge of the flat torus box is subdivided into $M = 25$ segments with the underlined grid associated to this subdivision. Considering also the boundary identification, those grids define a graph on each flat torus with vertices associated to the group Z_{25}^2. On the left we have the code C_1 generated by the element $(b_1, b_2) = (1, 7)$, which is a cyclic code in $Z_{25} \times Z_{25}$ of order $M = 25$ and minimum graph or

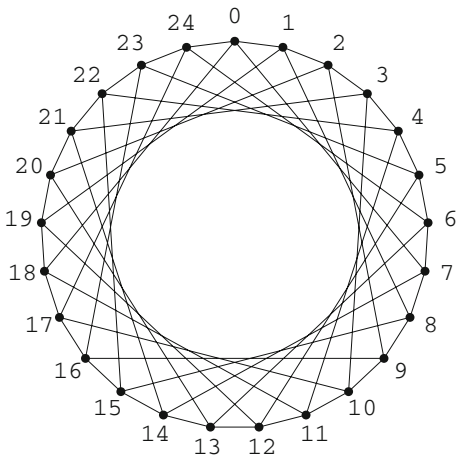


Fig. 5.6 The cyclic group code of Fig. 5.5 – left considered as generated by $(b_1, b_2) = (4, 3)$ and viewed as the circulant graph $C_{25}(1, 7)$

Lee distance equal to 7 and therefore a 3 – error correcting code (see Chap. 3, 3.2). Note that this code can also be generated by the element $(4, 3)$ and is a perfect code in $\mathbb{Z}_{25}^2$ (Chap. 3, Example 3.8). On the right of Fig. 5.5, we have the cyclic code C_2 generated by $(b_1, b_2) = (1, 10)$, which has a minimum graph distance 5. Thus, viewed as graph codes, the code on the left on Fig. 5.5 is better than the code on the right in opposition to the performance of their images as spherical codes in $\mathbb{R}^4$. To the code C_1 generated by $(4, 3)$, $C_1 = \{c_{1k} = k(4, 3) \text{ Mod } 25, k = 0, \cdots, 24\}$ (numbered in this order), it is associated the circulant graph $C_{25}(1, 7)$ (see Fig. 5.6). This circulant graph is equivalent to the graph given by the rotated squared grid defined by the elements of C_1. (Note that each point c_{1k} in this new graph is connected to c_{1j}, where $j = \pm 1 \text{ Mod } 25$ or $j = \pm 7 \text{ Mod } 25$.) This geometrical view through quotient of lattices may provide tools to analyze circulant and Cayley graphs which are used in parallel computing schemes [30].

5.4 Spherical Codes on Layers of Tori

5.4.1 Codes for the Gaussian Channel

Although commutative group codes discussed in the last section have applications based on their rich structure, those codes are not good in general for small distance concerning their trade-off between distance and number of points, since they are placed in just one torus of the sphere.

Flat tori layers can be used to construct spherical codes which combine the good structure of commutative group codes in each layer with a better packing density. A *torus layer spherical code (TLSC)* [105] can be generated by a finite set of orthogonal matrices and thus inherited group structure and homogeneity allowing efficient storage and decoding process, which is attached to lattices in the half of the code dimension.

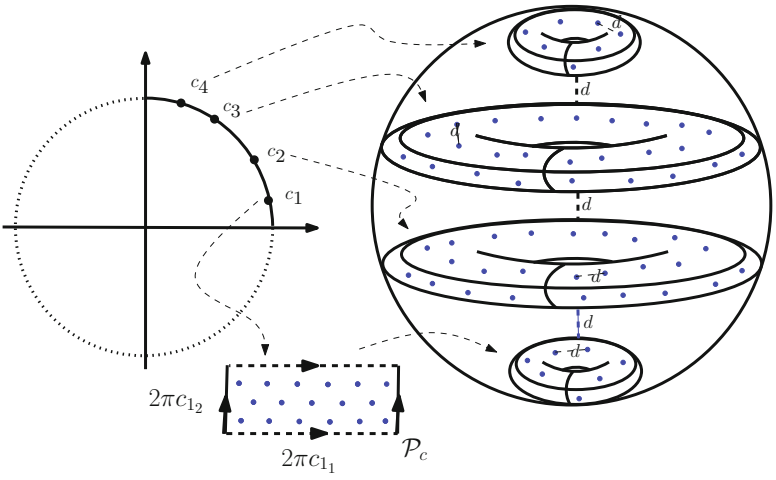


Fig. 5.7 An illustration of the construction of a four-dimensional torus layer spherical code

To design these codes, given a distance $d \in (0, \sqrt{2}]$, we first define a collection of tori in S^{2L-1} such that the minimum distance between any two of these tori is at least d. This can be done (Proposition 5.1) by designing a spherical code in $\mathbb{R}^L$ with minimum distance d and positive coordinates. Then, for each one of these tori, a finite set of points is chosen in $\mathbb{R}^L$ such that the distance between any two points, when embedded in $\mathbb{R}^{2L}$ by the standard parametrization (5.1), is greater than d, according to Proposition 5.2. This set of points may belong to a L-dimensional lattice, restricted to a hyperbox $\mathscr{P}_{\mathbf{c}}$ (5.2), chosen to approach a good packing density in $\mathbb{R}^L$ as described in Sect. 5.3. The $TLSC(2L, d)$ is the union of the commutative group codes associated to each one of the chosen tori. Figure 5.7 illustrates the construction of a $TLSC(4, d)$.

General spherical codes without any group structure, particularly for small distances and higher dimension, may present a much higher number of codewords for the same minimum distance since the packing density have greater bounds (attached to the packing density in the previous dimension). One advantage of the *TLSC* is regarding the simple coding/decoding processes. In [105], starting from a rectangular sublattice of the Leech lattice it is presented a *TLSC* in dimension 48 with more than 2^{113} points placed in 24 layers of flat tori with minimum distance 0.1. This code is generated by using just 12 matrices. For not very small distances (or non-asymptotic context), a torus layer spherical code may have comparable performance to other well-known spherical codes such as apple-peeling [35], wrapped [47], and laminated [48] codes, as illustrated in Table 5.3, and have the advantage of being constructive and homogeneous in each layer. For very small distance and higher dimension, the expected performance will decrease.

Table 5.3 Four-dimensional code sizes at various minimum distances

d	TLSC(4,d)	Apple-peeling	Wrapped	Laminated
0.5	172	136	*	*
0.4	308	268	*	*
0.3	798	676	*	*
0.2	2,718	2,348	*	*
0.1	22,406	19,364	17,198	16,976
0.01	2.27×10^7	1.97×10^7	2.31×10^7	2.31×10^7

*Unknown values

5.4.2 *Application: Coding for Continuous Alphabet Sources*

Curves on a sphere with good length, "distance," and structure are suitable to the following communication problem. A real value x (say, belonging to the interval $[0, 1]$) is to be transmitted over a power-constrained Gaussian channel of dimension n to a receiver. This can be achieved by first quantizing x, as in Sect. 2.5.1, and then encoding the quantized bits into a classical code. However, this "separated" approach necessarily incurs quantization errors and, ultimately, communication delay. Another possibility is to map the source, via a continuous (or piecewise continuous) function $\mathbf{s} : [0, 1) \to \mathbb{R}^L$, and then transmit it over the channel. Such a function is, indeed, a *curve* in $\mathbb{R}^n$. On the receiver side, a signal

$$\mathbf{y} = \mathbf{s}(x) + \mathbf{n}$$

is observed. The objective is to recover an estimate $\mathbf{x}$ of the sent value, attempting to minimize the mean square error (mse) $E[(x - \hat{x})^2]$ between the estimate and the true value.

The problem of building curves for such a transmission was first discussed by C. Shannon, pioneer of information theory in 1949 [91]. It is a remarkable result that if x has normal distribution and $n = 1$, the *optimal* distortion is achieved by the scaled identity mapping, i.e., $s(x) = \alpha x$ (e.g., [44]). For higher dimensions, however, the solution is not so simple. Perhaps surprisingly, the construction of continuous curves can be addressed by using lattices, a discrete structure. This relation is the subject of the next pages.

As a first example, consider the piecewise-linear mapping depicted in Fig. 5.8. If a receiver observes $\mathbf{y} = \mathbf{s}(x) + \mathbf{n}$, there are *two* possible types of errors:

1. *Small errors*: if the error is concentrated in a sufficiently small region, the closest curve value will be very close to the sent one.
2. *Large errors (or "jumps")*: in this case the noise is high enough so that the estimate "jumps" between two laps (or pieces) of the curve.

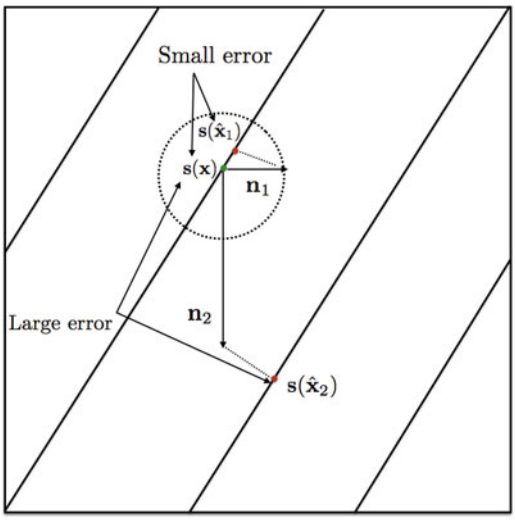


Fig. 5.8 Illustration of small and large errors

Large errors can be prevented by separating the laps apart, while for small errors it is desirable that the curve is as long as possible. These two objectives are, of course, contrary.

In the example of Fig. 5.8, the mapping $\mathbf{s} : [0, 1] \to \mathbb{R}^2$ can be defined as

$$\mathbf{s}(x) = (3x - \lfloor 3x \rceil, 2x - \lfloor 2x \rceil), \tag{5.6}$$

or if we denote the mod-1 operation by $x \bmod 1 = x - \lfloor x \rceil$, we can write, in a concise way, $\mathbf{s}(x) = (3x, 2x) \bmod 1$. Now the distance ρ_c between two pieces of this curve is the smallest distance between two integer translations of the straight line $(3x, 2x)$ or by homogeneity

$$\rho_c = \min_{u \in \mathbb{Z}^2} \min_{x \in \mathbb{R}} \|(3, 2)x - \mathbf{u}\| .$$

The first minimum is clearly obtained by projecting $\mathbf{u}$ onto the vector $(-2, 3)$ (orthogonal to $(3, 2)$). Therefore, we see that *the smallest distance between two laps of the curve is equal to the shortest vector of the projection of* $\mathbb{Z}^2$ *along* $(-2, 3)$.

This argument can be extended to any mapping of the form

$$\mathbf{s}(x) = \alpha(\mathbf{a}x(\bmod 1)),$$

where $\mathbf{a} \in \mathbb{Z}^L$, and α is a scaling factor chosen conveniently in order to satisfy the power constraint. Given a vector $\mathbf{a} \in \mathbb{Z}^L$, we may make a step further and consider the curves

$$\mathbf{s}(x) = \phi_{\mathbf{c}} \left(\frac{2\pi}{\sqrt{L}} \mathbf{a}x (\bmod 1) \right), \tag{5.7}$$

where $\mathbf{c} = \hat{\mathbf{e}} = (1/\sqrt{L})(1, \ldots, 1)$ (or we may consider different vectors) and ϕ is the torus mapping (5.1). These closed curves are contained on a flat torus T_c in the sphere of $\mathbb{R}^{2L}$ and are highly homogeneous (all their curvatures are constant [27]). From Proposition 5.1, the distance between the "laps" of the new curve is approximately the distance between two lines in the (mod 1) map. The length of the curve is given by $2\pi \|\mathbf{a}\| / \sqrt{L}$.

To summarize, good codes for continuous alphabet sources are related to curves that can be designed by choosing a vector $\mathbf{a} \in \mathbb{Z}^L$ such that:

1. The norm of $\mathbf{a}$ is large.
2. The projection of $\mathbb{Z}^L$ along the orthogonal hyperplane to $\mathbf{a}$ has large shortest vector.

As we will see next, these two objectives can be attained by finding projections of the cubic lattice $\mathbb{Z}^L$ with good packing density. In the next subsection, we consider the study of projections of lattices in a greater generality.

The problem of finding good projections of the cubic lattice (and thus curves for this communication problem) can be independently formulated as the "fat strut" [100] problem as follows. We want to find a point $\mathbf{a} \in \mathbb{Z}^L$ such that the cylinder anchored at the origin and $\mathbf{a}$ does not contain any other lattice point and has maximal volume.

Projections of Lattices The previous discussion motivates the study of *projections of lattices* along a vector space of $\mathbb{R}^L$. In fact, many notable lattices seen in Chap. 2 are naturally characterized through projections and intersections with hyperplanes. Furthermore, projections are strongly connected to the study of more advanced lattice structures, such as *laminated* and *perfect* lattices. The interested reader is invited to consult the references [26, Chap. 6] and [68] for a thorough account on these topics.

