UNIVERSIDADE ESTADUAL DE CAMPINAS

Instituto de Matemática, Estatística e Computação Científica

MAIARA FRANCINE BOLLAUF

Lattices for Communication Problems

Reticulados em Problemas de Comunicação

Campinas

2018

Maiara Francine Bollauf

Lattices for Communication Problems

Reticulados em Problemas de Comunicação

Tese apresentada ao Instituto de Matemática, Estatística e Computação Científica da Universidade Estadual de Campinas como parte dos requisitos exigidos para a obtenção do título de Doutora em Matemática Aplicada.

Thesis presented to the Institute of Mathematics, Statistics and Scientific Computing of the University of Campinas in partial fulfillment of the requirements for the degree of Doctor in Applied Mathematics.

Supervisor: Sueli Irene Rodrigues Costa

Co-supervisor: Vinay Anant Vaishampayan

Este exemplar corresponde à versão final da Tese defendida pela aluna Maiara Francine Bollauf e orientada pela Profa. Dra. Sueli Irene Rodrigues Costa.

Campinas

2018

Agência(s) de fomento e nº(s) de processo(s): CNPq, 140797/2017-3; CAPES

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca do Instituto de Matemática, Estatística e Computação Científica
Márcia Pillon D'Aloia - CRB 8/5180

B638L

Bollauf, Maiara Francine, 1991-
Lattices for communication problems / Maiara Francine Bollauf. – Campinas, SP : [s.n.], 2018.

Orientador: Sueli Irene Rodrigues Costa.
Coorientador: Vinay Anant Vaishampayan.
Tese (doutorado) – Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Teoria dos reticulados. 2. Códigos corretores de erros (Teoria da informação). 3. Teoria da informação em matemática. 4. Sistemas distribuídos. I. Costa, Sueli Irene Rodrigues. II. Vaishampayan, Vinay Anant. III. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. IV. Título.

Informações para Biblioteca Digital

Título em outro idioma: Reticulados em problemas de comunicação
Palavras-chave em inglês:
Lattice theory
Error-correcting codes (Information theory)
Information theory in mathematics
Distributed systems
Área de concentração: Matemática Aplicada
Titulação: Doutora em Matemática Aplicada
Banca examinadora:
Sueli Irene Rodrigues Costa [Orientador]
João Eloir Strapasson
Giuliano Gadioli La Guardia
Antonio Aparecido de Andrade
Antonio Carlos de Andrade Campello Junior
Data de defesa: 20-07-2018
Programa de Pós-Graduação: Matemática Aplicada

Tese de Doutorado defendida em 20 de julho de 2018 e aprovada pela banca examinadora composta pelos Profs. Drs.

Prof(a). Dr(a). SUELI IRENE RODRIGUES COSTA

Prof(a). Dr(a). JOÃO ELOIR STRAPASSON

Prof(a). Dr(a). GIULIANO GADIOLI LA GUARDIA

Prof(a). Dr(a). ANTONIO APARECIDO DE ANDRADE

Prof(a). Dr(a). ANTONIO CARLOS DE ANDRADE CAMPELLO JUNIOR

As respectivas assinaturas dos membros encontram-se na Ata de defesa

Acknowledgements

Firstly, I am grateful to God for the health and bless that were necessary to complete this thesis.

I would like to express my sincere gratitude to my parents Marisa and Rogério, and also to my brother Rodrigo, for the endless support through this four years of dedication.

Besides my family, I would like to thank my supervisor Prof. Sueli Costa for her patience, motivation and wisdom to guide this work.

I was also very fortunate to have two extraordinary persons who were essential to the development of this work. I acknowledge here my truly thanks for all their support. Prof. Vinay Vaishampayan hosted me for six months at City University of New York and made me see the theory with practical eyes; he believed in me and made me feel home when I was far away from it. Prof. Ram Zamir met me in the beginning of my PhD and from that moment we started a long-distance collaboration Brazil-Israel; I will bring with me forever his teaching about research, academic life and enthusiasm in doing what you love.

I would like to thank my thesis committee: Prof. João Strapasson, Prof. Giuliano La Guardia, Prof. Antonio de Andrade and Prof. Antonio Campello, for their insightful comments and careful reading.

I thank my partner in life, Samuel, for his care, strength and for supporting me every single moment of this daily choice.

Also I thank my labmates at UNICAMP and friends that I have brought from Santa Catarina, friends that I have made in São Paulo and friends from abroad (in special, to ones at 41 Fort Place).

Last but not the least, I would like to thank Capes, CNPq and FAPESP for the financial support.

“Things evolve, and then you look back at a character,
and it’s completely different from your first impression.
You have to spend some energy to see the beauty of math."

(Maryam Mirzakhani – Quanta Magazine, August 2014)

Resumo

O estudo de códigos no contexto de reticulados e outras constelações discretas para aplicações em comunicações é um tópico de interesse na área de teoria da informação. Certas construções de reticulados, como é o caso das Construções A e D, e de outras constelações que não são reticulados, como a Construção C, são utilizadas na decodificação multi-estágio e para quantização vetorial eficiente. Isso motiva a primeira contribuição deste trabalho, que consiste em investigar características da Construção C e propor uma nova construção baseada em códigos lineares, que chamamos de Construção $C^{\star}$, analisando suas propriedades (condições para ser reticulado, uniformidade geométrica e distância mínima) e relação com a Construção C. Problemas na área de comunicações envolvendo reticulados podem ser computacionalmente difíceis à medida que a dimensão aumenta, como é o caso de, dado um vetor no espaço real $n-$dimensional, determinar o ponto do reticulado mais próximo a este. A segunda contribuição deste trabalho é a análise desse problema restrito a um sistema distribuído, ou seja, onde o vetor a ser decodificado possui cada uma de suas coordenadas disponíveis em um nó distinto desse sistema. Nessa investigação, encontramos uma solução aproximada para duas e três dimensões considerando a partição de Babai e também estudamos o custo de comunicação envolvido.

Palavras-chave: Teoria dos reticulados. Códigos corretores de erros (Teoria da Informação). Teoria da informação em matemática. Sistemas distribuídos.

Abstract

The study of codes in the context of lattices and other discrete constellations for applications in communications is a topic of interest in the area of information theory. Some lattice constructions, such as the known Constructions A and D, and other special nonlattice constellations, as Construction C, are used in multi-stage decoding and efficient vector quantization. This motivates the first contribution of this work, which is to investigate characteristics of Construction C and to propose a new construction based on linear codes that we called Construction $C^{\star}$, analyzing its properties (latticeness, geometric uniformity and minimum distance) and relations with Construction C. Communication problems related to lattices can be computationally hard when the dimension increases, as it is the case of, given a real vector in the $n-$dimensional space, determine the closest lattice point to it. The second contribution of this work is the analysis of this problem restricted to a distributed system, i.e., where the vector to be decoded has each coordinate available in a separated node in this system. In this investigation, we find the approximate solution for two and three dimensions considering the Babai partition and study the communication cost involved.

Keywords: Lattices theory. Error correcting codes (Information theory). Information theory in mathematics. Distributed systems.

List of Figures

List of Tables

Contents

Introduction

"How do you best improve information transmission over a noisy channel?" This question proposed by Claude Shannon was just the first among a lot questions that contributes to the development of the information theory since his 1948 seminal paper [46], where he established a common basis to everything that communicates.

This approach is still present in the recent progress regarding to transmission, storage and security of information. Information theory studies mathematical notions and methods to guarantee the transmission of a message through a system with minimum losses.

The contributions of this work are related to two special communication problems: coding and quantization. The former is the act of converting a message into a symbol for a reliable transmission and the latter is the process of constraining an input from a large set of values to a discrete set, in order to simplify and make the communication feasible.

In the approaches presented here we have used a mathematical geometric structure called *lattice*, which is defined as an additive discrete subgroup of $\mathbb{R}^n$ and can be geometrically seen as a special periodic discrete arrangement of points in the $n-$dimensional space. Problems of interest involve lattices, such as its use to achieve low transmission error in the additive white Gaussian noisy (AWGN) channel [18] and the application of hard problems related to lattices to ensure the security of systems.

Lattices are commonly associated with linear codes in a lot of applications [56] and in our context, it is interesting to mention the lattice Constructions A and D. Construction A is used to obtain the checkerboard lattice D_n, the lattice E_7 [18, pp. 138] and also the body-centered cubic lattice (BCC), while Construction D is used for describing the Barnes-Wall lattice in dimension 16 [18, pp. 234].

In the scope of nonlattice periodic constellations construced from linear codes lies Construction C (or Forney's multilevel code formula [22, 23]), whose multi-stage decoding can achieve the high SNR uniform-input capacity of an AWGN channel asymptotically as the dimension n goes to infinity [25]. Two contributions of this thesis are related to this special construction: an alternative proof for the geometric uniformity of a $2-$level Construction C, counterexamples showing that this property does not hold for $L \geqslant 3$ and the proposal and detailed analysis of a construction which is a subset of Construction C, which we called Construction $C^{\star}$.

The use of lattices to assure security of modern systems are based in hard problems such as, given a real vector in the $n-$dimensional space, to find the closest lattice point to it (known as the closest lattice point problem) or to search for the lattice point with the minimum norm (known as the shortest vector problem). These two problems are NP-complete [21] and NP-hard [4], respectively and algorithms to approximate them are widely studied [2, 26].

In this work we investigate the closest lattice point problem regarding communication cost for a reliable transmission under a certain constrain. In general, in the literature, it is assumed that the vector components are available at the same location of a given system. We consider here the situation where the vector components are available at physically separated nodes (as antennas or devices, for example) of a centralized (with the presence of a fusion center) or interactive system (without a fusion center) and we are interested in the communication cost of exchanging this information in order to determine the closest lattice point.

This PhD thesis is structured in the following way: Chapter 1 is devoted to basic concepts related to codes and lattices, such as a detailed description of known constructions of lattices and nonlattice constellations using codes (Constructions A, C and D), a characterization of the communication problems to be explored in this work and special lattice bases such as Minkowski and obtuse superbase.

In Chapter 2, we mainly recall established properties of Construction C, present different ways of producing general geometrically uniform constellations and as a consequence of that, it follows an alternative proof for the geometric uniformity of a $L = 2$ Construction C. We also present counterexamples showing that for $L \geqslant 3$, Construction C does not always have equi-distance spectrum, so it cannot be geometrically uniform.

In Chapter 3, we define a new construction, called Construction $C^{\star}$, and study its characteristics, such as geometric uniformity, latticeness, minimum distance and comparisons with the associated Construction C. Finally, we compare a hybrid Construction $C^{\star}/C$ with Construction C for Gilbert-Varshamov achieving codes, pointing out potential advantages of the first one.

In Chapter 4, we address the problem of solving the closest lattice point problem in a distributed system, present a closed formula to compute the error probability based on a Babai partition for the two dimensional case and computationally estimate bounds for the same scenario in the three dimensional case. We also analyze the cost involved to reproduce the Babai partition in both centralized and interactive models.

To conclude, in Chapter 5 we summarize the contributions of this PhD thesis and present our perspectives for future works.

Chapter 1

Introductory concepts and properties

We start with fundamental concepts and properties that are essential to the development of this work. The main objects involved here are periodic discrete constellations in the $n-$dimensional Euclidean space, particularly lattices, which have been widely applied to several problems in information theory and cryptography. In the scope of these problems, we can mention lattice quantization [8] and multi-stage decoding [25], which will be explored with details in the next chapters. Lattices and other constellations constructions are associated to linear codes introduced next. This chapter is mainly based on [18], [20], [26] and [55].

1.1 Linear codes

We consider the binary field $\mathbb{F}_2 = \{0, 1\}$, with the standard modulo two operations. A binary code of length n is a subset of $\mathbb{F}_2^n$. For most results in this work the codes will be required to be linear.

Definition 1. *(Linear binary code) A linear binary code $\mathcal{C}$ of length n and rank k is a vector subspace of $\mathbb{F}_2^n$ with dimension k.*

A linear binary code of length n and rank k has 2^k elements (codewords) and can be given either as the image of a linear map $\phi : \mathbb{F}_2^k \to \mathbb{F}_2^n$, where $\phi(a_1, \dots, a_k) = G(a_1, \dots, a_k)^T$ or the kernel of a linear map $\psi : \mathbb{F}_2^n \to \mathbb{F}_2^{n-k}$, where $\psi(y_1, \dots, y_n) = H(y_1, \dots, y_n)^T$, $G \in \mathbb{F}_2^{n \times k}$ and$H \in \mathbb{F}_2^{n \times n-k}$ are binary matrices.

The matrix G is called a *generator matrix* and the matrix H is called *parity check matrix* of the linear code $\mathcal{C}$, since has the property to detect if an element $c \in \mathbb{F}_2^n$ is a codeword of $\mathcal{C}$, i.e.,

$$Hc^T = 0 \in \mathbb{F}_2^{n-k} \Leftrightarrow c \in \mathcal{C} \subset \mathbb{F}_2^n. \tag{1.1}$$

The Hamming distance counts the number of different coordinates between two distinct elements in $\mathbb{F}_2^n$:

Definition 2. *(Hamming distance) The Hamming distance between two elements* $x = (x_1, \dots, x_n), y = (y_1, \dots, y_n) \in \mathbb{F}_2^n$ *is defined as*

$$d_H(x, y) \;=\; |\{i : x_i \neq y_i, 1 \leqslant i \leqslant n\}|. \tag{1.2}$$

Definition 3. *(Minimum distance of a code* $\mathcal{C}$*) The minimum distance of a code* $\mathcal{C}$ *is the minimum Hamming distance between all distinct codewords, i.e.,*

$$d_{min}(\mathcal{C}) = \min\{d_H(x, y) : x, y \in \mathcal{C}, x \neq y\}. \tag{1.3}$$

Since a translation in $\mathbb{F}_2^n$ is an isometry, when the Hamming distance is considered, it follows that, if $\mathcal{C}$ is a linear code

$$d_{min}(\mathcal{C}) = \min\{d_H(0, c), c \in \mathcal{C}\}. \tag{1.4}$$

The distance $d_H(0, c)$ is also called the *Hamming weight* of the codeword c.

A linear code of length n, rank k and with minimum distance $d = d_{min}(\mathcal{C})$ is said to be an $[n, k, d]-$code.

Definition 4. *(Rate) The rate of an* $[n, k, d]-$*linear code* $\mathcal{C}$ *is*

$$R = \frac{1}{n}\log_2 2^k = \frac{k}{n}\log_2 2 = \frac{k}{n} \textit{ bits/symbol.} \tag{1.5}$$

1.2 Lattices

1.2.1 Definitions and properties

Definition 5. *(Lattice) A lattice* $\Lambda \subset \mathbb{R}^N$ *is a set of all integer linear combinations of a set of* n *linearly independent vectors* $\beta = \{v_1, v_2, \dots, v_n\} \in \mathbb{R}^N$ *(*β *is called lattice basis of* Λ*), i.e.,*

$$\Lambda = \{a_1 v_1 + a_2 v_2 + \cdots + a_n v_n,\; a_i \in \mathbb{Z},\; i = 1, \dots, n\}. \tag{1.6}$$

It can be shown that $\Lambda \subseteq \mathbb{R}^N$ is a lattice if and only if it is a discrete additive subgroup of $\mathbb{R}^N$ [40, pp. 24-25].

Definition 6. *(Generator matrix of a lattice* Λ*) A matrix* $V \in \mathbb{R}^{N\times n}$*, whose columns are basis vectors of a lattice* Λ *is called a generator matrix. In this case,*

$$\Lambda = \{Vu, u \in \mathbb{Z}^{n\times 1}\}. \tag{1.7}$$

Example 1. *Given a basis* $\beta = \{(1, 0), (1/2, \sqrt{3}/2)\}$*, the integer linear combinations of these basis vectors is the well known* A_2 *lattice [18] (illustrated in Figure 1), whose generator matrix is*

$$V = \begin{pmatrix} 1 & 1/2 \\ 0 & \sqrt{3}/2 \end{pmatrix}. \tag{1.8}$$

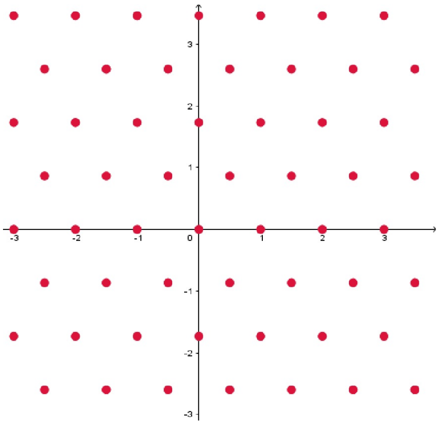

Figure 1 – A_2 lattice.

Two matrices V_1 and V_2 of order $N \times n$ and rank n are generator matrices of the same lattice if and only if $V_1 = V_2 \cdot U$, where U is an unimodular matrix (it has integer entries and $det(U) = \pm 1$).

Definition 7. *(Gram matrix) A Gram matrix of a lattice Λ is $A = V^T V$, where V is a generator matrix of Λ.*

Note that a Gram matrix is symmetric (for a lattice basis $\beta = \{v_1, v_2, ...v_n\}$, $A_{i,j} = \langle v_i, v_j \rangle$) and its determinant is independent of the basis choice for the lattice, since for two generator matrices V_1 and V_2 of Λ, $det(\Lambda) = det(V_1^T V_1) = det(U^T V_2^T V_2 U) = det(V_2^T V_2) > 0$.

Definition 8. *(Volume) The volume of a lattice Λ is $vol(\Lambda) = det(\Lambda)^{1/2} = (det(V^T V))^{1/2}$, where V is any generator matrix of Λ.*

We say a lattice is full rank if $n = N$. In this work **we only consider full rank lattices**. For a full rank lattice Λ, with a generator matrix V, $vol(\Lambda) = |det(V)|$.

To measure distances between points in a constellation[1] in $\mathbb{R}^n$ we use the standard Euclidean distance:

Definition 9. *(Euclidean distance) The Euclidean distance between two points $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n) \in \mathbb{R}^n$ is defined as*

$$d_E(x, y) \quad = \quad ||x - y|| = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2}. \tag{1.9}$$

Definition 10. *(Minimum distance of a constellation Γ) For a constellation $\Gamma \subseteq \mathbb{R}^n$, the minimum distance is defined as*

$$d_{min}(\Gamma) = \inf\{||x - y|| : x, y \in \Gamma, x \neq y\}. \tag{1.10}$$

[1] A constellation is a discrete set of points in $\mathbb{R}^n$.

For a lattice $\Lambda \subseteq \mathbb{R}^n$, we also have $d_{min} = \min\{d(x, 0) : x \in \Lambda\}$.

There exist some important lattice characteristics, such as Voronoi region, kissing number and geometric uniformity.

Definition 11. *(Fundamental region) A set $\mathcal{F}$ is called a fundamental region of a lattice Λ if all its translations $x + \mathcal{F} = \{x + y : y \in \mathcal{F}\}$, over all $x \in \Lambda$, define a partition*[2] *of $\mathbb{R}^n$.*

Definition 12. *(Voronoi region) The Voronoi region $\mathcal{V}(\lambda)$ of a lattice $\Lambda \subset \mathbb{R}^n$ is the subset of $\mathbb{R}^n$ containing all points nearer to lattice point λ than to any other lattice point:*

$$\mathcal{V}(\lambda) = \{x \in \mathbb{R}^n : ||x - \lambda|| \leqslant ||x - \tilde{\lambda}||, \ \textit{for all}\ \tilde{\lambda} \in \Lambda\}, \tag{1.11}$$

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

Example 2. *The Voronoi region of the well known A_2 lattice, with basis $\{(1, 0), (1/2, \sqrt{3}/2)\}$ is illustrated in Figure 2.*

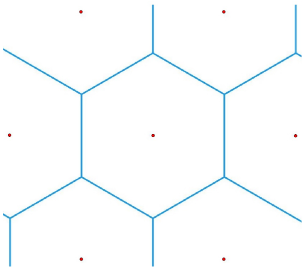

Figure 2 – Voronoi region of A_2 lattice.

