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.