We need some preliminary definitions on the linear algebra of projections along subspaces of $\mathbb{R}^L$. Let V be a vector subspace of $\mathbb{R}^L$, for example, a plane in $\mathbb{R}^3$ or a hyperplane in $\mathbb{R}^L$. Denote by $V^\perp$ its orthogonal complement (in the case of a plane, it is a straight line, generated by one single vector). Any vector $\mathbf{x} \in \mathbb{R}^L$ can be decomposed in a unique way as $\mathbf{x} = \mathbf{v} + \mathbf{v}^\perp$, where $\mathbf{v} \in V$ and $\mathbf{v}^\perp \in V^\perp$. Given $\mathbf{x} \in \mathbb{R}^L$, we define the *orthogonal projection* of $\mathbf{x}$ in V (or along $V^\perp$) as $P_V(\mathbf{x}) = \mathbf{v}$ and $P_{V^\perp}(\mathbf{x}) = \mathbf{v}^\perp$. One can show (e.g., [70, p. 430]) that $P_{V^\perp}(\mathbf{x}) = P\mathbf{x}$, where

$$P = (I - V(V^t V)^{-1} V^t).$$

We call P the orthogonal *projector* (or projection matrix) onto $V^\perp$.

Let $\Lambda \subset \mathbb{R}^L$ be a lattice. The *projection* of Λ in $V^\perp$ is denoted by $P_{V^\perp}(\Lambda)$. If B is a generator matrix and P is the projection matrix above, we have

$$P_{V^\perp}(\Lambda) = \{P\mathbf{x} : \mathbf{x} \in \Lambda\} = \left\{PB\mathbf{u} : \mathbf{u} \in \mathbb{Z}^L\right\}. \tag{5.8}$$

The projection of lattice along a vector space is certainly closed under addition and subtraction. Perhaps more surprising is the fact that it need not be discrete, as seen in the next example.

Example 5.4 Let $\Lambda = \mathbb{Z}^2$ and $\mathbf{v} = (1, \sqrt{2})$. A projection matrix onto $\mathbf{v}^\perp$ is given by

$$P = \begin{pmatrix} \frac{2}{3} & -\frac{\sqrt{2}}{3} \\ -\frac{\sqrt{2}}{3} & \frac{1}{3} \end{pmatrix}.$$

Applying the orthogonal transformation defined by matrix

$$Q = \begin{pmatrix} \sqrt{\frac{2}{3}} & -\frac{1}{\sqrt{3}} \\ \frac{1}{\sqrt{3}} & \sqrt{\frac{2}{3}} \end{pmatrix}$$

to the projection set (5.8), we have

$$P_{\mathbf{v}^\perp}(\mathbb{Z}^2)Q = \left\{QP\mathbf{x} : \mathbf{x} \in \mathbb{Z}^2\right\} = \frac{1}{\sqrt{3}}\left\{(\sqrt{2}x_1 + x_2, 0) : x_1, x_2 \in \mathbb{Z}\right\}.$$

It is an interesting exercise of combinatorics to use the pigeonhole principle to show that the above set is *not* discrete.
From the characterization of lattices as discrete sets (Theorem 2.1), it follows that the projection need not be a lattice. But as may be easily seen, there are examples in which the projection is indeed a lattice.

Example 5.5 The simplest example is the $\mathbb{Z}^L$ lattice. Its projection along the hyperplane orthogonal to any of the canonical vectors is equivalent to $\mathbb{R}^{L-1}$.
For a vector $\mathbf{v} \in \mathbb{R}^L$, we denote the hyperplane orthogonal to $\mathbf{v}$ by $\mathbf{v}^\perp$, i.e,

$$\mathbf{v}^\perp = \{\mathbf{x} \in \mathbb{R}^n : x_1 v_1 + \ldots + x_L v_L = 0\}.$$

The following proposition characterizes when the projection of a lattice is a discrete set and what does the new lattice "look like." Recall from Chap. 2 that a vector $\mathbf{x}$ in a lattice Λ is said to be *primitive* if it can be extended to a basis of Λ. The following proposition is rather well-known (an explicit proof can be found in [17]):

Proposition 5.9 *Let* $\mathbf{v}$ *be a primitive vector of a full-rank lattice* $\Lambda \subset \mathbb{R}^L$. *The following properties hold:*

(i) *The set* $P_{\mathbf{v}^\perp}(\Lambda)$ *is a lattice.*
(ii) *The volume of* $P_{\mathbf{v}^\perp}(\Lambda)$ *is given by*

$$V(P_{\mathbf{v}^\perp}(\Lambda)) = \frac{V(\Lambda)}{\|\mathbf{v}\|} \tag{5.9}$$

(iii) $P_{\mathbf{v}^\perp}(\Lambda)^* = \Lambda^* \cap \mathbf{v}^\perp$.

Item (ii) gives a very simple way of computing the discriminant of the projection, while item (iii) provides a simple characterization for its dual.

Example 5.6 Recall that A_L is defined in Sect. 2.4 as

$$A_L = \left\{\mathbf{x} \in \mathbb{Z}^{L+1} : x_1 + \cdots + x_L = 0\right\}.$$

In other words, if $\mathbf{v} = (1, \ldots, 1) \in \mathbb{Z}^{L+1}$, then $A_L = \mathbb{Z}^{L+1} \cap \mathbf{v}^{\perp}$. From the previous theorem, we have

$$A_L^* = P_{\mathbf{v}'}(\mathbb{Z}^{L+1}),$$

i.e., the dual of A_L is the projection of $\mathbb{Z}^{L+1}$ along $\mathbf{v}^{\perp}$.
Recalling the curve-packing problem in the previous subsection, we were to choose a vector $\mathbf{a} \in \mathbb{Z}^n$ such that:

1. The norm of $\mathbf{a}$ is large.
2. $P_{\mathbf{a}^{\perp}}(\mathbb{Z}^L)$ has a large shortest vector.

Or, having fixed the norm of $\mathbf{a}$, we would like maximize the minimum norm of $P_{\mathbf{a}^{\perp}}(\mathbb{Z}^L)$, say, $\lambda_1(\mathbf{a})$. Recalling the formula for the center density, and in light of Proposition 5.9, item (ii), this is equivalent to finding projections of $\mathbb{Z}^L$ with good packing density.

The Lifting Construction [100] gives a general solution for this problem. It is shown in [99] how to construct sequences of lattices which are, up to equivalence relations, similar to projections of $\mathbb{Z}^L$ and arbitrarily close to any target $(L-1)$-dimensional lattice.

Further Extensions

By using layers of tori, it is possible to generalize the construction in [108] as follows [18]. Let $T = \{T_1, \ldots, T_M\}$ be a collection of M tori in the unit sphere of $\mathbb{R}^{2L}$. For each one of these tori, consider closed curves of the form

$$\mathbf{s}_{T_c}(x) = \Phi_{\mathbf{c}}(x 2\pi \hat{\mathbf{u}}), \tag{5.10}$$

where $C = \operatorname{diag}(c_1, \ldots, c_L)$, $\hat{\mathbf{u}} = \mathbf{u}C = (c_1 u_1, \ldots, c_L u_L)$, $\Phi_{\mathbf{c}}$ is given by (5.1) and $x \in [0, 1]$.

Now let $\operatorname{Len} = \sum_{j=1}^{M} \operatorname{Len}_j$, where Len_j is the length of $\mathbf{s}_{T_j}$. We split the unit interval $[0, 1]$ into M pieces according to the length of each curve:

$$[0, 1) = I_1 \cup I_2, \ldots \cup I_M, \text{ where}$$

$$I_k = \left[\frac{\sum_{j=1}^{k-1} \operatorname{Len}_j}{\operatorname{Len}_j}, \frac{\sum_{j=1}^{k} \operatorname{Len}}{\operatorname{Len}}\right), \text{ for } k = 1, \ldots, M.$$

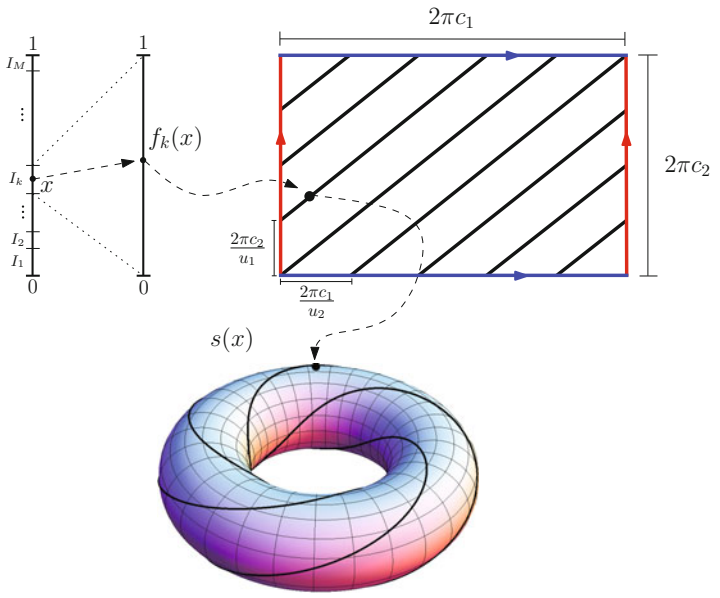


Fig. 5.9 Encoding process

and consider the bijective mapping

$$f_k : I_k \to [0, 1)$$
$$f_k(x) = \frac{x - \sum_{j=1}^{k-1} L_j/L}{l_k/L}.$$

Then the full encoding map $\mathbf{s}$ can be defined by

$$\mathbf{s}(x) := \mathbf{s}_{T_k}(f_k(x)), \text{ if } x \in I_k. \tag{5.11}$$

and is represented in Fig. 5.9. Finding a good collection of tori (i.e., such that each of them is separated at least a certain distance from each other) is related to finding a good spherical code of a given minimum distance, which can be approached through standard techniques (and even using layers of torus, as the construction presented in the previous section). On the other hand, finding good curves in each torus is equivalent to finding good projections of the rectangular lattice $c_1\mathbb{Z} \oplus \cdots \oplus c_L\mathbb{Z}$. In this case, it is possible to generalize the Lifting Construction and exhibit sequences of projections of $c_1\mathbb{Z} \oplus \cdots \oplus c_L\mathbb{Z}$ converging to any $(L-1)$-dimensional lattice, as in the later case. Through this, it is possible to meaningfully increase the length of the curves produced.

Discrete sets of points selected on a continuous closed curve on a flat torus as described in this section have also been used in [110] to approach good commutative group codes which are cyclic.

Chapter 6
Lattices and Index Coding

This chapter was written in collaboration with Lakshmi Natarajan (IIT Hyderabad, India) and Yi Hong (Monash University, Australia)

6.1 Introduction

A wireless channel is characterized by its broadcast nature: a signal transmitted by a source is received not only by the intended recipient but also by all the terminals within the transmission range. This can create a scenario where a passive listener becomes aware of the message originally intended for another node in the broadcast network, while the intended recipient himself is yet to receive the message packet successfully. This might occur, for example, if the main recipient is out of transmission range or if the packet is lost due to fading or channel noise, while the channel gain at the passive listener is strong enough for decoding to be successful. As a result, we have a broadcast channel where the source is required to transmit a finite set of messages intended to be delivered to finitely many receivers; each receiver desires to decode a subset of the transmitted messages while having prior knowledge of the values of a different subset of messages. This prior knowledge at the receivers, called *side information*, can arise when receivers overhear the previous transmissions as information propagates through a communication network in multiple hops or through multiple rounds of transmission.

