UNIVERSIDADE ESTADUAL DE CAMPINAS
Faculdade de Engenharia Elétrica e de Computação

HENRIQUE BUGLIA

VORONOI CONSTELLATIONS

CONSTELAÇÕES DE VORONOI

CAMPINAS
2020

HENRIQUE BUGLIA

VORONOI CONSTELLATIONS

CONSTELAÇÕES DE VORONOI

Dissertation presented to the Faculty of Electrical and Computer Engineering of the University of Campinas in partial fulfillment of the requirements for the Master degree in Electrical Engineering, in the area of Telecommunications and Telematics.

Dissertação apresentada à Faculdade de Engenharia Elétrica e de Computação da Universidade Estadual de Campinas como parte dos requisitos exigidos para obtenção do título de Mestre em Engenharia Elétrica, na Área de Telecomunicações e Telemática.

Supervisor/Orientador: Prof. Dr. Renato da Rocha Lopes

ESTE EXEMPLAR CORRESPONDE À VERSÃO FINAL DA DISSERTAÇÃO DEFENDIDA PELO ALUNO HENRIQUE BUGLIA, E ORIENTADA PELO PROF. DR. RENATO DA ROCHA LOPES

CAMPINAS
2020

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca da Área de Engenharia e Arquitetura
Rose Meire da Silva - CRB 8/5974

B865c

Buglia, Henrique, 1995-
Voronoi Constellations / Henrique Buglia. - Campinas, SP : [s.n.], 2020.

Orientador: Renato da Rocha Lopes.
Dissertação (mestrado) - Universidade Estadual de Campinas, Faculdade de Engenharia Elétrica e de Computação.

1. Comunicações Digitais. 2. Codificação. 3. Complexidade computacional. 4. Reticulados algébricos. 5. Voronoi, diagramas de. I. Lopes, Renato da Rocha, 1972-. II. Universidade Estadual de Campinas. Faculdade de Engenharia Elétrica e de Computação. III. Título.

Informações para Biblioteca Digital

Título em outro idioma: Constelações de Voronoi
Palavras-chave em inglês:
Digital Communications
Coding
Computational Complexity
Algebraic Lattices
Voronoi diagram
Área de concentração: Telecomunicações e Telemática
Titulação: Mestre em Engenharia Elétrica
Banca Examinadora:
Renato da Rocha Lopes [Orientador]
Danilo Silva
Darli Augusto de Arruda Mello
Data da defesa: 18-12-2020
Programa de Pós-Graduação: Engenharia Elétrica

Identificação e informações acadêmicas do(a) aluno(a)
- ORCID do autor: https://orcid.org/0000-0003-1634-0926
- Currículo Lattes do autor: http://lattes.cnpq.br/6852761519419406

COMISSÃO JULGADORA - DISSERTAÇÃO DE MESTRADO

Candidato: Henrique Buglia. RA 157981
Data da defesa: 18 de dezembro de 2020

Título da tese: Voronoi Constellations
Título em outro idioma: Constelações de Voronoi

Prof. Dr. Renato da Rocha Lopes (Presidente, FEEC/UNICAMP)
Prof. Dr. Danilo Silva (UFSC)
Prof. Dr. Darli Augusto de Arruda Mello (FEEC/UNICAMP)

A ata de defesa, com as respectivas assinaturas dos membros da Comissão Julgadora, encontra-se no SIGA (Sistema de Fluxo de Dissertação/Tese) e na Secretaria de Pós Graduação da Faculdade de Engenharia Elétrica e de Computação.

Acknowledgements

To Prof. Dr. Renato da Rocha Lopes for the guidance.

This study was financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Finance Code 001

Abstract

In this thesis, we deal with with lattices in communications. In a digital transmission, we can represent the information to be sent as points in space, as such, lattices are a natural tool which can be used into the framework of digital communication. Throughout this thesis, we analyse in detail these relations, dealing, more specifically, with channel coding.

We analyse how to construct Voronoi constellations, and how to achieve channel capacity using lattices. We show how the mathematical definitions are related to some figures of merit of digital communications. We also go deeply in the encoding and indexing procedures for lattice codes showing an alternative way to do it, aimed to achieve reduced encoding complexity.

The novelty of this thesis relies on the proposal of a Voronoi shaping method for integer shaping and coding lattices - as well as, multilevel code constructions - satisfying the chain $\Lambda_s \subseteq \mathbf{K}\mathbb{Z}^n \subseteq \Lambda_c$, with $\mathbf{K}$ as an integer diagonal matrix. As we will see, this assumption is easily satisfied for lattices obtained from error-correcting codes, and for multilevel code constructions. For these constructions, using this strategy, the encoding complexity is reduced to the underlying linear code encoding complexity, as opposed to that, found in the literature so far.

To show the potential complexity and performance gains of our method, we illustrate it in constructions by the code formula, with Gosset (E_8) and Leech (Λ_{24}) lattices as shaping lattices.

Keywords: Encoding, Complexity, Voronoi Shaping, Voronoi constellations, Lattices, Construction D, Construction by the Code Formula, Leech Lattice, E_8.

Resumo

Nesta tese, nós lidamos com reticulados aplicados em comunicações. Em uma comunicação digital, nos podemos representar a informação a ser transmitida como pontos no espaço, sendo assim, reticulados aparecem como uma ferramenta natural no contexto de comunicações digitais. Através desta tese, nos analisamos em detalhes estas relações, lidando mais especificamente com Codificação de Canal.

Nós analisamos em detalhes como construir constelações de Voronoi e como atingir a capacidade do canal utilizando reticulados. Nos mostramos como as definições matemáticas estão relacionadas com algumas figuras de mérito no contexto de comunicações digitais. Nós também analisamos a fundo os procedimentos de "encoding" e "indexing" para reticulados obtidos por códigos, mostrando um jeito alternativo de fazê-lo, obtendo complexidade reduzida.

A novidade desta tese, esta relacionada com uma nova proposta de realizar Shaping de Voronoi, em reticulados inteiros - assim como em construções de códigos multiníveis - que satisfazem a condição $\Lambda_s \subseteq \mathbf{K}\mathbb{Z}^n \subseteq \Lambda_c$, com $\mathbf{K}$ uma matriz diagonal inteira. Como veremos, esta condição é facilmente satisfeita para reticulados obtidos por códigos corretores de erro e para construções de códigos multiníveis. Para estas construções, usando esta estratégia, a complexidade da operação de encoding é reduzida para a complexidade do encoding do código linear utilizado para construir o reticulado de coding, oposto ao que é encontrado na literatura até agora.

Para mostrar a relevância dos ganhos de performance e complexidade, usando o método proposto, nós o ilustramos em construções obtidas pela code formula, em conjunto com os reticulados Gosset (E_8) e Leech (Λ_{24}), como reticulados de shaping.

Palavras-chave: Encoding, Complexidade, Shaping de Voronoi, Constelações de Voronoi, Reticulados, Construção D, Construção pela Code Formula, Reticulado Leech, E_8.

List of Figures

1.1 Source coding followed by channel coding Zamir [2014] 12
1.2 Source coding followed by channel coding Zamir [2014] 12

2.1 Hexagonal Lattice, also known as A_2 and two fundamental regions. 17
2.2 A construction-A lattice Λ_{A_2} obtained by a linear code in $\mathbb{Z}_5^2$ (black points). 22
2.3 Bit-error probability versus E_b/N_0 for uncoded 2-PAM, and symbol-error probability versus SNR_{norm} for uncoded M-PAM (M large) Forney and Ungerboeck [1998]. . . 28
2.4 Capacity of the ideal AWGN channel with Gaussian inputs and with equiprobable M-PAM inputs. 29
2.5 Two different shaping regions $\mathbb{S}$ for the $\mathbb{Z}^2$ coding lattice Barry et al. [2012]. 32
2.6 Shaping gains of N-spheres over N-cubes Forney and Ungerboeck [1998]. 33
2.7 Shaping gains of Voronoi regions of some lattices Forney and Wei [1989]. 33
2.8 Two different coding lattices for the same shaping region $\mathbb{S}$ Barry et al. [2012]. . . . 34

4.1 SER and WER performance of 2-level extended BCH code lattices with dimension n = 128 over AWGN channel without power constraint. 54
4.2 WER performance of 2-level extended BCH code lattices with dimension n = 128 over AWGN channel constrained by cubic lattice and E_8 lattice. 59
4.3 Symbol marginal distribution of cubic lattice shaping. 60
4.4 Symbol marginal distribution of E_8 lattice shaping. 60
4.5 Achievable rates (AR) for Construction-D lattices obtained from SC-LDPC codes over the AWGN channel, with different number of levels and shaping regions. 61

Summary

List of Figures **8**

1 Introduction **11**
1.1 Lattices in Communication 11
1.2 Channel Capacity with Lattices 13
1.3 Thesis Organization 14

2 Lattices over the AWGN Channel **16**
2.1 Lattice Definitions 17
2.1.1 Lattice Parameters 17
2.1.2 Lattice Cosets and Voronoi Shaping 19
2.2 Lattices from Codes 21
2.3 Modulation and Coding for AWGN Channel 27
2.4 Voronoi Lattices Codes 31

3 Lattice Encoding and Indexing **36**
3.1 Preliminaries 36
3.2 Rectangular Encoding 38
3.2.1 Encoding and Indexing Triangular Matrices 39
3.2.2 Encoding the chain $\Lambda_s \subseteq \mathbf{K}\mathbb{Z}^n \subseteq \Lambda_c$. 42
3.3 Encoding and Indexing for Lattices from Error Correcting Codes 44
3.4 Complexity 48

4 Construction and Implementation **49**
4.1 Shaping Lattice Design 49
4.1.1 Gosset Lattice (E_8) 51
4.1.2 Leech Lattice (Λ_{24}) 51
4.2 Coding Lattice Design 52

4.2.1 Extended BCH Codes Lattices 52
4.2.2 SC-LDPC Code Lattices 55
4.3 Quantization: Sphere Decoder Algorithm 56
4.4 Simulation Results 57
4.4.1 Gosset Constellations of Extended BCH Lattice Codes 57
4.4.2 Leech Constellations of SC-LDPC Lattice Codes 60

5 Conclusions **62**

References **64**

Chapter 1

Introduction

This thesis will be dealing with communications over the *additive white Gaussian noise (AWGN) channel* using lattices. A lattice is a periodic arrangement of points in the n-dimensional Euclidean space, which efficiently fits in framework of digital communication because this is how an information is generally represented. As we will see, lattices can be used in many steps of a transmission system, but in this thesis, our focus is in one of these steps: our goal is to construct *channel capacity-achieving signal constellations* using lattices. In this thesis, we propose a practical and general method to achieve this - and therefore to achieve channel capacity - which may have linear complexity in the lattice dimension.

In section 1.1 we describe how exactly lattices fits in the framework of transmitting a signal over the AWGN channel. A brief discussion of the requirements to achieve channel capacity with lattices is discussed in section 1.2. To conclude this chapter, section 1.3 describes the thesis organization.

1.1 Lattices in Communication

Lattices are a natural tool in the framework of digital communication since we can represent the information to be sent as points in Euclidean space. The description of points using lattices relies in the fundamentals of discrete algebra which open-up a vast field of new possibilities, since associating a well-known and structured field of mathematics in a specific problem, makes it possible to use all its tools to expand, improve and create new solutions to the problem addressed. In this sense, lattices provide an efficient way to describe, manipulate and select those points, in such a way that this choice can achieve the Gaussian channel capacity.

Consider the general block diagram of an information system, as illustrated in figure 1.1. We can divide it in two parts, the transmitter and the receiver. As we can represent the information in every step using lattices, it can naturally describe both the transmitter and the receiver. In the

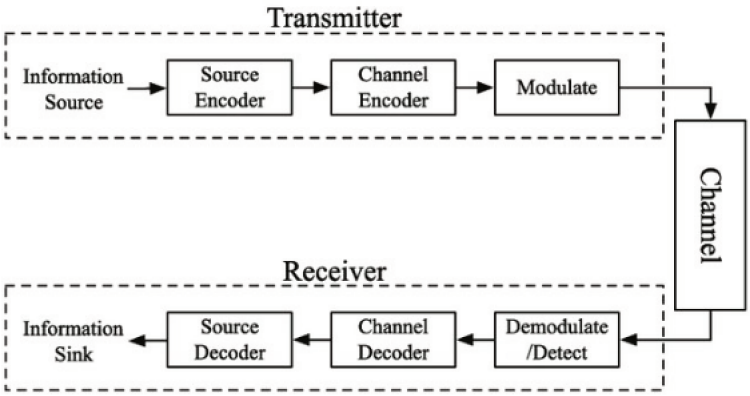


Figure 1.1: Source coding followed by channel coding Zamir [2014]

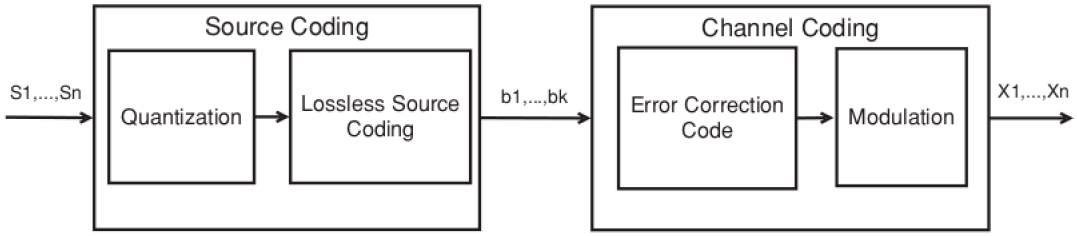


Figure 1.2: Source coding followed by channel coding Zamir [2014]

following we will show how lattices are used in the transmitter part, i.e, the source encoder and channel encoder/modulator, which is represented in figure 1.2 as source coding and channel coding, respectively. The receiver part is analogous to the transmitter and we let it to be understood throughout the remaining chapters.

To understand how exactly lattices fit in the problem of digital communication transmission of an information source over a noisy channel as illustrated in Figure 1.2. The transmission is divided in two stages Zamir [2014]: source coding, where the source samples is mapped into bits, and channel coding, where the digital representation of the source is mapped into a channel input signal.

For source coding, the goal is to compress the signal. Consider n samples of information, represented by the vector $\mathbf{s} = (s_1, .., s_i, ..., s_n)$. Suppose we have k-bits to represent $\mathbf{s}$, thus, the vector $\mathbf{s}$ is mapped in one of 2^k possible values giving rise to a new vector $\hat{\mathbf{s}}$. All the 2^k possible vectors $\hat{\mathbf{s}}$ is a *lattice quantizer codebook*. Note that, in this sense, quantization amounts to find the closest point of the lattice quantizer codebook $\hat{\mathbf{s}}$ to $\mathbf{s}$. After quantization, each vector $\hat{\mathbf{s}}$ with length n is compressed into vectors $\mathbf{b}$ of length $k = k(\mathbf{s})$, where $k < n$ for vectors with high frequency of appearance. Here,

lattices arise in the operation that maps **s** to a k-bits codeword.

For channel coding, the goal is to add redundancy in order to recover the transmitted signal in reception after channel noise is added. In this case, transmission amounts to map k bits of information of **b** into n bits, where $n > k$, which is done by an error-correction code. After that, the vector of length n is mapped into the vector **x**, which will be the transmitted vector, in a step called $modulation$. This last step is necessary to satisfy the system power constraint. Here, lattices arise, because, the overall channel coding step maps k-bits into a point in $\mathbb{R}^n$. The set of all 2^k possible input vectors **x** is called a *lattice constellation*.

As mentioned in Zamir [2014], one of the greatest advantage in using lattices is that, for source coding, quantization and coding (and for channel coding, coding and modulation), are combined as a single entity: a lattice code directly maps digital information into a vector in $\mathbb{R}^n$ and vice versa. As we will see, this is possible, because we can construct lattices using error-correcting codes and vise versa.

1.2 Channel Capacity with Lattices

In this section we describe the requirements for achieving channel capacity using lattice codes. Theoretical results that prove that lattices achieve capacity can be seen in Poltyrev [1994], Erez and Zamir [2004], Ordentlich and Erez [2016], which show that for a high-SNR band-limited AWGN channel a capacity-achieving constellation consists of a dense packing of high dimensional signal points that lie inside a hyper-sphere Forney and Ungerboeck [1998]. The fact that lattices provide a structured way to find such dense packing is due to the fact that the set of lattice points naturally forms a packing in the n-dimensional Euclidean space.

Due to that, a transmission using lattice codes is divided in two main steps: firstly, to find a high-dimensional lattice with a dense packing of points in an n-dimensional space. This is known as the *coding lattice*. Secondly, to find a method to select only the points of the coding lattice inside a specific region of the n-space, which optimally, should approximate to a hyper-sphere. This operation is called *shaping*, and ensures that the power constraints are satisfied, such that a finite number of points can be transmitted. As we will see, a lattice is a infinite set of points, thus, the shaping operation is essential to constrain the lattice, so that just a finite set of points can be transmitted over the channel.

For the first step, many authors have proposed good lattice designs, based on error-correcting codes, which consist in translating to the Euclidean space the techniques used for designing effective iteratively decodable error-correcting codes over finite fields Di Pietro and Boutros [2017]. Codes like turbo codes, low-density parity-check (LDPC) codes, polar codes and Bose-Chaudhuri-

Hocquenghem (BCH) codes, were recently proposed to construct lattice codes that have the potential to achieve the maximum coding gain when dimension grows to infinity Matsumine et al. [2018], Sakzad et al. [2011], Yan and Ling [2012], da Silva and Silva [2018].

In contrast to coding, shaping is less exploited in the literature. Usually, the power constraint satisfied using a hypercube for shaping, which can be implemented with very low complexity, but at the expense of the good gains provided by a good shaping.

In Voronoi shaping Zamir [2014], Kurkoski [2018], only points of the coding lattice inside the Voronoi region of a shaping lattice are transmitted. These points are known as coset leaders of the quotient group of the coding lattice modulo the shaping lattice. Traditionally, even for lattices obtained from error-correcting codes, Voronoi shaping requires the construction of the lattice generator matrix $\mathbf{G}$ Kurkoski [2018], a high-complexity matrix-vector product, a strategy to guarantee a bijection between the message vectors and the coset leadersKurkoski [2018], and a final quantization step.

To decrease complexity, the authors of Khodaiemehr et al. [2016] exploit the structure of Construction-A lattices obtained from quasi-cyclic low-density parity-check (QC-LDPC) codes, resulting in a matrix $\mathbf{G}$ that enables a linear-complexity computation of the product. An efficient Voronoi shaping scheme was also proposed in Di Pietro and Boutros [2017] for any Construction-A coding lattice, where the matrix-vector product is replaced by much simpler encoding operations on the underlying error-correcting code.

In this thesis we generalize the method proposed in Di Pietro and Boutros [2017] to a broad class of lattices that includes the Construction D. To that end, we will show that, for this class of lattices, the bijection in Kurkoski [2018] can be achieved from a simple mapping of the message vector, without a matrix-vector multiplication. Evidently, this greatly reduces the complexity of the system.

Our proposal is illustrated for the Construction-D coding lattices obtained from Bose-Chaudhuri-Hocquenghem (BCH) codes Matsumine et al. [2018] and spatially-coupled LDPC (SC-LDPC) codes Vem et al. [2014]. In these examples, shaping is performed by the Gosset lattice E_8 and the Leech lattice Λ_{24}, respectively, which are well-known for providing good gains despite their small dimensions Conway and Sloane [2013]. Additionally, their small dimension enables the use of algorithms with feasible computational complexity.

1.3 Thesis Organization

The remaining chapters are organized as follow:

- **Chapter 2**: In this chapter we present general lattice definitions, lattices obtained from error-correcting codes, and figures of merit for lattices when applied to AWGN channel. We also

highlight the requirements to achieve the AWGN channel capacity.

- **Chapter 3**: In this chapter we describe a way to obtain Voronoi constellations by performing shaping operation using two nested lattices - the shaping lattice, Λ_s, and the coding lattice, Λ_c. The encoding and indexing of these lattice codes are also described. Special attention is given when the coding lattice is obtained from error correcting codes, and when these lattices satisfy the chain $\Lambda_s \subseteq \mathbf{K}\mathbb{Z}^n \subseteq \Lambda_c \subseteq \mathbb{Z}^n$.