A Voronoi region of a lattice $\mathcal{V}(0)$ is an example of a fundamental region, what means that one can tile the entire $\mathbb{R}^n$ space considering translations of $\mathcal{V}(0)$, by elements $\lambda \in \Lambda$.

The volume of any fundamental region of a lattice is $vol(\Lambda)$ (Definition 8).

Definition 13. *(Voronoi and relevant vectors) A vector v is called a Voronoi vector if the hyperplane*

$$\left\{x \in \mathbb{R} : \langle x, v\rangle = \frac{1}{2}\langle v, v\rangle\right\} \tag{1.12}$$

has a non-empty intersection with $\mathcal{V}(0)$. A Voronoi vector is said to be relevant if this intersection is an $(n-1)-$dimensional face of $\mathcal{V}(0)$.

Definition 14. *(Kissing number) The kissing number is the number of nearest neighbors of a given point in a constellation of discrete points in $\mathbb{R}^n$.*

[2] We consider here a partition of $\mathbb{R}^n$ as a family of sets such that their union is $\mathbb{R}^n$ and the intersection of two different sets is contained in their boundaries.

For a lattice constellation, the kissing number is the same for every point.

The following definition, geometric uniformity, is important because it guarantees that a constellation which satisfies this definition has a special type of symmetry, in which every point sees the same spectrum of neighbor points and all Voronoi regions have the same shape.

Definition 15. *(Geometrically uniform set) A set $\Gamma \subset \mathbb{R}^n$ is geometrically uniform if for any two elements $c, c' \in \Gamma$, there exists a distance-preserving transformation T in $\mathbb{R}^n$ such that $c' = T(c)$ and $T(\Gamma) = \Gamma$.*

Remark 1. *Since any isometry in $\mathbb{R}^n$ is a composition of a translation by a vector with a linear orthogonal map (rotation of reflection), the above condition is equivalent to require that for any $c, c' \in \Gamma$, there exist an orthogonal map T_o and $x \in \mathbb{R}^n$, such that $T_o(c - x) = c'$ and $T_o(\Gamma - x) = \Gamma$.*

Every lattice Λ is geometrically uniform, due to the fact that any translation $\Lambda + x$ by a lattice point $x \in \Lambda$ is just Λ. This means that every point of the lattice has the same number of neighbors at each distance and all Voronoi regions are congruent. Indeed, any lattice translation $\Lambda + t$ is geometrically uniform.

Definition 16. *(Sphere packing) Given a discrete set $\mathcal{P} \subseteq \mathbb{R}^n$, a sphere packing of $\mathcal{P}$ is the union of $n-$balls of maximum radius r centered at points of $\mathcal{P}$, such that two distinct balls can only intersect at their boundaries.*

Definition 17. *(Packing radius and packing density of a lattice) The packing radius ρ of a lattice is the half of the lattice minimum distance $\rho = \dfrac{d_{min}(\Lambda)}{2}$ and the packing density Δ_Λ is the portion of the space $\mathbb{R}^n$ occupied by packing spheres centered at lattice points. Due to the geometric uniformity of lattices:*

$$\Delta_\Lambda = \frac{\textit{volume of a sphere of radius } \rho}{\textit{volume of fundamental region}} \tag{1.13}$$

$$= \frac{vol\ S(0,\rho)}{vol(\Lambda)}, \tag{1.14}$$

Example 3. *Considering Λ as the A_2 lattice (Example 1), it follows that*

$$\Delta_{A_2} = \frac{\pi\rho^2}{|\det V|} = \frac{\frac{\pi}{4}}{\frac{\sqrt{3}}{2}} \approx 0.9068... \tag{1.15}$$

where V is any generator matrix of Λ.

Lattices with the largest possible packing density are known in dimensions 1 to 8 and in dimension 24 [18]. For general discrete sets, the largest packing is only known in dimensions $1, 2, 3, 8$ and 24 and it is achieved for special lattices in these dimensions [16, 29, 52]:

- For $n = 2$, the densest packing of circles in the plane is the one whose circles are centered in the the hexagonal lattice [49] (Example 1).
- For $n = 3$, the densest packing of spheres in three dimension covers $\frac{\pi}{\sqrt{18}} \approx 0.7404...$ of the space and is achieved by spheres centered in the face centered cubic lattice [29], with basis $\{(1,1,-1),(1,-1,1),(-1,1,1)\}$.
- For $n = 8$, the densest packing [52] covers $\frac{\pi^4}{384} \approx 0.2537...$ of the 8−dimensional space and is achieved by the E_8 lattice, defined as
$$E_8 = \{(x_1,\dots,x_8) : \text{all } x_i \in \mathbb{Z} \text{ or all } x_i \in \mathbb{Z} + \frac{1}{2}, \text{ and} \sum x_i \text{ is even}\}. \tag{1.16}$$
- For $n = 24$, the densest packing [16], which has $\frac{\pi^{12}}{12!} \approx 0.001930...$ of the space covered, is given by the Leech lattice Λ_{24}, that consists of the vectors [18]
$$\begin{aligned} &a(0 + 2c + 4x), \\ &a(1 + 2c + 4y), \end{aligned} \tag{1.17}$$
where $a = 1/\sqrt{8}$, $0 = \underbrace{(0,\dots,0)}_{\in\mathbb{Z}^{24}}$, $1 = \underbrace{(1,\dots,1)}_{\in\mathbb{Z}^{24}}$ and $c \in \mathcal{C}_{24}$, which is the binary Golay code. Moreover, $x, y \in \mathbb{Z}^{24}$ such that $\sum_{i=1}^{24} x_i \equiv 0 \ (mod\ 2)$ and $\sum_{i=1}^{24} y_i \equiv 1 \ (mod\ 2)$.

Definition 18. *(Packing efficiency) Given the packing density, the packing efficiency is* $\chi(\Lambda) = (\Delta_\Lambda)^{1/n}$.

1.2.2 Constructions from linear codes

From linear codes it is possible to derive lattice and periodic constellations using the known Construction A, C and D. In what follows, to fix notation, consider the natural embedding $\psi : \mathbb{F}_2^n \to \mathbb{R}^n$.

Definition 19. *(Construction A) Let $\mathcal{C}$ be an $[n,k,d]-$binary code. We define the Construction A from $\mathcal{C}$ as*
$$\Lambda_A = \psi(\mathcal{C}) + 2\mathbb{Z}^n. \tag{1.18}$$

Observe that Λ_A is a lattice that contains $2\mathbb{Z}^n$ as a sublattice.

Definition 20. *(Construction D) Let $\mathcal{C}_1 \subseteq \cdots \subseteq \mathcal{C}_L \subseteq \mathbb{F}_2^n$ be a family of nested linear binary codes. Let $k_i = \dim(\mathcal{C}_i)$ and let $b_1, b_2, \dots, b_n$ be a basis of $\mathbb{F}_2^n$ such that $\{b_1, \dots, b_{k_i}\}$ are bases of $\mathcal{C}_i$. The lattice Λ_D consists of all vectors of the form*
$$\Lambda_D = \sum_{i=1}^{L} 2^{i-1} \sum_{j=1}^{k_i} \alpha_j^i \psi(b_j) + 2^L z, \tag{1.19}$$
where $\alpha_j^i \in \{0,1\}$ and $z \in \mathbb{Z}^n$.

Our study in the next Chapter 2 is focused in one particular construction which is not always a lattice, denoted by Construction C and defined for general codes $\mathcal{C}_i \subseteq \mathbb{F}_2^n, i = 1, \ldots, L$ as follows.

Definition 21. *(Construction C) Consider L binary codes $\mathcal{C}_1, \ldots, \mathcal{C}_L \subseteq \mathbb{F}_2^n$, not necessarily nested or linear. The infinite constellation Γ_C in $\mathbb{R}^n$, called Construction C, is defined as:*

$$\Gamma_C := \mathcal{C}_1 + 2\mathcal{C}_2 + \cdots + 2^{L-1}\mathcal{C}_L + 2^L\mathbb{Z}^n, \tag{1.20}$$

i.e.,

$$\Gamma_C \quad := \quad \{c_1 + 2c_2 + \cdots + 2^{L-1}c_L + 2^L z : c_i \in \mathcal{C}_i, i = 1, \ldots, L, \; z \in \mathbb{Z}^n\}. \tag{1.21}$$

Note that this definition is based on Forney's multilevel code formula [22] and it does not require the additional condition assumed in the definition from Conway and Sloane [18, pp. 150].

In general, even if the underlying codes are linear, Construction C produces a nonlattice constellation. Note that if $L = 1$, i.e., if we consider a single level with a linear code, then this construction, as well as Construction D, reduces to a lattice Construction A.

Example 4. *Consider $\mathcal{C}_1 = \{(0,0),(1,1)\}$ and $\mathcal{C}_2 = \{(0,0)\}$. The $2-$level Construction C from theses codes is given by $\Gamma_C = \mathcal{C}_1 + 2\mathcal{C}_2 + 4\mathbb{Z}^2$. Geometrically, we can see this constellation in Figure 26 and clearly Γ_C is not a lattice.*

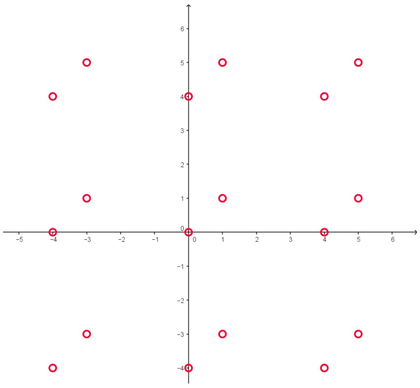

Figure 3 – Nonlattice Construction C.

Example 5. *A well-known lattice that we can construct using $2-$level Construction C is the body centered cubic lattice (BCC). Consider $\mathcal{C}_1 = \{(0,0,0)\}$ and $\mathcal{C}_2 = \{(0,0,0),(1,1,1)\}$, then $\Gamma_C = \{(0,0,0) + 4z, (2,2,2) + 4z\}, \; z \in \mathbb{Z}^3$. Note that this construction is a lattice with basis $\{(4,0,0),(0,4,0),(2,2,2)\}$, which generates a scaled equivalent version of the BCC lattice.*

Example 6. *Another important lattice we can construct via Construction C is the Barnes-Wall Λ_{16} [18], considering $\mathcal{C}_1 = \mathcal{R}(0,4)$, $\mathcal{C}_2 = \mathcal{R}(2,4)$ and $\mathcal{C}_3 = \mathbb{F}_2^{16}$, where $\mathcal{R}(r,m)$ represents the Reed-Muller code of length 2^m and of order $0 \leqslant r \leqslant m$. We have that*

$$\begin{aligned} \Lambda_{16} &= \mathcal{C}_1 + 2\mathcal{C}_2 + 4\mathcal{C}_3 + 8\mathbb{Z}^{16} \\ &= \mathcal{R}(0,4) + 2\mathcal{R}(2,4) + 4\mathbb{Z}_2^{16} + 8\mathbb{Z}^{16}. \end{aligned} \tag{1.22}$$

Definition 22. *(Schur product) For $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n) \in \mathbb{F}_2^n$, the Schur product is defined by $x * y = (x_1y_1, \ldots, x_ny_n) \in \mathbb{F}_2^n$.*

Regarding to the Schur product, for $x, y \in \mathbb{F}_2^n$, if $+$ denotes the sum in $\mathbb{R}^n$ and $\oplus$ the modulo two sum in $\mathbb{F}_2^n$, we have

$$x + y = x \oplus y + 2(x * y) \in \mathbb{R}^n. \tag{1.23}$$

Theorem 1. *[32] (Relation between Constructions C and D) Given a family of nested binary linear codes $\mathcal{C}_1 \subseteq \cdots \subseteq \mathcal{C}_L \subseteq \mathbb{F}_2^n$, then the following statements are equivalent:*

1. *Γ_C is a lattice.*
2. *$\mathcal{C}_1 \subseteq \cdots \subseteq \mathcal{C}_L \subseteq \mathbb{F}_2^n$ is closed under Schur product.*
3. *$\Gamma_C = \Lambda_D$.*

1.2.3 Communication problems involving lattices

The study of communication and information transmission involves the solution of special problems and we mention here the ones that are relevant to our work, such as the notion of multi-stage decoding and quantizers.

Multilevel constructions, such as Construction C and D, can be decoded through a very efficient method, called multi-stage decoding [25]. In multi-stage decoding, component codes are decoded one at a time into a sequence of decoding stages. The decoded information at one stage is passed to the next stage for decoding the next component code. Because the component codes are shorter and simpler, they can be decoded with soft-decision decoding to achieve good error performance. We will present in sequence the algorithm for multi-stage decoding, represented also in Figure 4.

Algorithm: Multi-stage decoding algorithm

Let $\mathcal{D}_1, \ldots, \mathcal{D}_L$ be, respectively, the decoders for the codes $\mathcal{C}_1, \ldots, \mathcal{C}_L$.

1. At the first stage $\mathcal{D}_1$ estimates the codeword $c_1 = (c_{11}, \ldots, c_{1n})$ under the assumption that the binary vectors of the upper levels, i.e., $c_2, \ldots, c_L$ are uncoded, getting $\hat{c}_1$.

2. The second stage decoder $\mathcal{D}_2$ works under the assumption that the output of the previous stage $\hat{c}_1$ correctly estimated the transmitted codeword c_1. Also, the vectors $c_3, \ldots, c_L$ of the upper levels is considered as uncoded.
3. Based on the assumptions that the decoder performed correctly in the previous stages, all remaining codewords $c_3, \ldots, c_L$ are estimated by their respective decoders.

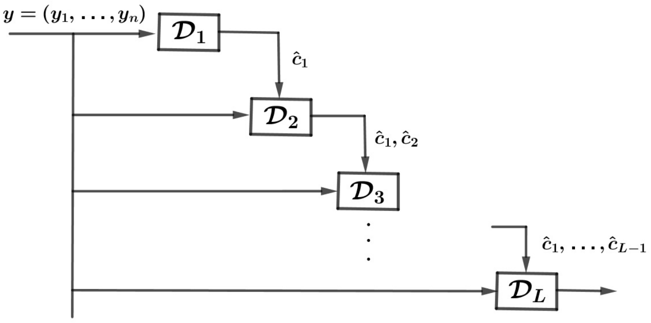

Figure 4 – Multi-stage decoding algorithm, based on [20, pp. 514].

Another well explored communication problem is quantization, which in general is the process of restricting a large set of values to a discrete set of values. Since a lattice is discrete, then there exists a special quantization which is done by using lattices.

The distance of a point $x \in \mathbb{R}^n$ from a lattice Λ is defined as $||x - \Lambda|| = \min\limits_{\lambda \in \Lambda} ||x - \lambda||$. The lattice quantizer maps x to its closest lattice point, i.e.,

$$Q_\Lambda(x) = arg \min_{\lambda \in \Lambda} ||x - \lambda||. \tag{1.24}$$

Observe that all points inside the Voronoi region $V(\lambda)$ are mapped to $\lambda \in \Lambda$. In case of a tie, the algorithm output must give all closest lattice points or just choose one of those.

An approach to lattice quantization is to quantize $x \in \mathbb{R}^n$ to a lattice point by considering other simpler fundamental regions.

In higher dimensions, to determine the closest lattice point to a given real vector is a NP-complete problem for general lattices and this fact justify its use in cryptosystems [26]. The following discussion aim to introduce as well as present some attempts to approach this problem using a method proposed by Babai [7]. Another formulation of quantization in lattices is:

Definition 23. *(Closest lattice point problem) The closest vector problem (CVP) in a lattice (denoted as closest lattice point problem) can be described as an integer least squares problem with the objective of determining u^*, such that*

$$u^* = \arg\min_{u \in \mathbb{Z}^n} || \, x - Vu \, ||^2 \tag{1.25}$$

where the norm considered is the standard Euclidean norm. A closest lattice point to x is then given by $x_{nl} = Vu^*$.

Observe that the mapping $g_{cl} : \mathbb{R}^n \to \Lambda$, $x \mapsto x_{nl}$ partitions $\mathbb{R}^n$ into Voronoi cells, each of volume $|\det V|$, where V is the generator matrix of the lattice Λ. Exact as well as approximate solutions to the closest lattice point problem have been well studied.

One approach to solve the closest lattice point problem approximately is perfoming the nearest plane (np) algorithm which computes x_{np}, an approximation to x_{nl}, given by $x_{np} = b_1v_1 + b_2v_2 + \ldots + b_nv_n$, where $b_i \in \mathbb{Z}$ is obtained as follows, derived from [7].

Algorithm: Babai nearest plane algorithm (np algorithm)

Let $\mathcal{S}_i$ denote the subspace spanned by the vectors $\{v_1, v_2, \ldots, v_i\}$, $i = 1, 2, \ldots, n$. Let $\mathcal{P}_i(z)$ be the orthogonal projection of z onto $\mathcal{S}_i$ and let $v_{i,i-1} = \mathcal{P}_{i-1}(v_i)$ be the nearest vector to v_i in $\mathcal{S}_{i-1}$. We have the following unique decomposition: $v_i = v_{i,i-1} + v_{i,i-1}^{\perp}$. Also, let $z_i^{\perp} = z_i - \mathcal{P}_i(z_i)$.

1. Start with $z_n = x$ and $i = n$.

2. Compute $b_i = \left[\langle z_i, v_{i,i-1}^{\perp}\rangle / \|v_{i,i-1}^{\perp}\|^2\right]$, $z_{i-1} = \mathcal{P}_{i-1}(z_i) - b_iv_{i,i-1}$, for $i = n, n-1, \ldots, 1$. Here $[x]$ denotes the nearest integer to x.

3. The vector $b = (b_1, b_2, \ldots, b_n)$ is called *Babai point*, which is an approximation to the given real vector x_{nl}.

Definition 24. *(Babai partition) The mapping $g_{cl} : \mathbb{R}^n \to \Lambda$, $x \mapsto x_{np}$ partitions $\mathbb{R}^n$ into hyper-rectangular cells with volume $|\det V|$ and we refer to this partition as a* Babai *partition.*

Example 7. *Figure 5 represents the Babai partition (black lines) and the Voronoi partition (pink lines) for the hexagonal lattice A_2 generated by $\{(1,0), (1/2, \sqrt{3}/2)\}$. It gives a geometric intuition to see why the np algorithm is an approximation to the nearest lattice point problem.*

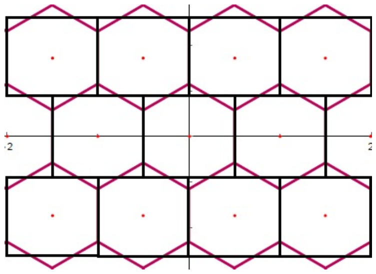

Figure 5 – Cells of Babai and Voronoi partitions of the hexagonal lattice A_2.

Note that Babai partition is basis dependent, as will be clearer in Example 26. In case the generator matrix V is upper triangular with (i, j) entry v_{ij}, each rectangular cell is axis-aligned and has sides of length $|v_{11}|, |v_{22}|, \ldots, |v_{nn}|$. Moreover, in this specific case, the vectors $v^{\perp}_{i,i-1}$ mentioned above are of type $(0, 0, \ldots, v_{ii}, 0, \ldots, 0)$ and solving the np algorithm is the same as solving the linear system $V\tilde{b} = x$, with $x \in \mathbb{R}^n$ and $b = [\tilde{b}] \in \mathbb{Z}^n$.

To illustrate this process for the two dimensional case, consider an upper triangular generator matrix given by

$$V = \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix}. \tag{1.26}$$

Then, we aim to find (u_1, u_2) such that $(x_1 - u_1 - au_2)^2 + (x_2 - bu_2)^2$ is minimum and using the np algorithm, we choose $u_2 = \left[\dfrac{x_2}{b}\right]$ and $u_1 = [x_1 - au_2]$. This method can be generalized for an arbitrary dimension n and provides an straightforward way of obtaining the Babai point (and consequently the Babai partition).