Example 6.1 Figure 6.1 shows a wireless relay network consisting of two sources BS_1 and BS_2, a relay BS_3 and three receivers U_1, U_2, U_3. Receiver U_1 (respectively U_2) demands the message w_2 (respectively w_1) from the source BS_2 (BS_1), while receiver U_3 demands both the messages. In the first phase, the two sources transmit the messages w_1 and w_2 to the relay. Receivers U_1 and U_2 overhear the messages intended for each other, while U_3 gains no side information from the first phase. This additional knowledge at the receivers can be utilized in the second phase of communication to improve communication rate, reduce transmission power, or increase reliability, when the relay broadcasts w_1 and w_2 to the three receivers.
Exploiting prior knowledge at the receivers (if any) is key to achieving high communication rates in the broadcast channel. *Index coding*, first introduced by

S.I.R. Costa et al., *Lattices Applied to Coding for Reliable and Secure Communications*, SpringerBriefs in Mathematics,
https://doi.org/10.1007/978-3-319-67882-5_6

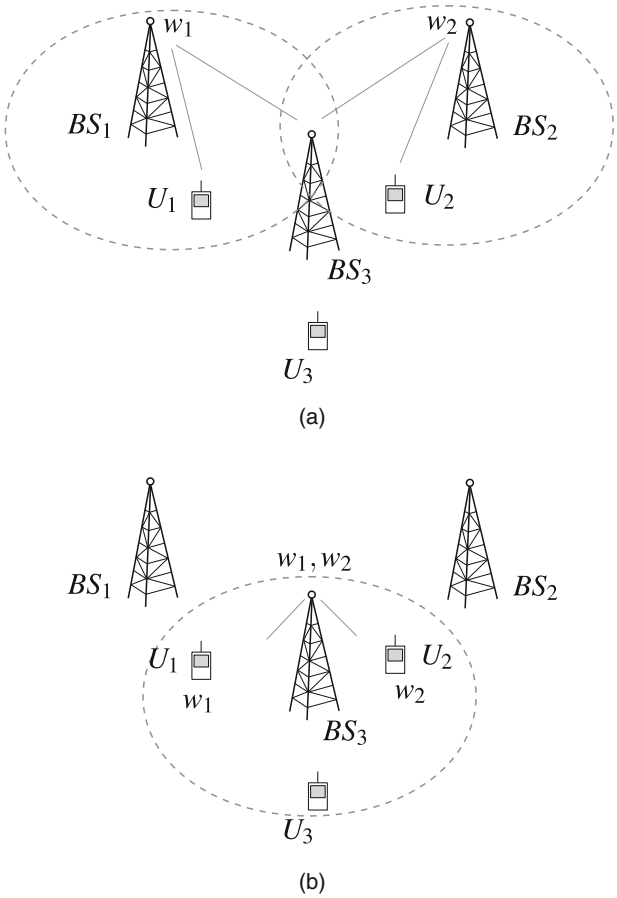


Fig. 6.1 Receiver side information in a wireless relay network. The relay (BS_3) can encode w_1, w_2 to exploit the side information at U_1 and U_2 to achieve higher transmission rates and/or increase reliability (**a**) Receivers U_1 and U_2 demand w_2 and w_1, respectively, while U_3 demands both the messages. The transmitters BS_1 and BS_2 simultaneously transmit messages w_1 and w_2 to BS_3. Receivers U_1 and U_2 overhear the messages w_1 and w_2, respectively (**b**) BS_3 must broadcast w_1 and w_2 to U_1, U_2 and U_3. The receivers U_1 and U_2 are aided by their respective side information

Birk and Kol [12], refers to communication techniques that exploit receiver side information to improve bandwidth efficiency of broadcast channels. The objective of index coding is to perform joint encoding of messages in order to simultaneously meet the demands of all the receivers while transmitting the messages at the highest possible rate.

Example 6.2 (Index Coding Solution for a Noiseless Broadcast Channel) Consider a broadcast channel where three receivers require the files w_1, w_2 and w_3 from the transmitter, respectively, and have the prior knowledge of w_2, w_3 and w_1,

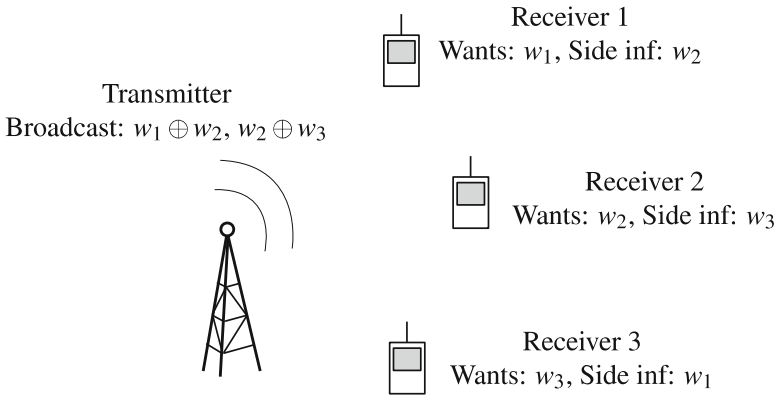


Fig. 6.2 Example of an index coding solution to a broadcast problem: each of the three receivers demands one file from the transmitter while having prior knowledge of another file. It is assumed that the broadcast channel is noise-free

respectively; see Fig. 6.2. Instead of the naive transmission scheme where the transmitter broadcasts the three files w_1, w_2, w_3 individually, the transmitter can broadcast just two packets: $x_1 = w_1 \oplus w_2$ and $x_2 = w_2 \oplus w_3$, where $\oplus$ denotes the XOR (binary sum) of the individual files. Each of the three receivers can retrieve its own desired data by computing appropriate linear combinations of the broadcast packets and the file available as side information:

$$\text{Receiver 1} : x_1 \oplus w_2 = (w_1 \oplus w_2) \oplus w_2 = w_1$$

$$\text{Receiver 2} : x_2 \oplus w_3 = (w_2 \oplus w_3) \oplus w_3 = w_2$$

$$\text{Receiver 3} : x_1 \oplus x_2 \oplus w_1 = (w_1 \oplus w_2) \oplus (w_2 \oplus w_3) \oplus w_1 = w_3$$

Under the assumption that the broadcast medium is noiseless, this index coding scheme provides 50% improvement in communication rate compared to the naive broadcast scheme.

The index coding problem captures the inherent broadcast nature of the wireless communication medium and is fundamental to a number of multi-user communication networks. It has several applications including wireless and wireline network coding, automatic repeat request (ARQ) in wireless channels, interference management, content distribution networks, etc. The noiseless version of the problem, where the broadcast medium is error-free, is related to number of other problems in information theory and discrete mathematics, such as interference alignment and management [55, 67], communication over arbitrary wireline networks [34], matroids [36], graph theory [5, 7, 13, 78, 93, 104], and coding for distributed storage [69, 92]. When the channel is noisy, one can use a channel code at the physical layer to create an effective error-free broadcast channel at the network layer

and then use an index code at the network layer to exploit the side information at the receivers. The transmission rates achievable by such separation-based schemes are limited by the fact that the side information available at the receivers are not utilized for channel coding and decoding at the physical layer. Consequently, the raw data rate available at the network layer is limited by the signal-to-noise ratio (SNR) of the weakest receiver, even if this receiver has enough side information which can be utilized to compensate the low SNR. An effective alternative solution is to design a joint coding scheme that performs channel coding (to combat noise) and index coding (to exploit receiver side information) simultaneously at the physical layer. Lattices, with their rich geometric and algebraic properties, are a powerful tool for this purpose.

This chapter can be read independently from the previous ones. The reader may refer to Chap. 2 for more details about lattice concepts used.

6.2 Voronoi Constellations

We recall from Sect. 2.5.1 that an n-dimensional code $\mathscr{C}$ for the additive white Gaussian noise channel is a finite collection of real vectors in $\mathbb{R}^n$. Such a code can be carved out of an infinite lattice Λ by using a *sublattice* Λ'.

Definition 6.1 Let $\Lambda \subset \mathbb{R}^n$ be a lattice with full-rank generator matrix B and let M be any $n \times n$ integer matrix with $\det M \neq 0$. Then $\Lambda' = \{BM\mathbf{u} \,|\, \mathbf{u} \in \mathbb{Z}^n\}$ is a *sublattice* of Λ.

Notice that Λ' is a subset of Λ and is closed under addition and negation: if $\mathbf{x}, \mathbf{y} \in \Lambda'$, then $\mathbf{x} + \mathbf{y} \in \Lambda'$, and for any $\mathbf{x} \in \Lambda'$, we have $-\mathbf{x} \in \Lambda'$. This makes Λ' a subgroup of Λ. The lattices $\Lambda' \subset \Lambda$ are said to form a *nested lattice pair*.

Example 6.3 Figure 6.3a shows a pair of two-dimensional nested lattices: $\Lambda = \mathbb{Z}^2$ generated by the 2×2 identity matrix and the sublattice Λ' with basis $\{(2,1),\ (-1,2)\}$. With

$$B = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ and } M = \begin{bmatrix} 2 & -1 \\ 1 & 2 \end{bmatrix},$$

we observe that Λ and Λ' are generated by B and BM, respectively.

Example 6.4 For any lattice Λ and any integer $c \in \mathbb{Z}$, $\Lambda' = c\Lambda$ is a sublattice of Λ. If Λ is generated by B, then Λ' is generated by cB. Further, Λ' and Λ are equivalent. Since Λ' is a subgroup of Λ, Λ can be partitioned into a set of cosets of Λ' which form the quotient group Λ/Λ'. Each of these cosets can be uniquely identified using a coset leader, which is an element of the coset contained in $\mathscr{V}_{\Lambda'}(\mathbf{0})$. We identify Λ/Λ' with the set $\Lambda \cap \mathscr{V}_{\Lambda'}(\mathbf{0})$, i.e., the set of all the points in Λ contained in the Voronoi region of Λ' at the origin. If a lattice point $\mathbf{x} \in \Lambda$ is on the boundary

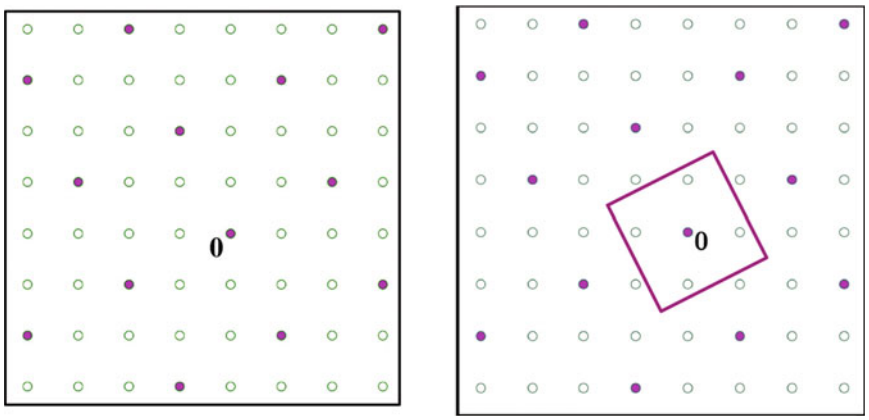


Fig. 6.3 Example of nested lattices and the resulting Voronoi constellation (**a**) A pair of nested lattices $\Lambda' \subset \Lambda$ in two dimensions. The filled circles denote the points in the sublattice Λ' (**b**) The skewed square centered at $\mathbf{0}$ is the boundary of $\mathcal{V}_{\Lambda'}(\mathbf{0})$. The five lattice points of Λ contained within $\mathcal{V}_{\Lambda'}(\mathbf{0})$ form the Voronoi constellation Λ/Λ'

of $\mathcal{V}_{\Lambda'}(\mathbf{0})$, then so is the lattice point $-\mathbf{x}$. In this case, Λ/Λ' is defined to include exactly one of $\mathbf{x}$ or $-\mathbf{x}$, which may be arbitrarily chosen.

Definition 6.2 Given a pair of nested lattices $\Lambda' \subset \Lambda$, the set Λ'/Λ is called a *Voronoi constellation*.

Example 6.5 (Pulse Amplitude Modulation) Consider the one-dimensional lattices $\Lambda = \mathbb{Z}$ and $\Lambda' = M\mathbb{Z}$, where $M \geq 2$ is an integer. Clearly $M\mathbb{Z} \subset \mathbb{Z}$, and $\mathbb{Z}/M\mathbb{Z}$ forms a one-dimensional Voronoi constellation. Observe that the Voronoi region $\mathcal{V}_{\Lambda'}(\mathbf{0})$ is the interval $[-M/2, M/2]$ on the real line and $\mathbb{Z}/M\mathbb{Z}$ is the set of all integers lying in the interval $[-M/2, M/2]$, where the points on the boundary, if any, are chosen systematically. Hence, we have

$$\mathbb{Z}/M\mathbb{Z} = \begin{cases} \left\{-\frac{M-1}{2}, -\frac{M-3}{2}, \ldots, \frac{M-3}{2}, \frac{M-1}{2}\right\} & \text{if } M \text{ is odd.} \\ \left\{-\frac{M}{2}, -\frac{M-2}{2}, \ldots, \frac{M-4}{2}, \frac{M-2}{2}\right\} & \text{if } M \text{ is even.} \end{cases}$$

This is the pulse amplitude modulation (PAM) constellation consisting of M points. Voronoi constellations are also known as *nested lattice codes* or, simply, *lattice codes*. The number of points in a Voronoi constellation equals the number of cosets of Λ' in Λ, which in turn is related to the volume of the lattices Λ and Λ' as follows:

$$|\Lambda/\Lambda'| = \frac{V(\Lambda')}{V(\Lambda)}.$$

The code Λ/Λ' has the same group structure as the quotient group of the set of cosets of Λ' in Λ. The group operation defining Λ/Λ' is the vector addition performed modulo Λ':

$$(\mathbf{x}+\mathbf{y}) \bmod \Lambda' \text{ for } \mathbf{x},\mathbf{y} \in \Lambda/\Lambda'.$$

The lattice Λ is called the *coding lattice* or the *fine lattice*, and Λ' is known as the *shaping lattice* or the *coarse lattice*. When used over the AWGN channel, we require the coding lattice to have a large packing density $\Delta(\Lambda)$. For a fixed $V(\Lambda)$, this will ensure that the points in Λ/Λ' are separated by a large distance, and hence, the probability of decoding error is small. The shaping lattice Λ' determines the boundary region of the finite code Λ/Λ' and, hence, the power required to transmit the codewords through the AWGN channel. In particular, the peak transmit power is determined by the covering radius of Λ'. For a given $V(\Lambda')$, we require the covering radius to be small, which is equivalent to a small covering density $\theta(\Lambda')$. More information and properties of Voronoi constellations can be found in [26, 41, 112].