- **Chapter 4**: This chapter uses the theoretical results from previous sections to construct the coding lattice based on extended BCH codes and spatially-coupled LDPC codes. Additionally, the shaping lattice is constructed based on scaled copies of the Gosset (E_8) and the Leech (Λ_{24}) lattices.

- **Chapter 5**: This chapter concludes this work, with our achievements and general conclusions.

Chapter 2

Lattices over the AWGN Channel

This chapter starts presenting some general lattice definitions which we will be using along this entire thesis. In the second part we will describe some figures of merit to measure the performance of a communication system over the AWGN channel. As we will see, these figures of merit can be described using lattice definitions, which will be presented in this chapter. Using these definitions, we will be able to measure the performance of a lattice, and its goodness in achieving the AWGN channel capacity. The last part of this chapter describes how we can obtain lattices from error-correcting codes and how the code choice, as well as the code parameters change the lattice performance. We give special attention to construction D, construction by the code formula and construction A, which are standard lattice constructions obtained from error-correcting codes. The motivation of constructing lattices from error-correcting codes relies in the fact that, as mentioned in chapter 1, we will be interested in map k-bits of information to a point in the n-dimensional euclidean space and error-correcting codes naturally provides this change of dimension as it is constructed over a finite field. Note that, an error-correcting code can be seen as a linear map $\mathbb{F}_q^k \to \mathbb{F}_q^n$. So basically, lattices are a structured way to embed a linear code over a finite field into the n-dimensional euclidean space.

This chapter is divided in four sections. In section 2.1 we present mathematical lattice definitions. Section 2.2 describes how to obtain lattices from error correct codes focused in the two constructions mentioned above. Section 2.3 describes figures of merit for lattices when applied to AWGN channel, as well as the power-limited regime and the bandwidth-limited regime. This chapter ends with section 2.4, which defines further figures of merit for lattices, and present the definitions of Voronoi constellations, and how to construct them to achieve the AWGN capacity.

2.1 Lattice Definitions

2.1.1 Lattice Parameters

A lattice Λ is a discrete additive subgroup of $\mathbb{R}^n$. Mathematically, a lattice Λ can be defined as the set of all $\mathbf{x}$, satisfying

$$\Lambda = \{\mathbf{x} = \mathbf{G} \cdot \mathbf{b}, \mathbf{b} \in \mathbb{Z}^n\}. \tag{2.1}$$

The $n \times n$ matrix $\mathbf{G} = [\mathbf{g}_1\ \mathbf{g}_2\ ...\ \mathbf{g}_n]$ is a lattice generator matrix, whose columns, known as lattice generator vectors, are given by $\mathbf{g}_i$. As $\mathbf{b} \in \mathbb{Z}^n$, a lattice is a symmetric set of n-dimensional points in $\mathbb{R}^n$. By symmetry we mean that each point has an equal number of neighbor points at the same distance. Figure 2.1(a) shows the hexagonal lattice, also known as A_2. This is a bi-dimensional lattice, with one possible generator matrix given as:

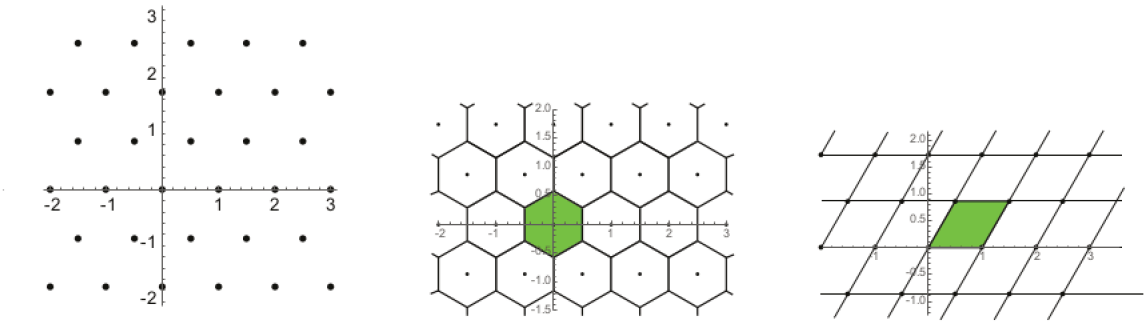
$$\mathbf{G} = \begin{pmatrix} 1 & \frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} \end{pmatrix} \tag{2.2}$$

The matrix $\mathbf{G}$ is not unique: the same lattice can be generated by different generator matrices. In fact, a matrix $\mathbf{G}'$ generates the same lattice as the matrix $\mathbf{G}$, if, and only if:

$$\mathbf{G}' = \mathbf{G}\mathbf{U} \tag{2.3}$$

with $\mathbf{U}$ an unimodular matrix, i.e., $|\det \mathbf{U}| = 1$.

Proof: It is sufficient to apply theorem 2.2 of Costa et al. [2017]. □



(a) A_2 Lattice. (b) A_2 Voronoi Region. (c) A_2 Fundamental Parallelotope.

Figure 2.1: Hexagonal Lattice, also known as A_2 and two fundamental regions.

Given a point $\mathbf{y} \in \mathbb{R}^n$, we may have interest in finding the lattice point $\mathbf{x} \in \Lambda$ closest to $\mathbf{y}$. This is done by the shortest-distance quantization operation $Q_\Lambda(\mathbf{y})$, which finds the closest point of the

lattice Λ to any point $\mathbf{y}$:

$$Q_\Lambda(\mathbf{y}) = \underset{\mathbf{x}\in\Lambda}{\operatorname{argmin}} ||\mathbf{y} - \mathbf{x}||^2. \tag{2.4}$$

For any lattice Λ, we can define a *fundamental region* $\mathcal{P}(\Lambda)$. Given a lattice point $\mathbf{x} \in \Lambda$, a fundamental region satisfies the following properties:

1.
$$\bigcup_{\mathbf{x}\in\Lambda}(\mathbf{x} + \mathcal{P}(\Lambda)) = \mathbb{R}^n, \tag{2.5}$$

2.
$$\forall \mathbf{x}_1, \mathbf{x}_2 \in \Lambda, \mathbf{x}_1 \neq \mathbf{x}_2 \rightarrow (\mathbf{x}_1 + \mathcal{P}(\Lambda))\bigcap(\mathbf{x}_2 + \mathcal{P}(\Lambda)) = \varnothing. \tag{2.6}$$

The first condition stands that the translations of any fundamental region by lattice points cover $\mathbb{R}^n$, i,e, the fundamental region tiles the entire space. This is also called the "Tiling Property". The second stands that there is no intersection between the translated regions.

We focus your attention in two special fundamental regions that can be defined for any lattice: The *Voronoi region* and the *Fundamental Parallelotope* of Λ.

The Voronoi region of the lattice, $\mathcal{V}(\Lambda)$, is the set of points that are closer to the origin than to any other point of the lattice Λ:

$$\mathcal{V}(\Lambda) = \{\mathbf{y} \in \mathbb{R}^n \mid Q_\Lambda(\mathbf{y}) = \mathbf{0}\}. \tag{2.7}$$

This region is shown in green in figure 2.1(b) for the hexagonal lattice. The Voronoi region is unique for each lattice and is a symmetric region over any lattice point.

The Fundamental Parallelotope $\mathcal{P}(\mathbf{G})$ is defined as the parallelotope formed by the lattice generator vectors:

$$\mathcal{P}(\mathbf{G}) = \{s_1\mathbf{g}_1 + \cdots + s_n\mathbf{g}_n, 0 \leq s_i < 1, i = 1, \ldots, n\}. \tag{2.8}$$

This region is shown in green in figure 2.1(c) for the hexagonal lattice generated by the generator matrix in (3.9). Given that a lattice generator matrix $\mathbf{G}$ is not unique, the fundamental parallelotope is also not unique. Note that, both regions are fundamental regions, and satisfy equations (2.5) and (2.6), which is easily seen in figure 2.1.

As discussed, the fundamental region is not unique. Moreover, certain parallelotopes $\mathcal{P}(\mathbf{P})$ described by an n-by-n full rank matrix $\mathbf{P}$ satisfy equations (2.5) and (2.5) and are also fundamental regions of Λ, which as equation (2.8) can be written as,

$$\mathcal{P}(\mathbf{P}) = \{\mathbf{P} \begin{bmatrix} s_1 \\ \vdots \\ s_n \end{bmatrix}, 0 \leq s_i < 1, i = 1, \ldots, n\}. \tag{2.9}$$

Of course, if $\mathbf{P} = \mathbf{G}$, then equation (2.9) turns to be the fundamental parallelotope (equation (2.8)). Finally, letting $\mathcal{P}(\Lambda) = \mathcal{P}(\mathbf{P})$, condition 1 described in equation (2.5), implies that any point $\mathbf{y} \in \mathbb{R}^n$ can be written as,

$$\mathbf{y} = \mathbf{x} + \mathcal{P}(\Lambda) = \mathbf{x} + \mathcal{P}(\mathbf{P}) = \mathbf{Gb} + \mathbf{Ps}, \tag{2.10}$$

while condition 2 described in equation (2.6), implies that (2.10) has unique solution for **b** and **s**.

For any lattice, we define its volume as the volume of any fundamental region:

$$\mathrm{Vol}\,(\Lambda) = \mathrm{Vol}\,\mathcal{P}(\Lambda) = |\det(\mathbf{P})| = |\det(\mathbf{G})| = \mathrm{Vol}\,(\mathcal{V}(\Lambda)), \tag{2.11}$$

where $\det(\mathbf{G})$ is the volume of the fundamental parallelotope formed by the lattice generator vectors, $\det(\mathbf{P})$ is the volume of a fundamental region formed by the parallelotope **P** and $\mathrm{Vol}\,(\mathcal{V}(\Lambda))$ is the Voronoi region volume. As all these regions are fundamental regions, all of them have the same volume, this is an important fact when dealing with lattices: it is sufficient to known a lattice basis **G** to determine the volume of a fundamental region, e.g, the Voronoi region. Although a lattice has infinite different basis, the volume is the same for any choice of **G**. Recalling equation (2.3), this is true because $|\det(\mathbf{G}')| = |\det(\mathbf{GU})| = |\det(\mathbf{G})||\det(\mathbf{U})| = |\det(\mathbf{G})|$. We invite the reader to see fig 2.6 of Zamir [2014] for a geometrical proof of (2.11).

Given two lattices Λ_s and Λ_c, an important condition that we may require is that every point of Λ_s be also a point of Λ_c. If this is true, then Λ_s is a subset of Λ_c, i.e, $\Lambda_s \subseteq \Lambda_c$ and these lattices are called a nested lattice pair. Equivalently, if $\Lambda_s \subseteq \Lambda_c$, the generator matrix of Λ_s can be related to that of Λ_c by an integer matrix **M** according to the relation:

$$\mathbf{G}_s = \mathbf{G}_c \cdot \mathbf{M}. \tag{2.12}$$

Proof: If $\mathbf{x} \in \mathbf{G}_s$, then according to (2.1), $\mathbf{x} = \mathbf{G}_s\mathbf{z}$. If $\Lambda_s \subseteq \Lambda_c$, then $\mathbf{x} = \mathbf{G}_s\mathbf{z} = \mathbf{G}_c\mathbf{Mz}$. As $\mathbf{Mz} = \mathbf{z}' \in \mathbb{Z}^n$, **x** is also a point of Λ_c because $\mathbf{x} = \mathbf{G}_c\mathbf{z}'$. □

2.1.2 Lattice Cosets and Voronoi Shaping

We now turn your attention into some interesting group properties of lattices. In this section we assume $\Lambda_s \subseteq \Lambda_c$. This is because if $\Lambda_s \subseteq \Lambda_c$, than Λ_s can be viewed as a subgroup of Λ_c, allowing

the utilization of some group theory notions in lattices, such as to define a *coset* and a finite *quotient group*.

Given two nested lattices Λ_s and Λ_c, for any $\mathbf{x} \in \Lambda_c$, the set $\mathbf{x} + \Lambda_s$ is a *coset* or a lattice shift of Λ_s by a point of Λ_c. The vector $\mathbf{x}$ is called *coset representative*. Each coset $\mathbf{x} + \Lambda_s$ belongs to Λ_c (the proof is direct from the nested condition). We say that $\mathbf{x} + \Lambda_s$ is the coset of Λ_s in Λ_c containing $\mathbf{x}$.

Note that two elements $\mathbf{x}_1$ and $\mathbf{x}_2 \in \Lambda_c$, can generate the same coset. Because of that, a natural question which we will be interested in answering is: how many are the numbers of different cosets?

Since a sublattice $\Lambda_s \subseteq \Lambda_c$ is a subgroup, we can define the finite quotient group Λ_c/Λ_s as the set of all coset, i.e.,

$$\frac{\Lambda_c}{\Lambda_s} = \{\mathbf{x} + \Lambda_s \mid \mathbf{x} \in \Lambda_c\}. \tag{2.13}$$

Similarly, if we consider a nested *lattice chain*, i.e, $\Lambda_s \subseteq \Lambda_{r-1} \subseteq \cdots \subseteq \Lambda_1 \subseteq \Lambda_c$ and the sets $A_1, \ldots, A_r$ as the set of coset representatives of the quotients $\Lambda_c/\Lambda_1, \ldots, \Lambda_{r-1}/\Lambda_s$, respectively. Then, a set of coset representatives of Λ_c/Λ_s is given by Forney et al. [2000]:

$$A = A_1 + \cdots + A_r. \tag{2.14}$$

Equivalently, (2.13), can be rewritten as

$$\begin{aligned} \frac{\Lambda_c}{\Lambda_s} &= \{\mathbf{a} + \Lambda_s \mid \mathbf{a} \in A\} \\ &= \{\mathbf{a}_1 + \cdots + \mathbf{a}_r + \Lambda_s \mid \mathbf{a}_i \in A_i\}. \end{aligned} \tag{2.15}$$

The number of distinct cosets M is the quotient group cardinally:

$$M = \left|\frac{\Lambda_c}{\Lambda_s}\right| = \frac{\mathrm{Vol}(\Lambda_s)}{\mathrm{Vol}(\Lambda_c)} = |\det(\mathbf{M})|. \tag{2.16}$$

By relating the volumes of Λ_s and Λ_c, equation (2.16) suggests that the number of distinct cosets are the number of points of Λ_c inside a fundamental region of Λ_s. This is in fact true, and is valid for any fundamental region of Λ_s. More than that, each point of Λ_c inside any fundamental region of Λ_s is a coset representative of a distinct coset. So, all the possible cosets can be represented by the elements inside any fundamental region of Λ_s. In the special case where the fundamental region of Λ_s is the Voronoi region, the coset representative is also called a *coset leader*. Let $\mathcal{P}(\Lambda_s)$ be any fundamental region of Λ_s. We can then, state:

$$\Lambda_c \cap \mathcal{P}(\Lambda_s) \text{ is a complete set of coset representatives,} \tag{2.17}$$

and

$$\Lambda_c \cap \mathcal{V}(\Lambda_s) \text{ is a complete set of coset leaders.} \tag{2.18}$$

The rightmost equality of the equation (2.16) is direct from (2.11) and (2.12). Of course, the complete proof of (2.16) and (2.17) is not trivial, and is omitted from this thesis. A theoretical proof based on geometrical arguments of these statements, using lattice partition notions is given by Zamir [2014] in section 8.2.

Suppose a point $\mathbf{x} \in \Lambda_c$. Suppose that this point is inside a fundamental region $\mathcal{P}(\Lambda_s)$. We can bring this point to the Voronoi region of Λ_s. Equivalently, we can find the coset leader $\mathbf{x}$' of a coset $\mathbf{x} + \Lambda_s$ by performing the modulo-Λ_s operation:

$$\mathbf{x}' = \mathbf{x} - Q_{\Lambda_s}(\mathbf{x}), \tag{2.19}$$

or equivalently,

$$\mathbf{x}' = \mathbf{G} \cdot \mathbf{b} - Q_{\Lambda_s}(\mathbf{G} \cdot \mathbf{b}). \tag{2.20}$$

In consequence, $\mathbf{x}' \in \Lambda_c \cap \mathcal{V}(\Lambda_s)$. Note that, this is the same as finding the element of the coset $\mathbf{x} + \Lambda_s$ with minimum Euclidean norm, because each different point of a coset is mapped in the same unique point of the set $\Lambda_c \cap \mathcal{V}(\Lambda_s)$. The mapping shown in equation (2.20) is also known as *Voronoi Shaping*. Note that, $\mathbf{b}$ is an integer vector, and as we have seen, there are many values of $\mathbf{b}$ which map to $\mathbf{x}$'. In chapter 3, we will be interested in limiting the range of $\mathbf{b}$, such that each vector $\mathbf{b}$ maps in a distinct coset leader $\mathbf{x}$'. Those vectors $\mathbf{b}$ with limited range will be called "the information vectors".

It is worth noting, as pointed also by Zamir [2014], that the modulo-Λ_s operation relies in bringing the vector $\mathbf{x}$ to the Voronoi region of lattice because we use an Euclidean norm in (2.4). We can use other norms in order to have different fundamental regions.

2.2 Lattices from Codes

One way to construct lattices is from linear codes. This type of construction associates a linear code $C \in \mathbb{Z}_q^n$ to a lattice $\Lambda \in \mathbb{Z}^n$, where $\mathbb{Z}_q^n$ is defined as the set $\{0, 1, ..., q-1\}^n$. Here q is any integer. As C is obtained from a message vector $\mathbf{u} \in \mathbb{F}_q^k$, with an independently choice in each coordinate of $\mathbf{u} \in \mathbb{Z}_q^k$, the overall mapping is $\mathbb{Z}_q^k \to \mathbb{Z}^n$. Let $C \in \mathbb{Z}_q^n$ be a linear code and $\mathbf{c}_i$ be one of its codewords. This association is done by the linear transformation ρ defined as:

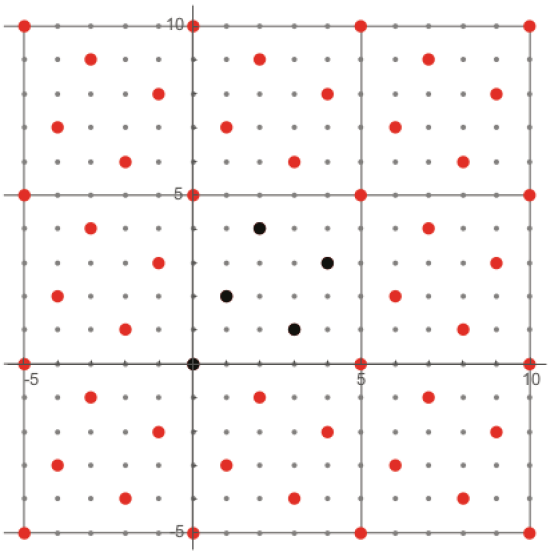


Figure 2.2: A construction-A lattice Λ_{A_2} obtained by a linear code in $\mathbb{Z}_5^2$ (black points).

$$\begin{aligned} \rho : \mathbb{Z}_q^n &\to \mathbb{Z}^n, \\ \rho(\mathbf{c}_i) &\to \mathbf{x}, \\ \rho(\mathbf{c}_i) = \mathbf{c}_i + q\mathbf{z}, \mathbf{z} &\in \mathbb{Z}^n, \end{aligned} \tag{2.21}$$

the inverse transformation ρ^{-1} associates a lattice point $\mathbf{x} = \mathbf{c}_i + q\mathbf{z}$ to the codeword $\mathbf{c}_i$, i.e, $\rho^{-1}(\mathbf{x}) = \mathbf{c}_i$. Here, ρ^{-1} is the reduction $\mod q$ operation. A lattice obtained the way described above is called a construction-A lattice.

Definition: Construction-A Lattice: A construction-A lattice, is the lattice obtained from a linear error-correcting code C, such that:

$$\Lambda_A = \{\rho(\mathbf{c}_i)\} = \{\mathbf{c}_i + q\mathbf{z}, \mathbf{z} \in \mathbb{Z}^n, \mathbf{c}_i \in C\}. \tag{2.22}$$

Note that Λ_A is an integer lattice, i.e., $\Lambda_A \subseteq \mathbb{Z}^n$. Also, if $\mathbf{c}_i = \mathbf{0}$, then, we have the lattice $q\mathbb{Z}^n$. Thus, for any construction A, holds that $q\mathbb{Z}^n \subseteq \Lambda_A$ because the codeword $\mathbf{0}$ belongs to any linear code by definition.