We remark that given a lattice Λ with an arbitrary generator matrix $V \in \mathbb{R}^{n\times n}$ we can apply QR decomposition, i.e., $V = QR$, where $Q \in \mathbb{R}^{n\times n}$ is an orthogonal matrix and $R \in \mathbb{R}^{n\times n}$ is an upper triangular matrix, that generates a rotation of the original lattice defined by V.

A natural way to obtain the QR decomposition of a generator matrix $V \in \mathbb{R}^{n\times n}$ is applying the standard Gram-Schmidt process to the column vectors v_i of V, $i = 1, \ldots, n$. Then, for:

$$\begin{aligned}
w_1 &= v_1, \\
w_2 &= v_2 - \frac{\langle v_2, q_1\rangle}{\langle q_1, q_1\rangle} q_1, \\
&\vdots \\
w_n &= v_n - \frac{\langle v_n, q_1\rangle}{\langle q_1, q_1\rangle} q_1 - \cdots - \frac{\langle v_n, q_{n-1}\rangle}{\langle q_{n-1}, q_{n-1}\rangle} q_{n-1},
\end{aligned} \tag{1.27}$$

where $\langle , \rangle$ is the usual inner product in $\mathbb{R}^n$ and $||.||$ is the Euclidean norm. Set $e_i = \dfrac{w_i}{||w_i||}$, $i = 1, \ldots, n$. Thus, $Q = [e_1 \ \ldots \ e_n]$,

$$R = \begin{pmatrix} \langle v_1, e_1\rangle & \langle v_2, e_1\rangle & \ldots & \langle v_n, e_1\rangle \\ 0 & \langle v_2, e_2\rangle & \ldots & \langle v_n, e_2\rangle \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \langle v_n, e_n\rangle \end{pmatrix} \tag{1.28}$$

and $V = QR$.

It is also possible to use known transformations as Householder reflections or Givens rotations instead of the Gram-Schmidt proccess, as carefully described in [27].

1.2.4 Special bases

We will now introduce now two types of special bases we will work closely in this thesis: Minkowski-reduced basis [38] and obtuse superbase [17].

Definition 25. *(Minkowski-reduced basis) A basis* $\{v_1, v_2, ..., v_n\}$ *of a lattice* Λ *in* $\mathbb{R}^n$ *is said to be Minkowski-reduced if* v_j, $j = 1, \dots, n$, *is such that* $\|v_j\| \leqslant \|v\|$, *for any* v *for which* $\{v_1, ..., v_{j-1}, v\}$ *can be extended to a basis of* Λ.

In particular, for lattices of dimension $n \leqslant 4$, the norms of the Minkowski-reduced basis vectors achieve the successive minima [43]. For two-dimensional lattices, a Minkowski-reduced basis is also called Lagrange-Gauss reduced basis and there is a simple characterization [18]: a lattice basis $\{v_1, v_2\}$ is a Minkowski-reduced basis if only if $\|v_1\| \leqslant \|v_2\|$ and $2\langle v_1, v_2\rangle \leqslant \|v_1\|^2$. It follows that the angle θ between the minimum norm vectors v_1 and v_2 must satisfy $\dfrac{\pi}{3} \leqslant \theta \leqslant \dfrac{2\pi}{3}$.

It is also possible to characterize Minkowski-reduced basis for lattices in dimensions less or equal than three according to the following proposition.

Proposition 1. *[18] Consider the Gram matrix* A *of a lattice* Λ *and the conditions below:*

$$\begin{aligned} 0 < a_{11} \leqslant \quad a_{22} &\leqslant a_{33} \leqslant \cdots \leqslant a_{nn} && (1.29)\\ 2|a_{st}| \quad &\leqslant \quad a_{ss} \quad (s < t) && (1.30)\\ 2|a_{rs} \pm a_{rt} \pm a_{st}| \quad &\leqslant \quad a_{rr} + a_{ss} \quad (r < s < t). && (1.31) \end{aligned}$$

Then, inequalities (1.29), (1.29)–(1.30) and (1.29)–(1.31) define a Minkowski-reduced basis for dimensions 1,2 and 3, respectively.

It is pertinent to remark that all lattices have a Minkowski-reduced basis and roughly speaking, it consists of short vectors that are "as perpendicular as possible". Nevertheless, it is computationally hard to get such a basis as the dimension of the lattice increase. One alternative is to use the basis obtained with the LLL algorithm [34], which approximates the Minkowski-reduced basis and can be derived in polynomial time. For a basis that is LLL reduced, the ratio of the distances $\|x - x_{np}\|/\|x - x_{nl}\|$ can be bounded above by a constant that depends on the dimension alone [7].

There is another important basis to our study, called obtuse superbase. The remainder of this section based mainly in [17] is devoted to describe it.

Definition 26. *(Voronoi's first kind and obtuse superbase) Let* $\{v_1, v_2, \dots, v_n\}$ *be a basis for a lattice* Λ. *A superbase* $\{v_0, v_1, \dots, v_n\}$ *with* $v_0 = -\sum_{i=1}^{n} v_i$, *is said to be obtuse if* $p_{ij} = \langle v_i, v_j\rangle \leqslant 0$, *for* $i, j = 0, \dots, n$, $\quad i \neq j$. *A lattice* Λ *is said to be of Voronoi's first kind if it has an obtuse superbase.*

The above parameters p_{ij} are called *Selling parameters* and if $p_{ij} < 0$ we say that the superbase is strictly obtuse.

Example 8. *Consider the standard basis $\{v_1, v_2, v_3\}$ for the body-centered cubic (BCC) lattice where $v_1 = (1, 1, -1), v_2 = (1, -1, 1), v_3 = (-1, 1, 1)$. We set $v_0 = -v_1 - v_2 - v_3 = (-1, -1, -1)$ and v_0, v_1, v_2, v_3 is a strictly obtuse superbase for BCC lattice. Observe that $p_{ij} = -1 < 0$ for all $i, j = 0, 1, 2, 3, i \neq j$ and BCC is of Voronoi's first kind.*

The existence of an obtuse superbase allows a characterization of the relevant Voronoi vectors for a lattice.

Theorem 2. *[17, Th.3, Sec. 2] Let Λ be a lattice of Voronoi's first kind with obtuse superbase $\{v_0, v_1, \ldots, v_n\}$. Vectors of the form $\sum_{i \in S} v_i$, where S is a strict non-empty subset of $\{0, 1, \ldots, n\}$ are Voronoi vectors of Λ.*

It was demonstrated [17] that all lattices with dimension less or equal than three are Voronoi's first kind. In three dimensions, considering an obtuse superbase, since $v_0 = -v_1 - v_2 - v_3$, all Voronoi vectors described in the above theorem can be written as one of the following seven vectors or their opposites [17]: $v_1, v_2, v_3, v_{12} = v_1 + v_2, v_{13} = v_1 + v_3, v_{23} = v_2 + v_3, v_{123} = v_1 + v_2 + v_3$.

Given an obtuse superbase, the norms $N(v_1), N(v_2), N(v_3)$, $N(v_{12}), N(v_{13})$, $N(v_{23})$, $N(v_{123})$, where $N(x) = \langle x, x \rangle$, are called *vonorms* and $p_{ij} = -\langle v_i, v_j \rangle$ $(0 \leqslant i < j \leqslant 3)$ are called *conorms*, of the superbase $\{v_0, v_1, v_2, v_3\}$.

The nonzero cosets of $\Lambda/2\Lambda$ naturally form a discrete projective plane of order 2. The vonorms are marked as the nodes of the projective plane and the corresponding conorms 0 and p_{ij} at the nodes of the dual plane in the following Figure 6.

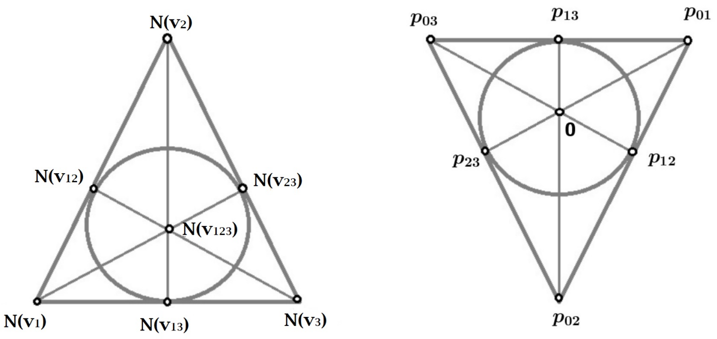

Figure 6 – Projective and dual planes labelled with vonorms and conorms respectively (based on [17], p. 61).

There exists an algorithm [17] to reduce any basis of a lattice in $\mathbb{R}^3$ to an obtuse superbase, based on projective planes. Here we use a more straightforward approach by starting from special bases.

An obtuse superbase is essential for us to characterize the five parallelohedra that are Voronoi cell of three-dimensional lattices: truncated octahedron, hexa-rhomic dodecahedron, rhombic dodecahedron, hexagonal prism and cuboid.

Let Λ be an arbitrary 3−dimensional lattice, with obtuse superbase $\{v_0, v_1, v_2, v_3\}$ and conorms $p_{i,j}$. A vector $t \in \mathbb{R}^3$ can be specified by its inner products

$$(\langle t, v_1\rangle, \langle t, v_2\rangle, \langle t, v_3\rangle) = (y_1, y_2, y_3) = y. \tag{1.32}$$

The most generic Voronoi region in three dimensions is the truncated octahedron, with 14 faces and 24 vertices. It is know [17] that the vertices of this Voronoi cell are all the 24 points p_{ijkl} where $\{i, j, k, l\}$ is any permutation of $\{0, 1, 2, 3\}$:

$$\begin{aligned} y_i = \frac{1}{2}(p_{ij} + p_{ik} + p_{il}), \quad y_j = \frac{1}{2}(-p_{ji} + p_{jk} + p_{jl}), \\ y_k = \frac{1}{2}(-p_{ki} - p_{kj} + p_{kl}), \quad y_l = \frac{1}{2}(-p_{li} - p_{lj} - p_{lk}). \end{aligned} \tag{1.33}$$

Using Equations (1.32) and (1.33) one can define all the points that generates a generic Voronoi region.

It is possible to guarantee that two lattices for which the correspondent conorms are zero have combinatorially equivalent Voronoi regions (since one can be continuously deformed into the other without any edges being lost).

When we construct the dual projective planes to represent the conorms, there are five choices for zeros: one, two, three collinear zeros, three non-collinear zeros or four zeros. Each of these configuration produces a different Voronoi cell according to Figure 7.

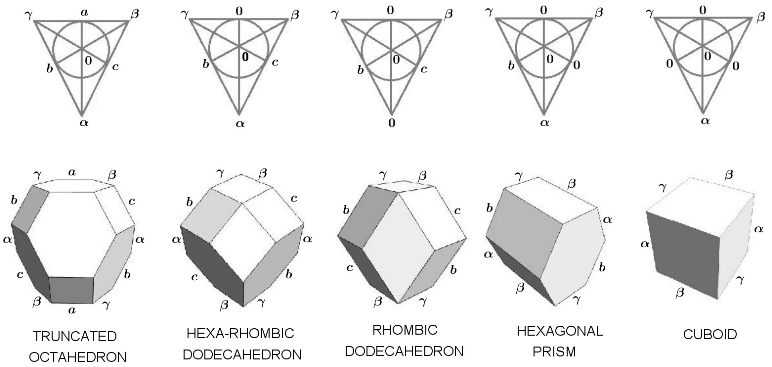

Figure 7 – Dual plane labeled with conorms and its correspondent Voronoi cells (based on [17], p. 65).

In the following example, we will illustrate with the *body-centered cubid lattice* (BCC), the method proposed by Conway and Sloane [17] to characterize the Voronoi region of a three dimensional lattice given an obtuse superbase.

Example 9. *Consider the BCC lattice, its obtuse superbase* $\{v_0, v_1, v_2, v_3\}$, *where* $v_0 = (-1,-1,-1), v_1 = (1,1,-1), v_2 = (1,-1,1), v_3 = (-1,1,1)$ *(Example 8) and its conorms* $p_{ij} = 1$, *for all* $i, j = 0, 1, 2, 3, i \neq j$.

Comparing the dual projective plane with the characterization in Figure 7 we can also claim that the Voronoi cell of this lattice is a truncated octahedron and the next step is to find the vertices that define it. To do that, we find the coordinates via Equation (1.33) and solve the linear system proposed in Equation (1.32), by considering the permutation $\{1, 0, 3, 2\} = \{i, j, k, l\}$. *Then:*

$$\begin{aligned} y_1 &= \frac{1}{2}(1+1+1) = 3/2, \quad & y_0 &= \frac{1}{2}(-1+1+1) = 1/2, \\ y_3 &= \frac{1}{2}(-1-1+1) = -1/2, \quad & y_2 &= \frac{1}{2}(-1-1-1) = -3/2. \end{aligned} \tag{1.34}$$

Thus,$(y_0, y_1, y_2, y_3) = (1/2, 3/2, -3/2, -1/2)$.

To continue, we need to solve the linear system given by $(\langle t, v_1\rangle, \langle t, v_2\rangle, \langle t, v_3\rangle) = (y_1, y_2, y_3) = (3/2, -3/2, -1/2)$, *which will give us* $(t_1, t_2, t_3) = (0, 1/2, -1)$. *Table 1 presents the vertices obtained after we perform this process through all the possible permutations.*

Table 1 – Vertices of Voronoi region given an obtuse superbase of the BCC lattice

Permutation $\{i, j, k, l\}$	(y_0, y_1, y_2, y_3)	*Voronoi vertex* (t_1, t_2, t_3)
$\{0,1,2,3\}$	$(3/2, 1/2, -1/2, -3/2)$	$(0, -1/2, -1)$
$\{0,1,3,2\}$	$(3/2, 1/2, -3/2, 1/2)$	$(-1/2, 0, -1)$
$\{0,2,1,3\}$	$(3/2, -1/2, 1/2, -3/2)$	$(0, -1, -1/2)$
$\{0,2,3,1\}$	$(3/2, -3/2, 1/2, -1/2)$	$(-1/2, -1, 0)$
$\{0,3,1,2\}$	$(3/2, -1/2, -3/2, 1/2)$	$(-1, 0, -1/2)$
$\{0,3,2,1\}$	$(3/2, -3/2, -1/2, 1/2)$	$(-1, -1/2, 0)$
$\{1,2,0,3\}$	$(1/2, 3/2, -1/2, -3/2)$	$(1/2, 0, -1)$
$\{1,0,3,2\}$	$(1/2, 3/2, -3/2, -1/2)$	$(0, 1/2, -1)$
$\{1,2,0,3\}$	$(-1/2, 3/2, 1/2, -3/2)$	$(1, 0, -1/2)$
$\{1,2,3,0\}$	$(-3/2, 3/2, 1/2, -1/2)$	$(1, 1/2, 0)$
$\{1,3,0,2\}$	$(-1/2, 3/2, -3/2, 1/2)$	$(0, 1, -1/2)$
$\{1,3,2,0\}$	$(-3/2, 3/2, -1/2, 1/2)$	$(1/2, 1, 0)$
$\{2,0,1,3\}$	$(1/2, -1/2, 3/2, -3/2)$	$(1/2, -1, 0)$
$\{2,0,3,1\}$	$(1/2, -3/2, 3/2, -1/2)$	$(0, -1, 1/2)$
$\{2,1,0,3\}$	$(-1/2, 1/2, 3/2, -3/2)$	$(1, -1/2, 0)$

$\{2,1,3,0\}$	$(-3/2,1/2,3/2,-1/2)$	$(1,0,1/2)$
$\{2,3,0,1\}$	$(-1/2,-3/2,3/2,1/2)$	$(0,-1/2,1)$
$\{2,3,1,0\}$	$(-3/2,-1/2,3/2,1/2)$	$(1/2,0,1)$
$\{3,0,1,2\}$	$(1/2,-1/2,-3/2,3/2)$	$(-1,1/2,0)$
$\{3,0,2,1\}$	$(1/2,-3/2,-1/2,3/2)$	$(1,0,1/2)$
$\{3,1,0,2\}$	$(-1/2,1/2,-3/2,3/2)$	$(-1/2,1,0)$
$\{3,1,2,0\}$	$(-3/2,1/2,-1/2,3/2)$	$(0,1,1/2)$
$\{3,2,1,0\}$	$(-1/2,-3/2,1/2,3/2)$	$(-1/2,0,1)$
$\{3,2,1,0\}$	$(-3/2,-1/2,1/2,3/2)$	$(0,1/2,1)$

Therefore, we determine the 24 vertices that are all the permutations of $(\pm 1, \pm\frac{1}{2}, 0)$. *Figure 8 represents the Voronoi cell of BCC lattice.*

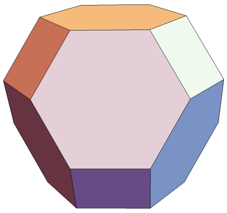

Figure 8 – Voronoi cell of the BCC lattice.

We would like to establish a result that defines under what circumstances a basis is both Minkowski-reduced and defines an obtuse superbase. The following result is the first contribution of our work.

Theorem 3. *In dimensions* $n = 1, 2, 3$, *if a lattice* $\Lambda \subset \mathbb{R}^n$ *has a Minkowski-reduced basis with vectors* $\{v_1, \dots, v_n\}$, *with* $\langle v_i, v_j \rangle \leqslant 0$, $i \neq j$, *then the superbase* $\{v_0, v_1, \dots, v_n\}$, *with* $v_0 = -\sum_{i=1}^{n} v_i$ *is an obtuse superbase for* Λ. *Conversely, if* Λ *has an obtuse superbase, then a Minkowski-reduced basis can be obtained from it with vectors suitably ordenated.*

Proof. The case $n = 1$ is trivial. For $n = 2$ ($\Rightarrow$) Suppose that $\{v_1, v_2\}$ is a Minkowski-reduced basis, then, according to Proposition 1, $0 < \langle v_1, v_1 \rangle \leqslant \langle v_2, v_2 \rangle$ and $2|\langle v_1, v_2 \rangle| \leqslant \langle v_1, v_1 \rangle$. Moreover, by hypothesis, $\langle v_1, v_2 \rangle \leqslant 0$. Define $v_0 = -v_1 - v_2$ and to guarantee that $\{v_0, v_1, v_2\}$ is an obtuse superbase, we need to check that $p_{01} \leqslant 0$ and $p_{02} \leqslant 0$. Indeed,

$$p_{01} = \langle v_0, v_1 \rangle = \langle -v_1 - v_2, v_1 \rangle = -\langle v_1, v_1 \rangle \underbrace{-\langle v_1, v_2 \rangle}_{|\langle v_1, v_2 \rangle|} \leqslant -2|\langle v_1, v_2 \rangle| + |\langle v_1, v_2 \rangle| \leqslant 0. \quad (1.35)$$

Similarly we have that $p_{02} \leqslant 0$.

($\Leftarrow$) If $\{v_0, v_1, v_2\}$ is an obtuse superbase, any permutation of it is also an obtuse superbase. So, we may consider one such that $|v_1| \leqslant |v_2| \leqslant |v_0|$. Then we have that $0 < \langle v_1, v_1\rangle \leqslant \langle v_2, v_2\rangle \leqslant \langle v_1 + v_2, v_1 + v_2\rangle$ and $v_1 \neq 0$.

From the last inequality, we have that

$$-2\langle v_1, v_2\rangle \quad \leqslant \quad \langle v_1, v_1\rangle \Rightarrow 2|\langle v_1, v_2\rangle| \leqslant \langle v_1, v_1\rangle. \tag{1.36}$$

For $n = 3$ ($\Rightarrow$) Consider a Minkowski-reduced basis $\{v_1, v_2, v_3\}$ such that $\langle v_1, v_2\rangle \leqslant 0, \langle v_1, v_3\rangle \leqslant 0$ and $\langle v_2, v_3\rangle \leqslant 0$. To check if $\{v_0, v_1, v_2, v_3\}$ is an obtuse superbase, we need to verify that $p_{01} \leqslant 0, p_{02} \leqslant 0$ and $p_{03} \leqslant 0$.