6.3 Index Coding in AWGN Channel

We now provide a framework for analyzing index coding schemes in the AWGN broadcast channel where every receiver desires to decode all the messages from the source, while the side information available at each receiver is arbitrary.

Consider the AWGN broadcast channel with a single transmitter and finitely many receivers. Assume the transmitter has K independent messages $w_1,\ldots,w_K$ that take values from finite sets $\mathscr{W}_1,\ldots\mathscr{W}_K$, respectively. The transmitter employs an n-dimensional channel code $\mathscr{C} \subset \mathbb{R}^n$ and jointly encodes the tuple $(w_1,\ldots,w_K)$ to a codeword $\psi(w_1,\ldots,w_K)=\mathbf{x}\in\mathscr{C}$ using a one-to-one correspondence

$$\psi : \mathscr{W}_1 \times \cdots \times \mathscr{W}_K \to \mathscr{C}.$$

Such an encoder is equivalent to a labelling scheme where each point of $\mathscr{C}$ is associated with a distinct message tuple $(w_1,\ldots,w_K)$. The resulting rate of transmission for the kth message w_k is

$$R_k = \frac{1}{n}\log_2|\mathscr{W}_k| \text{ b/dim},$$

where the unit is bits per dimension. The sum rate of all the messages at the source is $R = R_1+\cdots+R_K$.

Since every receiver demands all the messages from the source, the demands of all the receivers are identical. Therefore, a receiver is completely characterized by the signal-to-noise ratio (SNR) it experiences at the broadcast channel output and the subset $S \subset \{1,\ldots,K\}$ of messages that is available to it as side information.

Consider the channel output $\mathbf{y}$ at a receiver with parameters (SNR, S),

$$\mathbf{y} = \mathbf{x} + \mathbf{z},$$

where $\mathbf{x} \in \mathscr{C}$ is the transmitted codeword and $\mathbf{z}$ is a random Gaussian noise vector whose variance is proportional to $1/\mathsf{SNR}$. Further, the receiver also knows the exact realizations of the message symbols w_k, $k \in S$, say, $w_k = a_k$, $k \in S$. This side information is compactly written as $\mathbf{w}_S = \mathbf{a}_S$. The optimal decoder at this receiver utilizes the fact that the transmitted codeword $\mathbf{x}$ corresponds to a message tuple $(w_1, \ldots, w_K)$ for which $\mathbf{w}_S = \mathbf{a}_S$ and hence restricts its search to

$$\mathscr{C}_{\mathbf{a}_S} = \{\psi(w_1, \ldots, w_K) \mid \mathbf{w}_S = \mathbf{a}_S \text{ and } w_k \in \mathscr{W}_k, k \notin S\},$$

which is a subcode of $\mathscr{C}$; see Fig. 6.4. The receiver then decodes the received vector $\mathbf{y}$ to the closest codeword $\hat{\mathbf{x}}$ in $\mathscr{C}_{\mathbf{a}_S}$, i.e.,

$$\hat{\mathbf{x}} = \arg \min_{\mathbf{x} \in \mathscr{C}_{\mathbf{a}_S}} \|\mathbf{y} - \mathbf{x}\|^2.$$

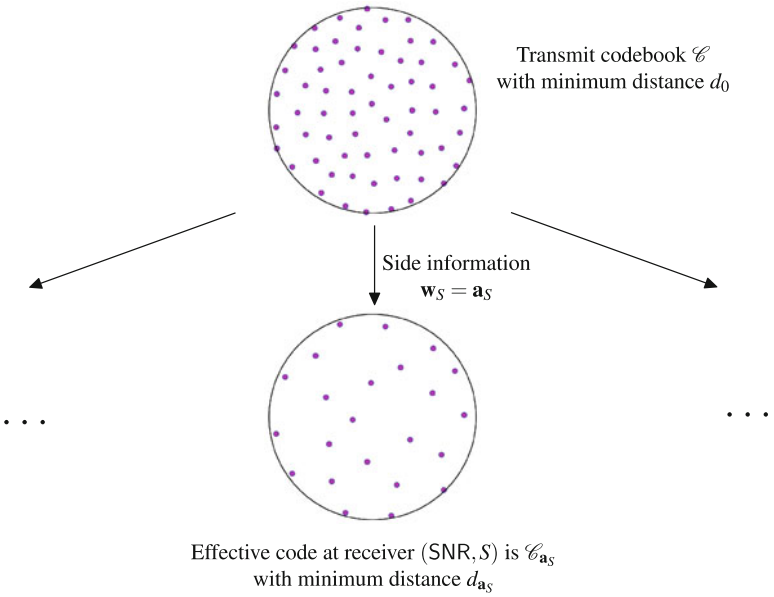


Fig. 6.4 Each receiver (SNR, S) of the broadcast channel expurgates $\mathscr{C}$ to arrive at an effective codebook $\mathscr{C}_{\mathbf{a}_S}$ which depends upon both the subset $S \subset \{1, \ldots, K\}$ of messages available as side information at the receiver and also the value $\mathbf{w}_S = \mathbf{a}_S$ of this side information. The smallest minimum distance $d_{\mathbf{a}_S}$ at the receiver (SNR, S) among all values $\mathbf{a}_S$ is denoted by d_S

At high SNR and when $\mathbf{w}_S = \mathbf{a}_S$, the probability of decoding error is dominated by the minimum distance $d_{\mathbf{a}_S}$ between the vectors in $\mathscr{C}_{\mathbf{a}_S}$,

$$d_{\mathbf{a}_S} = \min\{\|\mathbf{x}_1 - \mathbf{x}_2\| \mid \mathbf{x}_1, \mathbf{x}_2 \in \mathscr{C}_{\mathbf{a}_S},\ \mathbf{x}_1 \neq \mathbf{x}_2\}.$$

Note that the subcode $\mathscr{C}_{\mathbf{a}_S}$ is the effective code observed at the receiver and is a function of the available side information $\mathbf{w}_S$. The number of points in $\mathscr{C}_{\mathbf{a}_S}$ is equal to the number of distinct values that $\mathbf{w}_{S^c}$ can take, where S^c is the complement of S in $\{1, \ldots, K\}$,

$$|\mathscr{C}_{\mathbf{a}_S}| = 2^{n\sum_{k\in S^c} R_k}.$$

Since the source messages are random, so is the side information $\mathbf{w}_S$. Hence, the average performance at this receiver is dominated by the minimum value of $d_{\mathbf{a}_S}$ over all possible values that the side information $\mathbf{w}_S = \mathbf{a}_S$ can assume. We denote this smallest possible minimum distance by

$$d_S = \min\{d_{\mathbf{a}_S} \mid a_k \in \mathscr{W}_k,\ k \in S\}.$$

Using the union bounding technique and the fact $|\mathscr{C}_{\mathbf{a}_S}| = 2^{n\sum_{k\in S^c} R_k}$ for any choice of $\mathbf{a}_S$, we can upper bound the average probability of error at the receiver (SNR, S) as

$$P_S(\hat{\mathbf{x}} \neq \mathbf{x}) \leq \left(2^{n\sum_{k\in S^c} R_k} - 1\right) e^{-d_S^2/8\sigma^2}, \tag{6.1}$$

where σ^2 is the variance of each component of the Gaussian noise vector $\mathbf{z}$.

By comparing the error performance with that of a receiver with no side information, i.e., $S = \varnothing$, we can estimate the amount of apparent SNR gain that side information is translated into. The error probability at a receiver with no side information is dictated by the minimum distance d_0 of the channel code $\mathscr{C}$,

$$d_0 = \min\{\|\mathbf{x}_1 - \mathbf{x}_2\| \mid \mathbf{x}_1, \mathbf{x}_2 \in \mathscr{C},\ \mathbf{x}_1 \neq \mathbf{x}_2\}.$$

The error rate with no side information can be upper bounded as

$$P_0(\hat{\mathbf{x}} \neq \mathbf{x}) \leq (|\mathscr{C}| - 1)\, e^{-d_0^2/8\sigma^2} = \left(2^{nR} - 1\right) e^{-d_0^2/8\sigma^2}. \tag{6.2}$$

From (6.1) and (6.2), at high SNR, the knowledge of the value of $\mathbf{w}_S$ provides an additional coding gain of $10\log_{10}\left(d_S^2/d_0^2\right)$ dB at the receiver (SNR, S). In order to arrive at a fair figure of merit, this squared distance gain is normalized with respect to the *side information rate*

$$R_S = \sum_{k\in S} R_k,$$

which measures the amount of side information available at the receiver (SNR, S).

Definition 6.3 The *side information gain* $\Gamma(\mathscr{C})$ of the code $\mathscr{C}$ is the minimum squared distance gain provided by each bit per dimension of side information at the receivers

$$\Gamma(\mathscr{C}) = \min_{S \subset \{1,\ldots,K\}} \frac{10 \log_{10}(d_S^2/d_0^2)}{R_S}.$$

The side information gain is expressed in the unit dB/b/dim.
For a given code $\mathscr{C}$, the additional coding gain available from the knowledge of $\mathbf{w}_S$ is at least $R_S \times \Gamma(\mathscr{C})$ dB, for any choice of $S \subset \{1, \ldots, K\}$, with respect to the error performance of $\mathscr{C}$ with no receiver side information. It follows that for $\mathscr{C}$ to be a good index code for the AWGN broadcast channel,

1. $\mathscr{C}$ must be a good channel code for the point-to-point AWGN channel, i.e., it must have a large minimum distance d_0. This will minimize the SNR requirement at the receiver with no side information; and
2. $\Gamma(\mathscr{C})$ must be large, so as to maximize the minimum gain from the availability of side information at the other receivers.

6.4 Voronoi Constellations for Index Coding: An Illustration

The structure of Voronoi constellations allows us to label its codewords using algebraic techniques. A well-known algebraic labelling technique is *linear labelling*, where the points in Λ/Λ' are associated with messages in such a way that the sum of any two codeword points (modulo Λ') is mapped to the sum of the corresponding messages. Linear labelling is crucial in wireless network coding applications, such as in *compute-and-forward* [76], and utilizes the property that Λ/Λ' can be viewed as a module over an appropriate ring (such as the ring of integers $\mathbb{Z}$). As will be illustrated in this section, a specific linear labelling scheme arising from the *Chinese remainder theorem* will enable us to construct good Voronoi constellations for index coding. Let us first recall the Chinese remainder theorem using the language of nested lattices as

Theorem 6.1 (Chinese Remainder Theorem [87]) *Let $p_1, \ldots, p_K \in \mathbb{Z}$ be K relatively prime integers and let $M = \prod_{k=1}^{K} p_k$ and $M_k = M/p_k$, $k = 1, \ldots, K$. The function*

$$\varphi(w_1, \ldots, w_K) = (w_1 M_1 + \cdots + w_K M_K) \bmod M\mathbb{Z}$$

is a one-to-one correspondence between $\mathbb{Z}/p_1\mathbb{Z} \times \cdots \times \mathbb{Z}/p_K\mathbb{Z}$ and $\mathbb{Z}/M\mathbb{Z}$. Further, for any choice of $w_1 \in \mathbb{Z}/p_1\mathbb{Z}, \ldots, w_K \in \mathbb{Z}/p_K\mathbb{Z}$, $x = \varphi(w_1, \ldots, w_K)$ is the unique element of $\mathbb{Z}/M\mathbb{Z}$ with the property

$$x \bmod p_1\mathbb{Z} = w_1,\ x \bmod p_2\mathbb{Z} = w_2, \ldots,\ x \bmod p_K\mathbb{Z} = w_K.$$

Apart from the Chinese remainder theorem, the following elementary result from number theory will prove useful in our analysis.