Figure 2.2 illustrates a bi-dimensional construction-A lattice Λ_{A_2} generated by a linear code $C \subseteq \mathbb{Z}_5^2$ with generator matrix $(1, 2)^T$, and with codewords $C = \{(0, 0), (1, 2), (2, 4), (3, 1), (4, 3)\}$. The codewords are represented as black points. The application of the transformation ρ makes copies of the code C throughout all the space (red points), creating the lattice Λ_{A_2}. It is also easy to see from the figure, that the obtained lattice is an integer lattice, i.e, $\Lambda_{A_2} \subseteq \mathbb{Z}^2$ and the lattice $5\mathbb{Z}^2$ is contained

in Λ_{A_2}, so $5\mathbb{Z}^2 \subseteq \Lambda_{A_2}$.

The code rate of a construction-A lattice is defined as:

$$R_c = \frac{k}{n}, \tag{2.23}$$

and, for q being a prime number, its volume is given by:

$$\mathrm{Vol}\left(\Lambda_{An}\right) = q^{n-k}. \tag{2.24}$$

Proof: As we have the relation $q\mathbb{Z}^n \subseteq \Lambda_A$, we can define the quotient group: $\Lambda_A/q\mathbb{Z}^n$. As discussed in section 2.1, the quotient group carnality is the number of points of Λ_A inside a fundamental region of $q\mathbb{Z}^n$. Because of the definition of construction A, this number is the code carnality. For instance, in figure 2.2, it is easy to see that, the points inside the fundamental parallelotope of $5\mathbb{Z}^2$ is the points in black, which are the codewords of the code C. For a linear code, if q is a prime number, the code carnality is 2^k, given that the code C is a subspace of $\mathbb{Z}_q^n$ with exactly k generator vectors. Thus, the quotient group carnality is $M = q^k$. Also, the generator matrix of the lattice $q\mathbb{Z}^n$ is $q\mathbf{I}_n$. Thus, using (2.16), we have:

$$M = q^k = \left|\frac{\Lambda_A}{q\mathbb{Z}^n}\right| = \frac{\mathrm{Vol}\left(q\mathbb{Z}^n\right)}{\mathrm{Vol}\left(\Lambda_A\right)} = \frac{\det\left(q\mathbf{I}_n\right)}{\mathrm{Vol}\left(\Lambda_A\right)} = \frac{q^n}{\mathrm{Vol}\left(\Lambda_A\right)}. \tag{2.25}$$

Thus we have the relation $q^k = q^n/\mathrm{Vol}\left(\Lambda_A\right)$, which implies $\mathrm{Vol}\left(\Lambda_{An}\right) = q^{n-k}$, concluding the proof. □

One generator matrix of a construction-A lattice is given by:

$$\mathbf{G}_{n\times n} = \begin{pmatrix} I_{k\times k} & 0_{k\times n-k} \\ B_{n-k\times k} & qI_{n-k} \end{pmatrix}. \tag{2.26}$$

Proof: A systematic form generator matrix for any linear code is given by:

$$\mathbf{V}_{n\times k} = \begin{pmatrix} I_{k\times k} \\ B_{n-k\times k} \end{pmatrix}, \tag{2.27}$$

let $\mathbf{v}_j$ for $j = \{1, ..., k\}$ be the columns of the matrix $\mathbf{V}$ and $q\mathbf{e}_i$ for $i = \{1, ..., n\}$ be a basis for the lattice $q\mathbb{Z}^n$, where $\mathbf{e}_i$ is the canonical basis. We can write (2.22), as

$$\Lambda_A = \left\{ \sum_{i=1}^{k} u_i\mathbf{v}_i + \sum_{i=1}^{n} qh_i\mathbf{e}_i \right\}, \tag{2.28}$$

for some $u_i \in \{0, ..., q-1\}$ and $h_i \in \mathbb{Z}$. So, the vectors $[\mathbf{v}_1, ..., \mathbf{v}_k, q\mathbf{e}_1, ..., q\mathbf{e}_n]$ span the lattice Λ_A. So, the lattice generator matrix is $\mathbf{G} = (\mathbf{v}_1, ..., \mathbf{v}_k, q\mathbf{e}_1, ..., q\mathbf{e}_n)$. Clearly, we have $(n + k)$ vectors. To

reduce this matrix to n vectors, in order to obtain the matrix stated in (2.26), we need to perform a Gaussian elimination, which is left for the reader. This concludes the proof. □

Construction A is obtained from a single linear code C. We now focus in another type of construction, also known as a multilevel construction, called construction D.

Definition: Construction-D Lattice. Let $\mathbf{g}_1, \mathbf{g}_2, ..., \mathbf{g}_n$ be a basis for $\mathbb{Z}_q^n$. For $a \geq 1$, let $C_0 \subseteq C_1 \subseteq \cdots \subseteq C_a = \mathbb{Z}_q^n$ be a sequence of nested linear block codes over $\mathbb{Z}_q^n$. Let $\mathbf{G}_i = [\mathbf{g}_1, \cdots, \mathbf{g}_{k_i}]$ be a generator matrix of the code C_i and $\mathbf{u}_i$ a message vector with length k_i, with $i = \{0, \cdots, a-1\}$, then a construction-D lattice Λ_D, is the set

$$\Lambda_D = \left\{ \sum_{i=0}^{a-1} q^i \mathbf{G}_i \cdot \mathbf{u}_i + q^a \mathbf{G}_a \cdot \mathbf{z}. \right\} \tag{2.29}$$

In this definitions, all the operations are performed over $\mathbb{Z}^n$. This fact, combined with the codes C_i to be nested, ensure the construction D to be a lattice packing. If the codes are not nested, then the packing is generally not a lattice. The type of construction where the codes are not nested is called construction C, and is a general case of construction D, however, this construction is out of the scope of this thesis as we are interesting in lattice packings.

Alternatively, if the codes are nested, but the operations are performed over $\mathbb{Z}_q^n$, such that $\mathbf{G}_i \cdot \mathbf{u}_i = \mathbf{c}_i$, we obtain the so-called *code formula*.

Definition: Construction by Code Formula: For $a \geq 1$, let $C_0 \subseteq C_1 \subseteq \cdots \subseteq C_a = \mathbb{Z}_q^n$ be a sequence of nested linear block codes over $\mathbb{Z}_q^n$. Let $\mathbf{G}_i = [\mathbf{g}_1, \cdots, \mathbf{g}_{k_i}]$ be a generator matrix of the code C_i and $\mathbf{u}_i$ a message vector with length k_i, with $i = \{0, \cdots, a-1\}$. Then, each codeword $\mathbf{c}_i$ is given by $\mathbf{G}_i \cdot \mathbf{u}_i$, where these operations are performed over $\mathbb{Z}_q^n$. Thus, the packing obtained is called code formula Γ_{CF}:

$$\Gamma_{CF} = \left\{ \mathbf{c}_0 + q \cdot \mathbf{c}_1 + \cdots + q^i \cdot \mathbf{c}_i + \cdots + q^{a-1} \cdot \mathbf{c}_{a-1} + q^a \cdot \mathbf{z} \right\}, \tag{2.30}$$

where $\mathbf{c}_i \in C_i, i = \{0, \cdots, a-1\}, \mathbf{z} \in \mathbb{Z}^n$.

Despite the similarities of the construction D and the construction by code formula, the packings generated by these constructions are not always the same. The code formula do not always generate lattices, a lattice packing is generated by code formula if, and only if, the codes $\mathbf{C}_i$ are close under the so-called Schur product Kositwattanarerk and Oggier [2014], if, this fact is satisfied, then $\Gamma_{CF} = \Lambda_D$. In contrast, construction D always generates lattice packings. More, generally, when the construction by code formula does not generate a lattice packing, the following relation holds:

$$\Gamma_{CF} \subseteq \Lambda_D \tag{2.31}$$

For more details, we invite the reader to see Kositwattanarerk and Oggier [2014]. Despite the code formula does not always generate a lattice, its construction is still valid for a communication system in general, and will be used several times to illustrate further results presented throughout this thesis. Moreover, we sometimes refer to this construction as a lattice, without loss of generality.

For the construction by code formula and construction D, each code C_i has rate $R = k_i/n$ and minimum distance d_i. Because the codes are nested $R_0 \leq R_1 \leq \cdots \leq R_a$ and $d_0 \geq d_1 \geq \cdots \geq d_a$. Also, the basis vectors for the code C_i, with generator vectors $\mathbf{g}_1, \mathbf{g}_2, ..., \mathbf{g}_{k_i}$ are a subset of those for code C_{i+1} with generator vectors $\mathbf{g}_1, \mathbf{g}_2, ..., \mathbf{g}_{k_{i+1}}$. Finally, since $C_a = \mathbb{Z}_q^n$, then $R_a = 1$, $k_a = n$ and $d_a = 1$.

The construction D and the construction by the code formula share the same code rate which is defined as:

$$R_c = \sum_{i=0}^{a-1} R_i = \frac{\sum_{i=0}^{a-1} k_i}{n}. \tag{2.32}$$

Note that the construction A is a particular case of the construction D and the code formula, obtained when we set $a = 1$. As result, construction A yields lattices that are generated by a single code in $\mathbb{F}_q^n$, and is not a multilevel construction as the others. For code formula, each code C_i is a code over $\mathbb{Z}_q^n$, while we can define the "super code" C as a code over $\mathbb{Z}_{q^a}^n$:

$$C = \sum_{i=0}^{a-1} q^i C_i. \tag{2.33}$$

Furthermore, the code formula can be seen as a strategy to construct non binary codes, from nested binary codes. As for construction A, the code formula Γ_{CF} and the construction-D lattice Λ_D are integer constructions, so $\Lambda_D, \Gamma_{CF} \subseteq \mathbb{Z}^n$, if $\mathbf{c} = \mathbf{0}$, for $\mathbf{c} \in C$, then, we have the lattice $q^a\mathbb{Z}^n$. Thus, for both constructions, holds that $q^a\mathbb{Z}^n \subseteq \Lambda_D, \Gamma_{CF}$, because as we already mentioned the codeword $\mathbf{0}$ belongs to any linear code.

As the construction D is always a lattice, we can calculate its volume, which is given by:

$$\mathrm{Vol}\left(\Lambda_D\right) = \mathrm{Vol}\left(\Gamma_{CF}\right) = q^{an - \sum_{i=0}^{a-1} k_i}. \tag{2.34}$$

The proof is analogous of the proof of the volume for construction-A lattices, but here $M = q^{\sum_{i=0}^{a-1} k_i}$ and $\mathrm{Vol}(q^a\mathbb{Z}^n) = \det\left(q^a\mathbf{I}_n\right) = q^{an}$. The prove is left for the reader.

An $n \times n$ generator matrix $\mathbf{G}$ of a construction-D lattice, is a matrix of the form:

$$\mathbf{G} = \mathbf{G}_a \cdot \mathbf{D}, \tag{2.35}$$

where $\mathbf{G}_a = (\mathbf{g}_1, \cdots, \mathbf{g}_{k_i}, \cdots, \mathbf{g}_{k_a})$ and $\mathbf{D}$ is a diagonal matrix with diagonal entries

$$d_{ii} = q^j \text{ for } k_j \leq i < k_{j-1}. \tag{2.36}$$

Proof: From (2.29), the vectors which span the lattice Λ_D, are the vectors $[\mathbf{g}_1, \cdots, \mathbf{g}_{k_0}, \cdots, q^i\mathbf{g}_1, \cdots, q^i\mathbf{g}_{k_i}, \ldots, q^a\mathbf{g}_1, \cdots, q^a\mathbf{g}_{k_a}]$, which are $\sum_{i=0}^{a} k_i = \sum_{i=0}^{a-1} k_i + n$ vectors, because $k_a = n$. To reduce this matrix to n vectors, in order to obtain the generator matrix of Λ_D, we need to perform a Gaussian elimination, which yields to the matrix:

$$\mathbf{G} = \begin{pmatrix} | & | & & | & | & & | & | & & | & | \\ \mathbf{g}_1 & \mathbf{g}_2 & \cdots & \mathbf{g}_{k_1} & q\mathbf{g}_{k_1+1} & \cdots & q^i\mathbf{g}_{k_i} & q^{i+1}\mathbf{g}_{k_i+1} & \cdots & q^a\mathbf{g}_{k_a-1} & q^a\mathbf{g}_{k_a} \\ | & | & & | & | & & | & | & & | & | \end{pmatrix}. \tag{2.37}$$

which can be write as a multiplication of two matrix as in equation (2.35). □

For a construction-D lattices and the code formula, let the minimum square distance of the code C_i be $d_i^2 \geq q^{2(a-i)}/\gamma$ for $i = \{0, 1, ..., a-1\}$, where $\gamma \in \mathcal{H}$ with $\mathcal{H}$ the set of multiples of q. Then these constructions has square minimum distance satisfying,

$$d_{min}^2 \geq q^{2a}/\gamma. \tag{2.38}$$

Proof: Because of the multilevel construction characteristic, C_0 is a set of consecutive points of Λ_D, Γ_{CF}. Thus, the square minimum distance is the same as that of the code C_0, which is q^{2a}/γ, obtained when $i = 0$. □

Throughout the rest of this thesis, in order to reduce and simplify the notation, as well as the illustrations of the theorems which will be presented, we refer to the construction by the code formula as a construction-D lattice, given that, when it generates a lattice, this lattice is always a construction-D lattice. Note that, even if it does not generate a lattice, it is still applicable in a communications system as a multilevel code construction, and generally the approximation $\Gamma_{CF} \approx \Lambda_D$ can be used without loss of generality. Moreover, given the similarities of these two constructions, the extension from one to another of all the results presented in following chapters are straightforward.

2.3 Modulation and Coding for AWGN Channel

We now define some figures of merit for the AWGN channel and briefly discuss the performance of standard known constellations such as M-PAM and M^2-QAM over this channel.

Lattices are a mathematical tool, which provides a general method to construct constellations. Uncoded M-PAM constellations are obtained by setting $\Lambda_c = \mathbb{Z}$ and $\Lambda_s = M\mathbb{Z}$. Equivalently, we can choose a set of n symbols, in which each symbol belongs to a M-PAM constellation by setting $\Lambda_c = \mathbb{Z}^n$, and $\Lambda_s = M\mathbf{I}\mathbb{Z}^n$, with $\mathbf{I}$ the identity matrix. Here, the Voronoi region of Λ_s is a hypercube. As we will see, when the Λ_s is a hyperrectangle or a hypercube, we can choose any symbol independently, i.e, the choice of a present symbol do not depend on the choice of a previous one. This independence is provided by the hypercube shape of the Voronoi region of Λ_s. In other words, the marginal distribution of the symbols to be transmitted over the AWGN channel is an uniform distribution.

A standard measure of the constellation performance is the signal-to-noise ratio of the AWGN channel, which is given by

$$\text{SNR} = \frac{P}{N_0 W} = \frac{E_s}{\sigma^2} = 2R\frac{E_b}{N_0}, \tag{2.39}$$

where $P = \frac{1}{n}\mathbb{E}[||\mathbf{x}||_k^2]$ is the transmit average power per dimension of the constellation, $\sigma^2 = N_0/2$ is the noise variance, E_b is the energy per bit, E_s is the energy per symbol, and R is the *Information Rate*, defined as:

$$R = \frac{\log_2 M}{n}, \tag{2.40}$$

where M is the number of points of the constellation. As we will see, for Voronoi constellations, defined in the next section, this value is given in equation (2.16).

The capacity of the AWGN channel is given by:

$$C = W \log_2 (1 + \text{SNR}) \text{ bits/s} \tag{2.41}$$

for the continuous time, whereas for the discrete time, it is defined as,

$$C = \frac{1}{2} \log_2 (1 + \text{SNR}) \text{ bits/dim.} \tag{2.42}$$

Note that, in discrete time, the capacity formula can be rewritten as $\text{SNR} = 2^{2C} - 1$. This suggests defining the *normalized SNR*:

$$\underset{norm}{\mathrm{SNR}} = \frac{\mathrm{SNR}}{2^{2R}-1}, \tag{2.43}$$

where R is the actual data rate of a given modulation and coding scheme. For a capacity-achieving scheme, R is equal to the channel capacity C and $\mathrm{SNR}_{norm} = 1$ (0 dB). If, $R < C$ as will always be the case in practice, then $\mathrm{SNR}_{norm} > 1$. Thus, the value of SNR_{norm} signifies how far a system is operating from the Shannon limit, also called the "gap to capacity". The advantage of defining SNR_{norm} relies in the fact that its value is the same (0dB) for any capacity achieving scheme, i.e, it does not change with the information rate R. As we will see in the following, using SNR_{norm} is appropriate only for the bandwidth-limited regime, where M-PAM constellations with M large are used. For the power-limited regime, 2-PAM constellations are sufficient to achieve the channel capacity, and the traditional figure of merit E_b/N_0 is used. This is because in this regime, the bandwidth is unconstrained, and as bandwidth increases, both SNR and R tend toward zero, and SNR_{norm} becomes an undefined quantity. The disadvantage is that the value of E_b/N_0, for some capacity achieving scheme, changes with R.

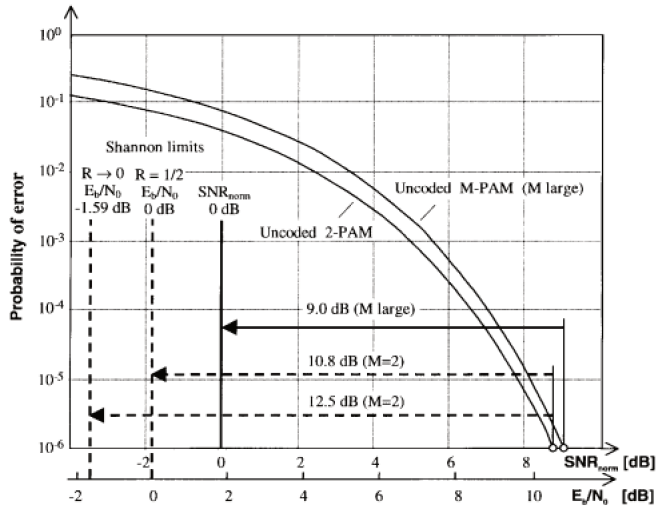


Figure 2.3: Bit-error probability versus E_b/N_0 for uncoded 2-PAM, and symbol-error probability versus SNR_{norm} for uncoded M-PAM (M large) Forney and Ungerboeck [1998].

Figure 2.3 shows the performance of uncoded M-PAM constellations (M large) as a function of SNR_{norm} for the bandwidth regime, and the performance of uncoded M-PAM constellations ($M = 2$) as a function of E_b/N_0 for the power limited regime. It is possible to see that the best we can do with uncoded M-PAM (M large) is always 9 dB from the channel capacity, while for $M = 2$, the gap to capacity in terms of E_b/N_0 changes with the rate R. For $R \to 0$, E_b/N_0 approximates the ultimate Shannon limit (-1.59 dB). Thus, in both regimes, to approach the channel capacity, we need

to code our modulation, i.e, to put an error-correcting code in it, in order to improve the constellation performance.

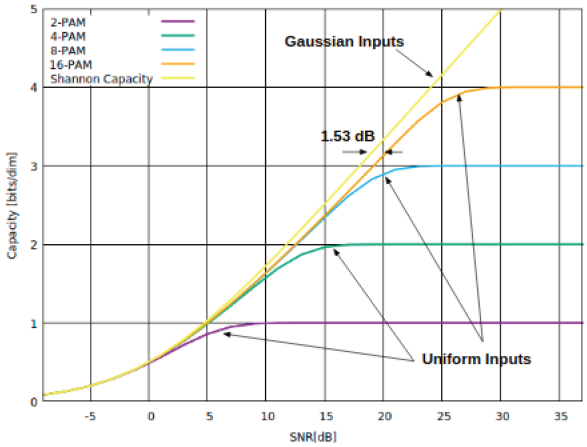


Figure 2.4: Capacity of the ideal AWGN channel with Gaussian inputs and with equiprobable M-PAM inputs.