Observe that

$$p_{01} = \langle v_0, v_1\rangle = -\langle v_1, v_1\rangle \underbrace{-\langle v_1, v_2\rangle}_{|\langle v_1,v_2\rangle|} \underbrace{-\langle v_1, v_3\rangle}_{|\langle v_1,v_3\rangle|} \leqslant -\langle v_1, v_1\rangle + \frac{\langle v_1, v_1\rangle}{2} + \frac{\langle v_1, v_1\rangle}{2} \leqslant 0. \tag{1.37}$$

With analogous arguments, we show that $p_{02} \leqslant 0$ and $p_{03} \leqslant 0$.

($\Leftarrow$) To prove the converse, up to a permutation, we may consider an obtuse superbase such that $|v_1| \leqslant |v_2| \leqslant |v_3| \leqslant |v_0|$, $|v_2| \leqslant |v_1 + v_2|$, $|v_3| \leqslant |v_1 + v_3|$ and $|v_3| \leqslant |v_2 + v_3|$. This basis will be Minkowski-reduced if we prove conditions (1.30) and (1.31) from Proposition 1, i.e.,

$$2|\langle v_1, v_2\rangle| \leqslant \langle v_1, v_1\rangle; \quad 2|\langle v_1, v_3\rangle| \leqslant \langle v_1, v_1\rangle; \quad 2|\langle v_2, v_3\rangle| \leqslant \langle v_2, v_2\rangle \tag{1.38}$$

and

$$2|\pm\langle v_1, v_2\rangle \pm \langle v_1, v_3\rangle \pm \langle v_2, v_3\rangle| \leqslant \langle v_1, v_1\rangle + \langle v_2, v_2\rangle. \tag{1.39}$$

The inequalities in Equation (1.38) are shown similarly to the two dimensional case starting from $\langle v_2, v_2\rangle \leqslant \langle v_1 + v_2, v_1 + v_2\rangle$, $\langle v_3, v_3\rangle \leqslant \langle v_1 + v_3, v_1 + v_3\rangle$ and $\langle v_3, v_3\rangle \leqslant \langle v_2 + v_3, v_2 + v_3\rangle$. Starting from $\langle v_3, v_3\rangle \leqslant \langle v_1 + v_2 + v_3, v_1 + v_2 + v_3\rangle$, it follows the inequality in Equation (1.39) concluding the proof.

□

Chapter 2

Construction C

This chapter is devoted to point out known properties of general Construction C and to find out how close to a lattice can this construction be, in case it does not satisfy the condition required in [32]. Our contributions are to demonstrate that a two-level ($L = 2$) Construction C is geometrically uniform (a result that can also be deduced from [24]) and to show that for three levels and up ($L \geqslant 3$) the distance spectrum between points of the constellation may vary and consequently, Construction C is not geometrically uniform in general. We also write derivations that shows how to construct more general geometrically uniform constellations. These results appear in [11, 13] and they were inspired by [18, pp. 150-156] and [24].

2.1 Why Construction C?

There exist significant properties and applications of Construction C that can be useful for communication purposes, such as the fact that Construction C with multi-stage decoding can achieve the high SNR uniform-input capacity of an AWGN channel asymptotically as the dimension n goes to infinity [25]. Moreover, if the underlying codes of this construction are linear, then all points in this constellation have the same minimum distance, but not necessarily the same kissing number.

Another application of nonlattice construction is the D_n+ tesselation [18], that could be conceived as a $2-$ level Construction C if we consider $\mathcal{C}_1$ as the $[n, 1, n]-$ repetition code and $\mathcal{C}_2$ as the $[n, n-1, 2]-$even parity check code. Note that for n even, this construction represents a lattice, because we would have nested linear codes that are closed under Schur product. Otherwise, when n is odd, we obtain a nonlattice constellation which coincides with Construction C.

Agrell and Eriksson [1] proved that the D_n+ tessellation [18] exhibits as a lower normalized second moment (i.e. a better quantization efficiency) than any known lattice tessellation in dimensions 7 and 9. Note that a tessellation of an $n-$dimensional space is a partition of $\mathbb{R}^n$ into regions, such that any pair of regions can be transformed into each other through a rotation, reflection or translation, so it is generally not a lattice.

2.2 Properties of Construction C

There are some known properties of Construction C already explored in the literature, such as minimum distance, kissing number and geometric uniformity for $L = 2$ levels.

2.2.1 Minimum distance

If the underlying codes of Construction C are linear, then the squared minimum distance can be expressed as

$$d^2_{min}(\Gamma_C) = \min\{d_H(\mathcal{C}_1), 2^2 d_H(\mathcal{C}_2), \ldots, 2^{2(L-1)} d_H(\mathcal{C}_L), 2^{2L}\}. \tag{2.1}$$

Indeed, observe that sets defined as $\Gamma_{\mathcal{C}_i} = 0 + 2\cdot 0 + \cdots + 2^{i-1}c_i + \cdots + 2^{L-1}\cdot 0 + 2^L \cdot 0$, where $0 \in \mathbb{R}^n$, are subsets of Γ_C, i.e., $\Gamma_{\mathcal{C}_i} \subseteq \Gamma_C$ for all $i = 1, \ldots, L$, then it follows that $d^2_{E_{min}}(\Gamma_C) \leqslant \min\{d_H(\mathcal{C}_1), 2^2 d_H(\mathcal{C}_2), \ldots, 2^{2(L-1)} d_H(\mathcal{C}_L), 2^{2L}\}$. On the other hand, according to the discussion in [18, pp. 150], if we consider two elements $x, y \in \Gamma_C$, where

$$x = c_1 + 2c_2 + \cdots + 2^{i-1}c_i + \cdots + 2^{L-1}c_L + 2^L z \tag{2.2}$$

$$y = \tilde{c}_1 + 2\tilde{c}_2 + \cdots + 2^{i-1}\tilde{c}_i + \cdots + 2^{L-1}\tilde{c}_L + 2^L \tilde{z}, \tag{2.3}$$

such that $c_j = \tilde{c}_j$, for $j = 1, \ldots, i-1$ and $c_i \neq \tilde{c}_i$. Their squared distance vary by at least $2^{2(i-1)}$ in at least $d_H(\mathcal{C}_i)$ coordinates. Hence, $d^2_{E_{min}}(\Gamma_C) \geqslant \min\{d_H(\mathcal{C}_1), 2^2 d_H(\mathcal{C}_2), \ldots, 2^{2(L-1)} d_H(\mathcal{C}_L), 2^{2L}\}$. It justifies the formula in Equation (2.1).

From the formula for the squared minimum distance, it also follows that all points in this constellation have the same minimum distance to other constellations points, i.e., it is equi-minimum distance.

2.2.2 Kissing number

The kissing number (number of nearest neighbors) of an element of Construction C may vary between the elements even when the underlying codes are linear, as it can be seen in our following Example 10, where the kissing number of an element varies between 1 and 2.

2.2.3 Geometric uniformity for $L = 2$ levels

The geometric uniformity of a two level ($L = 2$) Construction C can be deduced from the work of D. Forney [24] if we consider a 2−level Construction C as group code with isometric labeling over $\mathbb{Z}/4\mathbb{Z}$ (i.e., a $2-$level binary coset code over $\mathbb{Z}/2\mathbb{Z}/4\mathbb{Z}$). He proved that this type of construction produces a geometrically uniform generalized coset code. In Section 2.3, we provide an alternative proof, based on explicit isometric transformation (as a special case of a general class of geometric uniform constellations).

2.2.4 Equi-distance spectrum and geometric uniformity for $L \geqslant 3$

Geometric uniformity implies, in particular, that all points have the same set of Euclidean distances to their neighbors.

Definition 27. *(Distance spectrum) For a discrete constellation $\Gamma \subseteq \mathbb{R}^n$, the distance spectrum is*

$$N(c,d) = \textit{number of points in the constellation at a Euclidean distance } d \textit{ from an element } c \textit{ in the constellation.}$$

Definition 28. *(Equi-distance spectrum) A constellation Γ is said to have equi-distance spectrum (EDS) if $N(c,d)$ is the same for all $c \in \Gamma$.*

Geometric uniformity implies equi-distance spectrum for $L = 2$ levels in Construction C and we have the following:

Proposition 2. *(Equi-distance spectrum of Γ_C) For a $2-$level Construction C, the distance spectrum is identical for all codewords in Γ_C, i.e., $N(c,d) = N(0,d)$ for all $c \in \Gamma_C$.*

Proof. Let $N(c,d) = k$, with $c \in \Gamma_C$, which means that there are k elements $x_1, \ldots, x_k \in \Gamma_C$ such that $d_E(c, x_i) = d$, for $i = 1, \ldots, k$. From the fact that a $2-$level Construction C is geometrically uniform, we know that for any two elements $y, \tilde{y} \in \Gamma_C$ there is an isometry T such that $T(y) = \tilde{y}$.

If we consider in particular $y = c, \tilde{y} = 0 \in \Gamma_C$, then it follows directly that there are k elements $T(x_1), \ldots, T(x_k) \in \Gamma_C$ such that $d_E(T(x_i)) = d_E(0, T(x_i)) = d$, $i = 1, \ldots, k$ and $N(c,d) = k = N(d)$ as we wanted do prove. □

For $L \geqslant 3$ the equi-distance spectrum and hence the geometric uniformity property does not hold in general, as we will see in the next examples.

Example 10. *Consider the following linear codes, with $n = 1$ and $L = 3$:*

$$\mathcal{C}_1 = \{0,1\}, \quad \mathcal{C}_2 = \{0,1\}, \quad \mathcal{C}_3 = \{0\}.$$

Observe that some numbers obtained via Construction C, i.e., $\Gamma_C = \mathcal{C}_1 + 2\mathcal{C}_2 + 4\mathcal{C}_3 + 8\mathbb{Z}^3$ are represented in Figure 9 and $N(2,1) = 2 \neq 1 = N(0,1)$. Therefore, this constellation does not have equi-distance spectrum and it cannot be geometrically uniform.

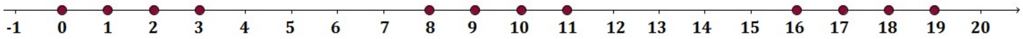

Figure 9 – Some elements of Construction C, with $\mathcal{C}_1 = \mathcal{C}_2 = \{0, 1\}$ and $\mathcal{C}_3 = \{0\}$.

Example 11. *Consider an $n = 2, L = 3$ Construction C with the following three component linear codes:*

$$\mathcal{C}_1 = \mathcal{C}_2 = \{(0, 0), (1, 1)\},\ \mathcal{C}_3 = \{(0, 0)\}. \tag{2.4}$$

We can write $\Gamma_C = \mathcal{C}_1 + 2\mathcal{C}_2 + 4\mathcal{C}_3 + 8\mathbb{Z}^3$ (Figure 10) in this case as

$$\Gamma_C = \{(8k_1 + j, 8k_2 + j) : k_1, k_2 \in \mathbb{Z}, j = 0, 1, 2, 3\}. \tag{2.5}$$

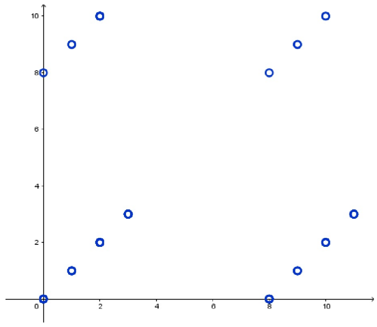

Figure 10 – Some elements of Construction C, with $\mathcal{C}_1 = \mathcal{C}_2 = \{(0, 0), (1, 1)\}$ and $\mathcal{C}_3 = \{(0, 0)\}$.

Note that $N((3, 3), \sqrt{2}) = 1 \neq 2 = N((1, 1), \sqrt{2})$, so it is not equi-distance spectrum and therefore, not geometrically uniform.

2.3 On geometrically uniform constellations

We can derive two ways of producing geometrically uniform constellations, as will be presented by the three main results in this section. In what follows we identify the code $\mathcal{C} \subseteq \mathbb{F}_2^n$ with its natural embedding $\psi(\mathcal{C}) \subseteq \mathbb{R}^n$.

Theorem 4. *(Geometric uniformity of $\Lambda + \mathcal{C}$) If Λ is a lattice which has symmetry with respect to all coordinate axes and $\mathcal{C} \subseteq \mathbb{F}_2^n$ is a linear binary code, then $\Gamma = \Lambda + \mathcal{C}$ is geometrically uniform.*

Proof. Given $x = \lambda_1 + c_1 \in \Gamma$, where $\lambda_1 \in \Lambda$ and $c_1 \in \mathcal{C}$. Consider the linear map $T_{c_1} : \mathbb{R}^n \to \mathbb{R}^n$, $T_{c_1}(z) = [T_{c_1}] \cdot z$ (z in the column format), where $[T_{c_1}]$ is defined as

$$[T_{c_1}] = \begin{pmatrix} (-1)^{c_{11}} & 0 & \dots & 0 \\ 0 & (-1)^{c_{12}} & \dots & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & \dots & (-1)^{c_{1n}} \end{pmatrix}_{(n \times n)}, \tag{2.6}$$

and $c_1 = (c_{11}, c_{12}, \dots, c_{1n})$. Observe that T_{c_1} is an isometry and ${T_{c_1}}^{-1} = T_{c_1}$.

The map $F_x : \mathbb{R}^n \to \mathbb{R}^n$, $F_x(y) = T_{c_1}(y - x)$ is an isometry and we show next that its restriction $F_x|_\Gamma : \Gamma \to \Gamma$ is also an isometry with $F_x(x) = 0$.

First, note that for $c_1, c_2 \in \mathcal{C}$ it is valid that $T_{c_1}(c_2 - c_1) = c_1 \oplus c_2$. Indeed,

$$(T_{c_1}(c_2 - c_1))_i = \begin{cases} 0, & \text{if } (c_{1i}, c_{2i}) = (0,0), \\ 1, & \text{if } (c_{1i}, c_{2i}) = (1,0), \\ 1, & \text{if } (c_{1i}, c_{2i}) = (0,1), \\ 0, & \text{if } (c_{1i}, c_{2i}) = (1,1) \end{cases} \tag{2.7}$$

which implies $T_{c_1}(c_2 - c_1) = c_1 \oplus c_2$.

Given $y \in \Gamma = \Lambda + \mathcal{C}$, $y = \lambda_2 + c_2$,

$$\begin{aligned} F_x(y) = T_{c_1}(y - x) &= T_{c_1}(\lambda_2 - \lambda_1 + c_2 - c_1) = T_{c_1}(\lambda_2 - \lambda_1) + T_{c_1}(c_2 - c_1) \\ &= \lambda_3 + (c_1 \oplus c_2) \in \Gamma = \Lambda + \mathcal{C}, \end{aligned} \tag{2.8}$$

since Λ is axes-symmetric. Therefore, we showed that $F_x(\Gamma) \subseteq \Gamma$.

As F_x is injective, it remains to prove that for any $w = \tilde{\lambda} + \tilde{c} \in \Gamma$ there exists $y \in \Gamma$ such that $w = F_x(y)$. By straightforward calculation we can see that

$$\begin{aligned} F_x(y) = \tilde{\lambda} + \tilde{c} &\Rightarrow T_{c_1}(y - (\lambda_1 + c_1)) = \tilde{\lambda} + \tilde{c} \Rightarrow T_{c_1}(T_{c_1}(y - (\lambda_1 + c_1))) = T_{c_1}(\tilde{\lambda} + \tilde{c}) \\ &\Rightarrow y = T_{c_1}(\tilde{\lambda}) + \lambda_1 + T_{c_1}(\tilde{c}) + c_1 = T_{c_1}(\tilde{\lambda}) + \lambda_1 + T_{c_1}(\tilde{c} - c_1) \\ &\Rightarrow y = T_{c_1}(\tilde{\lambda}) + \lambda_1 + T_{c_1}(\tilde{c} - c_1) = \underbrace{T_{c_1}(\tilde{\lambda}) + \lambda_1}_{\in \Lambda} + \underbrace{\tilde{c} \oplus c_1}_{\in \mathcal{C}} \in \Gamma. \end{aligned} \tag{2.9}$$

To conclude the proof, given any $x \in \Gamma$ and $w \in \Gamma$, we can consider the isometry

$$F : \Gamma \to \Gamma, \quad F = F_w \circ F_x, \tag{2.10}$$

for which we have $F(x) = F_w^{-1}(F_x(x)) = F_w^{-1}(0) = w$. □

Corollary 1. *(Special geometrically uniform Construction C) If a $L-$level Construction C has just two nonzero linear codes C_i and C_L, $i \in \{1, \dots, L-1\}$, then $\Gamma_C = 2^{i-1}\mathcal{C}_i + 2^{L-1}\mathcal{C}_L + 2^L\mathbb{Z}^n$ is geometrically uniform.*

Proof. We can write

$$\Gamma_C = 2^{i-1}(\mathcal{C}_i + 2^{L-i}(\mathcal{C}_L + 2\mathbb{Z}^n)). \tag{2.11}$$

Since the Construction A lattice $\mathcal{C}_L + 2\mathbb{Z}^n$ is axes-symmetric then also is its expansion by 2^{L-i}. From Theorem 4, it follows that $\mathcal{C}_i + 2^{L-i}(\mathcal{C}_{L-1} + 2\mathbb{Z}^n)$, $i = 1, \ldots, L-1$ is geometrically uniform and this also holds for the scaled version. □

As a special case of the above corollary we get the following result, which also can be deduced from [24] (as mentioned previously in Subsection 2.2.3).

Corollary 2. *(Geometric uniformity of a $L = 2$ Construction C) Consider $\Gamma_C = \mathcal{C}_1 + 2\mathcal{C}_2 + 4\mathbb{Z}^n$, where $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathbb{F}_2^n$ are linear codes. Then Γ_C is geometrically uniform.*

Proof. In Corollary 1, take $L = 2$ and $i = 1$. □

In this chapter we recalled known properties of Construction C, such as minimum distance and kissing number, and described some ways of producing geometrically uniform discrete constellations, from what we derived an alternative proof for the geometric uniformity of a $L = 2$ Construction C. We also have shown that in general, for three levels and up, Construction C is not geometrically uniform because it does not have equi-distance spectrum.

Chapter 3

Construction $C^\star$

A new process of constructing lattices and nonlattices periodic constellations, that we call Construction $C^\star$, is proposed in this chapter. We study its properties (geometric uniformity, latticeness and minimum distance) and present some comparison with its associated Construction C. A hybrid Construction $C^\star/C$ is introduced and compared with Construction C in terms of packing efficiency. The proposal of Construction $C^\star$ and the study of its characteristics are motivated by a coding scheme called bit-interleaved coded modulation (BICM) [47], [58] and the particular study of latticeness was inspired by [32]. The results in this chapter appear in [12, 13].

3.1 Why Construction $C^\star$?

A main challenge of communication problems is to transmit digital information over a channel with minimum losses and an alternative to approach it is by using coded modulation ([14, 15]), where not only coding, but also a way of mapping the code bits to constellation symbols is significant. In the latest years, a prevalent coded modulation is the bit-interleaved coded modulation (BICM), which is a motivation to our study.

The BICM, first introduced by Zehavi [58], requires mainly to have: a $nL-$dimensional binary code $\mathcal{C}$, an interleaver π and a one-to-one binary labeling map $\tilde{\mu} : \{0,1\}^L \to \mathcal{X}$, where $\mathcal{X}$ is a signal set $\mathcal{X} = \{0, 1, \dots, 2^L - 1\}$ in order to construct a constellation Γ_{BICM} in $\mathcal{X}^n \subseteq \mathbb{R}^n$. The code and interleaved bit sequence $c \in \mathcal{C}$ is partitioned into L subsequences c_i of length n :

$$c = (c_1, \dots, c_L), \quad \text{with} \quad c_i = (c_{i1}, c_{i2}, \dots, c_{in}). \tag{3.1}$$

The bits c_j are mapped at a time index j to a symbol x_j chosen from the 2^L-ary signal constellation $\mathcal{X}$ according to the binary labeling map $\tilde{\mu}$. Hence, for a $nL-$binary code $\mathcal{C}$ to encode all bits, then we have the scheme below:

$$\boxed{\text{codeword } (c)} \rightarrow \boxed{\text{interleaver } \pi} \rightarrow \boxed{\text{partitioning into L subsequences of length n}} \rightarrow$$

$$\boxed{\text{mapping } \tilde{\mu}} \rightarrow \boxed{x_j = \tilde{\mu}(c_{1j}, \ldots, c_{Lj}),\ j = 1, \ldots, n}$$

In the general case, by defining the natural labeling $\mu : \mathcal{C} \to \mathcal{X}^n$ as $\mu(c_1, c_2, \ldots, c_L) = c_1 + 2c_2 + \cdots + 2^{L-1}c_L$ and assuming $\pi(\mathcal{C}) = \mathcal{C}$, it is possible to define an extended BICM constellation in a way very similar to the well known multilevel Construction C, that we call Construction $C^\star$. Note that the constellation produced via Construction $C^\star$ is always a subset of the associated constellation produced via Construction C for the same projection codes (that will be defined in sequence) and it does not usually produce a lattice.