Theorem 6.2 (Greatest Common Divisor [87]) *For any two non-zero integers $a, b \in \mathbb{Z}$, the greatest common (*gcd*) divisor of a and b is the smallest positive integer in the set $\{ma + nb \,|\, m, n, \in \mathbb{Z}\}$.*

To illustrate the utility of the Chinese remainder theorem in designing index codes for the AWGN channel, we will now consider a one-dimensional channel code $\mathbb{Z}/M\mathbb{Z}$ (an M-ary PAM constellation) encoding K messages whose alphabets are $\mathscr{W}_1 = \mathbb{Z}/p_1\mathbb{Z}, \ldots, \mathscr{W}_K = \mathbb{Z}/p_K\mathbb{Z}$. Assume $K = 3$ and $p_1 = 2$, $p_2 = 3$, and $p_3 = 5$, resulting in $M = 30$, $M_1 = 15$, $M_2 = 10$ and $M_3 = 6$. The channel code used at the encoder is the 30-PAM signal set $\mathscr{C} = \mathbb{Z}/30\mathbb{Z} = \{-15, -14, \ldots, 13, 14\}$. The message alphabets of the three messages are

$$\mathscr{W}_1 = \mathbb{Z}/2\mathbb{Z} = \{-1, 0\},\ \mathscr{W}_2 = \mathbb{Z}/3\mathbb{Z} = \{-1, 0, 1\}, \mathscr{W}_3 = \mathbb{Z}/5\mathbb{Z} = \{-2, -1, 0, 1, 2\}.$$

The messages (w_1, w_2, w_3) are encoded to a point $x \in \mathscr{C}$ using the map arising from the Chinese remainder theorem

$$x = \sum_{k=1}^{K} w_k M_k \bmod M\mathbb{Z} = (15w_1 + 10w_2 + 6w_3) \bmod 30\mathbb{Z},$$

where the function $\bmod 30\mathbb{Z}$ returns the unique remainder in $\{-15, -14, \ldots, 14\}$ when the argument is divided by 30. It follows from the Chinese remainder theorem that $\mathscr{C}$ is the set of all possible values that x can assume, and there is a one-to-one correspondence between $\mathscr{C}$ and the set of messages $\mathscr{W}_1 \times \mathscr{W}_2 \times \mathscr{W}_3$. Since the dimension of $\mathscr{C}$ is $n = 1$, the rate of the k^{th} message is $R_k = \log_2 |\mathscr{W}_k|$ b/dim, i.e.,

$$R_1 = 1,\ R_2 = \log_2 3,\ \text{and}\ R_3 = \log_2 5 \text{ b/dim}.$$

We now analyze the minimum distance d_S and the side information gain Γ of this one-dimensional code. If a receiver in the broadcast channel has no side information ($S = \varnothing$), it decodes (w_1, w_2, w_3) by choosing the point in $\mathscr{C}$ that is nearest to the channel output. The corresponding minimum inter-codeword distance is $d_0 = 1$.

Figure 6.5 shows an example of a receiver with $S = \{3\}$ and when the side information is $w_3 = 1$. The expurgated code for this side information consists of 6 points corresponding to all possible choices of (w_1, w_2) when $w_3 = 1$ is a constant and is given

$$\{15w_1 + 10w_2 + 6 \bmod 30\mathbb{Z} \,|\, w_1 \in \mathbb{Z}/2\mathbb{Z}, w_2 \in \mathbb{Z}/3\mathbb{Z}\}\,.$$

Any two points in this signal set differ by $15\Delta w_1 + 10\Delta w_2$, where Δw_1 and Δw_2 are integers, both not equal to zero. Hence, from Theorem 6.2, the minimum distance of this codebook is $\gcd(15, 10) = 5$, which is easily verified from Fig. 6.5. Similarly, for any value of the side information w_3, the resulting codebook has distance $d_S = 5$. The side information rate at this receiver is $R_S = \log_2 5$ b/dim. Observe that R_S and d_S are related $R_S = \log_2 d_S$.

When $S = \{1, 2\}$, the set of possible transmit symbols is

$$\mathscr{C}_{(a_1,a_2)} = \{15a_1 + 10a_2 + 6w_3 \bmod 30\mathbb{Z} \,|\, w_3 \in \mathscr{W}_3\}\,,$$

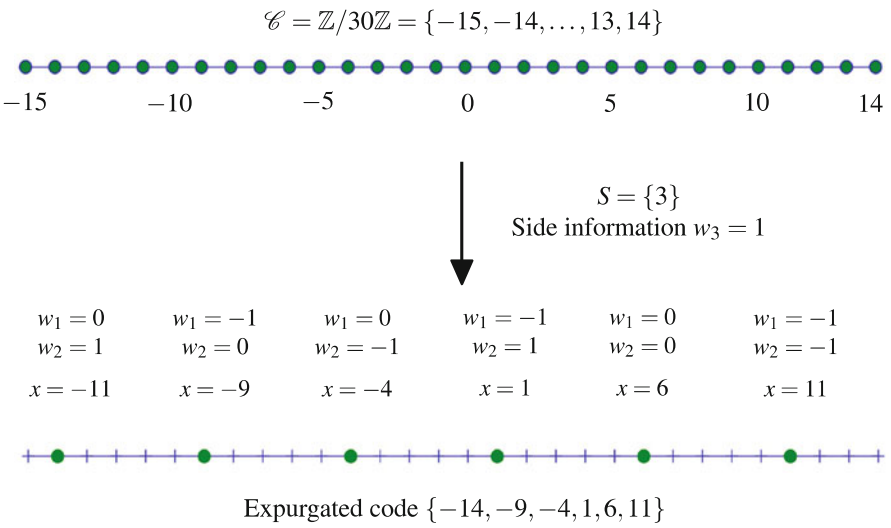


Fig. 6.5 The effective code at the receiver with $S = \{3\}$ and side information $w_3 = 1$. The expurgated code is $\{15w_1 + 10w_2 + 6 \bmod 30\mathbb{Z} \,|\, w_1 \in \mathbb{Z}/2\mathbb{Z}, w_2 \in \mathbb{Z}/3\mathbb{Z}\}$. The knowledge of the value of w_3 has increased the minimum distance by a factor of 5

where $w_1 = a_1$ and $w_2 = a_2$ are known to the receiver as side information, and hence, $15a_1 + 10a_2$ is a constant. The effective constellation $\mathscr{C}_{(a_1,a_2)}$ is a scaled and shifted 5-PAM signal set where the adjacent points are separated by a distance of 6. It follows that the minimum distance of this subcode is $d_S = 6$, while the side information rate is $R_S = R_1 + R_2 = \log_2 6$ b/dim. Again, we observe that $R_S = \log_2 d_S$.

Proceeding likewise, we observe that for every choice of $S \subset \{1, 2, 3\}$, the side information rate and minimum distance are related as

$$R_S = \log_2 d_S.$$

Using this relation in the definition of Γ, we see that the side information gain of this code is $\Gamma = 20 \log_{10} 2 \approx 6$ dB/b/dim. Hence, a side information of rate R_S b/dim translates into an additional coding gain of approximately $6 R_S$ dB.

Figure 6.6 shows the performance of the code with $S = \varnothing$, $S = \{1\}$ and $S = \{1, 2\}$, the corresponding values of d_S are 1, 2 and 6, respectively. From the figure we observe that at the probability of error of 10^{-4}, the side informations corresponding to $S = \{1\}$ and $S = \{1, 2\}$ provide SNR gains of 6 dB and 15.6 dB over $S = \varnothing$. This is close to the corresponding squared distance gains of $10 \log_{10} (2^2)$ dB and $10 \log_{10} (6^2)$ dB, respectively.

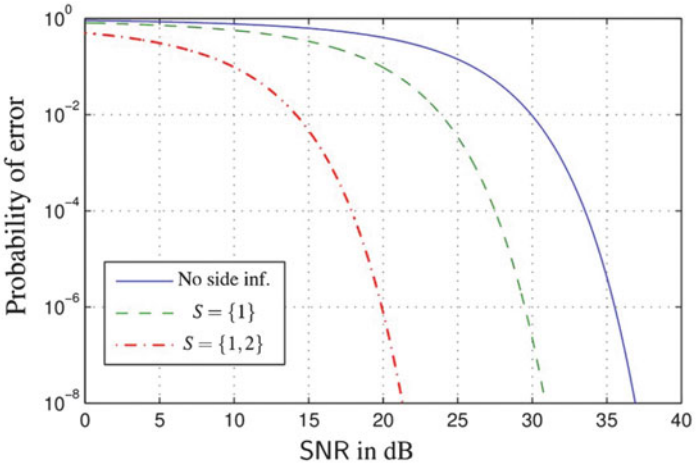


Fig. 6.6 Performance of the one-dimensional index code at three different receivers. The error performance improves as the amount of side information increases

6.5 Lattice Index Codes

Our purpose now is to construct Voronoi constellations in arbitrary dimensions to encode any number K of independent messages such that the resulting code has a large minimum distance d_0 and large side information gain Γ. To do so, we will utilize a set of K lattices $\Lambda_1, \ldots, \Lambda_K$ with a common sublattice Λ', i.e.,

$$\Lambda' \subset \Lambda_k,\ k = 1, \ldots, K.$$

Each of the K messages w_k will be mapped to a unique point $\mathbf{x}_k \in \Lambda_k/\Lambda'$, and the transmit codeword $\mathbf{x}$ will be generated as $\mathbf{x} = (\mathbf{x}_1 + \cdots + \mathbf{x}_K) \bmod \Lambda'$. For unique decodability, we will require that this correspondence between the tuple of messages $(w_1, \ldots, w_K)$ and the codeword $\mathbf{x}$ be one-to-one.

Definition 6.4 A *lattice index code* for K messages consists of K lattice constellations $\Lambda_1/\Lambda', \ldots, \Lambda_K/\Lambda'$ with a common shaping lattice Λ', and a bijective map $\psi : \Lambda_1/\Lambda' \times \cdots \times \Lambda_K/\Lambda' \to \mathscr{C}$ given by

$$\psi(\mathbf{x}_1, \ldots, \mathbf{x}_K) = (\mathbf{x}_1 + \cdots + \mathbf{x}_K) \bmod \Lambda', \tag{6.3}$$

where $\mathbf{x}_k \in \Lambda_k/\Lambda'$ and $\mathscr{C}$ is the set of all possible values of the transmit symbol $\mathbf{x} = \psi(\mathbf{x}_1, \ldots, \mathbf{x}_K)$.
Note that the bijection ψ is an algebraic method to label the codewords in $\mathscr{C}$ with elements of $\Lambda_1/\Lambda' \times \cdots \times \Lambda_K/\Lambda'$. If the lattices used are n-dimensional, then the rate of transmission of the k^{th} message w_k is

$$R_k = \frac{1}{n}\log_2 |\Lambda_k/\Lambda'| = \frac{1}{n}\log_2\left(\frac{V(\Lambda')}{V(\Lambda_k)}\right).$$

We now make the observation that the one-dimensional index code of Sect. 6.4 is a lattice index code.

Example 6.6 The index code of Sect. 6.4 encodes $K = 3$ messages to a symbol from the 30-PAM signal set. The component lattices that define this index code are $\Lambda_1 = 15\mathbb{Z}$, $\Lambda_2 = 10\mathbb{Z}$, and $\Lambda_3 = 6\mathbb{Z}$, and the shaping lattice is $\Lambda' = 30\mathbb{Z}$. The messages w_1, w_2, w_3 are first mapped to the symbols $x_1 = 15w_1$, $x_2 = 10w_2$, and $x_3 = 6w_3$, respectively, and the transmitted symbol is generated as

$$x = (x_1 + x_2 + x_3) \bmod 30\mathbb{Z}.$$

The Chinese remainder theorem (Theorem 6.1) shows that the set $\mathscr{C}$ of all possible transmit symbols x is $\mathbb{Z}/30\mathbb{Z}$ and that this encoding map is a bijection.
We now analyze some of the properties of a lattice index code in terms of its component lattice constellations $\Lambda_1/\Lambda', \ldots, \Lambda_K/\Lambda'$. Let

$$\Lambda = \Lambda_1 + \cdots + \Lambda_K = \{\mathbf{v}_1 + \cdots + \mathbf{v}_K \,|\, \mathbf{v}_k \in \Lambda_k,\, k = 1, \ldots, K\}$$

denote the lattice obtained as the sum of the component lattices. Note that $\Lambda_k \subset \Lambda$ for all $k = 1, \ldots, K$, and hence, for any choice of $\mathbf{x}_1 \in \Lambda_1/\Lambda, \ldots, \mathbf{x}_K \in \Lambda_K/\Lambda'$, we have $\mathbf{x}_1 + \cdots + \mathbf{x}_K \in \Lambda$. It follows that

$$\mathbf{x} = \psi(\mathbf{x}_1, \ldots, \mathbf{x}_K) = (\mathbf{x}_1 + \cdots + \mathbf{x}_K) \bmod \Lambda' \in \Lambda/\Lambda'.$$

Hence, we have $\mathscr{C} \subset \Lambda/\Lambda'$. Conversely, if $\mathbf{v} \in \Lambda/\Lambda'$, we have $\mathbf{v} \in \Lambda$, and therefore, there exist $\mathbf{v}_1 \in \Lambda_1, \ldots, \mathbf{v}_K \in \Lambda_K$ such that $\mathbf{v} = \mathbf{v}_1 + \cdots + \mathbf{v}_K$. Using the fact that $\mathbf{v} \in \mathscr{V}_{\Lambda'}(\mathbf{0})$, we obtain

$$\begin{aligned}\mathbf{v} = \mathbf{v} \bmod \Lambda' &= (\mathbf{v}_1 + \cdots + \mathbf{v}_K) \bmod \Lambda' \\ &= \left(\mathbf{v}_1 \bmod \Lambda' + \cdots + \mathbf{v}_K \bmod \Lambda'\right) \bmod \Lambda' \\ &= \psi\left(\mathbf{v}_1 \bmod \Lambda', \ldots, \mathbf{v}_K \bmod \Lambda'\right),\end{aligned}$$

where $\mathbf{v}_k \bmod \Lambda' \in \Lambda_k/\Lambda'$, for $k = 1, \ldots, K$. It follows that $\mathbf{v} \in \mathscr{C}$ and hence $\Lambda/\Lambda' \subset \mathscr{C}$. We have therefore shown that the transmit codebook $\mathscr{C}$ is itself a Voronoi constellation and is given by

$$\mathscr{C} = \Lambda/\Lambda'.$$

We are now in a position to characterize the minimum distances at a receiver with an arbitrary side information $S \subset \{1, \ldots, K\}$. First consider the case $S = \varnothing$; the minimum distance d_0 is the smallest distance between any pair of points in $\mathscr{C}$.