Figure 2.4 shows the best performance of coded M-PAM constellations. Based on this figure, we define two different regimes, the power-limited regime (low SNR) and the bandwidth-limited regime (high SNR). The difference of these two regimes are shown in table 2.1. The name power-limited regime comes from the fact that as $SNR = P/N_0W$, the capacity $C \approx W\,\mathrm{SNR}\log_2 e = \frac{P}{N_0}\log_2 e$ does not depend on the bandwidth W, i.e, the bandwidth in this regime is unconstrained, and this regime is limited by the power. For the bandwidth regime, $C \approx W\log_2 \mathrm{SNR}$, and the capacity changes with the bandwidth, which means that this regime is limited by the bandwidth.

From figure 2.4, it is also possible to note that, in the power-limited regime (SNR low), a coded 2-PAM constellation, i.e, binary constellations are sufficient to achieve Shannon capacity, and shaping is unnecessary. Thus, a simple binary error-correcting code C are a natural mapping for achieving capacity in this regime, this is because, each bit is associated to one symbol as

$$\begin{aligned} m(C) &: \mathbb{F}_2^k \rightarrow m(\mathbb{F}_2^n) \\ m &: \{0,1\} \rightarrow \{\pm d_0/2\}. \end{aligned} \tag{2.44}$$

In contrast, figure 2.4 shows that M-PAM constellations are required in the bandwidth regime. One interesting fact for this regime is that the best coded M-PAM constellations achieves a gap of 1.53 dB from Shannon capacity. The remaining 1.53 dB is due to the mismatch between Gaussian inputs, achieved when the shaping region is asymptotically a hypersphere. This is because, as mentioned, M-PAM constellations have uniform inputs, given that, the shaping regions is a hypercube. Thus, the

Table 2.1: Comparison between Low-SNR Regime and High-SNR Regime

Regime	**Low-SNR (Power-limited regime)**	**High-SNR (Bandwidth-limited regime)**
Capacity (bits/s)	$C \approx W\,\mathrm{SNR}\log_2 e$	$C \approx W\log_2 \mathrm{SNR}$
Capacity (bits/dim)	$C \approx \frac{1}{2}\,\mathrm{SNR}\log_2 e$	$C \approx \frac{1}{2}\log_2 \mathrm{SNR}$
Constellations Type	Binary	Nonbinary
Uncoded Modulation Baseline	2-PAM	M-PAM
Coded Modulations	Error-correcting code	Lattice code
General Mapping	$m(C) : \mathbb{F}_2^k \to m(\mathbb{F}_2^n)$ $m : \{0,1\} \to \{\pm d_0/2\}$	$\Lambda : \mathbb{F}_2^k \to \mathbb{Z}^n$
Coding Gain	$\gamma(C) = \frac{k}{n} d_{min}$	$\gamma(\Lambda) = \frac{d_{min}^2}{\mathrm{Vol}(\Lambda)^{2/n}} = d_{min}^2 \frac{\Delta^{2/n}}{\mathrm{Vol}(\mathcal{B})^{2/n}}$

challenge in this regime is to code our constellation, and change the shaping region in order to obtain the remaining 1.53 dB. This remaining gain comes at a price of creating a dependence between the symbols choice, as we no longer use a hypercube as shaping region. Finally, note that, in this regime, we associate a set of bits, to a set of non-binary symbols. Thus a lattice generated from an error-correcting code is a natural mapping for achieving capacity, because,

$$\Lambda : \mathbb{F}_2^k \to \mathbb{Z}^n. \tag{2.45}$$

For the power-limited regime the coding gain is equal to,

$$\gamma(C) = \frac{k}{n} d_{min}, \tag{2.46}$$

which improves as good linear codes is used, that is, codes which have a good compromise between the code rate R_c, and the minimum distance d_{min}. In this regime, as we are dealing with binary constellations, the code rate $R_c = k/n$ is the same of the information rate $R = \log_2 M/n = \log_2 2^k/n = k/n$. For the bandwidth-limited regime, the coding gain is defined as

$$\gamma(\Lambda) = \frac{d_{min}^2}{\mathrm{Vol}(\Lambda)^{2/n}} = d_{min}^2 \frac{\Delta^{2/n}}{\mathrm{Vol}(\mathcal{B})^{2/n}}, \tag{2.47}$$

where Δ is the packing density of the lattice, and $\mathrm{Vol}(\mathcal{B})$ is the volume of a ball in dimension n. Thus, in this regime, good coding gains are provided by lattices which have good packing densities for the same d_{min}.

2.4 Voronoi Lattices Codes

We now define some figures of merit for lattices over the AWGN channel. In this section, remember that each lattice point is a symbol vector, while each coordinate of the lattice point is a symbol to be transmitted over the AWGN channel. Therefore, choosing a lattice point, is equivalent of choosing a set of symbols to be transmitted.

As mentioned in section 1.2, good lattice code constellations consist in finding a high-dimensional lattice Λ, which is constrained by a shaping region around the origin that we denote by $\mathbb{S}$. Then, we can define lattice code $\mathcal{C}$ as the set of points of a translation of Λ inside the shaping region $\mathbb{S}$: $\mathcal{C} = (\Lambda - \mathbf{d}) \cap \mathbb{S}$. The translation $\mathbf{d}$ is applied to ensure that the final constellation has zero average, which implies minimal power, and it does not change the fundamental lattice parameters defined in the previous sections.

Given two nested lattices $\Lambda_s \subseteq \Lambda_c$, we call Λ_s the shaping lattice, and Λ_c the coding lattice. We define a *Voronoi constellation* or *Voronoi lattice code* as the lattice code $\mathcal{C}$ constrained by the Voronoi region of Λ_s, in other words: $\mathbb{S} = \mathcal{V}(\Lambda_s)$ and,

$$\mathcal{C} = (\Lambda_c - \mathbf{d}) \cap \mathcal{V}(\Lambda_s). \tag{2.48}$$

The average Voronoi constellation power per dimension $P(\mathcal{C})$ satisfies:

$$P(\mathcal{C}) = P(\Lambda_c) - P(\mathbf{d}), \tag{2.49}$$

where $P(\Lambda_c)$ is the average power per dimension of the lattice Λ_c constrained by the Voronoi region of Λ_s, and $P(\mathbf{d}) = \frac{1}{n}||\mathbf{d}||^2$.

Proof: The average Voronoi constellation power per dimension is given by: $P(\mathcal{C}) = \frac{1}{n}\mathbb{E}\{||\mathbf{x}_k||^2\}$, where $\mathbf{x}_k$ is the possible symbols of the Voronoi constellation, which are related to the corresponding vectors $\mathbf{x}'_k$ of the coding lattice as $\mathbf{x}_k = \mathbf{x}'_k - \mathbf{d}$. Thus,

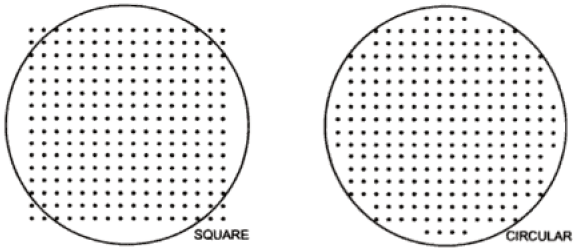
$$P(\mathcal{C}) = \frac{1}{n}\mathbb{E}\{||\mathbf{x}'_k - \mathbf{d}||^2\} = \frac{1}{n}\mathbb{E}\{||\mathbf{x}'_k||^2\} - \frac{2}{n}\mathbb{E}\{\mathbf{d} \cdot \mathbf{x}'_k\} + \frac{1}{n}\mathbb{E}\{||\mathbf{d}||^2\}. \tag{2.50}$$

Because $\mathbf{d}$ is not random, $\mathbb{E}\{||\mathbf{d}||^2\} = ||\mathbf{d}||^2$, and $\mathbb{E}\{\mathbf{d} \cdot \mathbf{x}'_k\} = \mathbf{d} \cdot \mathbb{E}\{\mathbf{x}'_k\}$. By definition, $\mathbf{d}$ ensures that the final constellation has zero average, and it is true if $\mathbb{E}\{\mathbf{x}'_k\} = \mathbf{d}$, because to ensure that the final constellation has zero average, we need to subtract exactly the average. Finally, we have,

$$P(\mathcal{C}) = \frac{1}{n}\mathbb{E}\{||\mathbf{x}'_k||^2\} - \frac{2}{n}\mathbf{d} \cdot \mathbf{d} + \frac{1}{n}||\mathbf{d}||^2 = \frac{1}{n}\mathbb{E}\{||\mathbf{x}'_k||^2\} - \frac{1}{n}||\mathbf{d}||^2 = P(\Lambda_c) - \frac{1}{n}||\mathbf{d}||^2, \tag{2.51}$$

and this concludes the proof. □

Note that, each point of Λ_c inside the shaping region $\mathcal{V}(\Lambda_s)$ is associated with a different coset, as we already discussed in 2.1. Thus, choosing a point in the Voronoi constellation $\mathcal{C}$, can be seen as finding the coset leader of a coset in the quotient group, and then, to apply the translation vector $\mathbf{d}$.



(a) Cubic Shaping Region. (b) Sphere Shaping Region.

Figure 2.5: Two different shaping regions $\mathbb{S}$ for the $\mathbb{Z}^2$ coding lattice Barry et al. [2012].

What is a good shaping region? To answer this question, consider figure 2.5, where the cubic lattice $\mathbb{Z}^2$ constrained by two different shaping regions is shown. In figure 2.5(a), square shaping is shown, while in figure 2.5(b), circular shaping is shown. Both lattice constellations have the same amount of point. The difference is the average power of these constellations. As discussed in section 1.2, the sphere is the best shaping region in any dimension, because this region makes possible to have the minimum average power per dimension. For a visual interpretation of 2.5(a), we see that the points outside the sphere in 2.5(a) spend a large amount of energy. Thus, we can put these points in the free positions inside the sphere, which spends less energy, as show in 2.5(b).

The power savings achieved by a given shaping region is always compared to a standard PAM constellation ($\mathbb{Z}^n$ Lattice). Additionally, the power savings is captured by the shaping gain. To define it, let $\mathbb{S}$ be a compact bounded region of the n-space, which we called so far the shaping region. Let $\mathrm{Vol}(\mathbb{S})$ be its volume, and $P(\mathbb{S})$ be its average power per dimension, computed assuming that the transmitted points are continuously and uniformly distributed in $\mathbb{S}$[1]. The shaping gain $\gamma_s(\mathbb{S})$ is defined as Forney and Ungerboeck [1998],

$$\gamma_s(\mathbb{S}) = \frac{\mathrm{Vol}(\mathbb{S})^{\frac{2}{n}}}{12P(\mathbb{S})}, \tag{2.52}$$

where the normalized factor of 12 is because, for the cubic lattice $\mathbb{Z}^n$, $\frac{\mathrm{Vol}(\mathbb{S})^{\frac{2}{n}}}{P(\mathbb{S})} = 12$, consequently $\gamma_s(\mathbb{S}) = 1$ or 0 dB, and as expected, the cubic lattice has no shaping gain. As we will be working with nested lattices, $\mathbb{S}$ will be the Voronoi region of the shaping lattice Λ_s.

[1]This is known as the continuous approximation. Even though the transmitted points in $\mathcal{C}$ are discrete, this approximation is good for large lattice constellations, and makes some computations much easier.

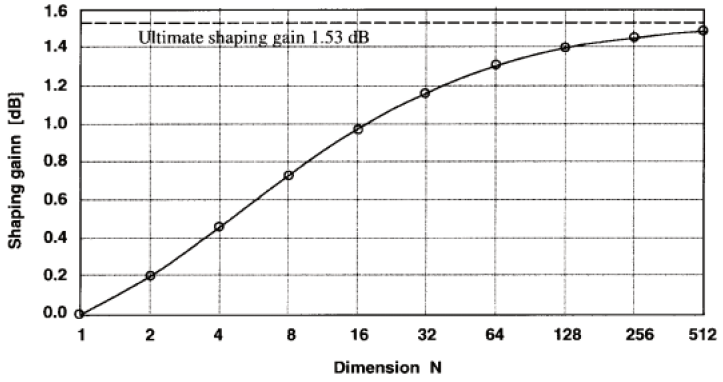


Figure 2.6: Shaping gains of N-spheres over N-cubes Forney and Ungerboeck [1998].

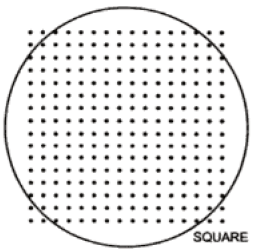
N	Λ_s	$G(\Lambda_s)$	$\gamma_s(\Lambda_s)$	dB	$\gamma_\Phi(N)$	$\gamma_{CS}(N)$
1	Z	1/12	1	0.00	0.00	0.00
2	A_2	$5/[36\cdot 3^{1/2}]$	$3^{3/2}/5 = 1.039$	0.17	0.20	0.17
4	D_4	$13/[120\cdot 2^{1/2}]$	$10\cdot 2^{1/2}/13 = 1.088$	0.37	0.46	0.39
6	$E_6^{\perp}$	$12619/[68040\cdot 3^{5/6}]$	1.122	0.50	0.62	0.55
8	E_8	929/12960	1080/929 = 1.163	0.65	0.73	0.66
12	K_{12}	0.070100	1.189	0.75	0.88	0.81
16	Λ_{16}	0.068299	1.220	0.86	0.98	0.91
24	Λ_{24}	0.065771	1.267	1.03	1.10	1.04

Figure 2.7: Shaping gains of Voronoi regions of some lattices Forney and Wei [1989].

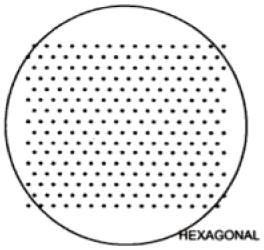
As shown in figure 2.6, the maximum shaping gain achievable is 1.53 dB, which is achieved by a hypersphere when dimension goes asymptotically to infinity. Unfortunately, there is no lattice whose the Voronoi region is a hypersphere. In fact, this is not a problem, because for some lattices, as dimension increases, the Voronoi shape approximates the shape of a hypersphere. Conversely, as its dimension increases, its shaping gain approximates the 1.53 dB. Those lattices are called *lattices good for shaping*, also known as *lattices good for quantization* because mean-squared value of vector error quantization is analogous of definition (2.52), see section 3.2 of Zamir [2014] for details. In figure 2.7, we present the shaping gain of some known quantizers. For the leech lattice (Λ_{24}), for instance, which is the best quantizer in its dimension (as well as Gosset (E_8) Lattice), we have 1.03dB of shaping gain, 0.1 dB away from the optimum shaping gain of a sphere in dimension 24 (last column of the table). Note that, this gain is close to the maximum shaping gain of 1.53dB. So, for shaping, the dimension does not need to be extremely large to achieve a good shaping gain.

As a good shaping region decreases the average power of the transmitted symbols, we need a lower value of SNR to achieve the same error probability in comparison with a cubic shaping. This, evidently increases our performance.

So far, we have seen how to choose a good shaping region, and consequently, a good shaping



(a) $\mathbb{Z}^2$ Lattice for Sphere Shaping Region.



(b) Hexagonal (A_2) Lattice for Sphere Shaping Region.

Figure 2.8: Two different coding lattices for the same shaping region $\mathbb{S}$ Barry et al. [2012].

lattice Λ_s, given that we will be dealing with Voronoi regions for $\mathbb{S}$. We now, focus in choosing a good coding lattice Λ_c, which will be our constellation symbol vectors.

Let the *minimum distance* d_{min} be the minimum distance between any two lattice points. Figure 2.8 shows two different coding lattices with the same d_{min}, and constrained by the same shaping region, which is a circle. Figure 2.8(a) shows the cubic lattice $\mathbb{Z}^2$, whereas figure 2.8 shows the hexagonal lattice A_2. It is easy to see that for the A_2 lattice, we can put more points inside the circle when compared with the $\mathbb{Z}^2$. As d_{min} keeps constant for both lattices, the probability of error does not change for both situations. So, by changing the lattice, we change the amount of symbol vectors to be transmitted over the channel. The information to be transmitted, in bits per dimension is the information rate R.

From figure 2.8 and equation (2.40), we note that by changing the lattice geometry, we change the information rate R for the same error probability, and consequently, for the same SNR. For a transmission system we are interested in increasing the amount of information for the same SNR, keeping the transmission reliable.

In comparison with the $\mathbb{Z}^2$ lattice, the gain provided by changing the lattice geometry is called *coding gain*, and is defined in (2.47). This gain can be as big as 1.53 dB from Shannon capacity, because the remaining 1.53 dB is obtained with the shaping operation. The coding gain increases with the lattice dimension. Consequently, as dimension increases we can put more points inside a bounded region in the n-space, such that the average number of points per dimension is also increased. Lattices which achieves 1.53 dB from Shannon capacity as dimension increases, and with vanishing error probability for some $\sigma < \sigma_{max}$, are called *lattices good for coding*, also known as *lattices good for packing*, this is because the coding gain can be expressed in terms of the packing density of a lattice as shown in equation (2.47). See section 3.1.1 of Zamir [2014] for details. As stated by Poltyrev in Poltyrev [1994], $\sigma^2_{max} = \frac{\mathrm{Vol}(\Lambda)^{\frac{2}{n}}}{2\pi e}$. This quantity is known as Poltyrev threshold.

For coding, a standard measure of lattice performance, without considering any shaping region is the so called volume-to-noise ratio, defined as

$$\text{VNR} = \frac{\text{Vol}\,(\Lambda)^{\frac{2}{n}}}{2\pi e\sigma^2(P_e)}. \tag{2.53}$$

This quantity measures the possible performance advantage of the lattice Λ, in comparison with the cubic lattice for a given error probability P_e. We write $\sigma^2(P_e)$ to call attention that, a fair comparison between lattices is obtained when fixing a value of P_e, and not a value of σ. We wish to find the densest lattice, i.e., the lattice with the lowest VNR. This would imply the largest information rate R. Also, for a given family of lattices with increasing dimension, a necessary condition for its error probability to vanish as the lattice dimension increases is that VNR > 1. To see this, it is enough to insert σ_{max} in equation (2.53).

For a detailed mathematical prove of all stated in this section we invite the reader to see Erez and Zamir [2004], Forney and Ungerboeck [1998], Poltyrev [1994], Zamir [2014].

Chapter 3

Lattice Encoding and Indexing

In chapter 2, we presented general lattice definitions and the requirements to achieve Shannon capacity by applying lattice theory in the channel coding stage of a communication system, yielding to multidimensional constellations, specifically Voronoi constellations or Voronoi lattice codes. As we have seen, this is equivalent of finding a set of coset leaders for the quotient group defined in (2.13). Despite that, we have not discussed how to find a coset representative of each coset.

In this chapter we present the requirements, and a method to find these coset representatives, which will allow the encoding and indexing operation for these lattices, obtaining a Voronoi lattice code. Encoding is the process of mapping the information to be transmitted, represented by a vector of integers, to the symbol vectors of $\mathcal{C}$. Indexing is the inverse operation, mapping symbol vectors of $\mathcal{C}$ to information integer vectors. For an additional complementing of this chapter, we recommend the reader to read Kurkoski [2018].

This chapter is divided in three sections. In section 3.1, we present the motivation of the problem, and some additional definitions, which will be useful for the next sections. Section 3.2 describes a general encoding scheme for lattices, called Rectangular Encoding, which allows the creation of Voronoi lattice codes. If the basis of a shaping lattices are "aligned" with the basis of a coding lattice in the sense that will be clearly later, then a rectangular encoding is trivial. Section 3.3 applies the rectangular encoding in a particular case of lattices obtained from error-correcting codes, as we will see, it allows to obtain a complete set of cosets representatives of each coset allowing an efficient construction of the Voronoi lattice code with reduced encoding complexity.