3.2 Definition

This section is devoted to the introduction of a new method of constructing constellations from binary codes, which we call Construction $C^\star$.

Definition 29. *(Construction $C^\star$) Let $\mathcal{C}$ be a linear code in $\mathbb{F}_2^{nL}$. Construction $C^\star \in \mathbb{R}^n$ is defined as*

$$\begin{aligned} \Gamma_{C^\star} \quad := \quad & \{c_1 + 2c_2 + \cdots + 2^{L-1}c_L + 2^L z : (c_1, c_2, \ldots, c_L) \in \mathcal{C}, \\ & c_i \in \mathbb{F}_2^n, i = 1, \ldots, L, z \in \mathbb{Z}^n\}. \end{aligned} \tag{3.2}$$

Definition 30. *(Projection codes) Let $c = (c_1, c_2, ..., c_L)$ be a partition of a codeword $c = (c_{11}, \ldots, c_{1n}, ..., c_{L1}, \ldots, c_{Ln}) \in \mathcal{C}$ into length n subvectors $c_i = (c_{i1}, ..., c_{in})$, for $i = 1, \ldots, L$. Then, a projection code $\mathcal{C}_i$ consists of all subvectors c_i that appear as we scan through all possible codewords $c \in \mathcal{C}$.*

Note that if $\mathcal{C}$ is linear, then every projection code $\mathcal{C}_i, i = 1, \ldots, L$, is also linear.

Definition 31. *(Associated Construction C) Given a Construction $C^\star$ defined by a linear binary code $\mathcal{C} \subseteq \mathbb{F}_2^{nL}$, we call the associated Construction C the constellation defined as*

$$\Gamma_C = \mathcal{C}_1 + 2\mathcal{C}_2 + \cdots + 2^{L-1}\mathcal{C}_L + 2\mathbb{Z}^n, \tag{3.3}$$

such that $\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_L \in \mathbb{F}_2^n$ are the projection codes of $\mathcal{C}$ as in Definition 30.

Remark 2. *If $\mathcal{C} = \mathcal{C}_1 \times \mathcal{C}_2 \times \cdots \times \mathcal{C}_L$, then Construction $C^\star$ coincides with Construction C, because the projection codes are independent. However, in general, the projection codes are dependent, i.e., not all combinations compose a codeword in the main code $\mathcal{C}$, so we get a subset of the associated Construction C., i.e., $\Gamma_{C^\star} \subseteq \Gamma_C$.*

The following examples illustrate the process of Construction $C^\star$.

Example 12. *Consider a linear binary code $\mathcal{C}$ with length $nL = 4$, $(L = n = 2)$, where $\mathcal{C} = \{(0,0,0,0),\ (1,0,0,1), (1,0,1,0),\ (0,0,1,1)\} \subseteq \mathbb{F}_2^4$. Thus, an element $x(c,z) \in \Gamma_{C^\star}$, $c \in \mathcal{C}, z \in \mathbb{Z}^2$ can be written as*

$$x(c,z) = c_1 + 2c_2 + 4z \ \in \Gamma_{C^\star}, \tag{3.4}$$

for a pair $(c_1, c_2) \in \mathcal{C}$ and $z \in \mathbb{Z}^2$. Geometrically, the resulting constellation is given by the blue points represented in Figure 11. Note that $\Gamma_{C^\star}$ is not a lattice because, for example, $(1,2), (3,0) \in \Gamma_{C^\star}$, but $(1,2) + (3,0) = (4,2) \notin \Gamma_{C^\star}$. However, if we consider the associated Construction C with codes $\mathcal{C}_1 = \{(0,0),(1,0)\}$ and $\mathcal{C}_2 = \{(0,0),(1,1),(0,1),(1,0)\}$, we have a lattice (pink points in Figure 11), because $\mathcal{C}_1$ and $\mathcal{C}_2$ satisfy the condition given by Theorem 1, Subsection 1.2.2.

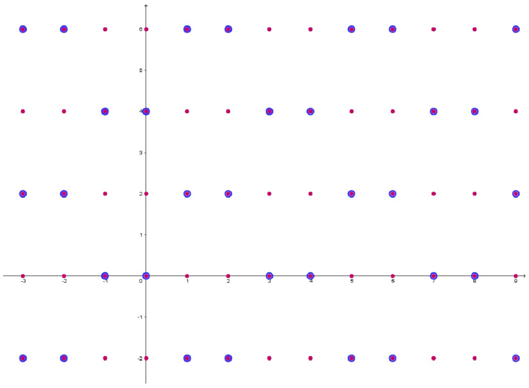

Figure 11 – (Nonlattice) Construction $C^\star$ constellation in blue and its associated (lattice) Construction C constellation in pink.

The next example presents a case where both Constructions $C^\star$ and C are lattices, but they are not equal.

Example 13. *Let a linear binary code $\mathcal{C} = \{(0,0,0,0),\ (0,0,1,0), (1,0,0,1), (1,0,1,1)\} \subseteq \mathbb{F}_2^4$ $(nL = 4,\ L = n = 2)$. The projection codes are $\mathcal{C}_1 = \{(0,0),(1,0)\}$ and $\mathcal{C}_2 = \{(0,0),(1,0),\ (0,1),(1,1)\}$. An element $x(c,z) \in \Gamma_{C^\star}$ can be described as*

$$x(c,z) = \begin{cases} (0,0) + 4z, & \textit{if } c_1 = (0,0) \textit{ and } c_2 = (0,0) \\ (1,2) + 4z, & \textit{if } c_1 = (1,0) \textit{ and } c_2 = (0,1) \\ (2,0) + 4z, & \textit{if } c_1 = (0,0) \textit{ and } c_2 = (1,0) \\ (3,2) + 4z, & \textit{if } c_1 = (1,0) \textit{ and } c_2 = (1,1), \end{cases} \tag{3.5}$$

for all $c = (c_1, c_2) \in \mathcal{C}$ and $z \in \mathbb{Z}^2$. This construction is represented by black points in Figure 12. Note that $\Gamma_{C^\star}$ is a lattice and $\mathcal{C} \neq \mathcal{C}_1 \times \mathcal{C}_2$, which implies that $\Gamma_{C^\star} \neq \Gamma_C$. Nevertheless, the associated Construction C is also a lattice (Figure 12).

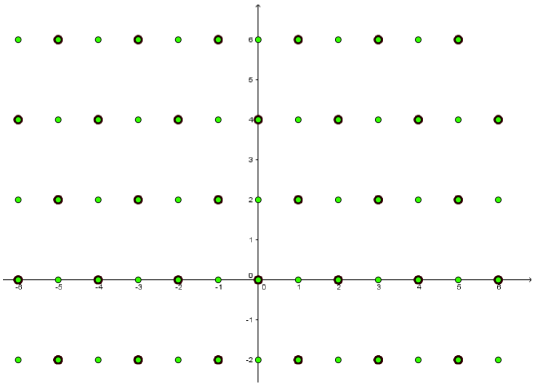

Figure 12 – (Lattice) Construction $C^{\star}$ constellation in black and its associated (lattice) Construction C constellation in green.

To appreciate the advantage of $\Gamma_{C^{\star}}$ *over the associated* Γ_C*, one can notice that the packing densities are, respectively* $\Delta_{\Gamma_{C^{\star}}} = \dfrac{\Pi}{4} \approx 0.7853$ *and* $\Delta_{\Gamma_C} = \dfrac{\Pi}{8} \approx 0.3926$*. Therefore, in this example,* $\Gamma_{C^{\star}}$ *has a better packing density than* Γ_C *(more on that in Section 3.4).*

We can also describe the densest lattice in dimension 24, the Leech lattice Λ_{24}, in terms of Construction $C^{\star}$ constellation with $L = 3$ levels.

Example 14. *Based on the construction given by Conway and Sloane [18] (pp. 131-132) and Amrani et al [5], we start by considering three special linear binary codes*

- $\mathcal{C}_1 = \{(0, \dots, 0), (1, \dots, 1)\} \subseteq \mathbb{F}_2^{24}$;
- $\mathcal{C}_2$ *as a Golay code* $\mathcal{C}_{24} \subset \mathbb{F}_2^{24}$ *achieved by adding a parity bit to the original* $(23, 12, 7)-$*binary Golay code* $\mathcal{C}_{23}$*, which consists in a quadratic residue code of length 23;*
- $\mathcal{C}_3 = \tilde{\mathcal{C}}_3 \cup \overline{\mathcal{C}}_3 = \mathbb{F}_2^{24}$*, where* $\tilde{\mathcal{C}}_3 = \{(x_1, \dots, x_{24}) \in \mathbb{F}_2^{24} : \sum_{i=1}^{24} x_1 \equiv 0 \mod 2\}$ *and* $\overline{\mathcal{C}}_3 = \{(y_1, \dots, y_{24}) \in \mathbb{F}_2^{24} : \sum_{i=1}^{24} y_1 \equiv 1 \mod 2\}$.

Observe that $\mathcal{C}_1, \mathcal{C}_2$ *and* $\mathcal{C}_3$ *are linear codes. Consider a code* $\mathcal{C} \subseteq \mathbb{F}_2^{72}$ *whose codewords are described in one of two possible ways:*

$$\mathcal{C} = \{(0, \dots, 0, \underbrace{a_1, \dots, a_{24}}_{\in \mathcal{C}_{24}}, \underbrace{x_1, \dots, x_{24}}_{\in \tilde{\mathcal{C}}_3}), (1, \dots, 1, \underbrace{a_1, \dots, a_{24}}_{\in \mathcal{C}_{24}}, \underbrace{y_1, \dots, y_{24}}_{\in \overline{\mathcal{C}}_3})\}. \tag{3.6}$$

Thus, we can define the Leech lattice Λ_{24} *as a* $3-$*level Construction* $C^{\star}$ *given by*

$$\Lambda_{24} = \Gamma_{C^{\star}} = \{c_1 + 2c_2 + 4c_3 + 8z : (c_1, c_2, c_3) \in \mathcal{C}, z \in \mathbb{Z}^{24}\}. \tag{3.7}$$

Observe that $\Gamma_{C^\star} \neq \Gamma_C$ and in this case, the associated Construction C has packing density $\Delta_{\Gamma_C} \approx 0.00012 < 0.001929 \approx \Delta_{\Gamma_{C^\star}}$, which is the packing density of Λ_{24}, the best known packing density in dimension 24 [18, pp. 133], [16].

3.3 Properties

3.3.1 Geometric uniformity

According to Subsection 2.2.3, a 2−level Construction C, $\Gamma_C = \mathcal{C}_1 + 2\mathcal{C}_2 + \mathbb{Z}^n$, where $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathbb{F}_2^n$ are linear codes, is geometrically uniform even in the case it is not a lattice. Another question that emerges is as follows: is a 2-level Construction $C^\star$ also geometrically uniform? As we show below, the answer is affirmative.

Theorem 5. *(Geometric uniformity of 2−level Construction $C^\star$) Consider the binary linear code $\mathcal{C} \subseteq \mathbb{F}_2^{2n}$. Then, $\Gamma_{C^\star} = \{c_1 + 2c_2 + 4z : (c_1, c_2) \in \mathcal{C}, z \in \mathbb{Z}^n\}$ is geometrically uniform.*

Proof. Let a binary linear code $\mathcal{C} \subseteq \mathbb{F}_2^{2n}$, which generates a 2−level Construction $C^\star$. Fix an element $x = c_1 + 2c_2 + 4z \in \Gamma_{C^\star}$ and take another arbitrary element $y = \tilde{c}_1 + 2\tilde{c}_2 + 4\tilde{z} \in \Gamma_{C^\star}$, such that $(c_1, c_2), (\tilde{c}_1, \tilde{c}_2) \in \mathcal{C}$ and $z, \tilde{z} \in \mathbb{Z}^n$. Assume the isometry T_{c_1} as given by (2.6). Then,

$$[T_{c_1}(y - x)]_i = (\tilde{c_{1i}} - c_{1i}) \ mod\ 2 \ + 2[(\tilde{c_{2i}} - c_{2i}) \ mod\ 2] + 4z_i',$$

where

$$z_i' = \begin{cases} \tilde{z}_i - z_i, & \text{if } c_{1i} = 0 \text{ and } \tilde{c_{2i}} - c_{2i} \geqslant 0 \\ \tilde{z}_i - z_i + 1, & \text{if } c_{1i} = 0 \text{ and } \tilde{c_{2i}} - c_{2i} < 0 \\ z_i - \tilde{z}_i, & \text{if } c_{1i} = 1 \text{ and } \tilde{c_{2i}} - c_{2i} \leqslant 0 \\ z_i - \tilde{z}_i + 1, & \text{if } c_{1i} = 1 \text{ and } \tilde{c_{2i}} - c_{2i} > 0. \end{cases} \tag{3.8}$$

Clearly $T_{c_1}(y - x) = ((\tilde{c}_1 - c_1) \ mod\ 2, (\tilde{c}_2 - c_2) \ mod\ 2) \in \mathcal{C}$, because $(c_1, c_2) \in \mathcal{C}$ and $(\tilde{c}_1, \tilde{c}_2) \in \mathcal{C} \Rightarrow (\tilde{c}_1 - c_1, \tilde{c}_2 - c_2) \ mod\ 2 \in \mathcal{C}$.

This covers all the possibilities which guarantees that $T_{c_1}(y - x)$ is an element of $\Gamma_{C^\star}$. Moreover, as $T_{c_1}(y - x)$ is an isometry (as a function of y) we can guarantee that for each $y \in \Gamma_{C^\star}$, there exists $y' \in \Gamma_{C^\star}$ such that $T_{c_1}(y' - x) = y$. Therefore, for $L = 2$, $\Gamma_{C^\star}$ is geometrically uniform. □

As we have seen in Example 10, Construction C is not geometrically uniform for general $L \geqslant 3$. If we consider $\mathcal{C} \subseteq \mathbb{F}_2^{3n}$, as the product $\mathcal{C} = \mathcal{C}_1 \times \mathcal{C}_2 \times \mathcal{C}_3$, we get in this particular example, $\Gamma_C = \Gamma_{C^\star}$ and therefore $\Gamma_{C^\star}$ is not geometrically uniform in general for $L \geqslant 3$.

3.3.2 Latticeness

Regarding to latticeness, in general, it is possible to have a lattice $\Gamma_{C^\star}$, with $\Gamma_{C^\star} \neq \Gamma_C$, as can be observed in Example 13. This fact motivates our search for a condition to guarantee the latticeness of Construction $C^\star$, paralleling Theorem 1. Note that in [32] the approach consisted to compare Construction C with the lattice Construction D and in our case, there is no known lattice to be compared, which requires a different strategy. In the upcoming discussion, we will exhibit some definitions and present a necessary and sufficient condition for $\Gamma_{C^\star}$ to be a lattice.

Definition 32. *(Antiprojection) The antiprojection $\mathcal{S}_i(c_1, \ldots, c_{i-1}, c_{i+1}, \ldots, c_L)$ consists of all vectors $c_i \in \mathcal{C}_i$ that appear as we scan through all possible codewords $c \in \mathcal{C}$, while keeping $c_1, \ldots, c_{i-1}, c_{i+1}, \ldots, c_L$ fixed:*

$$\mathcal{S}_i(c_1, ..., c_{i-1}, c_{i+1}, ..., c_L) = \{c_i \in \mathcal{C}_i : (c_1, \ldots, c_{i-1}, \underbrace{c_i}_{i\text{-th posititon}}, c_{i+1}, \ldots, c_L) \in \mathcal{C}\}. \quad (3.9)$$

Example 15. *In Example 13, we can define the antiprojection*

$$\mathcal{S}_2(c_1) = \{c_2 \in \mathcal{C}_2 : (c_1, c_2) \in \mathcal{C}\}. \quad (3.10)$$

For $c_1 = (0,0) \in \mathcal{C}_1$ it follows that $\mathcal{S}_2(c_1) = \{(0,0),(1,0)\}$ and for $c_1 = (1,0) \in \mathcal{C}_1$, $\mathcal{S}_2(c_1) = \{(0,1),(1,1)\}$.

We introduce next the following auxiliary result:

Lemma 1. *(Sum in $\Gamma_{C^\star}$) Let $\mathcal{C} \subseteq \mathbb{F}_2^{nL}$ be a binary linear code. If $x, y \in \Gamma_{C^\star}$ are such that*

$$\begin{aligned} x &= c_1 + 2c_2 + \cdots + 2^{L-1}c_L + 2^L z & (3.11)\\ y &= \tilde{c}_1 + 2\tilde{c}_2 + \cdots + 2^{L-1}\tilde{c}_L + 2^L \tilde{z}, & (3.12)\end{aligned}$$

with $(c_1, c_2, \ldots, c_L), (\tilde{c}_1, \tilde{c}_2, \ldots, \tilde{c}_L) \in \mathcal{C}$ and $z, \tilde{z} \in \mathbb{Z}^n$, then

$$\begin{aligned} x + y &= c_1 \oplus \tilde{c}_1 + 2(s_1 \oplus (c_2 \oplus \tilde{c}_2)) + \cdots + +2^{L-1}(s_{L-1} \oplus (c_L \oplus \tilde{c}_L)) + \\ &\quad +2^L(s_L^\star + z + \tilde{z}), \quad (3.13)\end{aligned}$$

where $s_i \in \mathbb{F}_2^n$ is the "carry" from level i to level $i+1$, given by

$$\begin{gathered} s_i = (c_i * \tilde{c}_i) \oplus r_i^1 \oplus r_i^2 \oplus \cdots \oplus r_i^{i-1} = (c_i * \tilde{c}_i) \bigoplus_{j=1}^{i-1} r_i^j, \\ r_i^1 = (c_i \oplus \tilde{c}_i) * (c_{i-1} * \tilde{c}_{i-1}), \quad r_i^j = r_i^{j-1} * r_{i-1}^{j-1}, \\ 2 \leqslant j \leqslant i-1, i = 1, \ldots, L-1 \quad (3.14)\end{gathered}$$

$s_0 = (0, \ldots, 0)$ and the formula for $s_L^\star$ is the same for s_i but with real sum instead of modulo-2 sum.

Proof. By induction in the number L of levels, we have:

Base case: For $L = 1$ level, $\mathcal{C} \subseteq \mathbb{F}_2^n$ has only one projection code $\mathcal{C}_1$. Consider $x, y \in \Gamma_{C^\star}$ such that $x = c_1 + 2z$ and $y = \tilde{c}_1 + 2\tilde{z}$. Then

$$x + y = c_1 + \tilde{c}_1 + 2(z + \tilde{z}) = c_1 \oplus \tilde{c}_1 + 2(\underbrace{c_1 * \tilde{c}_1}_{s_1 \in \mathbb{Z}^n} + z + \tilde{z}) \tag{3.15}$$

and the result is valid.