Since $\mathscr{C}$ is carved from the lattice Λ, the minimum distance of $\mathscr{C}$ is the smallest distance between any two lattice points in Λ which in turn is equal to the minimum norm of Λ or twice the packing radius

$$d_0 = \lambda = 2\rho(\Lambda).$$

Now suppose a receiver has side information $\mathbf{x}_k = \mathbf{a}_k$ for $k \in S$ for some $S \subset \{1, \ldots, K\}$. Denoting the complement of S in $\{1, \ldots, K\}$ as S^{c}, the subcode used for decoding at this receiver is

$$\begin{aligned}
\mathscr{C}_{\mathbf{a}_S} &= \left\{ \psi\left(\mathbf{x}_1, \ldots \mathbf{x}_K\right) \mid \mathbf{x}_k = \mathbf{a}_k, k \in S \text{ and } \mathbf{x}_k \in \Lambda_k/\Lambda', k \in S^{\mathsf{c}} \right\} \\
&= \left\{ \left(\sum_{k\in S} \mathbf{a}_k + \sum_{k\in S^{\mathsf{c}}} \mathbf{x}_k \right) \bmod \Lambda' \;\middle|\; \mathbf{x}_k \in \Lambda_k/\Lambda',\ k \in S^{\mathsf{c}} \right\} \\
&= \left\{ \left(\sum_{k\in S} \mathbf{a}_k + \sum_{k\in S^{\mathsf{c}}} \mathbf{v}_k \right) \bmod \Lambda' \;\middle|\; \mathbf{v}_k \in \Lambda_k,\ k \in S^{\mathsf{c}} \right\}, \qquad (6.4)
\end{aligned}$$

where the last equality follows from the observations

$$\left(\sum_{k\in S} \mathbf{a}_k + \sum_{k\in S^{\mathsf{c}}} \mathbf{v}_k \right) \bmod \Lambda' = \left(\sum_{k\in S} \mathbf{a}_k + \sum_{k\in S^{\mathsf{c}}} \mathbf{v}_k \bmod \Lambda' \right) \bmod \Lambda'.$$

and $\mathbf{v}_k \bmod \Lambda' \in \Lambda_k/\Lambda'$. Denoting the lattice obtained as the sum of the component lattices Λ_k, $k \in S^{\mathsf{c}}$ by

$$\Lambda_{S^{\mathsf{c}}} = \sum_{k\in S^{\mathsf{c}}} \Lambda_k = \left\{ \sum_{k\in S^{\mathsf{c}}} \mathbf{v}_k \;\middle|\; \mathbf{v}_k \in \Lambda_k,\ k \in S^{\mathsf{c}} \right\},$$

we can express (6.4) as

$$\mathscr{C}_{\mathbf{a}_S} = \left(\sum_{k\in S} \mathbf{a}_k + \Lambda_{S^{\mathsf{c}}} \right) \bmod \Lambda'.$$

Hence, the effective codebook $\mathscr{C}_{\mathbf{a}_S}$ is the set obtained by translating the Voronoi constellation $\Lambda_{S^{\mathsf{c}}}/\Lambda'$ by the vector $\sum_{k\in S} \mathbf{a}_k$ modulo the shaping lattice Λ'. It follows that the minimum distance of this code, irrespective of the value of the side information $\mathbf{a}_k$, $k \in S$, is

$$d_S = 2\,\rho\left(\Lambda_{S^{\mathsf{c}}}\right).$$

6.5.1 An Upper Bound on the Side Information Gain

Recall from the discussion in Sect. 6.3 that for $\mathscr{C}$ to be a good index code in the AWGN broadcast channel, we require $\mathscr{C}$ to have a large side information gain $\Gamma(\mathscr{C})$ as well as a large coding gain in the traditional point-to-point AWGN channel. If $\mathscr{C}$ is a Voronoi constellation Λ/Λ', its coding gain in the point-to-point AWGN channel is determined by the packing density $\Delta(\Lambda)$ of the coding lattice Λ. It is then natural to seek the best possible side information gain when the Voronoi constellation uses the coding lattice Λ with the optimum packing density. We will now see that the side information gain of lattice index codes is upper bounded by $20\log_{10} 2 \approx 6$ dB/b/dim when Λ chosen to provide the best lattice packing in $\mathbb{R}^n$. In Sect. 6.6 we provide a construction of lattice index codes that achieves this upper bound.

Assume that $\Lambda_1/\Lambda', \ldots, \Lambda_K/\Lambda'$ define an n-dimensional lattice index code for K messages such that the sum lattice $\Lambda = \Lambda_1 + \cdots + \Lambda_K$ has the optimal packing density $\Delta(\Lambda)$ among all lattices in n dimensions. Let us now consider a receiver with side information configuration $S = \{1, \ldots, K-1\}$, i.e., the receiver knows the values of all the messages except w_K. For this receiver, $\Lambda_{S^c} = \sum_{k\in S^c} \Lambda_k = \Lambda_K$, and the minimum distance is

$$d_S = 2\,\rho(\Lambda_{S^c}) = 2\,\rho(\Lambda_K).$$

The side information rate at this receiver is

$$R_S = R_1 + \cdots + R_{K-1} = R - R_K,$$

where R is the sum rate of all the K messages. Since the messages are uniquely mapped to codewords in Λ/Λ', we have $|\Lambda/\Lambda'| = 2^{nR}$. Using this observation together with the identity $|\Lambda_K/\Lambda'| = 2^{nR_K}$, we obtain

$$\begin{aligned} R_S = R - R_K &= \frac{1}{n}\log_2 |\Lambda/\Lambda'| - \frac{1}{n}\log_2 |\Lambda_K/\Lambda'| \\ &= \frac{1}{n}\log_2 \frac{V(\Lambda')}{V(\Lambda)} - \frac{1}{n}\log_2 \frac{V(\Lambda')}{V(\Lambda_K)} \\ &= \frac{1}{n}\log_2 \frac{V(\Lambda_K)}{V(\Lambda)} \end{aligned} \tag{6.5}$$

We now relate R_S to the packing densities of Λ and Λ_K through their packing radii. From the definition of the packing density Δ, we observe that

$$V(\Lambda) = \frac{\text{vol}\,\mathscr{B}^n(\rho(\Lambda))}{\Delta(\Lambda)} = \text{vol}\mathscr{B}^n(1)\,\frac{\rho^n(\Lambda)}{\Delta(\Lambda)},$$

where $\mathscr{B}^n(r)$ is the n-dimensional Euclidean ball of radius r. Using a similar identity for $V(\Lambda_K)$, we rewrite (6.5) as

$$R_S = \frac{1}{n}\log_2 \frac{\rho^n(\Lambda_K)}{\Delta(\Lambda_K)}\frac{\Delta(\Lambda)}{\rho^n(\Lambda)} = \frac{1}{n}\log_2 \frac{\rho^n(\Lambda_K)}{\rho^n(\Lambda)} + \frac{1}{n}\log_2 \frac{\Delta(\Lambda)}{\Delta(\Lambda_K)}$$
$$= \log_2 \frac{\rho(\Lambda_K)}{\rho(\Lambda)} + \frac{1}{n}\log_2 \frac{\Delta(\Lambda)}{\Delta(\Lambda_K)}.$$

Utilizing the assumption that Λ has the highest packing density among all n-dimensional lattices, we observe that $\Delta(\Lambda) \geq \Delta(\Lambda_K)$, and hence,

$$R_S \geq \log_2 \frac{\rho(\Lambda_K)}{\rho(\Lambda)}.$$

Since $d_S = 2\rho(\Lambda_K)$ and $d_0 = 2\rho(\Lambda)$, we therefore have $R_S \geq \log_2(d_S/d_0)$. To conclude, for $S = \{1, \ldots, K-1\}$, we have the inequality

$$\frac{d_S}{d_0} \leq 2^{R_S} = 2^{R-R_K}.$$

We can now upper bound the side information gain of Λ/Λ' as follows

$$\begin{aligned}
\Gamma(\Lambda/\Lambda') &= \min_{S\subset\{1,\ldots,K\}} \frac{10\log_{10}\left(d_S^2/d_0^2\right)}{R_S} \\
&\leq \left.\frac{10\log_{10}\left(d_S^2/d_0^2\right)}{R_S}\right|_{S=\{1,\ldots,K-1\}} \\
&\leq \frac{10\log_{10}\left(2^{2(R-R_K)}\right)}{(R-R_K)} \\
&= \frac{20\,(R-R_K)\,\log_{10}2}{(R-R_K)} \\
&= 20\log_{10}2.
\end{aligned}$$

We conclude that if the code Λ/Λ' is optimized for minimum distance or channel coding gain for the AWGN channel, the side information gain can be at the most $20\log_{10}2 \approx 6$ dB/b/dim. Conversely, any side information gain of more than 6 dB/b/dim can be attained only if a lattice Λ of suboptimal packing efficiency is used as the coding lattice. In this case the higher value of side information gain is attained at the cost of a poorer error performance at the receiver with no side information ($S = \varnothing$).

6.6 A Construction of Lattice Index Codes Using the Chinese Remainder Theorem

The encoding technique used in the example of Sect. 6.4 can be generalized to higher dimensions and arbitrary number of messages K. The ingredients for this construction are K relatively prime positive integers $p_1, \ldots, p_K$ and an arbitrary n-dimensional lattice Λ. We will use scaled versions of Λ to design $\Lambda_1, \ldots, \Lambda_K$ and Λ', where the scaling coefficients are borrowed from the Chinese remainder theorem. With $M = \prod_{k=1}^{K} p_k$ and $M_k = M/p_k$, let

$$\Lambda_k = M_k \Lambda \text{ for } k = 1, \ldots, K \text{ and } \Lambda' = M\Lambda. \tag{6.6}$$

We will now show that this set of component lattices defines a lattice index code with $\Gamma \approx 6$ dB/b/dim. Note that the size of the kth message alphabet is

$$|\Lambda_k/\Lambda'| = \frac{V(\Lambda')}{V(\Lambda_k)} = \frac{M^n V(\Lambda)}{M_k^n V(\Lambda)} = p_k^n,$$

and the rate of the kth message is

$$R_k = \frac{1}{n} \log_2 |\Lambda_k/\Lambda'| = \log_2 p_k \text{b/dim}.$$

The side information rate at the receiver (SNR, S) is

$$R_S = \sum_{\ell \in S} R_k = \sum_{\ell \in S} \log_2 p_k = \log_2 \left(\prod_{\ell \in S} p_\ell \right).$$

We will utilize the following observation to analyze the constructed lattice index code.

Lemma 6.1 *For any* $S \subset \{1, \ldots, K\}$, $\gcd(M_k, k \in S^{\mathsf{c}}) = \prod_{\ell \in S} p_\ell$.

Proof Observe that $p_1, \ldots, p_K$ are relatively prime and $M_k = \prod_{\ell \neq k} p_\ell$. Since p_k is not a factor of M_k, none of the integers p_k, $k \in S^{\mathsf{c}}$, divides $\gcd(M_k, k \in S^{\mathsf{c}})$. The lemma follows from the observation that each M_k, $k \in S^{\mathsf{c}}$, contains $\prod_{\ell \in S} p_\ell$ as a factor, and hence, their greatest common divisor $\gcd(M_k, k \in S^{\mathsf{c}})$ is divisible by $\prod_{\ell \in S} p_\ell$.