3.1 Preliminaries

As we have seen in section 2.1.2, the set of points of Λ_c inside any fundamental region of the shaping lattice $\mathcal{P}(\Lambda_s)$ is a complete set of coset representatives. We are now interested in finding those

points. To that end, consider the nested lattice pair, $\Lambda_s \subseteq \Lambda_c$, which are related by $\mathbf{G}_s = \mathbf{G}_c \cdot \mathbf{M}$, with $\mathbf{M} = diag(M_1, \ldots, M_n)$, a diagonal matrix with integer entries M_i. Now, choose the fundamental parallelotope $\mathcal{P}(\mathbf{G}_s)$ as a fundamental region of Λ_s. Thus, following equation (2.8), this region is the set of all points satisfying:

$$\mathcal{P}(\mathbf{G}_s) = \{\alpha_1 M_1 \mathbf{g}_1 + \cdots + \alpha_n M_n \mathbf{g}_n, 0 \leq \alpha_i < 1, i = 1, \ldots, n\}. \tag{3.1}$$

The set of all points of Λ_c can be written as equation (2.1):

$$\Lambda_c = \{\mathbf{G}_c \cdot \mathbf{b} = b_1 \mathbf{g}_1 + \cdots + b_n \mathbf{g}_n, \mathbf{b} \in \mathbb{Z}^n\}. \tag{3.2}$$

By the similarity of equations (3.1) and (3.2), it is straightforward to see that, the points of Λ_c inside $\mathcal{P}(\mathbf{G}_s)$, or a set of coset representatives of the quotient group defined in (2.13) is the set of points:

$$\Lambda_c \cap \mathcal{P}(\mathbf{G}_s) = \{\mathbf{G}_c \cdot \mathbf{b} = b_1 \mathbf{g}_1 + \cdots + b_n \mathbf{g}_n, b_i = 0, \ldots, M_i - 1\}. \tag{3.3}$$

This is what we mean by the basis be "aligned", ie, each shaping lattice generator vector is a linear combination of the respective coding lattice generator vector. Of course, this is possible because $\mathbf{M}$ is diagonal. A lattice pair with these characteristics is called "near-ellipsoidal lattices", while if $M_i = M$ or $\mathbf{M} = M\mathbf{I}_n$ the basis are still aligned, and this lattice pair is called "self-similar" lattices.

Furthermore, as shown in equation (2.12) in section 2.1.1, in general $\mathbf{M}$ is not diagonal, but an integer matrix. Fortunately, for any nested lattice pairs, we can find a new basis for Λ_c and Λ_s, such that Λ_c and Λ_s become near-ellipsoidal. This is done by the Smith decomposition of the matrix $\mathbf{M}$. Smith decomposition stands that we can decompose $\mathbf{M}$ as:

$$\mathbf{M} = \mathbf{U} \cdot \mathbf{D} \cdot \mathbf{W} \tag{3.4}$$

with $\mathbf{U}$ and $\mathbf{W}$ unimodular matrices and $\mathbf{D}$ a diagonal matrix. We can then replace (3.4) in (2.12), obtaining the relation:

$$\mathbf{G}_s = \mathbf{G}_c \cdot \mathbf{U} \cdot \mathbf{D} \cdot \mathbf{W}, \tag{3.5}$$

and if we multiply both sides of (3.5) by $\mathbf{W}^{-1}$ we have:

$$\mathbf{G}'_s = \mathbf{G}_s \cdot \mathbf{W}^{-1} = \mathbf{G}_c \cdot \mathbf{U} \cdot \mathbf{D} \cdot \mathbf{W} \cdot \mathbf{W}^{-1} = \mathbf{G}_c \cdot \mathbf{U} \cdot \mathbf{D} = \mathbf{G}'_c \cdot \mathbf{D}. \tag{3.6}$$

Thus, because $\mathbf{U}$ and $\mathbf{W}$ are unimodular matrices, we have a new basis matrix $\mathbf{G}'_s$ of Λ_s and a new basis matrix $\mathbf{G}'_c$ of Λ_c, satisfying the relations $\mathbf{G}'_s = \mathbf{G}_s \cdot \mathbf{W}^{-1}$ and $\mathbf{G}'_c = \mathbf{G}_c \cdot \mathbf{U}$, which are now near-ellipsoidal, because $\mathbf{D}$ is diagonal.

It seems that the problem is solved. Actually, by a mathematical point of view yes, but practically we have some drawbacks. Firstly, achieving capacity requires that the lattice dimension goes to infinity. The Smith decomposition is not feasible for high dimensions because of its complexity. Moreover, after performing Smith decomposition, we need to use $\mathbf{G}_c'$ and $\mathbf{G}_s'$ to find the coset representatives, but in many applications we will be interested in take advantage of the structure of the matrix $\mathbf{G}_c$ and $\mathbf{G}_s$, and not to obtain other basis matrices. This will be the problem which we will be dealing in section 3.3. Because of that, in section 3.2 we will be interested in finding the coset representatives by looking for the structure of $\mathbf{G}_c$ and $\mathbf{G}_s$ and letting $\mathbf{M}$ be as it is.

3.2 Rectangular Encoding

Definition: Rectangular Encoding. The Voronoi lattice code $\mathcal{C}$ has rectangular encoding, if there exist $\mathbf{G}_c$ and positive integers $I_1, \ldots, I_n$ such that the function

$$\mathbf{x} = \mathbf{G}_c\mathbf{b} - Q_{\Lambda_s}(\mathbf{G}_c\mathbf{b}) - \mathbf{d} \tag{3.7}$$

is a bijective mapping between the integers $b_i \in \{0, 1, \ldots, I_i - 1\}$, and the codebook $\mathbf{x} \in \mathcal{C}$. In other words, the encoding generates $\mathcal{C}$ exactly. The encoding operation (3.7) is abbreviated as $\mathbf{x} = \mathrm{enc}(\mathbf{b})$, while the inverse operation, called indexing operation is abbreviated as $\mathbf{b} = \mathrm{index}\,(\mathbf{x})$, and amounts to find the element of the set $\mathbf{x} + \Lambda_s$ inside the fundamental region, which is used for the encoding operation $\mathcal{P}(\Lambda_s)$. "Rectangular" emphasizes that each b_i is selected independently of the other integers, or in a less systematic method, the integer range b_i does not depend on the integers selected in other positions. Also, $I_i = 1$ implies that b_i encodes no information.

Additionally, if a rectangular encoding exists, i.e, if it is possible to find $I_1, \ldots, I_n$, such that the above definition holds, then, analysing equation (3.7), the term $\mathbf{G}_c\mathbf{b}, b_i \in \{0, \ldots, I_i\}$ is a set of coset representatives of the quotient group defined in (2.13), or a set of points of Λ_c inside a fundamental region of Λ_s, in particular, if $\mathbf{M}$ is diagonal, this fundamental region is the fundamental parallelotope of Λ_s. The term $Q_{\Lambda_s}(\mathbf{G}_c\mathbf{b})$ is responsible for finding the coset leaders of (2.13), given the coset representatives, which is done by performing the quantization operation defined in (2.4), or, in other words, to translate the points inside any fundamental region of Λ_s to its Voronoi region, remembering that any set of points of Λ_c inside any fundamental region of Λ_s is a set of coset representatives. Finally, the term $\mathbf{d}$ is responsible for the minimal average Voronoi constellation power.

As motivated in section 3.1, if $\mathbf{M}$ is diagonal, encoding is trivial because $I_i = M_i$. Also, we would not like to change the lattice basis $\mathbf{G}_c$ to accomplish a rectangular encoding. To that end, we now analyse the case where $\mathbf{M}$ is not diagonal. More specifically, $\mathbf{G}_c$ and $\mathbf{G}_s$ are both upper triangular or lower triangular matrices, in this case, rectangular encoding is always possible without changing

the lattice basis matrix.

3.2.1 Encoding and Indexing Triangular Matrices

Before formalizing encoding and indexing for triangular matrices, it will be useful to show the following. Let **G** be a triangular generator matrix for any lattice Λ and **P** be also a triangular matrix with the same diagonal elements of **G**:

$$\mathbf{G} = \begin{pmatrix} g_{11} & 0 & \dots & 0 \\ g_{21} & g_{22} & \dots & 0 \\ \vdots & & \ddots & \vdots \\ g_{n1} & g_{n2} & \dots & g_{nn} \end{pmatrix}, \tag{3.8}$$

$$\mathbf{P} = \begin{pmatrix} g_{11} & 0 & \dots & 0 \\ p_{21} & g_{22} & \dots & 0 \\ \vdots & & \ddots & \vdots \\ p_{n1} & p_{n2} & \dots & g_{nn} \end{pmatrix}, \tag{3.9}$$

here, **G** and **P** need to be both upper triangular or both lower triangular. The convention lower triangular is used. We can state that, the parallelotope $\mathcal{P}(\mathbf{P})$ is a fundamental region of the lattice Λ generated by the matrix **G**.

Proof: To verify that $\mathcal{P}(\mathbf{P})$ is a fundamental region of Λ we need to verify conditions 1 and 2 of equations (2.5) and (2.6). These two conditions imply the verification of the volume preserving of a fundamental region, i.e, $\det(\mathbf{G}) = \det(\mathbf{P})$, and to show that equation (2.10) has unique solution in **b** and **s**, where $\mathbf{b} \in \mathbb{Z}^n$ and $0 \leq s_i < 1$. The volume condition holds because both matrices are triangular with the same diagonal elements. For the unique solution, consider the triangular system for any $\mathbf{y} \in \mathbb{R}^n$,

$$\mathbf{y} = \mathbf{Gb} + \mathbf{Ps}. \tag{3.10}$$

The first row of (3.10) is

$$y_1 = g_{11}b_1 + g_{11}s_1, \tag{3.11}$$

and has unique solution, b_1 and s_1 are the integer and fractional parts of $\frac{y_1}{g_{11}}$, respectively. Row two is,

$$y_2 = g_{21}b_1 + g_{22}b_2 + p_{21}s_1 + g_{22}s_2, \tag{3.12}$$

and also has unique solution, b_2 and s_2 are the integer and fractional parts of $\frac{y_2 - g_{21}b_1 - p_{21}s_1}{g_{22}}$, respectively. This continues recursively so that all b_i and s_i for $i = 1, 2, \ldots, n$ have unique solutions, which concludes the proof. □

With the stated above, we can easily find a rectangular encoding for triangular matrices. For equation (2.12), in the case where **M** is diagonal, the basis of $\mathbf{G}_c$ are aligned with that of the fundamental parallelotope. But, as we already discussed, the coset representatives do not need to lie inside the fundamental parallelotope, but in any fundamental region Λ_s, this implies that, if we can find a diagonal matrix **D**, such that

$$\mathbf{P} = \mathbf{G}_c \cdot \mathbf{D} \tag{3.13}$$

is a fundamental region of Λ_s, then rectangular encoding exists and $I_i = d_i$. To verify this argument, it is sufficient to compare equation (3.1), with the parallelotope $\mathcal{P}(\mathbf{P}) = \mathcal{P}(\mathbf{G}_c \cdot \mathbf{D})$ and equation (3.2), and to verify the alignment between $\mathbf{G}_c$ and **P**. Thus, consider $\mathbf{G}_c$ and $\mathbf{G}_s$ given respectively by,

$$\mathbf{G}_c = \begin{pmatrix} g_{c_{11}} & 0 & \ldots & 0 \\ g_{c_{21}} & g_{c_{22}} & \ldots & 0 \\ \vdots & & \ddots & \vdots \\ g_{c_{n1}} & g_{c_{n2}} & \ldots & g_{c_{nn}} \end{pmatrix}, \quad \mathbf{G}_s = \begin{pmatrix} g_{s_{11}} & 0 & \ldots & 0 \\ g_{s_{21}} & g_{s_{22}} & \ldots & 0 \\ \vdots & & \ddots & \vdots \\ g_{s_{n1}} & g_{s_{n2}} & \ldots & g_{s_{nn}} \end{pmatrix}. \tag{3.14}$$

Note that $\mathbf{M} = \mathbf{G}_c^{-1} \cdot \mathbf{G}_s$ is a triangular matrix, with diagonal elements $M_{ii} = \frac{g_{s_{ii}}}{g_{c_{ii}}}$. Now, choose the matrix **D**, equal to,

$$\mathbf{D} = \begin{pmatrix} \frac{g_{s_{11}}}{g_{c_{11}}} & 0 & \ldots & 0 \\ 0 & \frac{g_{s_{22}}}{g_{c_{22}}} & \ldots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \ldots & \frac{g_{s_{nn}}}{g_{c_{nn}}} \end{pmatrix} = \begin{pmatrix} M_{11} & 0 & \ldots & 0 \\ 0 & M_{22} & \ldots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \ldots & M_{nn} \end{pmatrix}. \tag{3.15}$$

Finally, using (3.13), we have,

$$\mathbf{P} = \begin{pmatrix} g_{c_{11}} & 0 & \ldots & 0 \\ g_{c_{21}} & g_{c_{22}} & \ldots & 0 \\ \vdots & & \ddots & \vdots \\ g_{c_{n1}} & g_{c_{n2}} & \ldots & g_{c_{nn}} \end{pmatrix} \cdot \begin{pmatrix} \frac{g_{s_{11}}}{g_{c_{11}}} & 0 & \ldots & 0 \\ 0 & \frac{g_{s_{22}}}{g_{c_{22}}} & \ldots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \ldots & \frac{g_{s_{nn}}}{g_{c_{nn}}} \end{pmatrix} = \begin{pmatrix} g_{s_{11}} & 0 & \ldots & 0 \\ g_{c_{21}} & g_{s_{22}} & \ldots & 0 \\ \vdots & & \ddots & \vdots \\ g_{c_{n1}} & g_{c_{n2}} & \ldots & g_{s_{nn}} \end{pmatrix}, \tag{3.16}$$

and here, **P** is a fundamental region of Λ_s because it has the same diagonal elements of $\mathbf{G}_s$. Thus, we

conclude that, $\mathbf{G}_c$ and $\mathbf{D}$ form a rectangular encoding, and $I_i = M_{ii} = \frac{g_{s_{ii}}}{g_{c_{ii}}}$. In other words, if $\mathbf{G}_c$ and $\mathbf{G}_s$ are both upper or lower triangular, the set

$$\Lambda_c \cap \mathcal{P}(\mathbf{P}) = \{\mathbf{G}_c \cdot \mathbf{b} = b_1\mathbf{g}_1 + \cdots + b_n\mathbf{g}_n, b_i = 0, \ldots, M_{ii} - 1\} \tag{3.17}$$

is a complete set of coset representatives of the quotient group defined in (2.13), and of course, here $\frac{g_{s_{ii}}}{g_{c_{ii}}} \in \mathbb{Z}^n$ because $\mathbf{M}$ is an integer matrix.

Furthermore, note that, if $\mathbf{M}$ is diagonal, then rectangular encoding exists and the coset representatives lie inside the fundamental parallelotope $\mathcal{P}(\mathbf{G}_s)$. If $\mathbf{M}$ is not diagonal (here $\mathbf{M}$ is triangular), and $\mathbf{G}_c$ and $\mathbf{G}_s$ are both upper or lower triangular, then rectangular encoding exists and the coset representatives lie inside the parallelotope $\mathcal{P}(\mathbf{P})$. Of course, as diagonal matrices are a particular case of a triangular matrices, equation (3.17) is a general case of equation (3.3), because, it is straightforward to see that if $\mathbf{M}$ is diagonal, then $I_i = M_i = \frac{g_{s_{ji}}}{g_{c_{ji}}}$, for $j = 1, \ldots, i, \ldots, n$.

For triangular matrices, our Voronoi constellation is all the $\mathbf{x}$ obtained by applying equation (3.7), and with $\mathbf{G}_c\mathbf{b}$ satisfying equation (3.17). The indexing $\mathbf{b} = \text{index}\,(\mathbf{x})$, i.e, the process to obtain $\mathbf{b}$ from $\mathbf{x}$ is done as follows.

Firstly, we translate our point $\mathbf{x}$ in equation (3.7) by $\mathbf{d}$, obtaining $\mathbf{x} + \mathbf{d}$. Then, we multiply the obtained point by $\mathbf{G}_c^{-1}$, obtaining

$$\mathbf{b}' = \mathbf{G}_c^{-1}(\mathbf{x} + \mathbf{d}) = \mathbf{b} - \mathbf{G}_c^{-1}Q_{\Lambda_s}(\mathbf{G}_c\mathbf{b}). \tag{3.18}$$

Now, note that $Q_{\Lambda_s}(\mathbf{G}_c\mathbf{b})$ is a point of Λ_s by definition of quantization operation (2.4). Thus, it can be written as $\mathbf{G}_s \cdot \mathbf{z}$ for some $\mathbf{z} \in \mathbb{Z}^n$,

$$\mathbf{b}' = \mathbf{b} - \mathbf{G}_c^{-1}\mathbf{G}_s\mathbf{z} = \mathbf{b} - \mathbf{M}\mathbf{z}, \tag{3.19}$$

as the matrix $\mathbf{M}$, with elements M_{ij} for $i \geq j$, is triangular, this is a triangular system. The first row is,

$$b_1' = b_1 - M_{11}z_1. \tag{3.20}$$

Note that, from (3.17), $b_i \leq M_{ii} - 1$, so b_1 can be obtained as,

$$b_1 = b_1' \mod M_{11}, \tag{3.21}$$

and z_1 is then,

$$z_1 = \frac{b_1' - b_1}{M_{11}}. \tag{3.22}$$

Generalizing, the following lines $k = 2, \ldots, n$ is:

$$b'_k = b_k - \sum_{j=1}^{k-1} M_{kj} z_j - M_{kk} z_k, \tag{3.23}$$

which have solutions given by:

$$b_k = (b'_k + \sum_{j=1}^{k-1} M_{kj} z_j) \mod M_{kk}, \tag{3.24}$$

$$z_k = \frac{b_k - b'_k - \sum_{j=1}^{k-1} M_{kj} z_j}{M_{kk}}. \tag{3.25}$$

The above procedure computes the b_i one at a time, in sequence. This a standard and effective technique for triangular matrices. Finally, for easy of exposition during the rest of chapter 3 we consider the translation vector $\mathbf{d} = 0$.

3.2.2 Encoding the chain $\Lambda_s \subseteq \mathbf{K}\mathbb{Z}^n \subseteq \Lambda_c$.

We now turn our attention to a special case of nested lattice pairs, such that the chain $\Lambda_s \subseteq \mathbf{K}\mathbb{Z}^n \subseteq \Lambda_c$ is satisfied, for $\mathbf{K}$ a diagonal matrix. For these lattice families, we announce a theorem that gives an alternative method to compute a complete set of distinct coset representatives of the quotient group Λ_s/Λ_c. As we will see in the next section, when the coding lattice Λ_c is obtained from an error-correcting code, this theorem eliminates the requirement of a matrix multiplication for encoding lattices, providing reduced encoding complexity, in the sense that it never exceeds the encoding complexity of the underlying linear code used to construct Λ_c.

Theorem 1: Let Λ_s and Λ_c be any integer lattices satisfying the lattice chain $\Lambda_s \subseteq \mathbf{K}\mathbb{Z}^n \subseteq \Lambda_c$, for $\mathbf{K}$ a diagonal matrix with entries $k_i > 0$. Let $\mathbf{G}_s$ be a triangular generator matrix of Λ_s that is defined as

$$\mathbf{G}_s = \begin{pmatrix} g_{s_{1,1}} & 0 & \ldots & 0 \\ g_{s_{2,1}} & g_{s_{2,2}} & \ldots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ g_{s_{n,1}} & \ldots & g_{s_{n,n-1}} & g_{s_{n,n}} \end{pmatrix} \in \mathbb{Z}^{n \times n}. \tag{3.26}$$

Define a set $\mathcal{S}$ as the Cartesian product:

$$\mathcal{S} = \{0, \dots, \left|\frac{g_{s_{1,1}}}{k_1}\right| - 1\} \times \cdots \times \{0, \dots, \left|\frac{g_{s_{n,n}}}{k_n}\right| - 1\}.^{1} \tag{3.27}$$

Let $\mathcal{X} = \Lambda_c \cap \mathcal{P}(\mathbf{K})$ be the set of points of Λ_c in the parallelotope associated with $\mathbf{K}$, as defined in (2.9). Then, a complete set of coset representatives of the quotient group Λ_c/Λ_s is provided by

$$\mathcal{X} + \mathbf{K} \cdot \mathcal{S} = \{\mathbf{x} + \mathbf{K} \cdot \mathbf{s} \mid \mathbf{x} \in \mathcal{X}, \mathbf{s} \in \mathcal{S}\}. \tag{3.28}$$

Moreover, this set lies in the hyper-rectangle with sides $(|g_{s_{1,1}}|, \dots, |g_{s_{n,n}}|)$ from the origin.