Induction step: Assume that the formula in Equation (3.13) is valid for $L = k - 1$, where the main code $\tilde{\mathcal{C}} \in \mathbb{F}_2^{n(k-1)}$ has projection codes $\mathcal{C}_1, \ldots, \mathcal{C}_{k-1} \in \mathbb{F}_2^n$. Therefore, our induction hypothesis affirms that for $x, y \in \Gamma_{C^\star}$ such that

$$x = c_1 + 2c_2 + \cdots + 2^{k-2}c_{k-1} + 2^{k-1}z \tag{3.16}$$

$$y = \tilde{c}_1 + 2\tilde{c}_2 + \cdots + 2^{k-2}\tilde{c}_{k-1} + 2^{k-1}\tilde{z}, \tag{3.17}$$

with $z, \tilde{z} \in \mathbb{Z}^n$, is true that

$$\begin{aligned} x + y &= c_1 \oplus \tilde{c}_1 + 2(s_1 \oplus (c_2 \oplus \tilde{c}_2)) + \cdots + 2^{k-2}(s_{k-2} \oplus (c_{k-1} \oplus \tilde{c}_{k-1})) \\ &+ 2^{k-1}(s_{k-1}^\star + z + \tilde{z}), \end{aligned} \tag{3.18}$$

where $s_{k-1}^\star$ and $s_i, i = 1, \ldots, L$ are as in Equation (3.14).

We aim to prove that the formula presented in Equation (3.13) is also satisfied for $L = k$. So, consider the main code $\mathcal{C} \in \mathbb{F}_2^{nk}$ with subcodes $\mathcal{C}_1, \ldots, \mathcal{C}_{k-1}, \mathcal{C}_k \in \mathbb{F}_2^n$. Suppose $\overline{x}, \overline{y} \in \Gamma_{C^\star}$ such that

$$\overline{x} = c_1 + 2c_2 + \cdots + 2^{k-2}c_{k-1} + 2^{k-1}c_k + 2^k z \tag{3.19}$$

$$\overline{y} = \tilde{c}_1 + 2\tilde{c}_2 + \cdots + 2^{k-2}\tilde{c}_{k-1} + 2^{k-1}\tilde{c}_k + 2^k\tilde{z}. \tag{3.20}$$

So we can write, applying the induction hypothesis

$$\begin{aligned} \overline{x} + \overline{y} &= c_1 \oplus \tilde{c}_1 + 2(s_1 \oplus (c_2 \oplus \tilde{c}_2)) + \cdots + 2^{k-2}(s_{k-2} \oplus (c_{k-1} \oplus \tilde{c}_{k-1})) + \\ & 2^{k-1}(s_{k-1}^\star + c_k + \tilde{c}_k) + 2^k(z + \tilde{z}), \end{aligned} \tag{3.21}$$

where $s_{k-1}^\star$ is s_{k-1} with the real sum instead of modulo-2 sum. By doing all the decompositions to change the real sum $s_{k-1}^\star + c_k + \tilde{c}_k$ to $s_{k-1} \oplus c_k \oplus \tilde{c}_k$ we have

$$\begin{aligned} \overline{x} + \overline{y} &= c_1 \oplus \tilde{c}_1 + 2(s_1 \oplus (c_2 \oplus \tilde{c}_2)) + \cdots + 2^{k-2}(s_{k-2} \oplus (c_{k-1} \oplus \tilde{c}_{k-1})) + \\ & 2^{k-1}(s_{k-1} \oplus (c_k \oplus \tilde{c}_k)) + 2^k(\underbrace{(c_k * \tilde{c}_k) + r_k^1 + r_k^2 + \cdots + r_k^{k-1}}_{s_k^\star} + z + \tilde{z}). \end{aligned} \tag{3.22}$$

This formula is exactly as we expected and it concludes the proof. □

The mathematical intuition behind the necessary and sufficient condition to guarantee that $\Gamma_{C^\star}$ is a lattice lies in the fact that since $a+b = a \oplus b + 2(a * b)$ for $a, b \in \mathbb{F}_2^n$, when adding two points in $\Gamma_{C^\star}$, each codeword at level $i \geqslant 2$ has the form of $c_i \oplus \tilde{c}_i \oplus carry_{(i-1)}$, where $carry_{(i-1)}$ is the "carry" term from the addition in the lower level. Since the projection code $\mathcal{C}_i$ is linear, $c_i \oplus \tilde{c}_i$ is a codeword in the $i-$th level. Hence, closeness of $\Gamma_{C^\star}$ under addition amounts to the fact that $carry_{(i-1)}$ is also a codeword in $\mathcal{C}_i$, which is essentially the condition of the theorem. Formally,

Theorem 6. *(Lattice condition for $\Gamma_{C^\star}$) Let $\mathcal{C} \subseteq \mathbb{F}_2^{nL}$ be a linear binary code that generates $\Gamma_{C^\star}$ and let the set $\mathcal{S} = \{(0, s_1, \ldots, s_{L-1})\} \subseteq \mathbb{F}_2^{nL}$ defined for all pairs $c, \tilde{c} \in \mathcal{C}$ (including the case $c = \tilde{c}$), where*

$$s_i = (c_i * \tilde{c}_i) \oplus r_i^1 \oplus r_i^2 \oplus \cdots \oplus r_i^{i-1} = (c_i * \tilde{c}_i) \bigoplus_{j=1}^{i-1} r_i^j,$$
$$r_i^1 = (c_i \oplus \tilde{c}_i) * (c_{i-1} * \tilde{c}_{i-1}), \quad r_i^j = r_i^{j-1} * r_{i-1}^{j-1},$$
$$2 \leqslant j \leqslant i-1, i = 2, \ldots, L-1, \tag{3.23}$$

$s_0 = (0, \ldots, 0)$ and $s_1 = c_1 * \tilde{c}_1$. Then, the constellation $\Gamma_{C^\star}$ is a lattice if and only if $\mathcal{S} \subseteq \mathcal{C}$.

Proof. ($\Rightarrow$) First, $\Gamma_{C^\star}$ is assumed to be lattice, which implies that if $x, y \in \Gamma_{C^\star}$ then $x + y \in \Gamma_{C^\star}$. From the notation and result from Lemma 1, more specifically Equations (3.16), (3.17), (3.13) and (3.14), it means that

$$(c_1 \oplus \tilde{c}_1, s_1 \oplus (c_2 \oplus \tilde{c}_2), \ldots, s_{L-1} \oplus (c_L \oplus \tilde{c}_L)) \in \mathcal{C}. \tag{3.24}$$

We can write this $L-$tuple as

$$\underbrace{(c_1 \oplus \tilde{c}_1, s_1 \oplus (c_2 \oplus \tilde{c}_2), \ldots, s_{L-1} \oplus (c_L \oplus \tilde{c}_L))}_{\in \mathcal{C}} =$$
$$\underbrace{(c_1 \oplus \tilde{c}_1, c_2 \oplus \tilde{c}_2, \ldots, c_L \oplus \tilde{c}_L)}_{\in \mathcal{C},\ \text{by linearity of } \mathcal{C}} \oplus (0, s_1, \ldots, s_{L-1}) \Rightarrow (0, s_1, \ldots, s_{L-1}) \in \mathcal{C}, \tag{3.25}$$

which is the same as saying that for all $x, y \in \Gamma_{C^\star}$, $\mathcal{S} \subseteq \mathcal{C}$.

($\Leftarrow$) The converse is immediate, because given $x, y \in \Gamma_{C^\star}$ as in Equations (3.16) and (3.17), with the fact that $\mathcal{C}$ is linear and $\mathcal{S} \subseteq \mathcal{C}$, it is valid that

$$(c_1 \oplus \tilde{c}_1, c_2 \oplus \tilde{c}_2, \ldots, c_L \oplus \tilde{c}_L) \oplus (0, s_1, \ldots, s_{L-1}) \in \mathcal{C}$$
$$\Rightarrow \quad (c_1 \oplus \tilde{c}_1, s_1 \oplus (c_2 \oplus \tilde{c}_2), \ldots, s_{L-1} \oplus (c_L \oplus \tilde{c}_L)) \in \mathcal{C} \tag{3.26}$$

and $x + y \in \Gamma_{C^\star}$. We still need to prove that there exist the inverse element $-x \in \Gamma_{C^\star}$. It is true that for $x \in \Gamma_{C^\star}$, $x + x \in \Gamma_{C^\star}$ and also $(x + x) + (x + x) \in \Gamma_{C^\star}$. If we do this sum recursively, i.e., $\underbrace{x + x + x + \cdots + x}_{2^L \text{ times}} = 2^L j$, for a suitably $j \in \mathbb{Z}^n$. So, if we consider $y = \underbrace{x + x + \cdots + x}_{2^L - 1 \text{ times}} + 2^L(-j) \in \Gamma_{C^\star}$, it follows that $x + y = 0 \in \mathbb{R}^n$ and $y = -x$. □

Example 16. *Consider the linear binary code given by* $\mathcal{C} = \{(0,0,0,0,0,0), (1,0,1,1,0,1), (0,0,1,0,1,1), (1,0,0,1,1,0), (0,0,0,0,1,0), (0,0,1,0,0,1), (1,0,0,1,0,0), (1,0,1,1,1,1)\} \subseteq \mathbb{F}_2^6$ *with* $L = 3, n = 2$*. In this specific case, it is possible to describe the set* $\mathcal{S} = \{(0,0,0,0,0,0),\ (0,0,1,0,1,1), (0,0,0,0,1,0), (0,0,1,0,0,1)\} \subseteq \mathcal{C}$*. Therefore, according to Theorem 6,* $\Gamma_{C^\star}$ *is a lattice (Figure 13).*

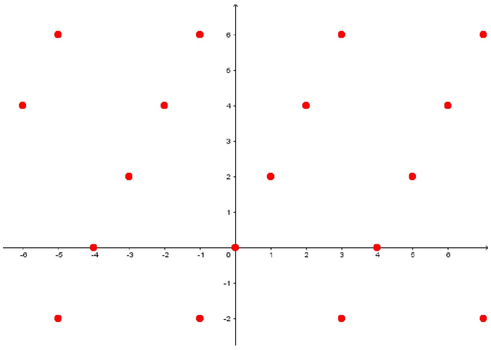

Figure 13 – Lattice Construction $C^\star$ constellation.

Remark 3. *Note that with the assumption that* $\mathcal{C} = \mathcal{C}_1 \times \mathcal{C}_2 \times \cdots \times \mathcal{C}_L$*, i.e.,* $\Gamma_C = \Gamma_{C^\star}$*, it follows that* $\mathcal{S} \subseteq \mathcal{C}$ *is equivalent to* $\mathcal{C}_1 \subseteq \mathcal{C}_2 \subseteq \cdots \subseteq \mathcal{C}_L$ *and the chain is closed under Schur product (Theorem 1). Indeed,*

i) $\mathcal{S} \subseteq \mathcal{C} \Rightarrow \mathcal{C}_1 \subseteq \mathcal{C}_2 \subseteq \cdots \subseteq \mathcal{C}_L$ *and the chain is closed under Schur product: we know that* $\mathcal{S} \subseteq \mathcal{C}$ *for any pair* $c, \tilde{c}$ *of codewords, so we take in particular* $\tilde{c} = c$ *and it follows that* $\mathcal{C}_1 \subseteq \mathcal{C}_2 \subseteq \cdots \subseteq \mathcal{C}_L$*. The fact that* $\mathcal{C} = \mathcal{C}_1 \times \mathcal{C}_2 \times \cdots \times \mathcal{C}_L$ *allows us to guarantee that the element* $(0, c_1 * \tilde{c}_1, c_2 * \tilde{c}_2, \ldots, c_{L-1} * \tilde{c}_{L-1}) \in \mathcal{S} \subseteq \mathcal{C}$ *and then the above chain will be closed under Schur product.*

ii) $\mathcal{C}_1 \subseteq \mathcal{C}_2 \subseteq \cdots \subseteq \mathcal{C}_L$ *and the chain is closed under Schur product* $\Rightarrow \mathcal{S} \subseteq \mathcal{C}$ *: consider an element* $(0, s_1, s_2, \ldots, s_{L-1}) \in \mathcal{S}$*, we want to prove that this element is also in* $\mathcal{C}$ *and to do that it is enough to prove that* $s_1 \in \mathcal{C}_2, s_2 \in \mathcal{C}_3, \ldots,\ s_{L-1} \in \mathcal{C}_L$*. Indeed, due to the chain be closed under Schur product,*

$$
\begin{aligned}
s_1 &= c_1 * \tilde{c}_1 \in \mathcal{C}_2 && (3.27)\\
s_2 &= \underbrace{((c_1 * \tilde{c}_1) * (c_2 \oplus \tilde{c}_2))}_{\in \mathcal{C}_3} \oplus \underbrace{(c_2 * \tilde{c}_2)}_{\in \mathcal{C}_3} \in \mathcal{C}_3 && (3.28)\\
s_3 &= \underbrace{((c_3 \oplus \tilde{c}_3) * (c_2 * \tilde{c}_2)) * (c_2 \oplus \tilde{c}_2 * (c_1 * \tilde{c}_1))}_{\in \mathcal{C}_4}\\
&\oplus \ \underbrace{((c_3 \oplus \tilde{c}_3) * (c_2 * \tilde{c}_2))}_{\in \mathcal{C}_4} \oplus \underbrace{(c_3 * \tilde{c}_3)}_{\in \mathcal{C}_4} \in \mathcal{C}_4 && (3.29)\\
&\ \ \vdots
\end{aligned}
$$

and proceeding recursively, we can prove that $s_i \in \mathcal{C}_{i+1}, i = 1, \ldots, L-1$.

The previous remark lead the us to the following result.

Corollary 3. *(Latticeness of the associated Construction C) Let $\mathcal{C} \subseteq \mathbb{F}_2^{nL}$ be a linear code. If $\Gamma_{C^\star}$ is a lattice then the associated Construction C is also a lattice.*

Proof. If $\Gamma_{C^\star}$ is a lattice, then according to Theorem 6, $\mathcal{S} \subseteq \mathcal{C}$. When we construct the associated Construction C, we make $\mathcal{C} = \mathcal{C}_1 \times \mathcal{C}_2 \times \cdots \times \mathcal{C}_L$, where $\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_L$ are the projection codes. Hence, according to the Remark 3, $\mathcal{S} \subseteq \mathcal{C}$ is equivalent to $\mathcal{C}_1 \subseteq \mathcal{C}_2 \subseteq \cdots \subseteq \mathcal{C}_L$ and the chain being closed under Schur product, which is sufficient to guarantee that Γ_C is a lattice. □

Observe that the condition given by Theorem 6 is well-established. However, it is not easy to check for lattices in higher dimensions. For this reason, we introduce the following consequent result which is weaker, but easier to verify in general.

Corollary 4. *(Special lattice condition for $\Gamma_{C^\star}$) Let $\mathcal{C} \subseteq \mathbb{F}_2^{nL}$ be a linear binary code with projection codes $\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_L$ such that $\mathcal{C}_1 \subseteq \mathcal{S}_2(0, \ldots, 0) \subseteq \mathcal{C}_2 \subseteq \cdots \subseteq \mathcal{C}_{L-1} \subseteq \mathcal{S}_L(0, \ldots, 0) \subseteq \mathcal{C}_L \subseteq \mathbb{F}_2^n$. Then the constellation given by $\Gamma_{C^\star}$ is a lattice if and only if $\mathcal{S}_i(0, \ldots, 0)$ closes $\mathcal{C}_{i-1}$ under Schur product for all levels $i = 2, \ldots, L$.*

Proof. ($\Leftarrow$) For any $x, y \in \Gamma_{C^\star}$, written as in Equations (3.16) and (3.17), we have $x + y$ as given in Lemma 1 (Equations (3.13) and (3.14)) and we need to verify if $x + y \in \Gamma_{C^\star}$.

Clearly $x + y \in \mathcal{C}_1 + 2\mathcal{C}_2 + \cdots + 2^{L-1}\mathcal{C}_L + 2^L\mathbb{Z}^n$. It remains to demonstrate that $(c_1 \oplus \tilde{c}_1, s_1 \oplus c_2 \oplus \tilde{c}_2, \ldots, s_{L-1} \oplus c_L \oplus \tilde{c}_L) \in \mathcal{C}$.

Indeed, using the fact that the chains $\mathcal{C}_{i-1} \subseteq \mathcal{S}_i(0, \ldots, 0)$ for all $i = 2, \ldots, L$ are closed under the Schur product, it is an element of $\mathcal{C}$ because it is a sum of elements in $\mathcal{C}$, i.e.,

$$\begin{aligned}
&(c_1 \oplus \tilde{c}_1, s_1 \oplus c_2 \oplus \tilde{c}_2, \ldots, s_{L-1} \oplus c_L \oplus \tilde{c}_L) = \\
&\underbrace{(c_1 \oplus \tilde{c}_1, c_2 \oplus \tilde{c}_2, \ldots, c_L \oplus \tilde{c}_L)}_{\in \mathcal{C}} \oplus \underbrace{(0, s_1, \ldots, 0)}_{\in \mathcal{C}} \oplus \cdots \oplus \\
&\oplus \underbrace{(0, \ldots, 0, s_{L-1})}_{\in \mathcal{C}} \Rightarrow (0, s_1, \ldots, s_{L-1}) \in \mathcal{C}
\end{aligned} \tag{3.30}$$

and from Theorem 6, $\Gamma_{C^\star}$ is a lattice. Observe that any $nL-$tuple $(0, \ldots, s_{i-1}, \ldots, 0)$ is in $\mathcal{C}$ because by hypothesis, the chain $\mathcal{S}_i(0, \ldots, 0)$ closes $\mathcal{C}_{i-1}$ under Schur product, hence $S_i(0, \ldots, 0)$ contains $(c_{i-1} * \tilde{c}_{i-1}), r_{i-1}^1, ..., r_{i-1}^{i-2}$ which is sufficient to guarantee that $s_{i-1} \in \mathcal{S}_i(0, \ldots, 0)$ so $(0, \ldots, s_{i-1}, \ldots, 0) \in \mathcal{C}$, for all $i = 2, \ldots, L - 1$. Using analogous arguments to the ones in Theorem 6, given $x \in \Gamma_{C^\star}$ it is true that $-x \in \Gamma_{C^\star}$.

($\Rightarrow$) For the converse, we know that given $x, y \in \Gamma_{C^\star}$ then $x + y \in \Gamma_{C^\star}$. From the notation and result from Lemma 1, more specifically Equations (3.16), (3.17), (3.13) and (3.14), it means that

$$(c_1 \oplus \tilde{c}_1, s_1 \oplus (c_2 \oplus \tilde{c}_2), \ldots, s_{L-1} \oplus (c_L \oplus \tilde{c}_L)) \in \mathcal{C} \tag{3.31}$$

and from the result of Theorem 6 follows that

$$(0, s_1, \ldots, s_{L-1}) \in \mathcal{C}, \tag{3.32}$$

where s_i, $i = 1, \ldots, L-1$ are defined as in Equations (3.28)–(3.30).

Due to the nesting $\mathcal{C}_1 \subseteq \mathcal{S}_2(0,\ldots,0) \subseteq \cdots \subseteq \mathcal{C}_{L-1} \subseteq \mathcal{S}_L(0,\ldots,0) \subseteq \mathcal{C}_L$, we can guarantee that there exist codewords with particular Schur products $c_i * \tilde{c}_i = 0$, for $i = 1, \ldots, L-2$. Thus, $s_{L-1} = (c_{L-1} * \tilde{c}_{L-1})$ and from Equation (3.32), $(0, 0, \ldots, c_{L-1} * \tilde{c}_{L-1}) \in \mathcal{C}$, i.e., $S_L(0,\ldots,0)$ must close $\mathcal{C}_{L-1}$ under Schur product. Proceeding similarly, we demonstrate that $S_i(0,\ldots,0)$ must close $\mathcal{C}_{i-1}$, for all $i = 2, \ldots, L$ and it completes our proof. □

While $\mathcal{S}_i(0,\ldots,0) \subseteq \mathcal{C}_i$ by construction, note that the assumption that $\mathcal{C}_i \subseteq \mathcal{S}_{i+1}(0,\ldots,0)$, for $i = 2, \ldots, L$ in Corollary 4 is not always satisfied by a general Construction $C^\star$, sometimes even if this Construction $C^\star$ is a lattice (see Example 16). In this cases we need the more general condition stated by Theorem 6.