We now show that with the component lattices as defined in (6.6), the transmit codebook is $\mathscr{C} = \Lambda/\Lambda'$ and the encoding map $(\mathbf{x}_1, \ldots, \mathbf{x}_K) \to (\mathbf{x}_1 + \cdots + \mathbf{x}_K) \bmod \Lambda'$ is injective. From Lemma 6.1, $\gcd(M_k, k \in S^{\mathsf{c}}) = \prod_{\ell \in S} p_\ell$ for any S. Hence, there exists a tuple $(b_k, k \in S^{\mathsf{c}})$ of integers such that

$$\sum_{k \in S^{\mathsf{c}}} b_k M_k = \gcd(M_k, k \in S^{\mathsf{c}}) = \prod_{\ell \in S} p_\ell.$$

It follows that, for every $\mathbf{v} \in \Lambda$, we have $\prod_{\ell \in S} p_\ell \mathbf{v} = \sum_{k \in S^c} b_k M_k \mathbf{v}$, where $M_k \mathbf{v} \in \Lambda_k$ and $b_k M_k \mathbf{v} \in \Lambda_k$. Hence

$$\prod_{\ell \in S} p_\ell \, \Lambda \subset \sum_{k \in S^c} M_k \Lambda = \sum_{k \in S^c} \Lambda_k = \Lambda_{S^c}.$$

Considering cosets modulo Λ',

$$\prod_{\ell \in S} p_\ell \, \Lambda \, / \Lambda' \subset \Lambda_{S^c} / \Lambda'. \tag{6.7}$$

Let $\psi|_{S^c}$ be the restriction of the encoding map (6.3) to the message symbols with indices in S^c, i.e.,

$$\psi|_{S^c} \left(\mathbf{x}_k, k \in S^c \right) = \sum_{k \in S^c} \mathbf{x}_k \bmod \Lambda'.$$

Note that Λ_{S^c} / Λ' is the image of the map $\psi|_{S^c}$. From (6.7), $\prod_{\ell \in S} p_\ell \Lambda / \Lambda'$ is a subset of this image. Hence, the image of the function $\psi|_{S^c}$ has cardinality

$$\left| \Lambda_{S^c} / \Lambda' \right| \geq \left| \prod_{\ell \in S} p_\ell \Lambda / \Lambda' \right| = \frac{M^n \, V(\Lambda)}{\prod_{\ell \in S} p_\ell^n \, V(\Lambda)} = \prod_{k \in S^c} p_k^n \tag{6.8}$$

Now, the domain of the function $\psi|_{S^c}$ has cardinality

$$\prod_{k \in S^c} \left| \Lambda_k / \Lambda' \right| = \prod_{k \in S^c} p_k^n$$

which equals the lower bound (6.8). Hence, we conclude that $\psi|_{S^c}$ is an injective map, and the subset $\prod_{\ell \in S} p_\ell \Lambda / \Lambda'$ equals the entire image Λ_{S^c} / Λ'. This implies that

$$\prod_{\ell \in S} p_\ell \Lambda = \Lambda_{S^c} = \sum_{k \in S^c} \Lambda_k. \tag{6.9}$$

Choosing $S = \varnothing$, we observe that $\psi|_{S^c} = \psi$ is injective, and $\sum_{k=1}^{K} \Lambda_k = \Lambda$. Hence, the transmit codebook $\mathscr{C} = \sum_{k=1}^{K} \Lambda_k / \Lambda' = \Lambda / \Lambda'$.

As we will show next, the Voronoi constellation $\mathscr{C}$ enjoys a side information gain of approximately 6 dB/b/dim. Since $\mathscr{C} = \Lambda / \Lambda'$, we have $d_0 = 2\,\rho(\Lambda)$. Further, using (6.9) and the relation $R_S = \log_2 \prod_{\ell \in S} p_\ell$, we have

$$d_S = 2\,\rho\left(\Lambda_{S^c}\right) = 2\,\rho\left(\prod_{\ell \in S} p_\ell \Lambda \right) = \prod_{\ell \in S} p_\ell \; 2\rho(\Lambda) = \prod_{\ell \in S} p_\ell \; d_0 = 2^{R_S} \, d_0.$$

Substituting $d_S/d_0 = 2^{R_S}$ in

$$\Gamma = \min_S \frac{10 \log_{10} \left(d_S^2/d_0^2\right)}{R_S},$$

we obtain $\Gamma = 20 \log_{10} 2 \approx 6$ dB/b/dim.

The above construction has the flexibility to encode any number of messages K and can utilize any lattice Λ in an arbitrary dimension n. If Λ has the highest packing density in n dimensions, such as when Λ is $\mathbb{Z}$, A_2, E_8, or Λ_{24}, we have already observed in Sect. 6.5.1 that $\Gamma \leq 20 \log_{10} 2$. Hence, for such choices of Λ, our construction provides the optimal side information gain.

Since the minimum distance $d_S = 2^{R_S} d_0 = 2^{R_S} 2\rho(\Lambda)$ is related to the packing radius of Λ, the performance of all the receivers in the broadcast channel can be simultaneously improved by choosing a coding lattice Λ with a high packing density $\Delta(\Lambda)$. Further, the shaping region of the code $\mathscr{C}$ is the Voronoi region $\mathscr{V}_{\Lambda'}(\mathbf{0})$ of $\Lambda' = M\Lambda$ which is geometrically similar to the Voronoi region $\mathscr{V}_{\Lambda}(\mathbf{0})$ of the lattice Λ. Hence, to achieve a large coding gain, Λ must be chosen to provide a large shaping gain in addition to a high packing density.

6.7 Discussion

Index coding is gathering considerable attention not only due to its wide applications but also because of its strong theoretical connections to other major areas in communication and information theory. This chapter introduced a framework for analyzing and constructing index codes for the AWGN broadcast channel. The algebraic construction of lattice index codes relies on the Chinese remainder theorem and the property that any lattice is a module over the ring of integers $\mathbb{Z}$, i.e., any integer linear combination of lattice points is also a lattice point. While the side information gain is high, the encoding rates of the messages are unequal and are limited to be logarithms of relatively prime integers. More advanced techniques utilize lattices that are modules over the ring of integers of an algebraic number field [51] or over multidimensional principal ideal domains [75]. In the former case, the construction uses relatively prime ideals in the ring of algebraic integers together with the Chinese remainder theorem. This generalization provides a greater choice of transmission rates, allows one to encode all the messages at the same rate, and also achieves diversity gains in fading channels in addition to side information gain.

The main algebraic ingredient used in the construction of lattice index codes, viz., labelling the points of a Voronoi constellation using the Chinese remainder theorem, also plays a key role in the construction of a family of multilevel lattice codes [52] that can be decoded at low complexity using multistage decoding.

From an engineering perspective, it is important to encode all the messages at the same rate with the alphabet size of each message being a power of 2. No theoretical constructions index codes are known for this practically relevant case, although a few codes in small dimensions obtained using a computer search are available [74].

References

1. J.F. Adams, *Lectures on Lie Groups (Midway Reprints Series)* (University of Chicago Press, Chicago, 1983)
2. E. Agrell, T. Eriksson, A. Vardy, K. Zeger, Closest point search in lattices. IEEE Trans. Inf. Theory **48**(8), 2201–2214 (2002)
3. M. Ajtai, Generating hard instances of lattice problems, in *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, STOC '96, New York, NY (ACM, 1996), pp. 99–108
4. C. Alves, S.I.R. Costa, Commutative group codes in and —approaching the bound. Discret. Math. **313**(16), 1677–1687 (2013)
5. F. Arbabjolfaei, Y.H. Kim, Local time sharing for index coding, in *IEEE International Symposium on Information Theory* (2014), pp. 286–290
6. W. Banaszczyk, New bounds in some transference theorems in the geometry of numbers. Math. Ann. **296**(1), 625–635 (1993)
7. Z. Bar-Yossef, Y. Birk, T.S. Jayram, T. Kol, Index coding with side information. IEEE Trans. Inf. Theory **57**(3), 1479–1494 (2011)
8. E.S. Barnes, G.E. Wall, Some extreme forms defined in terms of abelian groups. J. Aust. Math. Soc. **1**(1), 47–63 (1959)
9. E. Bayer-Fluckiger, F. Oggier, E. Viterbo, New algebraic constructions of rotated $\mathbb{Z}^n$-lattice constellations for the Rayleigh fading channel. IEEE Trans. Inf. Theory **50**(4), 702–714 (2004)
10. M. Bhargava, J. Hanke, Universal quadratic forms and the 290 theorem. Invent. Math. (to appear)
11. E. Biglieri, M. Elia, Cyclic-group codes for the gaussian channel (corresp.). IEEE Trans. Inf. Theory **22**(5), 624–629 (1976)
12. Y. Birk, T. Kol, Informed-source coding-on-demand (ISCOD) over broadcast channels, in *Proceedings of IEEE Seventeenth Annual Joint Conference of the IEEE Computer and Communications Societies INFOCOM '98*, vol. 3 (1998), pp. 1257–1264
13. A. Blasiak, R. Kleinberg, E. Lubetzky, Broadcasting with side information: bounding and approximating the broadcast rate. IEEE Trans. Inf. Theory **59**(9), 5811–5823 (2013)
14. N. Bourbaki, *Lie Groups and Lie Algebras: Chapters 4–6 (Elements of Mathematics)* (Springer, Berlin, 2002)
15. J. Boutros, E. Viterbo, C. Rastello, J.C. Belfiore, Good lattice constellations for both rayleigh fading and gaussian channels. IEEE Trans. Inf. Theory **42**(2), 502–518 (1996)

S.I.R. Costa et al., *Lattices Applied to Coding for Reliable and Secure Communications*, SpringerBriefs in Mathematics,
https://doi.org/10.1007/978-3-319-67882-5

16. G. Caire, E. Biglieri, Linear block codes over cyclic groups. IEEE Trans. Inf. Theory **41**(5), 1246–1256 (1995)
17. A. Campello, J. Strapasson, S.I.R. Costa, On projections of arbitrary lattices. Linear Algebra Appl. **439**(9), 2577–2583 (2013)
18. A. Campello, C. Torezzan, S.I.R. Costa, Curves on flat tori and analog source-channel codes. IEEE Trans. Inf. Theory **59**(10), 6646–6654 (2013)
19. A. Campello, G.C. Jorge, J.E. Strapasson, S.I.R. Costa, Perfect codes in the l p metric. Eur. J. Comb. **53**(C), 72–85 (2016)
20. J.W.S. Cassels, *An Introduction to the Geometry of Numbers* (Springer, Berlin, 1997)
21. H. Cohen, *A Course in Computational Algebraic Number Theory* (Springer, New York, 1996)
22. H. Cohn, N. Elkies, New upper bounds on sphere packings I. Ann. Math. **157**(2), 689–714 (2003)
23. J. Conway, N. Sloane, Voronoi regions of lattices, second moments of polytopes, and quantization. IEEE Trans. Inf. Theory **28**(2), 211–226 (1982)
24. J.H. Conway, N.J.A. Sloane, Laminated lattices. Ann. Math. **116**(3), 593–620 (1982)
25. J.H. Conway, N.J.A. Sloane, On the voronoi regions of certain lattices. SIAM J. Algebr. Discret. Methods **5**(3), 294–305, (1984)
26. J.H. Conway, N.J.A. Sloane, *Sphere-Packings, Lattices, and Groups* (Springer, New York, 1998)
27. S.I.R. Costa, On closed twisted curves. Proc. Am. Math. Soc. **109**(1), 205–214 (1990)
28. S.I.R. Costa, E. Agustini, M. Muniz, R. Palazzo, Slepian-type codes on a flat torus, in *IEEE International Symposium on Information Theory* (2000), p. 58
29. S.I.R. Costa, M. Muniz, E. Agustini, R. Palazzo, Graphs, tessellations, and perfect codes on flat tori. IEEE Trans. Inf. Theory **50**(10), 2363–2377 (2004)
30. S.I.R. Costa, J.E. Strapasson, M.M.S. Alves, T.B. Carlos, Circulant graphs and tesselations on flat tori. Linear Algebra Appl. **432**, 369–382 (2010)
31. S.I.R. Costa, C. Torezzan, A. Campello, V.A. Vaishampayan, Flat tori, lattices and spherical codes, in *2013 Information Theory and Applications Workshop (ITA)*, (2013), pp. 1–8
32. S.I.R. Costa, A. Campello, G.C. Jorge, J.E. Strapasson, C. Qureshi, Codes and lattices in the lp metric, in *2014 Information Theory and Applications Workshop (ITA)* (2014), pp. 1–4
33. W. Ebeling, *Lattices and Codes* (Springer, Berlin, 2013)
34. M. Effros, S. El Rouayheb, M. Langberg, An equivalence between network coding and index coding. IEEE Trans. Inf. Theory **61**(5), 2478–2487 (2015)
35. A.A. El Gamal, L.A. Hemachandra, I. Shperling, V.K. Wei, Using simulated anneling to design good codes. IEEE Trans. Inf. Theory **IT-33**(1), 116–123 (1987)
36. S. El Rouayheb, A. Sprintson, C. Georghiades, On the index coding problem and its relation to network coding and matroid theory. IEEE Trans. Inf. Theory **56**(7), 3187–3195 (2010)
37. T. Ericson, V. Zinoviev, *Codes on Euclidean Spheres*. (North-Holland Mathematical Library, Amsterdam, 2001)
38. T. Etzion, A. Vardy, E. Yaakobi, Coding for the Lee and Manhattan metrics with weighing matrices. IEEE Trans. Inf. Theory **59**(10), 6712–6723 (2013)
39. C. Feng, D. Silva, F.R. Kschischang, An algebraic approach to physical-layer network coding. IEEE Trans. Inf. Theory **59**(11), 7576–7596 (2013)
40. G.D. Forney Jr., Coset codes. I. Introduction and geometrical classification. IEEE Trans. Inf. Theory **34**(5), 1123–1151 (1988)
41. G.D. Forney, Multidimensional constellations. ii. voronoi constellations. IEEE J. Sel. Areas Commun. **7**(6), 941–958 (1989)
42. G.D. Forney Jr., Geometrically uniform codes. IEEE Trans. Inf. Theory **37**(5), 1241–1260 (1991)
43. F.R. Gantmacher, *The Theory of Matrices*, vol. 1 (Translated from the Russian by K. A. Hirsch. Reprint of the 1959 translation). (AMS Chelsea Publishing, Providence, 1998)
44. T.J. Goblick, Theoretical limitations on the transmission of data from analog sources. IEEE Trans. Inf. Theory **11**(4), 558–567 (1965)