Proof: A complete set of coset representatives of the quotient group Λ_c/Λ_s is the set of points of Λ_c inside any fundamental region of Λ_s Zamir [2014]. Thus, a complete set of coset representatives of $\Lambda_c/\mathbf{K}\mathbb{Z}^n$ is the set of points of Λ_c inside the fundamental parallelotope of $\mathbf{K}\mathbb{Z}^n$, which is the hyperrectangle $\mathcal{P}(\mathbf{K})$, with sides $(k_1, \dots, k_n)$. This is the set $\mathcal{X}$. According to section 3.2.1, a fundamental region of Λ_s is the hyperrectangle with sides $(g_{s_{1,1}}, \dots, g_{s_{n,n}})$. Thus, by the tiling property of fundamental regions (2.5), a complete set of coset representatives of $\mathbf{K}\mathbb{Z}^n/\Lambda_s$ can be written as $\mathbf{K}\mathcal{S}$, with $\mathcal{S}$ given in (3.27), because of the triviality of the lattice $\mathbf{K}\mathbb{Z}^n$. Finally, by Lemma 2, a complete set of coset representatives of the quotient group Λ_s/Λ_c is the sum of the coset representatives of the quotients $\Lambda_c/\mathbf{K}\mathbb{Z}^n$ and $\mathbf{K}\mathbb{Z}^n/\Lambda_s$, which is $\mathcal{X} + \mathbf{K}\mathcal{S}$ as stated in (3.28).

□

Theorem 1 provides an efficient way to explicitly construct a set of coset representatives for any integer lattices satisfying the chain $\Lambda_s \subseteq \mathbf{K}\mathbb{Z}^n \subseteq \Lambda_c$, for any diagonal matrix $\mathbf{K}$. It can be directly applied to near-ellipsoidal lattice codes (Ragot et al. [2003]) $\Lambda_c/\mathbf{K}\Lambda_c$, with $\mathbf{K}$ an integer diagonal matrix. In this case, the shaping lattice is an expansion per coordinate of the coding lattice, $\Lambda_s = \mathbf{K}\Lambda_c$ and the chain condition is naturally satisfied because $\Lambda_s = \mathbf{K}\Lambda_c \subseteq \mathbf{K}\mathbb{Z}^n \subseteq \Lambda_c$. Self-similar lattices codes $\Lambda_c/k\Lambda_c$ are a particular case of near-ellipsoidal lattices, with $\mathbf{K} = k\mathbf{I}$, in this case, the shaping lattice is an uniform expansion of the coding lattice, so the theorem can also be employed to them.

In general, for other lattices pairs and any diagonal matrix $\mathbf{K}$, a shaping lattice $\Lambda_s \subseteq \mathbf{K}\mathbb{Z}^n$ can be found by first choosing any integer lattice Λ', then computing $\Lambda_s = \mathbf{K}\Lambda'$. Since Λ' is integer, this ensures that $\mathbf{K}\Lambda' \subseteq \mathbf{K}\mathbb{Z}^n$. For some diagonal matrix $\mathbf{K}$, the condition $\mathbf{K}\mathbb{Z}^n \subseteq \Lambda_c$, can be easily satisfied if a coding lattice is obtained from an error correcting code, because Λ_c can be written as $\lambda_c = C + \mathbf{K}\mathbb{Z}^n$, which naturally satisfies the chain condition $\mathbf{K}\mathbb{Z}^n \subseteq \Lambda_c$. For construction-A and construction-D lattices, $\mathbf{K} = q\mathbf{I}$ and $\mathbf{K} = q^a\mathbf{I}$, respectively.

[1] Note that, $g_{s_{1,1}}/k_i$ is an integer value since $\Lambda_s \subseteq \mathbf{K}\mathbb{Z}^n$.

3.3 Encoding and Indexing for Lattices from Error Correcting Codes

As we have seen in section 3.2.1, finding a set of coset representatives requires a matrix multiplication (see equation 3.17). However, in this section we show that, if the underlying coding lattice Λ_c is a lattice obtained from an error-correcting code, and Λ_c and Λ_s are lattices satisfying the chain $\Lambda_s \subseteq \mathbf{K}\mathbb{Z}^n \subseteq \Lambda_c$ as in section 3.2.2, then, the matrix multiplication in (3.17) is unnecessary.

Note that the condition $\mathbf{K}\mathbb{Z}^n \subseteq \Lambda_c$ is always satisfied for lattices from codes. Indeed, for construction-A lattices, as stated in section 2.2, $q\mathbb{Z}^n \subseteq \Lambda_c$, while for construction-D lattices $q^a\mathbb{Z}^n \subseteq \Lambda_c$. This suggests that $\mathbf{K} = q\mathbf{I}_n$ and $\mathbf{K} = q^a\mathbf{I}_n$, respectively. In fact, this is a natural choice, but there is no need to restrict $\mathbf{K}$ to these values, given that the chain condition is satisfied for other values of this matrix. The choice of the shaping lattice, Λ_s, must satisfy the condition $\Lambda_s \subseteq \mathbf{K}\mathbb{Z}^n$, and can be obtained as described in section 3.2.2.

Now, consider the application of Theorem 1 in construction-D lattices, shown in Corollary 1.

Corollary 1: Construction-D Lattices: For construction D, shaping is normally done in the last level code, which implies $\mathbf{K} = q^a\mathbf{I}_n$. Let Λ' be any integer lattice with a triangular generator matrix **G**' with entries g'_{ij}. Choose $\Lambda_s = q^a\Lambda'$. Let $\Lambda_c = \sum_{i=0}^{a-1} q^i C_i + q^a\mathbb{Z}^n$ be a construction-D lattice. A complete set of coset representatives is:

$$\sum_{n=0}^{a-1} q^i C_i + q^a\mathcal{S} = \left\{ \sum_{n=0}^{a-1} q^i \mathbf{c}_i + q^a\mathbf{s} \mid \mathbf{c}_i \in C_i, \mathbf{s} \in \mathcal{S} \right\}, \tag{3.29}$$

with $\mathcal{S}$ given as:

$$\mathcal{S} = \{0, \ldots, g'_{1,1} - 1\} \times \cdots \times \{0, \ldots, g'_{n,n} - 1\}. \tag{3.30}$$

Proof: Applying theorem 1, a complete set of cosets are:

$$\begin{aligned} \mathcal{X} + q^a\mathcal{S} &= \left(\sum_{i=0}^{a-1} q^i C_i + q^a\mathbb{Z}^n \right) \mod q^a + q^a\mathcal{S} \\ &= \sum_{i=0}^{a-1} q^i C_i + q^a\mathcal{S} = \left\{ \sum_{n=0}^{a-1} q^i \mathbf{c}_i + q^a\mathbf{s} \right\}, \end{aligned} \tag{3.31}$$

By theorem 1, the set $\mathcal{S}$ is given by:

$$\begin{aligned}\mathcal{S} &= \{0,\ldots,\frac{q^a g'_{1,1}}{q^a}-1\}\times\cdots\times\{0,\ldots,\frac{q^a g'_{n,n}}{q^a}-1\}\\ &= \{0,\ldots,g'_{1,1}-1\}\times\cdots\times\{0,\ldots,g'_{n,n}-1\}.\end{aligned} \tag{3.32}$$

□

Note that, the matrix multiplication is unnecessary. Corollary 1 says that, for construction-D lattices, it is possible to identify the coset representatives looking just for the codewords of the underlying linear code C, and elements of the set $\mathcal{S}$, which determine the shaping lattice.

This result is easily extended for construction-A lattices:

Corollary 2: Construction-A Lattices: Let $\Lambda_c = C + q\mathbb{Z}^n$ be a construction-A lattice. A complete set of coset representatives is:

$$C + q\mathcal{S} = \{\mathbf{c} + q\mathbf{s} \mid \mathbf{c} \in C, \mathbf{s} \in \mathcal{S}\}. \tag{3.33}$$

Proof: It is sufficient to set $a = 1$ in equation (3.31) of corollary 1 and a construction-A lattice is obtained via construction-D lattice. □

Note that, the information is no longer provided by the information vector $\mathbf{b}$ as shown in section 3.2.1. In this case, information is given by the message vectors $\mathbf{u}_i$ and the vector $\mathbf{s}$, i.e, information is taken from $(\mathbf{u}_0,\ldots,\mathbf{u}_{a-1},\mathbf{s})$ for construction-D lattices and from $(\mathbf{u},\mathbf{s})$ for construction-A lattices. Also, note that, messages are taken from $\sum_{i=0}^{a-1} k_i + n$ coordinates for construction D and from $k+n$ for construction A, whereas the vector $\mathbf{b}$ has n-coordinates. An interpretation for corollary 1 and corollary 2 is to first apply a hypercube shaping in the coding lattice Λ_c, obtaining the set of codewords of the underlying code C, and then translating each point by points of the set $q^a\mathcal{S}$, obtaining the coset representatives of Λ_c/Λ_s. Moreover, from 3.2.1, these coset representatives lie inside the hyperrectangle with sides equal to the diagonal elements of the triangular generator matrix of Λ_s.

Based on Corollary 1, we show an alternative encoding and indexing procedure for lattices obtained from error-correcting codes. This alternative procedure has reduced encoding complexity, as the matrix multiplication $\mathbf{G}\cdot\mathbf{b}$ is unnecessary. We show this procedure for construction-D lattices, given that the extension to construction-A lattices is trivial as it can be obtained by setting $a = 1$.

As suggested by corollary 1, to find a coset representative we need to choose a codeword $\mathbf{c}_i$ of each code C_i, and an element of the set $\mathcal{S}$. Each codeword is obtained by encoding a message vector $\mathbf{u}_i \in \mathbb{Z}_q^{k_i}$. Then, each message $\mathbf{m}$ is chosen from the set $\mathcal{M} = \mathbb{Z}_q^{k_0}\times\mathbb{Z}_q^{k_1}\times\cdots\times Z_q^{k_{a-1}}\times\mathcal{S}$. An element of this set is of the form $\mathbf{m} = (\mathbf{u}_0,\mathbf{u}_1,\ldots,\mathbf{u}_{a-1},\mathbf{s})$, which has $\sum_{i=0}^{a-1} k_i + n$ coordinates.

The encoding procedure is done as follows:

1. Pick an element of the set $\mathcal{M}$.

2. Encode each element $\mathbf{u}_i$ in order to obtain $\mathbf{c}_i$.

3. Find the coset representative by computing:

$$\mathbf{x} = \sum_{i=0}^{a-1} q^i \mathbf{c}_i + q^a \mathbf{s}.$$

4. Find the element of the coset of **x** inside the Voronoi region of the shaping lattice Λ_s by performing modulo-Λ_s operation:

$$\mathbf{x}' = \mathbf{x} - Q_{\Lambda_s}(\mathbf{x}).$$

and as **x** and **x**' belong to the same coset, each coset representative corresponds to a different coset leader, which is a point inside the Voronoi region of Λ_s.

The inverse operation of encoding is called indexing or demapping. It obtains the message $\mathbf{m} = (\mathbf{u}_0, \mathbf{u}_1, \ldots, \mathbf{u}_{a-1}, \mathbf{s})$ given a Voronoi constellation point **x**'. The indexing procedure is done as follows:

1. Denote $\mathbf{r}_j = \sum_{i=0}^{j} q^i \mathbf{c}_i$, for $j = 1, \ldots, a-1$. So $\mathbf{r}_0 = \mathbf{c}_0, \mathbf{r}_1 = \mathbf{c}_0 + q\mathbf{c}_1, \ldots, \mathbf{r}_j, \ldots, \mathbf{r}_{a-1} = \sum_{i=0}^{a-1} q^i \mathbf{c}_i$. The point **x'** can be written as **x'** $= \mathbf{r}_{a-1} + q^a \mathbf{s} - Q_{\Lambda_s}(\mathbf{x})$, where **x** is a coset leader obtained at step 3 of the encoding procedure. Applying $\mod q$ operation to **x'** we obtain $\mathbf{r}_0 = \mathbf{c}_0$, and the codeword $\mathbf{c}_0$ is obtained. That is because $Q_{\Lambda_s}(\mathbf{x}) \in q^a \Lambda$' by definition. Applying $\mod q^2$ operation to **x**' we obtain $\mathbf{r}_1 = \mathbf{c}_0 + q\mathbf{c}_1$. As we already have $\mathbf{c}_0$, then $\mathbf{c}_1$ is obtained as $\mathbf{c}_1 = \frac{\mathbf{r}_1 - \mathbf{r}_0}{q}$. Generalizing, let $\mathbf{r}_{-1} = 0$, starting by $i = 1$ moving upwards to $i = 2, \ldots, a-1$, any codeword $\mathbf{c}_i$ is obtained as:

   - First, obtain $\mathbf{r}_i$ by performing $\mod q^{i+1}$ operation:

$$\mathbf{r}_i = \mathbf{x}' \mod q^{i+1}.$$

   - Second, obtain $\mathbf{c}_i$ by:

$$\mathbf{c}_i = \frac{\mathbf{r}_i - \mathbf{r}_{i-1}}{q^i}.$$

2. Obtain $\mathbf{u}_i$ by indexing each $\mathbf{c}_i \in C_i$. This step depends on code choice and how it was encoded.

3. Since we know each $\mathbf{c}_i \in C_i$ and **x'**, we can recover:

$$\mathbf{v} = \frac{\mathbf{x}' - \mathbf{r}_{a-1}}{q^a} = \mathbf{s} - \frac{1}{q^a} Q_{\Lambda_s}(\mathbf{x}) = \mathbf{s} - \mathbf{p} \in \mathbb{Z}^n.$$

Note that **v** can be written as **v = s - G'z** for some unknown $\mathbf{z} \in \mathbb{Z}^n$ because $\mathbf{p} = \frac{1}{q^a} Q_{\Lambda_s}(\mathbf{x}) \in \Lambda'$. This is a triangular system with unknown variables **s** and **z**. The first row is,

$$v_1 = s_1 - g'_{11} z_1. \tag{3.34}$$

Note that from (3.30), $s_i \leq g'_{ii} - 1$, so s_1 can be obtained as,

$$s_1 = v_1 \mod g'_{11}, \tag{3.35}$$

and z_1 is then,

$$z_1 = \frac{v_1 - s_1}{g_{11}}. \tag{3.36}$$

Generalizing, the following lines $k = 2, \ldots, n$ is:

$$v_k = s_k - \sum_{j=1}^{k-1} g'_{kj} z_j - g'_{kk} z_k, \tag{3.37}$$

which have solutions given by:

$$s_k = (v_k + \sum_{j=1}^{k-1} g'_{kj} z_j) \mod g'_{kk}, \tag{3.38}$$

$$z_k = \frac{s_k - v_k - \sum_{j=1}^{k-1} g'_{kj} z_j}{g'_{kk}}. \tag{3.39}$$

The above procedure computes s_i one at a time, in sequence. This a standard and effective technique for triangular matrices. Note the similarity between the step 3 with the indexing procedure for triangular matrices in section 3.2.1. In fact, steps 1 and 2, is the indexing of a standard multilevel code construction, with standard hypercube shaping (see Forney et al. [2000]), i.e the indexing of $\Lambda_c / q^a \mathbb{Z}^n$, while step 3 is the indexing procedure for Voronoi shaping, i.e the indexing of $q^a \mathbb{Z}^n / \Lambda_s$ (see Kurkoski [2018]).

Note that, as we are referring the construction by code formula as a construction-D lattice, this indexing procedure, followns the Forney's indexing of a standard multilevel code construction. How-

ever, if one choose to use construction D as in equation (2.29), a reencoding step is necessary for indexing this construction. See Matsumine et al. [2018] for details.

3.4 Complexity

The overall complexity of encoding Voronoi lattices codes, relies in the Voronoi shaping operation defined in (2.20). This operation is divided in two steps. The fist step is to find a complete set of coset representatives by performing the matrix multiplication $\mathbf{G}_c \cdot \mathbf{b}$. The second step relies in finding the shaping lattice point closest to the point $\mathbf{G}_c \cdot \mathbf{b}$, which is the result of the quantization operation $Q_{\Lambda_s}(\mathbf{G}_c \cdot \mathbf{b})$.

The overall complexity of a Voronoi shaping scheme is dominated by the quantization operation $Q_{\Lambda_s}(\mathbf{G}_c \cdot \mathbf{b})$ which is generally np-hard. However as discussed in section 2.3 (also see Ferdinand et al. [2016]), some low-dimensional shaping lattices, already provides shaping gains which is close to the maximum shaping gain of 1.53 dB, e.g, the Leech lattice Λ_{24}, which provides a nominal shaping gain of 1.03 dB in dimension 24. Thus we do not need to increase the dimension to much. If we keep small dimensions for shaping, the overall encoding complexity is no longer dominated by the quantization. Instead, its dominated by the matrix multiplication $\mathbf{G}_c \cdot \mathbf{b}$ which is generally proportional to n^2.

In contrast, with the proposed corollary 1 and corollary 2, which are particular applications of theorem 1, the coset representatives can be explicitly computed if the coding lattice, is a lattice obtained from an error-correcting code, e.g, construction-D or construction-A lattices. As showed in section 3.3 the matrix multiplication $\mathbf{G}_c \cdot \mathbf{b}$ is unnecessary and the complexity is dominated by the encoding of the underlying linear code C with is generally smaller than $O(n^2)$. In fact, if a linear code encoding strategy is adopted, the encoding complexity is linear in the block length.

Chapter 4

Construction and Implementation

In this chapter we discuss the practical aspects in the implementation of Voronoi constellations. We describe the construction of coding lattices based in error-correcting codes. More specifically, we focus in the utilization of spatially-coupled low-density parity-check (SC-LDPC) codes, as described in Vem et al. [2014], and extended Bose-Chaudhuri-Hocquenghem (BCH) codes, as described in Matsumine et al. [2018], to construct the coding lattice using the construction D. Other types of codes can be vastly found in the literature. As references, we cite Liu et al. [2018] and Yan and Ling [2012], which use polar codes combined with the construction D, Di Pietro and Boutros [2017] which uses LDPC codes, and Khodaiemehr et al. [2016] which uses QC-LDPC codes, both using a construction A.

We then focus in the construction of the shaping lattice using two good small-dimensional lattices, which have the best shaping gain among all lattices in their dimensions: the Gosset lattice (E_8), and the Leech lattice (Λ_{24}). All the implementation details are described, as well as a technique that matches the dimension of the coding lattice to the dimension of the shaping lattice.

The decoding techniques of the linear codes used to construct these lattices is described. Finally, we remember the reader that, the general encoding and indexing operation, for the lattice codes constructed in this chapter is described in chapter 3.

4.1 Shaping Lattice Design

In this section, we discuss the construction of the shaping lattice, the idea is to use low-dimensional lattices, which achieve good shaping gains in small dimensions, such those of figure 2.7. It is always possible to obtain a high-dimensional lattice with scaled copies of a low-dimensional one. In fact, an n-dimensional shaping lattice can be obtained from an n'-dimensional shaping lattice, with $n' < n$, as long as $l = n/n' \in \mathbb{Z}$. For this, it is sufficient to construct the generator matrix $\mathbf{G}'$ of the n-

dimensional shaping lattice as,

$$\mathbf{G}' = \begin{pmatrix} \alpha\mathbf{G}'_s & 0 & \dots & 0 \\ 0 & \alpha\mathbf{G}'_s & \dots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & \alpha\mathbf{G}'_s \end{pmatrix} \in \mathbb{Z}^{n\times n}, \tag{4.1}$$

where $\mathbf{G}'$ is the generator matrix of the lattice Λ' described in Theorem 1 (see section 3.2.2), and $\mathbf{G}'_s$ is the generator matrix of the low-dimensional shaping lattice in a triangular form, and α is a scaling factor. In this type of construction, the overall shaping gain is that of the low-dimensional lattice. More generally, the n-dimensional lattice is obtained as the Cartesian product of the n'-dimensional lattice, this is equivalent of applying the shaping operation l times in n' coordinates at a time.