We will see in the following example that the construction of the Leech lattice described in Example 14 satisfies the condition proposed by Corollary 4, which is easier to verify.

Example 17. *Observe that for the codes $\mathcal{C}_1, \mathcal{C}_2$ and $\mathcal{C}_3$ from Example 14, $\mathcal{S}_2(0,\ldots,0) = \mathcal{C}_2$ and $\mathcal{S}_3(0,\ldots,0) = \tilde{\mathcal{C}}_3 = \{(x_1,\ldots,x_{24}) \in \mathbb{F}_2^{24} : \sum_{i=1}^{24} x_1 \equiv 0 \mod 2\}$. Hence we need to verify that $\mathcal{C}_1 \subseteq \mathcal{S}_2(0,\ldots,0) \subseteq \mathcal{C}_2 \subseteq \mathcal{S}_3(0,\ldots,0) \subseteq \mathcal{C}_3$ and that $\mathcal{S}_i(0,\ldots,0)$ closes $\mathcal{C}_{i-1}$ under Schur product for $i = 2, 3$.*

Indeed $\mathcal{C}_1 \subseteq \mathcal{S}_2(0,\ldots,0) = \mathcal{C}_2$, since $(0,\ldots,0) \in \mathcal{C}_2$ and if we consider the parity check matrix $H \in \mathbb{F}_2^{12\times 24}$ of the $[24,12,8]-$Golay code $H = \left(B_{12\times 12} \quad | \quad I_{12\times 12},\right)$, where

$$B_{12\times 12} = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix} \tag{3.33}$$

it is easy to check that $H \cdot (1, \ldots, 1)^T = 0 \in \mathbb{F}_2^{12}$*, so* $(1, \ldots, 1) \in \mathcal{C}_2$ *which implies that* $\mathcal{C}_1 \subseteq \mathcal{S}_2(0, \ldots, 0)$*.*

Moreover, an element $c_2 \in \mathcal{C}_2$ *can be written as* $c_2 = G.h$*, where* $G = \begin{pmatrix} I_{12\times 12} \\ \hline B_{12\times 12} \end{pmatrix}$ *is the generator matrix of the Golay code and* $h = (h_1, h_2, h_3, h_4, h_5, h_6, h_7, h_8, h_9, h_{10}, h_{11}, h_{12})^T \in \mathbb{F}_2^{12}$*. Thus, when we sum all the coordinates of the resulting vector* $c_2 = G.h$ *we have* $8h_1 + 8h_2 + 8h_3 + 8h_4 + 8h_5 + 8h_6 + 8h_7 + 8h_8 + 8h_9 + 8h_{10} + 8h_{11} + 12h_{12} \equiv 0 \mod 2 \Rightarrow c_2 \in \tilde{\mathcal{C}_3} = \mathcal{S}_3(0, \ldots, 0)$*. Hence,*

$$\mathcal{C}_1 \subseteq \mathcal{S}_2(0, \ldots, 0) \subseteq \mathcal{C}_2 \subseteq \mathcal{S}_3(0, \ldots, 0) \subseteq \mathcal{C}_3. \tag{3.34}$$

We still need to prove that

- $\mathcal{S}_2(0, \ldots, 0)$ *closes* $\mathcal{C}_1$ *under Schur product and this is clearly true because the Schur product of any elements in* $\mathcal{C}_1$ *belong to* $\mathcal{S}_2(0, \ldots, 0)$*.*
- $\mathcal{S}_3(0, \ldots, 0)$ *closes* $\mathcal{C}_2$ *under Schur product: if we consider* $c_2 = G.h \in \mathcal{C}_2$ *and* $\tilde{c}_2 = G.\tilde{h} \in \mathcal{C}_2$*, we have checked computationally that the sum of all coordinates of the Schur product* $c_2 * \tilde{c}_2 \equiv 0 \mod 2 \Rightarrow c_2 * \tilde{c}_2 \in \mathcal{S}_3(0, \ldots, 0) = \tilde{\mathcal{C}_3}$*.*

3.3.3 Minimum Euclidean distance

In this section we will study the minimum Euclidean distance of Construction $C^\star$ considering the identity interleaver and a random interleaver.

An important remark is that unlike Construction C, Construction $C^\star$ is not equi-minimum distance . More precisely, if the minimum distance d is achieved by two points $x, y \in \Gamma_{C^\star}$, i.e., $||x - y|| = d$ there may be some other $x' \in \Gamma_{C^\star}$ such that there is no $y' \in \Gamma_{C^\star}$ that makes $||x' - y'|| = d$.

Example 18. *Consider an* $L = 3$ *and* $n = 1$ *Construction* $C^\star$ *with main binary code* $\mathcal{C} = \{(0,0,0), (1,0,1), (0,1,1), (1,1,0)\} \subset \mathbb{F}_2^3$*. Thus, elements in* $\Gamma_{C^\star}$ *are*

$$\Gamma_{C^\star} = \{0 + 8z, 5 + 8z, 6 + 8z, 3 + 8z\}, z \in \mathbb{Z}. \tag{3.35}$$

The minimum Euclidean distance is $||6 - 5|| = 1$ *and if we fix* $x' = 0 \in \Gamma_{C^\star}$ *there is no element* $y' \in \Gamma_{C^\star}$ *such that* $||y'|| = 1$*.*

3.3.3.1 Identity interleaving

If $\Gamma_{C^\star}$ is equi-minimum distance, $d^2_{min}(\Gamma_{C^\star}) = d^2_{min}(\Gamma_{C^\star}, 0)$ (distance from any constellation point to zero), we know that to each $c \in \mathcal{C} \subseteq \mathbb{F}_2^{nL}, c \neq 0$ we associate a unique element $x(c) \in \Gamma_{C^\star} \subseteq \mathbb{R}^n$ in the hypercube $[-2^{L-1}, 2^{L-1}]^n$, which gives the minimum distance of $\Gamma_{C^\star}(c)$ (constellation points generated by $c \in \mathcal{C}$.)

An explicit expression for the nearest constellation point to zero regarding signals is

$$d^2_{min}(\Gamma_{C^\star}, 0) = m_1 + 2^2 m_2 + 3^2 m_3 + \cdots + (2^{L-1}-1)^2 m_{2^{L-1}-1} + (2^{L-1})^2 m_{2^{L-1}}, \quad (3.36)$$

where $m_i, i = 1, \ldots, 2^{L-1}$ are obtained as follows. For $c = (c_{11}, \ldots, c_{1n}, c_{21}, \ldots, c_{2n}, \ldots, c_{L1}, \ldots, c_{Ln})$ we consider the $L-$tuples $c_1 = (c_{11}, \ldots, c_{L1})$, $c_2 = (c_{12}, \ldots, c_{L2}), \ldots, c_L = (c_{1n}, \ldots, c_{Ln})$ and $m_j, j = 1, \ldots, 2^{L-1}$ as

$$\begin{aligned} m_j \;&=\; \text{number of } L-\textit{tuples } c_i \text{ such that } c_i \text{ is the binary representation} \\ &\quad\; \text{of j or the binary representation of } 2^{L-1}-j. \qquad (3.37) \end{aligned}$$

To be more specific,

$$\begin{aligned} m_1 &= \text{the number of } c_i's \text{ such that } c_i = v_i = (1,0,\ldots,0) \text{ or } c_i = \tilde{v}_i = (1,1,\ldots,1) \\ m_2 &= \text{the number of } c_i's \text{ such that } c_i = v_i = (0,1,\ldots,0) \text{ or } c_i = \tilde{v}_i = (0,1,\ldots,1) \\ m_3 &= \text{the number of } c_i's \text{ such that } c_i = v_i = (1,1,0,\ldots,0) \text{ or } c_i = \tilde{v}_i = (1,0,1,\ldots,1) \\ m_4 &= \text{the number of } c_i's \text{ such that } c_i = v_i = (0,0,1,\ldots,0) \text{ or } c_i = \tilde{v}_i = (0,0,1,\ldots,1) \\ &\vdots \qquad \vdots \\ m_{2^{L-1}-1} &= \text{the number of } c_i's \text{ such that } c_i = v_i = (1,0,\ldots,1,0) \text{ or } c_i = \tilde{v}_i = (1,1,\ldots,0,1) \\ m_{2^{L-1}} &= \text{the number of } c_i's \text{ such that } c_i = (0,0,0,\ldots,0,1). \qquad (3.38) \end{aligned}$$

Note that $\tilde{v}_i$ have the same coordinates of v_i up to the first non vanishing coordinate and after that all coordinates are different. Moreover, $\sum_{i=1}^{2^L-1} m_i = n$.

Remark 4. *From the expression above, we can see that given a codeword $c \in \mathcal{C}$ of weight $\omega(\mathcal{C}) = k$,*

$$d^2_{min}(\Gamma_{C^\star}, 0) \geqslant \frac{k}{L}, \quad (3.39)$$

since the minimum distance will be achieved when the projection codewords of c are more equal as possible. Therefore, if the minimum weight w of the code $\mathcal{C}$ is such that $w \geqslant L2^{2L}$, we can assert that

$$d^2_{min}(\Gamma_{C^\star}, 0) = 2^{2L}. \quad (3.40)$$

Example 19. *For $L = 2$ and $w \geqslant 32$, ($n \geqslant 16$, n is as large as we want),*

$$d^2_{min}(\Gamma_{C^\star}, 0) = 2^4. \quad (3.41)$$

A more concise expression for the minimum distance to zero in $\Gamma_{C^\star}$ can also be derived from (3.37), by observing that for $c = (c_1, c_2, \ldots, c_L) \in \mathcal{C}$, with $c \neq 0$ and $c_i = (c_{i1}, c_{i2}, \ldots, c_{in})$, $i = 1, \ldots, L$:

$$d^2_{min}(\Gamma_{C^\star}(c), 0) = ||2^{L-1}c_L - 2^{L-2}c_{L-1} - \cdots - 2c_2 - c_1||^2. \quad (3.42)$$

From that we get the following result:

Proposition 3. *(Minimum distance of a geometrically uniform $\Gamma_{C^\star}$) Consider a linear code $\mathcal{C} \subseteq \mathbb{F}_2^{nL}$ which defines $\Gamma_{C^\star}$. If $\Gamma_{C^\star}$ is geometrically uniform, then its minimum distance is given by*

$$d^2_{min}(\Gamma_{C^\star}, 0) = \min_{\substack{c=(c_1,c_2,\ldots,c_L)\in\mathcal{C}\\ c\neq 0}} \left\{ ||2^{L-1}c_L - \sum_{i=1}^{L-1} 2^{i-1}c_i||^2, 2^{2L} \right\}. \tag{3.43}$$

If $\Gamma_{C^\star}$ is geometrically uniform, the above expression provides a closed formula for the minimum distance of $\Gamma_{C^\star}$, otherwise it is an upper bound for this distance. Therefore (3.43) presents a closed formula for the minimum distance of a $L = 2$ Construction $C^\star$ (Theorem 5) and also when $\Gamma_{C^\star}$ is a lattice (Theorem 6).

From (3.43), it could be expected that given a code $\mathcal{C} \subseteq \mathbb{F}_2^{nL}$ with minimum weight of projection codes $d_H(\mathcal{C}_1), \ldots, d_H(\mathcal{C}_L)$, a larger minimum distance will be achieved as $d_H(\mathcal{C}_i)$ increases with i.

For example, for $L = 2$ and weights of projection codes given by $d_H(\mathcal{C}_1)$ and $d_H(\mathcal{C}_2)$, respectively, if $d_H(\mathcal{C}_2) > d_H(\mathcal{C}_1)$, by considering $||2c_2 - c_1||^2 = \langle 2c_2 - c_1, 2c_2 - c_1\rangle$, we can derive from (3.43) that

$$d^2_{min}(\Gamma_{C^\star}) \geqslant \min\{4d_H(\mathcal{C}_2) - 3d_H(\mathcal{C}_1), 16\}. \tag{3.44}$$

Example 20. *In Example 12, we have $\mathcal{C} = \{(0,0,0,0), (1,0,0,1), (1,0,1,0), (0,0,1,1)\}$ and then, according to 3.43,*

$$d^2_{min}(\Gamma_{C^\star}) = \min\{5, 1, 8, 16\} = 1. \tag{3.45}$$

Regarding to general upper and lower bounds, since $\Gamma_{C^\star}$ is a subset of Γ_C, $d^2_{min}(\Gamma_{C^\star}) \geqslant d^2_{min}(\Gamma_C)$, where Γ_C is the associated Construction C (Definition 31). A looser and easier upper bound for $d^2_{min}(\Gamma_{C^\star})$ is given by:

$$d^2_{min}(\Gamma_{C^\star}) \leqslant d^2_{min}(\Gamma_{C^\star}, 0) \leqslant d^2_{min}(\overline{\mathcal{S}}) = \min_{d_H(\mathcal{S}_i(0,\ldots,0))\neq 0} \{2^{2(i-1)} d_H(\mathcal{S}_i(0,\ldots,0)), 2^{2L}\}, \tag{3.46}$$

for $i = 1, \ldots, L$.

Example 21. *For the Leech lattice presented in Example 14, it follows that $d^2_{min}(\Gamma_C) = \min\{24, 32, 32, 64\} = 24$, $d^2_{min}(\overline{\mathcal{S}}) = \min\{32, 32, 64\} = 32$ as $\mathcal{S}_1(0,\ldots,0)$ is a null set and $d^2_{min}(\Gamma_{C^\star}, 0) = 32$. In this case, $d^2_{min}(\Gamma_{C^\star}) = 32$.*

Example 22. *In Example 16, $d^2_{min}(\Gamma_C) = \min\{1, 4, 16\} = 1$ and $d^2_{min}(\overline{\mathcal{S}}) = \min\{16\} = 16$ as $\mathcal{S}_1(0,\ldots,0)$ and $\mathcal{S}_2(0,\ldots,0)$ are null sets. Also, $d^2_{min}(\Gamma_{C^\star}, 0) = 5$, which coincides with $d^2_{min}(\Gamma_{C^\star})$, because in this case Construction $C^\star$ is a lattice.*

Example 23. *In Example 18, if we consider the associated Construction C, we have* $d^2_{min}(\Gamma_C) = \min\{1, 4, 16, 64\} = 1$*,* $d^2_{min}(\overline{\mathcal{S}}) = \min\{64\} = 64$ *as* $\mathcal{S}_i(0, \ldots, 0)$ *are null sets for all* $i = 1, 2, 3$ *and* $d^2_{min}(\Gamma_{C^\star}, 0) = 2$*. Here,* $d^2_{min}(\Gamma_{C^\star}) = 1$*.*

To derive a condition that states when Construction $C^\star$ have a better packing density than its associated Construction C, we observe that both constellations contains the lattice $2^L\mathbb{Z}^n$, i.e., $2^L\mathbb{Z}^n \subseteq \Gamma_{C^\star} \subseteq \Gamma_C$. If the number of points of $\Gamma_{C^\star}$ and Γ_C inside the hypercube $[0, 2^L]^n$ are respectively $|\mathcal{C}|$ and $|\mathcal{C}_1| \ldots |\mathcal{C}_L|$, where $\mathcal{C}_i, i = 1, \ldots, L$ are the projection codes, we can assert

$$\Delta(\Gamma_{C^\star}) = \frac{|\mathcal{C}| \; vol\left(B\left(0, \frac{d_1}{2}\right)\right)}{2^{nL}} \quad \text{and} \quad \Delta(\Gamma_C) = \frac{|\mathcal{C}_1| \ldots |\mathcal{C}_L| \; vol\left(B\left(0, \frac{d_2}{2}\right)\right)}{2^{nL}}, \tag{3.47}$$

where $d_1 = d_{min}(\Gamma_{C^\star})$ and $d_2 = d_{min}(\Gamma_C)$. Hence, we can write the following remark:

Remark 5. *1.* $\Delta(\Gamma_{C^\star}) \geqslant \Delta(\Gamma_C)$ *if and only if* $\left(\frac{d_1}{d_2}\right)^n \geqslant \frac{|\mathcal{C}_1| \ldots |\mathcal{C}_L|}{|\mathcal{C}|}$,

2. $\chi(\Gamma_{C^\star}) \geqslant \chi(\Gamma_C)$ *if and only if* $\frac{d_1}{d_2} \geqslant \left(\frac{|\mathcal{C}_1| \ldots |\mathcal{C}_L|}{|\mathcal{C}|}\right)^{1/n}$.

Example 24. *Let* $\mathcal{C} \subseteq \mathbb{F}_2^{2n}$*, i.e., we are considering a Construction* $C^\star$ *with* $L = 2$ *(therefore, geometrically uniform). If the minimum distance of the projection codes are* $d_H(\mathcal{C}_1) = 1$ *and* $d_H(\mathcal{C}_2) = 4$*, then, according to the formula in (3.44),* $d^2_{min}(\Gamma_{C^\star}) \geqslant \min\{13, 16\} = 13$ *and* $d^2_{min}(\Gamma_C) = 1$*. From the previous discussion,* $\Delta(\Gamma_{C^\star}) \geqslant \Delta(\Gamma_C)$ *if*

$$(13)^{n/2} \geqslant \frac{|\mathcal{C}_1| \ldots |\mathcal{C}_L|}{|\mathcal{C}|}. \tag{3.48}$$

Example 25. *Consider the constellation* $\Gamma_{C^\star}$ *with* $L = 2, n = 4$*, generated by the main code* $\mathcal{C} = \{(0,0,0,0,0,0,0,0), (1,1,1,1,1,1,0,0), (0,0,0,0,1,1,1,1), (1,1,1,1,0,0,1,1)\}$*. Observe that* $d^2_{min}(\Gamma_{C^\star}) = d^2_{min}(\Gamma_C) = 4$ *and* $|\Gamma_C|/|\Gamma_{C^\star}| = 2$ *and Construction C presents a better packing density in this case.*

However, if we consider a code $\overline{\mathcal{C}}$ *obtained as permutation of the projection codes of* $\mathcal{C}$ *(*$c = (c_1, c_2) \in \mathcal{C} \Leftrightarrow \bar{c} = (c_2, c_1) \in \overline{\mathcal{C}}$*), we can see from (3.43) that* $d^2_{min}(\Gamma_{C^\star}) = 4$*,* $d^2_{min}(\Gamma_C) = 2$ *and again* $|\Gamma_C|/|\Gamma_{C^\star}| = 2$*. Here,* $\left(\frac{2}{\sqrt{2}}\right)^4 > 2$ *and* $\Gamma_{C^\star}$ *has a better packing density.*

Table 2 summarizes density properties of previous examples according to the discussion presented previously in this subsection.

Table 2 – Properties of Construction $C^\star$ and its associated Construction C.

Example	Dimension	$d^2_{min}(\Gamma_{C^\star})$	$d^2_{min}(\Gamma_C)$	$\Delta(\Gamma_{C^\star})$	$\Delta(\Gamma_C)$	$\chi(\Gamma_{C^\star})$	$\chi(\Gamma_C)$
12*	2	1	1	$\pi/16$	$\pi/8$	0.4431	0.6266
13	2	4	1	$\pi/4$	$\pi/8$	0.8862	0.4431
14	24	32	24	0.001929	0.00012	0.7707	0.6236
16	2	5	1	0.8781	0.7853	0.9209	0.8861
18*	1	1	1	0.5	1	0.5	1

3.3.3.2 Random interleaving

From the analysis in the previous subsection, it is clear that the estimation of the minimum distance of Construction $C^\star$ is in general not an easy process, particularly if the equi-minimum distance does not hold. Since in order to compare Construction $C^\star$ with Construction C in terms of packing density or packing efficiency, the minimum distance is essential, we will work with *random interleaving* to approximate its average. This is also meaningful for communication applications, where the average error probability (in the presence of white Gaussian noise) is of interest.

The first analysis is regarding a deterministic interleaver. Let $c \in \mathcal{C} \subseteq \mathbb{F}_2^{nL}$, $z \in \mathbb{Z}^n$ and $x(c,z)$ be the point in $\Gamma_{C^\star}$ given by the natural labeling. Note that each coordinate $x_j, j = 1, \ldots, n$ of $x(c,z)$ is generated by a vector of L bits and an integer z_j.