45. S. Golomb, A general formulation of error matrices (corresp.). IEEE Trans. Inf. Theory **15**(3), 425–426 (1969)
46. S.W. Golomb, L.R. Welch, Perfect codes in the Lee metric and the packing of polyominoes. SIAM J. Appl. Math. **18**, 302–317 (1970)
47. J. Hamkins, K. Zeger, Asymptotically dense spherical codes. I. Wrapped spherical codes. IEEE Trans. Inf. Theory **43**(6), 1774–1785 (1997)
48. J. Hamkins, K. Zeger, Asymptotically dense spherical codes II. Laminated spherical codes. IEEE Trans. Inf. Theory **43**(6), 1786–1798 (1997)
49. B. Hassibi, H. Vikalo, On the sphere-decoding algorithm I. Expected complexity. IEEE Trans. Signal Process. **53**(8), 2806–2818 (2005)
50. P. Horak, O. Grosek, A new approach towards the Golomb–Welch conjecture. Eur. J. Comb. **38**, 12–22 (2014)
51. Y.C. Huang, Lattice index codes from algebraic number fields. IEEE Trans. Inf. Theory **63**(4), 2098–2112 (2017)
52. Y.C. Huang, K.R. Narayanan, Multistage compute-and-forward with multilevel lattice codes based on product constructions, in *IEEE International Symposium on Information Theory* (2014), pp. 2112–2116
53. W.C. Huffman, V. Pless, *Fundamentals of Error-Correcting Codes* (Cambridge University Press, Cambridge, 2010)
54. I. Ingemarsson, Group Codes for the Gaussian Channel, in *Topics in Coding Theory*. Lecture Notes in Control and Information Sciences, vol.128 (Springer, Berlin, 1989), pp. 73–108
55. S.A. Jafar, Topological interference management through index coding. IEEE Trans. Inf. Theory **60**(1), 529–568 (2014)
56. G.C. Jorge, Reticulados *q-ários e algébricos (in Portuguese)*, PhD thesis, University of Campinas, 2012
57. G.C. Jorge, A. Campello, S.I.R. Costa, q-ary lattices in the l_p norm and a generalization of the Lee metric, in *Proceedings of The International Workshop on Coding and Cryptography (WCC)* (2013), pp. 15–19
58. G.C. Jorge, A.A. de Andrade, S.I.R. Costa, J.E. Strapasson, Algebraic constructions of densest lattices. J. Algebra **429**, 218–235 (2015)
59. W. Kositwattanarerk, S.S. Ong, F. Oggier, Construction a of lattices over number fields and block fading (wiretap) coding. IEEE Trans. Inf. Theory **61**(5), 2273–2282 (2015)
60. C.C. Lavor, M.M.S. Alves, R.M. Siqueira, S.I.R. Costa, *Uma introdução à teoria de códigos*. Notas em Matemática Aplicada, vol. 21, (Sociedade Brasileira de Matemática Aplicada e Computacional (SBMAC), 2006)
61. C. Lee, Some properties of nonbinary error-correcting codes. IRE Trans. Inf. Theory **4**(2), 77–82 (1958)
62. S. Leung-Yan-Cheong, M. Hellman, Concerning a bound on undetected error probability (corresp.). IEEE Trans. Inf. Theory **22**(2), 235–237 (1976)
63. C. Ling, L. Luzzi, J.-C. Belfiore, Lattice codes with strong secrecy over the mod-λ gaussian channel, in *IEEE International Symposium on Information Theory* (2012), pp. 2306–2310
64. H.-A. Loeliger, Signal sets matched to groups. IEEE Trans. Inf. Theory **37**(6), 1675–1682 (1991)
65. J. Lu, J. Harshan, F.E. Oggier, Performance of lattice coset codes on a USRP testbed. CoRR, abs/1607.07163 (2016)
66. F.J. MacWilliams, N.J.A. Sloane, *The Theory of Error-Correcting Codes* (North-Holland, Amsterdam, 1955)
67. H. Maleki, V.R. Cadambe, S.A. Jafar, Index coding – an interference alignment perspective. IEEE Trans. Inf. Theory **60**(9), 5402–5432 (2014)
68. J. Martinet, *Perfect Lattices in Euclidean Spaces* (Springer, Berlin, 2013)
69. A. Mazumdar, On a duality between recoverable distributed storage and index coding, in *IEEE International Symposium on Information Theory* (2014), pp. 1977–1981
70. C.D. Meyer, *Matrix Analysis and Applied Linear Algebra* (Society for Industrial Mathematics (SIAM), Philadelphia, 2000)

71. D. Micciancio, Generalized compact knapsacks, cyclic lattices, and efficient one-way functions. Comput. Complex. **16**, 365–411 (2007)
72. D. Micciancio, S. Goldwasser, *Complexity of Lattice Problems*. The Kluwer International Series in Engineering and Computer Science, vol. 671 (Kluwer Academic Publishers, Boston, MA, 2002). A cryptographic perspective
73. D. Micciancio, O. Regev, *Lattice-Based Cryptography*. Post-Quantum Cryptography (Springer, Berlin, 2009)
74. L. Natarajan, Y. Hong, E. Viterbo, Index codes for the Gaussian broadcast channel using quadrature amplitude modulation. IEEE Commun. Lett. **19**(8), 1291–1294 (2015)
75. L. Natarajan, Y. Hong, E. Viterbo, Lattice index coding. IEEE Trans. Inf. Theory **61**(12), 6505–6525 (2015)
76. B. Nazer, M. Gastpar, Compute-and-forward: harnessing interference through structured codes. IEEE Trans. Inf. Theory **57**(10), 6463–6486 (2011)
77. G. Nebe, E.M. Rains, N.J.A. Sloane, A simple construction for the barnes-wall lattices, in *Codes, Graphs, and Systems* (Springer, Berlin, 2002), pp. 333–342
78. M.J. Neely, A.S. Tehrani, Z. Zhang, Dynamic index coding for wireless broadcast networks. IEEE Trans. Inf. Theory **59**(11), 7525–7540 (2013)
79. F. Oggier, E. Viterbo, Algebraic number theory and code design for rayleigh fading channels. Found. Trends Commun. Inf. Theory **1**(3), 333–415 (2004)
80. F. Oggier, P. Solé, J.C. Belfiore, Lattice codes for the wiretap gaussian channel: construction and analysis. IEEE Trans. Inf. Theory **62**(10), 5690–5708 (2016)
81. L.H. Ozarow, A.D. Wyner, Wire-tap channel II. AT&T Bell Lab. Tech. J. **63**(10), 2135–2157 (1984)
82. C. Peikert, Limits on the hardness of lattice problems in l_p norms, in *IEEE 27th Conference on Computational Complexity* (2007), pp. 333–346
83. C. Peikert, A decade of lattice cryptography. Found. Trends® Theor. Comput. Sci. **10**(4), 283–424 (2016)
84. W.W. Peterson, J.B. Nation, M.P. Fossorier, Reflection group codes and their decoding. IEEE Trans. Inf. Theory **56**(12), 6273–6293 (2010)
85. C. Qureshi, S.I.R Costa, On perfect q-ary codes in the maximum metric, in *2014 Information Theory and Applications Workshop (ITA)* (2016), pp. 1–4
86. C.A. Rogers, *Packing and Covering* (Cambridge University Press, Cambridge, 1964)
87. K.H. Rosen, *Elementary Number Theory and Its Applications* (Addison-Wesley, Boston, 2005)
88. R.M. Roth, P.H. Siegel, Lee-metric BCH codes and their application to constrained and partial-response channels. IEEE Trans. Inf. Theory **40**(4), 1083–1096 (1994)
89. J.A. Rush, N.J.A. Sloane, An improvement to the Minkowski-Hlawka bound for packing superballs. Mathematika **34**, 8–18 (1987)
90. A. Schurmann, F. Vallentin, Computational approaches to lattice packing and covering problems. Discret. Comput. Geom. **35**(1), 73–116 (2006)
91. C.E. Shannon, Communication in the presence of noise. Proc. IRE **37**(1), 10–21 (1949)
92. K. Shanmugam, A.G. Dimakis, Bounding multiple unicasts through index coding and locally repairable codes, in *IEEE International Symposium on Information Theory* (2014), pp. 296–300
93. K. Shanmugam, A.G. Dimakis, M. Langberg, Graph theory versus minimum rank for index coding, in *IEEE International Symposium on Information Theory* (2014), pp. 291–295
94. M.Z. Shieh, S.C. Tsai, Decoding frequency permutation arrays under chebyshev distance. IEEE Trans. Inf. Theory **56**(11), 5730–5737 (2010)
95. P.W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput. **26**(5), 1484–1509 (1997)
96. R.M. Siqueira, S.I.R. Costa, Flat tori, lattices and bounds for commutative group codes. Des. Codes Crypt. **49**(1–3), 307–321 (2008)
97. D. Slepian, Group codes for the gaussian channel. Bell Syst. Tech. J. **47**, 575–602 (1968)
98. N.J.A. Sloane, The sphere packing problem. Doc. Math. Extra Volume ICM, 387–396 (1998)

99. N.J.A. Sloane, V.A. Vaishampayan, S.I.R. Costa, A note on projecting the cubic lattice. Discret. Comput. Geom. **46**(3), 472–478 (2011)
100. N.J.A. Sloane, V.A. Vaishampayan, S.I.R. Costa, The lifting construction: a general solution for the fat strut problem, in *IEEE International Symposium on Information Theory* (2010), pp. 1037–1041
101. Y. Song, N. Devroye, Lattice codes for the gaussian relay channel: decode-and-forward and compress-and-forward. IEEE Trans. Inf. Theory **59**(8), 4927–4948 (2013)
102. D. Stehlé, Ideal lattices. Talk given at Berkeley, 07 July 2015, https://simons.berkeley.edu/sites/default/files/docs/3472/stehle.pdf
103. J. Stillwell, *Geometry of Surfaces*. Universitext (Springer, New York, 1992)
104. C. Thapa, L. Ong, S.J. Johnson, Generalized interlinked cycle cover for index coding, in *2015 IEEE Information Theory Workshop - Fall (ITW)* (2015), pp. 4–8
105. C. Torezzan, S.I.R. Costa, V.A. Vaishampayan, Constructive spherical codes on layers of flat tori. IEEE Trans. Inf. Theory **59**(10), 6655–6663 (2013)
106. C. Torezzan, J.E. Strapasson, S.I.R. Costa, R.M. Siqueira, Optimum commutative group codes. Des. Codes Crypt. **74**(2), 379–394 (2015)
107. V.A. Vaishampayan, S.I.R. Costa, Curves on a sphere, shift-map dynamics, and error control for continuous alphabet sources. IEEE Trans. Inf. Theory **49**(7), 1658–1672 (2003)
108. V.A. Vaishampayan, N.J.A. Sloane, S.I.R. Costa, Dynamical systems, curves and coding for continuous alphabet sources, in *Proceedings of International Telecommunications Symposium*, ITW2002, Bangalore (2002)
109. E. Viterbo, J. Boutros, A universal lattice code decoder for fading channels. IEEE Trans. Inf. Theory **45**(5), 1639–1662 (1999)
110. A. Zaghloul, R.M. Taylor Jr., L. Mili, Structured spherical codes with optimal distance distributions, in *IEEE International Symposium on Information Theory* (2017)
111. R. Zamir, Lattices are everywhere, in IEEE Xplore (ed.), *Information Theory and Applications Workshop* (2009), pp. 392–421
112. R. Zamir, *Lattice Coding for Signals and Networks: A Structured Coding Approach to Quantization, Modulation, and Multiuser Information Theory* (Cambridge University Press, Cambridge, 2014)

Index

S.I.R. Costa et al., *Lattices Applied to Coding for Reliable and Secure Communications*, SpringerBriefs in Mathematics,
https://doi.org/10.1007/978-3-319-67882-5