Note that, $\mathbf{G}'_s$ is scaled by α for two reasons. First, it makes $\mathbf{G}'$ an integer matrix and consequently Λ_s an integer lattice as required in theorem 1. Second it allows us to change the information rate, by expanding the shaping region and consequently increasing the number of points of $\mathcal{C}$. Obviously, this expansion also increases the transmit power. Also, as mentioned, this type of construction reduces the quantization complexity of the Voronoi shaping operation given that it is reduced to l quantizations, each in dimension n', instead of one quantization in dimension n.

With this configuration, we can calculate the information rate R of our transmission system. Using equations (2.16) and (2.34). Firstly, the carnality of the quotient group is given by,

$$M = \frac{\mathrm{Vol}\,(\Lambda_s)}{\mathrm{Vol}\,(\Lambda_c)} = \frac{q^{an}\,\mathrm{Vol}\,\Gamma}{q^{an-\sum_{i=0}^{a-1} k_i}} = \alpha^n (\det \mathbf{G}_s)^l q^{\sum_{i=0}^{a-1} k_i}, \tag{4.2}$$

thus, using equations (2.32) and (2.40), the information rate of the Voronoi constellation is given by

$$R = \log_2 \alpha + \frac{1}{n'} \log_2(\det \mathbf{G}'_s) + R_c \log_2 q \ \text{ bits/dim}. \tag{4.3}$$

Based on Corollary 1 of section 3.3, the shaping lattice Λ_s will be constructed as $\Lambda_s = q^a\Lambda'$, which is equivalent of choosing the matrix $\mathbf{K} = q^a\mathbf{I}$. Also, given that Λ' is an integer lattice as it is scaled by the factor α. Thus, Λ_s and Λ_c are nested lattices, and satisfy the chain condition of Theorem 1, because,

$$\Lambda_s = q^a\Lambda' \subseteq q^a\mathbb{Z}^n \subseteq \Lambda_c \subseteq \mathbb{Z}^n. \tag{4.4}$$

4.1.1 Gosset Lattice (E_8)

The first low-dimensional shaping lattice which we will be considering is the so called Gosset Lattice or E_8 lattice. This lattice is an 8-dimensional lattice with one possible generator matrix given by:

$$\mathbf{G}_{E_8} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix} \in \mathbb{Z}^{8\times 8}. \tag{4.5}$$

Additionally, in dimension eight, the E_8 lattice has the greatest packing density, is the best-known quantizer Conway and Sloane [2013], and its dimension is low enough that quantization operation (2.4) is feasible.

Given the optimally of the E_8 lattice in its dimension, it also has the best shaping gain in dimension eight, which using the continuous approximation Forney and Ungerboeck [1998], is shown to be 0.65 dB, i.e, 0.88 dB from the optimal shaping gain of 1.53 dB. In section 4.4, we use this lattice to shape the coding lattice constructed using extended BCH codes.

4.1.2 Leech Lattice (Λ_{24})

The second low-dimensional shaping lattice is the so called Leech Lattice or Λ_{24}. This lattice is a 24-dimensional lattice, and its generator matrix in triangular form can be found in Conway and Sloane [2013]. An integer triangular version of this matrix, obtained by a multiplication by $2\sqrt{2}$, can be found in [Costa et al., 2017, p. 25], where the diagonal elements are given by: $(8, 4, 4, 4, 4, 4, 4, 2, 4, 4, 4, 2, 4, 2, 2, 2, 4, 2, 2, 2, 2, 2, 2, 1)$. This lattice has the greatest packing density, and is the best known quantizer in dimension 24, even considering non-lattice packings Costa et al. [2017].

In comparison with the E_8 lattice, this lattice is expected to have a better shaping gain, given its optimally in dimension 24 and the fact that we are increasing the dimension to 24. In fact, its shaping gain is equal to 1.03 dB, only 0.5 dB from the optimum shaping gain of 1.53 dB. Furthermore, in section 4.4, we use this lattice to shape the coding lattice constructed using SC-LDPC codes.

4.2 Coding Lattice Design

In this section, the construction of the coding lattice based on construction D is described. We start by constructing a 2-level construction-D lattice using two nested extended BCH codes. Then, we construct a 3 and 4-level construction-D lattices using nested SC-LDPC codes. The decoding of both codes are also described.

4.2.1 Extended BCH Codes Lattices

The BCH codes form a class of cyclic error-correcting codes that are constructed using polynomials over a binary finite field. Extended BCH codes are BCH codes with an additional parity check bit. The set of BCH codes with code parameters (n, k, d_{min}) can be found in numerous tables in the literature. The parameters are such that $n = 2^m - 1$, $n - k \leq mt$ and $d_{min} \geq 2t + 1$. Adding an additional parity check bit in a standard BCH codes, changes the dimension to $n+1$ and the minimum distance to $d_{min} + 1$ and it is called an extended BCH code.

This section describes the design of a 2-level nested extended BCH lattice code, where each codeword is obtained from a BCH code with an additional parity check bit. Remembering the construction-D levels a, and the definition of q-ary codes, we see that, as BCH codes are binary codes we have $q = 2$, and as we construct a 2-level construction-D $a = 2$. Additionally, our lattice is based in two extended BCH codes denoted by C_0 and C_1, such that $C_1 \subseteq C_0$, as required for the Construction D.

Despite of no efficient linear encoding strategies for cyclic codes, the motivation of use BCH codes is due to the superiority of these codes in comparison with several others, as pointed in the results shown in Matsumine et al. [2018]. We start by fixing the dimension of the BCH code in $n = 127$. As we have seen, ideally the lattice dimension n must go to infinity, but the lack of linear encoding strategies for BCH codes makes the growth of the dimension not feasible. This value of n allows a practical algorithm implementation of the code, which is sufficient to apply, and show the reduced complexity shaping scheme proposed in this thesis.

Here, minimum distance is used as a design criteria, we want to maximize the minimum distance of the lattice at the lowest cost in the total rate. From (2.38), if $\gamma = 1$, the minimum distance, for C_0 and C_1 are 4 and 16, respectively, while if $\gamma = 2$ the minimum distances are 2 and 8. As we want to maximize the minimum distance of the lattice, we set $\gamma = 1$, which implies $d_{min} = 4$ for C_0 and $d_{min} = 16$ for C_1. Note that, for primitive BCH codes, the minimum distance are odd values, this is the reason why we use extended BCH codes.

Thus, from primitive BCH code tables found in the literature, we select the BCH codes $(127, 120, 3)$ and $(127, 78, 15)$, which implies C_0 and C_1, respectively as $(128, 120, 4)$, with a code rate of $R_{c_1} =$

$128/120 = 0.9375$, and $(128, 78, 16)$ with a code rate of $R_{c_2} = 78/120 = 0.6094$. The code rate of the construction-D lattice is given by equation (2.32), i.e, $R_c = 1.54$.

The nested constraint ($C_1 \subseteq C_0$) must also be satisfied. For this purpose, a generator polynomial $g_i(x)$ of degree $n - k_i$ of the code C_i must satisfy $g_j(x) = g(x)g_i(x)$ for $j < i$, for $g_j(x)$ a generator polynomial of the code C_j. In this case $C_i \subseteq C_j$. In our case with $a = 2$ we have $g_0(x) = g(x)g_1(x)$. Finally, with $\mathbf{c}_0 \in C_0$, $\mathbf{c}_1 \in C_1$ and $\mathbf{z} \in \mathbb{Z}^n$, the coding lattice Λ_c is the set

$$\Lambda_c = \{\mathbf{c}_0 + 2\mathbf{c}_1 + 4\mathbf{z}\}. \tag{4.6}$$

Using equation (2.34), the volume of the constructed lattice is given by $\mathrm{Vol}\,(\Lambda_D)^{\frac{2}{128}} = 1.8741$. The VNR is then,

$$\text{VNR} = \frac{\mathrm{Vol}\,(\Lambda)^{\frac{2}{n}}}{2\pi e\sigma^2(P_e)} = \frac{0.1097}{\sigma^2}. \tag{4.7}$$

For generating the polynomial $g_1(x)$ and $g(x)$, the Matlab function "bchgenpoly" was used. This function returns the narrow-sense generator polynomial of a BCH code, and as mentioned $g_0(x)$ was obtained as the multiplication: $g_0(x) = g(x)g_1(x)$. Additionally, each codeword is obtained as $c_i(x) = g_i(x)u_i(x)$, where $u_i(x)$ is the polynomial of degree k_i with coefficients u_i over the binary field $\mathbb{F}_2^{k_i}$.

The encoding of the extended BCH codes constructed was performed via generator polynomials as described above. The lattice point **x'**, which is transmitted in the channel is obtained from equation (2.19), where **x** is obtained from equation (3.31). The point received is a noisy version of **x'**, which can be written as

$$\mathbf{y} = \mathbf{x}' + \mathbf{w}, \tag{4.8}$$

where **w** is the Gaussian noise added by the channel. Here $\mathbf{x} \in \Lambda_c \cap \mathcal{P}(q^a\mathbf{I})$, and $\mathbf{x}' \in \Lambda_c \cap \mathcal{V}(\Lambda_s)$, while $\mathbf{y} \in \mathbb{R}^n$, given the noisy characteristic of **w**. However, before decoding the channel output, we multiply $\mathbf{y} \in \mathbb{R}^n$ by a constant c:

$$c = \frac{\text{SNR}}{1 + \text{SNR}} = \frac{P}{P + \sigma^2}, \tag{4.9}$$

which is known as Wiener coefficient. The use of this factor is important for achieving the capacity using lattices, as explained in Forney Jr [2004]. Thus, what we actually decode is $c\mathbf{y}$, with c as in (4.9).

In order to find the point $\mathbf{x}' \in \Lambda_c$ closest to $c\mathbf{y}$, soft-input decoding of binary codes is used. Each

noisy level $\mathbf{y}_i$ is recovered from $c\mathbf{y}$ with the application of $\mod 2^i$ operation and the subtraction of the previous decoded levels. The modulo operation applies to the noise as well, and distance to $(0, 1)$ should be preserved. As pointed in Matsumine et al. [2018], the following "triangle function" preserves these distances, and performs the modulo 2^i operation as:

$$|(c\mathbf{y}_i + 1) \mod 2^i - 1|. \tag{4.10}$$

In our case, ordered statistics decoding (OSD) algorithm with order-l reprocessing is used as described in Fossorier and Lin [1995]. Also, as described in Matsumine et al. [2018], for our construction, order-4 reprocessing for code C_0 and order-1 reprocessing for code C_1 yield a performance close to the maximum likelihood decoding. However, we use a order-3 reprocessing for decoding C_0, this is because it achieves only slightly higher error-rate performance than that of order-4 reprocessing (see Matsumine et al. [2018]), and because of the reduced computational complexity.

We now assume an infinite constellation. This means that we do not have any power constraint in our system, and we can transmit any lattice point. We show the performance of the 2-level construction-D extended BCH lattice code. The unconstrained scenario performance is analysed in terms of the symbol-error rate (SER), and the word-error-rate (WER) as a function of the VNR parameter, which is a measure of the performance of the coding lattice, defined in (2.53).

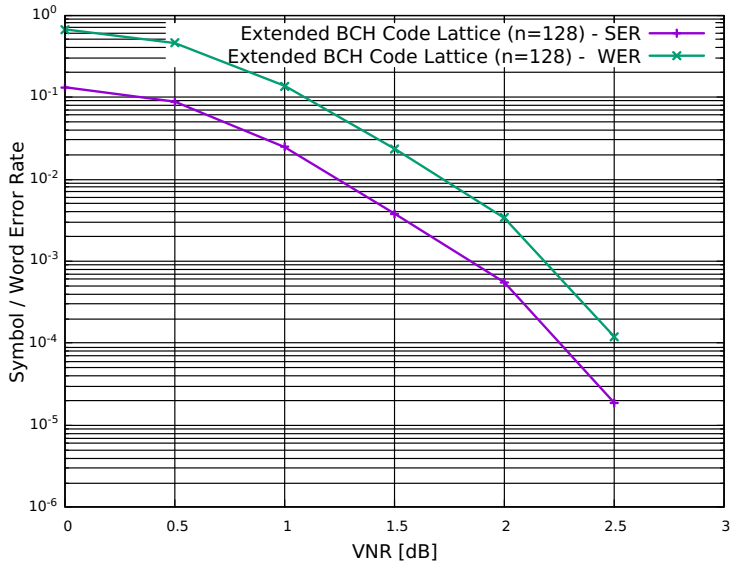


Figure 4.1: SER and WER performance of 2-level extended BCH code lattices with dimension n = 128 over AWGN channel without power constraint.

Figure 4.1 shows the symbol-error rate (SER) and word-error-rate (WER) as a function of VNR of our construction-D lattice. We define WER as the probability of detecting a lattice point, which is

different than the point transmitted. Analogously, we define the SER as the probability of error in any one of the n coordinates.

As pointed in Matsumine et al. [2018], for $n = 128$, a construction-D lattice with extended BCH code outperforms turbo lattices Sakzad et al. [2011], and LDLC lattices Sommer et al. [2008]. For more results in this type of construction, see Matsumine et al. [2018].

4.2.2 SC-LDPC Code Lattices

In this section, we propose a class of lattices constructed using Construction D, where the underlying linear codes are nested binary spatially-coupled low-density parity-check codes (SC-LDPC) codes. This construction is the same construction proposed by Vem et al. [2014].

The construction of SC-LDPC codes is done by coupling together a set of independent LDPC codes such that these codes are nested. In this construction, each independent LDPC code is regular, i.e, it has uniform left and right degrees. The focus of this chapter is on the construction of SC-LDPC codes, and then, the lattice associated with this code, which is obtained using the construction D. This section is based on chapter 4 of Vem [2017], which we invite the reader to consult for further details of the construction described.

We want to construct a set of $a-1$ LDPC codes C_i such that $C_0 \subseteq C_1 \subseteq \cdots \subseteq C_{a-1}$. To that end, we construct a Tanner Graph of the code C_{a-1} which we denote by $\mathcal{G}_{a-1}$. We then, obtain the Tanner Graphs $\mathcal{G}_i$ of the remaining codes by removing a fraction of the parity checks and the edges incident on these checks in a systematic fashion, in a way that $\mathcal{G}_i$ is also regular. Let denote the variable node degree of each code C_i by d_v^i and the check node degree by d_c, which is the same for all codes C_i given the construction described above. This construction generates a SC-LDPC code ensemble denoted by $(d_v^0, \ldots, d_v^{a-1}, d_c)$.

For any $d_v^i > 0$, the code rate of each individual code is given by:

$$R_{c_i} = 1 - \frac{d_v^i}{d_c}. \tag{4.11}$$

The construction is done as follows (this is a replication of Chap 4, section IV.B.1 of Vem [2017]): fix $M \in \mathbb{N}$, place Md_c variable nodes at each position in the range $[1:L] := \{1, 2, \ldots, L\}, L \in \mathbb{N}$ and Md_v^1 check nodes at each position in the range $[1 : L+w-1]$, where $w \in \mathbb{N}$ is coupling width. At each position divide the Md_v^0 check nodes into d_v^0 groups where each group contains M check nodes. At any position we refer to all check nodes belonging to k^{th} group as of type $\mathcal{T}_k$. This is equivalent to, at each position, Md_c edges coming from check nodes of type $\mathcal{T}_k$ for all $k \in [1 : d_v^0]$. Similarly, for each variable node, we arbitrarily classify the d_v^0 edges into types, where k^{th} edge is referred to as type $\mathcal{E}_k$ which equates to Md_c edges of each type at any position. For a fixed $k \in [1 : d_v^0]$, for all

$i \in [1 : L]$, each edge of type $\mathcal{E}_k$ at position i is assigned uniformly at random to a type $\mathcal{T}_k$ check node from positions $[i : i + w - 1]$. The main idea is that, for each $k \in [1 : d_v^0]$, if we consider the sub-graph containing only the type $\mathcal{T}_k$ check nodes and variable nodes with single edge (type $\mathcal{E}_k$ edges) the above mimics the construction of a $(1, d_c, L, w)$ ensemble on the sub-graph. This results in a Tanner graph in which every variable node has exactly one edge connected to type $\mathcal{T}_k$ check node, for all $k \in [1 : d_v^0]$. We call such a graph, a check-uniform connected graph and the proposed construction as (d_v^0, dc, L, w) check-uniform SC-LDPC (CU-SC-LDPC) ensemble of codes.

Choose a Tanner graph uniformly at random from the above described (d_v^0, dc, L, w) CU-SC-LDPC ensemble, call it $\mathcal{G}_0$. Observe that, removal of all check nodes of a particular type, say $\mathcal{T}_{d_v^0}$, from $\mathcal{G}_0$ results in a regular $(d_v^0 - 1, dc)$ Tanner graph. One can see that removal of all check nodes of types $\mathcal{T}_{d_v^1+1}, \mathcal{T}_{d_v^1+2}, \ldots, \mathcal{T}_{d_v^0}$ from $\mathcal{G}_0$ results in a graph from the (d_c, d_v^1, L, w) CU-SC-LDPC ensemble, which let's refer to as $\mathcal{G}_1$. More importantly, all the check-nodes in the derived graph $\mathcal{G}_1$ are also contained in $\mathcal{G}_0$ and hence any codeword satisfying all the check constraints in $\mathcal{G}_0$ also satisfies all the check constraints in $\mathcal{G}_1$. Thus we can say that the binary code C_0 defined by $\mathcal{G}_0$ is a sub-code of the binary code C_1 defined by $\mathcal{G}_1$. One can obtain a sequence of nested linear codes $C_0 \subseteq C_1 \subseteq \cdots \subseteq C_{a-1}$ by repeatedly performing the above operation. Given $(d_c, d_v^0, \ldots, d_v^{a-1})$, for each code C_0 from the (d_c, d_v^0, L, w) CU-SC-LDPC ensemble, we can obtain a nested sequence of codes $C_0 \subseteq C_1 \subseteq \cdots \subseteq C_{a-1}$ where $C_i \in (dc, d_v^i, L, w)$ CU-SC-LDPC ensemble. We call the proposed ensemble of nested sequences of codes as $(d_c, d_v^0, \ldots, d_v^{a-1}, L, w)$ CU-SC-LDPC ensemble.

For our construction, we use $d_c = 60$, $L = 72$, $w = 12$, $M = 47$, which yield a lattice code of dimension $n = 200000$. We use a construction D with $a = 3$ levels to construct the following two SC-LDPC lattice codes: $(26, 3, 3, 60)$ and $(35, 3, 3, 60)$ which using equation (4.11), yield a code rate $R_c = 2.47$ and $R_c = 2.32$, respectively. We also use a construction with $a = 4$ levels to construct the following codes: $(26, 3, 3, 3, 60)$ and $(35, 3, 3, 3, 60)$, which using equation (4.11), yield a code rate $R_c = 3.42$ and $R_c = 3.27$ respectively. Additionally, for decoding each codeword, we use belief propagation decoding. The simulation results for these type of lattices, and the construction described above is shown in section 4.4.2.

4.3 Quantization: Sphere Decoder Algorithm

Finding the nearest lattice point, i.e, performing the quantization operation (2.4), is performed by the Sphere Decoder Algorithm proposed in Viterbo and Boutros [1999]. Generally, this a np-hard problem, which is why we proposed a low-dimensional quantization (section 4.1), given that special low-dimensional shaping lattices already provide good shaping gain in their dimension (see sections 4.1.1 and 4.1.2).

As shown in Eq. (7) of Viterbo and Boutros [1999], the sphere decoder complexity can be polynomial in the block length if a special sequence of lattices is used. We invite the reader to see Viterbo and Boutros [1999] for a complete complexity analysis and implementation of the sphere decoder algorithm.

4.4 Simulation Results

In this section we combine the construction of the coding lattice and the shaping lattice to form a multidimensional constellations, which is the set of symbols that we can transmit over the channel.

In section 4.4.1, we use the E_8 lattice to shape the coding lattice constructed in section 4.2.1, whereas in section 4.4.2, we use the Leech lattice to shape the coding lattice constructed in 4.2.2.

In both cases, we analyse the performance of our system in comparison with the cubic shaping, and the complexity reduction provided by the use of the strategy described in section 3.2.2, i.e, when both lattices, Λ_c and Λ_s, satisfy the chain condition $\Lambda_s \subseteq \mathbf{K}\mathbb{Z}^n \subseteq \Lambda_c$.

4.4.1 Gosset Constellations of Extended BCH Lattice Codes

In this section we assume a finite constellation, limiting the points to be transmitted over the channel. The title of this section, relies on the fact that we use the E_8 lattice (section 4.1.1) for shaping, combined with the extended BCH code described in section 4.2.1, to construct the coding lattice.

As mentioned in section 4.2.1, we use a 2-level Construction D for our construction, so that, the results present in this section are obtained using Corollary 1 of section 3.3. Moreover, as discussed in section 3.4, the encoding complexity is reduced to the encoding complexity of the underlying linear code, and since we use polynomials to encode each codeword of our BCH code, the encoding complexity is $O((d_0 + d_1)n \log n)$ Roth and Seroussi [1988], where d_0 and d_1 are the minimum distances of each BCH code C_0 and C_1 (see section 4.2.1). This complexity is quasi-linear in the block length, whereas the standard matrix multiplication has polynomial complexity ($O(n^2)$).

Since we are using an extended BCH code with dimension $n = 128$, this strategy can be used with the Gosset lattice E_8, since 128 is a multiple of 8. Setting $\alpha = 2$ in equation (4.1), in order that the matrix $\mathbf{G}'$ be an integer lattice, as required by Corollary 1 of section 3.3, the shaping lattice is

$$\Lambda_s = q^a\Gamma = 4\Gamma. \tag{4.12}$$

Remembering the definition of the coding lattice (equation (4.6)), it is easy to note that Λ_s and Λ_c are nested and satisfy the requirements of Corollary 1 of section 3.3, because,

$$\Lambda_s = q^a\Gamma = 4\Gamma \subseteq q^a\mathbb{Z}^n = 4\mathbb{Z}^n \subseteq \Lambda_c. \tag{4.13}$$

From section 4.2.1, $R_c = (78 + 120)/128 = 1.54$ is the code rate of our extended 2-level BCH code. Now, using (4.3), the information rate is,

$$R = \log_2 2 + \frac{1}{8} \times \log_2 1 + 1.54 = 2.54 \text{ bits/dim}. \tag{4.14}$$

The average power per dimension can be obtained by the continuous approximation as in (2.52). From Forney [1989], its known that $\gamma_s(\mathbb{S}) = 1.163$ when $\mathbb{S}$ is the E_8 Voronoi region. As our shaping lattice is as in (4.12), and $\alpha = 2$, we have,

$$\text{Vol}\,\mathbb{S}^{2/n} = \text{Vol}(4\Gamma)^{2/n} = 4^n(\det \mathbf{T})^{2/n} = (8^n)^{2/n} = 64, \tag{4.15}$$

and the average power is,

$$P(\mathbb{S}) = \frac{64}{12 \times 1.163} = 4.5858. \tag{4.16}$$

As mentioned in section 2.4, the average value of the constellation, **d**, is subtracted from all the symbols before transmission, this is done to ensure minimal energy consumption (2.51). We estimated **d** taking the sample mean of 20,000 randomly generated symbols. The largest absolute value of the elements of this estimation was 0.07231, which is negligible compared to the entries of the lattice constellation. Therefore, $P(\mathbf{d}) \approx 0$ in (2.51), and we ignored this subtraction and transmitted the lattice constellation directly.

In order to verify the shaping gain of our system, we also design the same coding lattice shaped with an hypercube, which is nothing more than a coded M-PAM constellation. To that end, a generator matrix for a cubic lattice is the identity matrix $\mathbf{I}_n$. As before, $R_c = (78+120)/128 = 1.54$ is the code rate of our extended 2-level extended BCH code. To ensure the same information rate, we choose α in (4.3), so that both shaping lattices have the same volume, the code rate is then,

$$R = \log_2 2 + \frac{1}{128} \times \log_2 1 + 1.54 = 2.54 \text{ bits/dim}. \tag{4.17}$$

The shaping lattice is $\Lambda_s = 8\mathbf{I}$, yielding a hypercube shaping. The shaping operation in this case is trivial. Firstly, we reduce $\mod 8$ every transmitted point, yielding to the possible symbols $\{0, 1, 2, 3, 4, 5, 6, 7\}$. In order to put points inside Voronoi region of Λ_s, we subtract 4 from every coordinate obtaining the hypercube constellation with possible values $\{-4, -3, -2, -1, 0, 1, 2, 3\}$. To have the minimum average power, the average of all the possible transmitted points must be zero. To achieve this, we sum 0.5 to all points - this makes the constellation symmetric - to obtain the zero

average hypercube constellation, with possible values $\{\pm 0.5, \pm 1.5, \pm 2.5, \pm 3.5\}$. This is equivalent of translating the coding lattice from a vector **d** as in (2.51) with all entries equal to 0.5. This is a coded 8-PAM constellation. Since all coordinates are equally likely, in this case the average power is trivial to compute: $P(\mathbb{S}) = 5.25$.

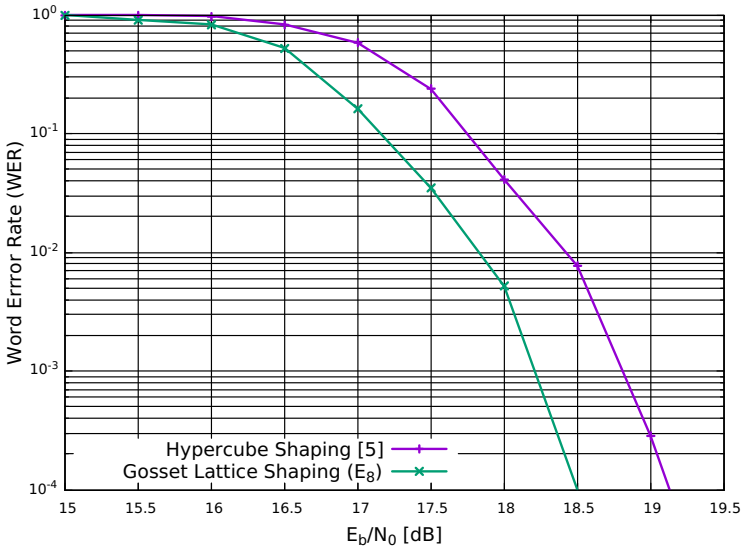


Figure 4.2: WER performance of 2-level extended BCH code lattices with dimension n = 128 over AWGN channel constrained by cubic lattice and E_8 lattice.

Figure 4.2 shows the performance of our system when shaping is performed with the E_8 and the Cubic lattices. We consider two-dimensional passband transmission, which means that we have a complex Gosset (E_8) constellation and a 64-QAM constellation. In comparison with the hypercube shaping, a gain of 0.63 dB is obtained for WER of 10^{-3} when using the E_8 to construct the shaping lattice. This value is close to the 0.65 dB, which verifies the theoretical shaping gain for the E_8 lattice Forney and Ungerboeck [1998]. This small difference is possibly due to the several approximations involved in the definition and computation of the theoretical shaping gain Forney and Ungerboeck [1998].

As discussed in section 2.3 and 2.4, the 1.53 dB of shaping gain is achieved when the inputs of the channel are Gaussian. Equivalently, when the shaping region is an n-dimensional hypersphere with $n \to \infty$. As mentioned, there are a set of lattices that, when increasing its dimension, the Voronoi region tends to an hypershpere when $n \to \infty$. To verify this, Figures 4.3 and 4.4, show the marginal distribution of the input symbols for the cubic and the E_8 lattice shaping respectively. As we can see, the E_8 lattice distribution starts to look as a Gaussian distribution, while as expected the cube is equivalent to a uniform distribution.

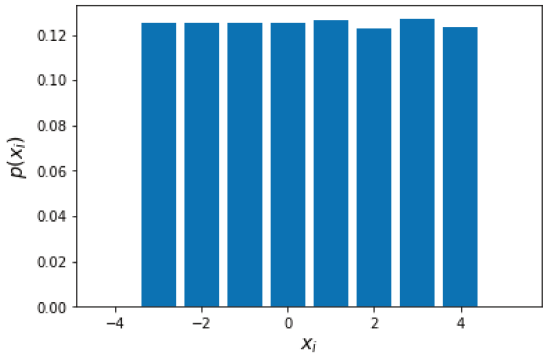


Figure 4.3: Symbol marginal distribution of cubic lattice shaping.

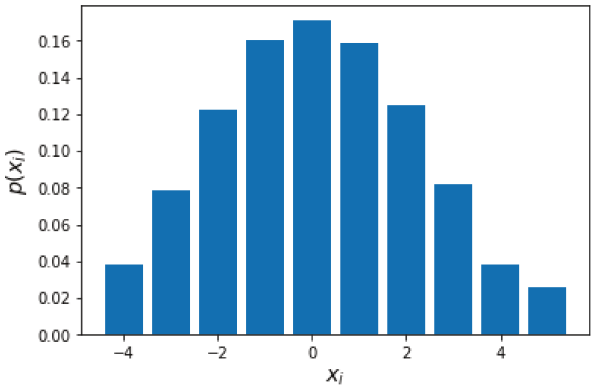


Figure 4.4: Symbol marginal distribution of E_8 lattice shaping.

4.4.2 Leech Constellations of SC-LDPC Lattice Codes

In this section we assume a finite constellation, limiting the points to be transmitted over the channel. The title of this section, relies on the fact that we use the Leech Lattice Λ_{24} (section 4.1.2) for shaping, combined with the SC-LDPC lattice design described in the last paragraph of section 4.2.2 to construct the coding lattice. In contrast with section 4.4.1, in this section we plot the achievable rates of our construction and not the performance.

The proposed strategy described in 3.2.2 is applied to the Construction-D lattice based on nested binary SC-LDPC proposed in Vem et al. [2014], and described in section 4.2.2. We now use $\mathbf{G}'_s$ as the unimodular Leech lattice Λ_{24} generator matrix, which has the greatest packing density, and is the best known quantizer in dimension 24 Conway and Sloane [2013]. We set $\alpha = \sqrt{8}$ in (4.1) to yield an integer shaping lattice as required by Corollary 1 of section 3.3. Using (4.3), we see that the Leech lattice achieves an additional rate of $\log_2 \sqrt{8} = 1.5$ bits/dim compared to the standard hypercube shaping obtained with $\mathbf{G}' = \mathbf{I}_n$. Since the Leech lattice provides a nominal shaping gain of 1.03 dB Di Pietro and Boutros [2017], and using (4.6) and (4.10) of Forney and Ungerboeck [1998],

we see that this extra rate comes at the cost of an additional transmit power of 8 dB ($10\log_{10} 8 - 1.03$ dB).

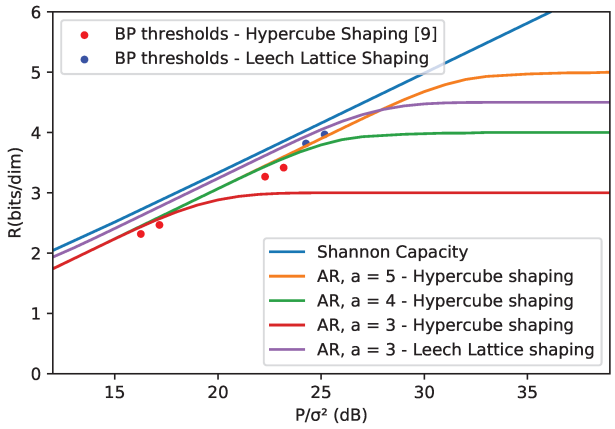


Figure 4.5: Achievable rates (AR) for Construction-D lattices obtained from SC-LDPC codes over the AWGN channel, with different number of levels and shaping regions.

Figure 4.5 shows the achievable rates (AR) for Construction-D lattices with hypercube shaping, with $a = 3, 4$ and 5 levels, these curves are also shown in 2.4. The figure also shows the achievable rate using the Leech lattice for 3 levels as a function of SNR, which is obtained by simulation. The SNRs required to successfully decode ten consecutive codewords using belief propagation (BP) are shown as BP thresholds for the same code designs and construction levels in Vem et al. [2014] (red dots), which is the same described in section 4.2.2. Our scheme is simulated for $R = 3.96$ and $R = 3.71$ bits/dim (blue dots), using the 3-level construction of section 4.2.2 (remember that the additional information rate of 1.5 bits/dim is due to the use of the Leech lattice). Note that shaping with the Leech lattice achieves a rate that is better than that achievable by any system with hypercube shaping.

As before, Corollary 1 of section 3.3 enables shaping with the Leech lattice while retaining the encoding complexity of the underlying LDPC code. For instance, an encoding complexity of $O(n)$ may be obtained with nested SC-LDPC codes that combine the construction strategies described in Vem et al. [2014] and Mitchell et al. [2015].

Chapter 5

Conclusions

Throughout this thesis we presented a general discussion on lattices applied in communications. We started with an introduction, clarifying how lattices is applied in the context of communications. In chapter 2 we presented general lattice definitions, as well as, how those definitions is related with some figures of merit of digital communications. In this chapter we also presented how to construct general lattice constellations, which is the title of this thesis. In chapter 3 we focus in some parts of the construction of Voronoi constellations described in chapter 2, which relies on the encoding and indexing procedure. Still in this chapter we presented the novelty of this work, which is an efficient way for encoding lattices obtained from error-correcting codes and multilevel code constructions. In chapter 4 we showed the potential of our method, which achieves reduced encoding complexity, as opposed to what is presented in the literature so far.

Moreover, a general method to identify a set of coset representatives and to construct Voronoi constellations was presented. The scheme is valid for all full rank lattices that satisfy the conditions of Theorem 1 of section 3.2.2. As mentioned, this scheme enables reduced encoding complexity for lattices obtained from codes. More specifically, the complexity of the encoding is reduced to that of the underlying error-correcting code used to construct the coding lattice. Additionally, our method was applied in chapter 4 to the SC-LDPC and BCH lattice codes. In all cases, reduced encoding complexities and shaping gains was obtained using the proposed Voronoi shaping scheme with good small dimensional lattices such as Λ_{24} and E_8 lattices.

For further works, one may note that, even if the focus of this thesis is for lattices packings, the utilization of the code formula shows that, our proposed theorem is valid for any multilevel code constructions, even if it is not a lattice. Thus, one may generalize these results for infinite constellations generated by codes (linear or not).

Another direction is to apply the shaping strategy to other types of lattices which are found in the literature. Another question that remains is, how to obtain efficient encoding for lattices obtained

from the original construction-D definition 2.29, given that, even with the application of our theorem, the matrix multiplication is still needed. In other words, to find if there is an efficient way to construct nested codes in equation 2.30, such that the codes are closed under the Schur product.

Bibliography

John R Barry, Edward A Lee, and David G Messerschmitt. *Digital communication*. Springer Science & Business Media, 2012.

John Horton Conway and Neil James Alexander Sloane. *Sphere packings, lattices and groups*, volume 290. Springer Science & Business Media, 2013.

Sueli IR Costa, Frédérique Oggier, Antonio Campello, Jean-Claude Belfiore, and Emanuele Viterbo. *Lattices Applied to Coding for Reliable and Secure Communications*. Springer, 2017.

Paulo Ricardo Branco da Silva and Danilo Silva. Multilevel LDPC lattices with efficient encoding and decoding and a generalization of construction D'. *IEEE Transactions on Information Theory*, 65(5):3246–3260, 2018.

Nicola Di Pietro and Joseph J Boutros. Leech constellations of construction-A lattices. *IEEE Transactions on Communications*, 65(11):4622–4631, 2017.

Uri Erez and Ram Zamir. Achieving 1/2 log (1+ SNR) on the AWGN channel with lattice encoding and decoding. *IEEE Transactions on Information Theory*, 50(10):2293–2314, 2004.

Nuwan S Ferdinand, Brian M Kurkoski, Matthew Nokleby, and Behnaam Aazhang. Low-dimensional shaping for high-dimensional lattice codes. *IEEE Transactions on Wireless Communications*, 15 (11):7405–7418, 2016.

G David Forney. Multidimensional constellations. ii. voronoi constellations. *IEEE Journal on Selected Areas in Communications*, 7(6):941–958, 1989.

G David Forney and Gottfried Ungerboeck. Modulation and coding for linear gaussian channels. *IEEE Transactions on Information Theory*, 44(6):2384–2415, 1998.

G David Forney and L-F Wei. Multidimensional constellations. i. introduction, figures of merit, and generalized cross constellations. *IEEE journal on selected areas in communications*, 7(6):877–892, 1989.

G David Forney, Mitchell D Trott, and Sae-Young Chung. Sphere-bound-achieving coset codes and multilevel coset codes. *IEEE Transactions on Information Theory*, 46(3):820–850, 2000.

G David Forney Jr. On the role of MMSE estimation in approaching the information-theoretic limits of linear gaussian channels: Shannon meets wiener. *arXiv preprint cs/0409053*, 2004.

Marc PC Fossorier and Shu Lin. Soft-decision decoding of linear block codes based on ordered statistics. *IEEE Transactions on Information Theory*, 41(5):1379–1396, 1995.

Hassan Khodaiemehr, Mohammad-Reza Sadeghi, and Amin Sakzad. Practical encoder and decoder for power constrained QC LDPC-lattice codes. *IEEE Transactions on Communications*, 65(2): 486–500, 2016.

Wittawat Kositwattanarerk and Frédérique Oggier. Connections between construction D and related constructions of lattices. *Designs, codes and cryptography*, 73(2):441–455, 2014.

Brian M Kurkoski. Encoding and indexing of lattice codes. *IEEE Transactions on Information Theory*, 64(9):6320–6332, 2018.

Ling Liu, Yanfei Yan, Cong Ling, and Xiaofu Wu. Construction of capacity-achieving lattice codes: Polar lattices. *IEEE Transactions on Communications*, 67(2):915–928, 2018.

Toshiki Matsumine, Brian M Kurkoski, and Hideki Ochiai. Construction D lattice decoding and its application to BCH code lattices. In *2018 IEEE Global Communications Conference (GLOBECOM)*, pages 1–6. IEEE, 2018.

David GM Mitchell, Michael Lentmaier, and Daniel J Costello. Spatially coupled LDPC codes constructed from protographs. *IEEE Transactions on Information Theory*, 61(9):4866–4889, 2015.

Or Ordentlich and Uri Erez. A simple proof for the existence of "good" pairs of nested lattices. *IEEE Transactions on Information Theory*, 62(8):4439–4453, 2016.

Gregory Poltyrev. On coding without restrictions for the AWGN channel. *IEEE Transactions on Information Theory*, 40(2):409–417, 1994.

Stéphane Ragot, Minjie Xie, and Roch Lefebvre. Near-ellipsoidal voronoi coding. *IEEE Transactions on Information Theory*, 49(7):1815–1820, 2003.

Ron M Roth and Gadiel Seroussi. Encoding and decoding of BCH codes using light and short codewords. *IEEE transactions on information theory*, 34(3):593–596, 1988.

Amin Sakzad, Mohammad-Reza Sadeghi, and Daniel Panario. Turbo lattices: Construction and error decoding performance. *arXiv preprint arXiv:1108.1873*, 2011.

Naftali Sommer, Meir Feder, and Ofir Shalvi. Low-density lattice codes. *IEEE Transactions on Information Theory*, 54(4):1561–1585, 2008.

Avinash Vem. *Applications of Coding Theory to Massive Multiple Access and Big Data Problems*. PhD thesis, 2017.

Avinash Vem, Yu-Chih Huang, Krishna R Narayanan, and Henry D Pfister. Multilevel lattices based on spatially-coupled LDPC codes with applications. In *2014 IEEE International Symposium on Information Theory*, pages 2336–2340. IEEE, 2014.

Emanuele Viterbo and Joseph Boutros. A universal lattice code decoder for fading channels. *IEEE Transactions on Information theory*, 45(5):1639–1642, 1999.

Yanfei Yan and Cong Ling. A construction of lattices from polar codes. In *2012 IEEE Information Theory Workshop*, pages 124–128. IEEE, 2012.

Ram Zamir. *Lattice Coding for Signals and Networks: A Structured Coding Approach to Quantization, Modulation, and Multiuser Information Theory*. Cambridge University Press, 2014.