Given two codewords $c, \tilde{c} \in \mathcal{C}, c \neq \tilde{c}$ and $z, \tilde{z} \in \mathbb{Z}^n$, let n_m be the number of coordinates where the vectors $x(c,z)$ and $x(\tilde{c},\tilde{z})$ agree in the $m-1$ lower levels and disagree in the $m-$th level, $m = 1, \ldots, L$. Let n_0 be the number of coordinates where all levels are zero. Clearly, $n_0 + n_1 + n_2 + \cdots + n_L = n$, $n_1 + n_2 + \cdots + n_L \leqslant d_H(c,\tilde{c})$ and $n_1 + n_2 + \cdots + n_L = d_H(c,\tilde{c})$ if and only if $x(c,z)$ and $x(\tilde{c},\tilde{z})$ differ in each coordinate in at most one bit.

Proposition 4. *(Bound on the squared minimum distance) The squared minimum distance* $||x(c,z) - x(\tilde{c},\tilde{z})||^2$ *between two points in Construction* $C^\star$ *is greater than or equal to*

$$n_1 + 4n_2 + \cdots + 4^{L-1}n_L. \tag{3.49}$$

For the special case when $L = 2$ and each coordinate of the integer vector z_2 is $z_1 - 1$ or $z_1 + 1$, according to which one gives the lowest distance:

$$||x(c,z) - x(\tilde{c},\tilde{z})||^2 = n_1 + 4n_2. \tag{3.50}$$

If the interleaver π is random, then the numbers $n_1, \ldots, n_L$ above are random variables. Their expected value over all interleaver permutations is given by $E(n_m) = P_m \cdot n$, where

$$P_m = \frac{\binom{N-m}{d-1}}{\binom{N}{d}} \approx P_1(1-P_1)^{m-1} \quad \text{for} \quad N \to \infty, \tag{3.51}$$

and $d = d_H(c, \tilde{c})$.

In particular, $P_1 = d/N$, $N = nL$. It follows from Equations (3.49) and (3.51) that the expected Euclidean distance between $x(c, z)$ and $x(\tilde{c}, \tilde{z})$, for $c \neq \tilde{c}$ is lower bounded by

$$E\{||x(\pi(c), z) - x(\pi(\tilde{c}), \tilde{z})||^2\} \geqslant n(P_1 + 4P_2 + \cdots + 2^{2L}P_L), \tag{3.52}$$

where $E(\cdot)$ denotes expectation with respect to all permutations π.

Considering the approximation in (3.51) for the probabilities when the dimension n goes to infinity, we have for $n \to \infty$:

$$E\left\{||x(\pi(c), z) - x(\pi(\tilde{c}), \tilde{z})||^2\right\} \geqslant d_c \sum_{l=1}^{L} \left[4\left(1 - \frac{d_c}{n}\right)\right]^{l-1}, \tag{3.53}$$

where $d_c = d_H(c, \tilde{c})/L$.

If we consider a Construction $C^\star$ with a random interleaver, then the average minimum squared distance between two distinct points in $\Gamma_{C^\star}$ is

$$\overline{d_E^2(\Gamma_{C^\star})} = E\left(\min_{y \neq \tilde{y} \in \Gamma_{C^\star}} ||y - \tilde{y}||^2\right), \tag{3.54}$$

for $y = x(\pi(c), z)$ and $\tilde{y} = (\pi(\tilde{c}), \tilde{z})$. That is, we take the closest two points for each permutation and then take an average. This quantity is what we wish we could estimate, however its estimation is hard. Instead, let us define the *minimum average* squared distance between two different points in $\Gamma_{C^\star}$ as

$$d_E^2(\overline{\Gamma_{C^\star}}) = \min_{y \neq \tilde{y} \in \Gamma_{C^\star}} E(||y - \tilde{y}||^2), \tag{3.55}$$

for $y = x(\pi(c), z)$ and $\tilde{y} = (\pi(\tilde{c}), \tilde{z})$. That is, we switch the order of expectation and minimum: take the two points which are closest on the average. Since Equation (3.52) lower bounds the expected squared distance for any two distinct codewords c and $\tilde{c}$, it follows that the minimum average squared distance of $\Gamma_{C^\star}$ is lower bounded by

$$d_E^2(\overline{\Gamma_{C^\star}}) \geqslant \min\left\{d_c \sum_{l=1}^{L} \left[4\left(1 - \frac{d_c}{n}\right)\right]^{l-1}, 2^{2L}\right\}, \tag{3.56}$$

where $d_c = d_H(\mathcal{C})/L$, and $d_H(\mathcal{C})$ is the minimum Hamming distance of the main code.

Clearly, the average minimum is smaller than the minimum average, i.e., $\overline{d_E^2(\Gamma_{C^\star})} \leqslant d_E^2(\overline{\Gamma_{C^\star}})$. In fact, since concentration occurs for most pairs but not for all pairs, the average minimum distance will be dictated by *atypical* pairs, whose distance is strictly below the average. Hence the estimate in Equation (3.55) is in general strictly larger than the desired quantity $\overline{d_E^2(\Gamma_{C^\star})}$. Nevertheless, in the next section we shall use the simple bound in Equation (3.56) to assess the packing efficiency of Construction $C^\star$.

3.4 Comparison of a hybrid Construction $C^\star/C$ and Construction C for Gilbert-Varshamov bound achieving codes

In this section, we aim to compare a hybrid Construction $C^\star/C$ to Construction C in terms of packing efficiency. To do that, we will use Gilbert-Varshamov Bound (GVB) achieving codes, i.e., codes whose size is related to their minimum Hamming distance d_H via

$$|C| \geqslant \frac{2^n}{|B(d-1,n)|}, \tag{3.57}$$

where $B(r,n)$ is an $n-$dimensional zero-centered Hamming ball of radius r, which is the set of all n length binary vectors with Hamming weight smaller than or equal to r. For a large n, $|B(r,n)| \doteq 2^{nH(\overline{q})}$, with $\overline{q} = r/n$ and where $H(\overline{q}) = -\overline{q}\log_2 \overline{q} - (1-\overline{q})\log_2(1-\overline{q})$ is the binary entropy function for $\overline{q} \in [0,1]$.

Suppose we start with a Construction $C^\star$ with $L^\star$ levels, so that its distance satisfies

$$d^2_{min}(\Gamma_{C^\star}) = \min\left\{\min_{c \neq \tilde{c}} ||x(c,z), x(\tilde{c},\tilde{z})||^2, 2^{2L^\star}\right\}, \tag{3.58}$$

$c, \tilde{c} \in \mathcal{C} \subseteq \mathbb{F}_2^{nL}$. If the cubic term $2^{2L^\star}$ is the minimum, we add one level of Construction C above the $L^\star$ levels of Construction $C^\star$, with a code $\mathcal{C}_{L^\star+1}$ whose minimum Hamming distance is $d_{L^\star+1}$. The new construction is thus given by

$$\Gamma_{C^\star/C} = \{c_1 + 2c_2 + \cdots + 2^{L^\star-1}c_{L^\star} + 2^{L^\star}c_{L^\star+1} + 2^{L^\star+1}z\}, \tag{3.59}$$

$(c_1, \ldots, c_{L^\star}) \in \mathcal{C}, c_{L^\star+1} \in \mathcal{C}_{L^\star+1}, z \in \mathbb{Z}^n$. Its minimum distance satisfies

$$d^2_{min}(\Gamma_{C^\star/C}) = \min\left\{\min_{c \neq \tilde{c}} ||x(c,z), x(\tilde{c},\tilde{z})||^2, 2^{2L^\star}d_H(\mathcal{C}_{L^\star+1}), 2^{2(L^\star+1)}\right\}. \tag{3.60}$$

We choose the minimum Hamming distance $d_{L^\star+1}$ of the code $\mathcal{C}_{L^\star+1}$ large enough so that the second term will be the minimum. Again we check whether the cubic term $2^{2(L^\star+1)}$ minimizes. If it still does, then we add another level of Construction C and so on. We continue this process of adding more levels of Construction C until the cubic term stops being the minimum and we stop. Assuming we stopped after a total of L levels, the final formula is

$$\begin{aligned} d^2_{min}(\Gamma_{C^\star/C}) &= \min\{\min_{c \neq \tilde{c}} ||x(c,z), x(\tilde{c},\tilde{z})||^2, 2^{2L^\star}d_H(\mathcal{C}_{L^\star+1}), 2^{2(L^\star+1)}d_H(\mathcal{C}_{L^\star+2}), \ldots, \\ &\quad 2^{2(L-1)}d_H(\mathcal{C}_L)\}. \end{aligned} \tag{3.61}$$

$c, \tilde{c} \in \mathcal{C}$.

We choose the minimum Hamming distances of the added codes in a balanced way, i.e., $d_{i+1} = d_i/4$, for all $L^\star < i < L$, similarly to what is required for Construction C in the definition from Conway and Sloane [18, pp. 150]. Then, we have $2^{2(L^\star+j)}d_H(\mathcal{C}_{L^\star+j+1}) =$

$2^{2(L-1)}d_H(\mathcal{C}_L)$, for all $0 \leqslant j \leqslant L - L^\star - 1$ and $d^2_{min}(\Gamma_{C^\star/C}) = \min\{\min_{c \neq \tilde{c}} ||x(c,z), x(\tilde{c},\tilde{z})||^2$, $2^{2(L^\star+j)}d_H(\mathcal{C}_{L^\star+j+1})\}$, for any j. We also assume a balancing condition with respect to the distances of Construction $C^\star$ and C, i.e., $\min_{c\neq\tilde{c}} ||x(c,z), x(\tilde{c},\tilde{z})||^2 = 2^{2(L^\star+j)}d_H(\mathcal{C}_{L^\star+j+1})$, for any j.

According to the process described above and to take advantage of the special $L^\star = 2$ Construction $C^\star$, which is geometrically uniform, we define a hybrid Construction $C^\star/C$ as:

Definition 33. *(Hybrid Construction $C^\star/C$ for $L^\star = 2$) Let $\mathcal{C}$ be a code in $\mathbb{F}_2^{2n}$ and $\mathcal{C}_3, \ldots, \mathcal{C}_L$ be binary linear codes in $\mathbb{F}_2^n$. Then the hybrid Construction $C^\star/C$ is defined by*

$$\begin{aligned} \Gamma_{C^\star/C} \quad := \quad & \{c_1 + 2c_2 + 4c_3 + \cdots + 2^{L-1}c_L + 2^L z : (c_1, c_2) \in \mathcal{C} \ \textit{and} \\ & c_i \in \mathcal{C}_i, \ i = 3, \ldots, L, \ z \in \mathbb{Z}^n\}. \end{aligned} \tag{3.62}$$

Suppose that, in terms of Definition 33, $\mathcal{C} \subseteq \mathbb{F}_2^{2n}$ and $\mathcal{C}_3, \ldots, \mathcal{C}_L \subseteq \mathbb{F}_2^n$ are all VGB achieving codes and also that 2^{2L} is not the minimum squared distance of the $\Gamma_{C^\star/C}$. Assume also the balanced condition of Construction C, i.e., the Hamming distance $d_H(\mathcal{C}_i)$ of $\mathcal{C}_i$ is 4 times smaller than $d_H(\mathcal{C}_{i-1})$ for $i = 4, \ldots, L$. For large n, we may admit the approximation of $\min_{c\neq\tilde{c}} ||x(c,z), x(\tilde{c},\tilde{z})||^2$ as lower bounded by the average $d_{min}(\overline{\Gamma_{C^\star}})$ as in Equation (3.56). Taking $q = d_H(\mathcal{C})/2n$ and $q_3 = d_H(\mathcal{C}_3)/n$, we have:

$$d^2_E(\Gamma_{C^\star/C}) \quad \approx \quad \min\{d^2_E(\overline{\Gamma_{C^\star}}), 2^4 d_H(\mathcal{C}_3)\} \tag{3.63}$$

Due to the balancing condition considered, i.e., $d^2_E(\overline{\Gamma_{C^\star}}) = 2^4 d_H(\mathcal{C}_3)$. Thus, Equation (3.63) reduces to:

$$d^2_E(\Gamma_{C^\star/C}) \quad \approx \quad \min\{nq[1 + 4(1-q)], 2^4 nq_3\} \tag{3.64}$$

where it follows that $q_3 = q[1 + 4(1-q)]/16$ (or also $d_H(\mathcal{C}_3) = \dfrac{5}{32} d_H(\mathcal{C})$, for large n.)

We can then estimate the packing efficiency of hybrid Construction $C^\star/C$ and compare it with that of Construction C. Remember that for large n, $vol(B(0,\rho)) \approx \dfrac{2\pi e}{n}^{n/2} \rho^n$ and we also consider GVB codes achieving the equality in Equation (3.57) in order to have a fair comparison, then:

$$\begin{aligned} \chi(\Gamma_{C^\star/C}) \quad &= \quad \frac{\frac{1}{2}\sqrt{nq[1+4(1-q)]}}{\left[\frac{2^{nL}}{|\Gamma_{C^\star/C}|\left(\frac{2\pi e}{n}\right)^{n/2}}\right]^{1/n}} = \frac{\sqrt{nq[1+4(1-q)]}|\Gamma_{C^\star/C}|^{1/n}\left(\frac{2\pi e}{n}\right)^{1/2}}{2^{L+1}} \\ &\approx \quad \frac{\sqrt{q[1+4(1-q)]}(2\pi e)^{1/2}2^L}{2^{L+1}\left(2^{2H(q)} \cdot 2^{H(q_3)} \cdot \ldots \cdot 2^{H(q_3/2^{2(L-1)})}\right)}, \end{aligned} \tag{3.65}$$

which gives

$$\chi(\Gamma_{C^\star/C}) \approx \frac{\sqrt{q[1+4(1-q)]}(2\pi e)^{1/2}}{2 \cdot 2^{LH(q)} \cdot 2^{H(q_3)} \cdot \ldots \cdot 2^{H(q_3/2^{2(L-1)})}}, \tag{3.66}$$

where $\chi(\Lambda) = (\Delta(\Lambda))^{1/n}$ and from the balancing, $q_3 = q[1 + 4(1 - q)]$.

For Construction C, with $\mathcal{C}_1, \ldots, \mathcal{C}_L$ codes and a balanced distance such that the Hamming distance $d_H(\mathcal{C}_i)$ is 4 times smaller than $d_H(\mathcal{C}_{i-1})$ for $i = 2, \ldots, L$, if we define $q_1 = d_H(\mathcal{C}_1)/n$, it follows that

$$\chi(\Gamma_C) = \frac{\frac{1}{2}\sqrt{d_1}}{\left[\frac{2^{nL}}{|\Gamma_C|\left(\frac{2\pi e}{n}\right)^{n/2}}\right]^{1/n}} = \frac{\frac{1}{2}\sqrt{q_1 n}\left(\frac{2\pi e}{n}\right)^{1/2} 2^L}{2^L 2^{H(q_1)} \cdot \ldots \cdot 2^{H(q_1/2^{2(L-1)})}} \tag{3.67}$$

and

$$\chi(\Gamma_C) = \frac{\sqrt{q_1 \pi e}}{\sqrt{2} \cdot 2^{H(q_1)} \cdot \ldots \cdot 2^{H(q_1/2^{2(L-1)})}}. \tag{3.68}$$

To compare both performances, Figure 14 illustrates the packing estimated efficiency as a function of the information rate of the hybrid Construction $C^\star/C$ compared with that of Construction C for GVB achieving codes and $L = 1000$.

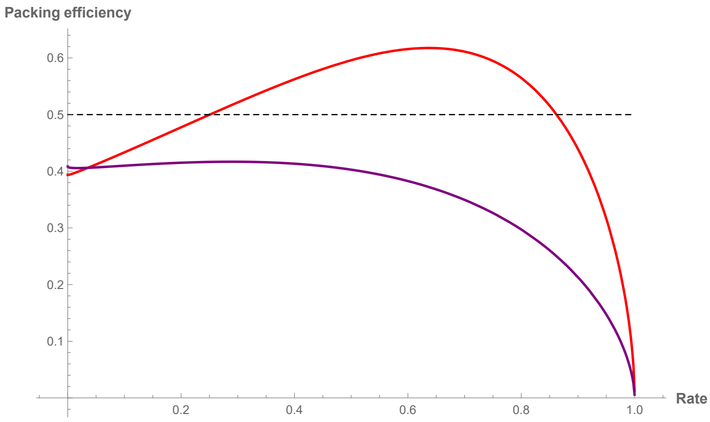

Figure 14 – Packing efficiency *versus* information rate – hybrid $C^\star/C$ (red) and C (purple).

Remark 6. *The performance represented in Figure 14 is overestimated, because we considered the minimum average squared distance $d_E^2(\overline{\Gamma_{C^\star}})$, which is easier to obtain, instead of the average minimum squared distance $\overline{d_E^2(\Gamma_{C^\star})}$. This is clear because it is widely believed that for large n it is not feasible to have a packing efficiency greater than 0.5 (the packing efficiency guaranteed by the Minkowski bound [6, pp.247]). Thus our estimation must be loose. However, Figure 14 should therefore be viewed as a good indication for the potential superiority of Construction $C^\star$.*

In this chapter, we introduced a new multilevel construction, called Construction $C^\star$, and study its properties: geometric uniformity, conditions to be a lattice and minimum distance. Regarding to minimum distance, we presented a closed formula to express it when

Construction $C^\star$ is geometrically uniform and used this formula to relate Construction $C^\star$ with its associated Construction C. We also discussed the average minimum distance in the presence of a random interleaver and adopted it in a hybrid Construction $C^\star/C$ to compare this construction, in terms of packing efficiency, with Construction C.

Chapter 4

Approximate closest lattice point in a distributed system

In the present chapter, we consider the closest lattice point problem in a distributed network setting [1] and aim to study the communication cost and the error probability for computing an approximate nearest lattice point under this constraint, using the nearest plane algorithm (defined in Subsection 1.2.3), due to Babai [7]. Our contribution consists of bounds for the error probability in dimensions 2 (Theorem 7) and 3 (Figure 22, Conjecture 1), where it is shown that the error probability increases with the packing density of the lattice. We also study the rate computation that underlies the decoding process in a distributed system (Section 4.3). The results discussed in this chapter can also be found in [9, 10].

4.1 Why solving a hard lattice problem in a distributed system?

Consider a function that computes, for a given lattice, the closest lattice point to a real vector $x = (x_1, x_2, \dots, x_n)$ in a given lattice Λ. This process is widely used for decoding lattice codes and for quantization. Lattice coding offers significant coding gains [18] for noisy channel communication and for quantization, leads to performance approaching the rate distortion bound [8] for some sources and distortion measures.

Algorithms for the closest lattice point problem have been studied in great detail; see [2] and the references therein. However, in all these algorithms it is assumed that the vector components are available at the same location. In our work, we consider communication settings where the vector components are available at physically separated nodes and we are interested in the communication cost of exchanging this information in order to determine the closest lattice point.

[1] A collection of independent systems, that can be computers or antennas, as considered, for example in [48].

Problems in distributed function computation [6] arise in a broad range of modern settings. We mention two such applications here, network MIMO systems for next generation wireless networks [45], and network management in wide area networks [31]. In MIMO wireless systems, each antenna is considered to be an individual node, and the received signal constellation (assumed to be a rectangular lattice at the transmitter) forms a lattice whose basis is determined by the channel tap weights. The fusion center seeks to decode the received signal to the nearest lattice point. Exact decoding requires that real or complex numbers be sent from the antenna to the fusion center. However, since the network has limited bandwidth, it becomes necessary to quantize the information prior to transmission.

Distributed network management includes problems such as distributed threat detection, or more generally distributed change detection. One potential application is that of determining a denial of service attack in a distributed framework [31]. Threat detection at a centralized point can place an enormous communication burden on the network. Efficient quantization can mitigate this problem meaningfully.

The closest lattice point problem has also been proposed as a basis for lattice cryptography ([3], [26], [30], [37], [42]), which is a topic of great interest in recent years. Some examples are the GGH and LWE cryptosystems. The idea is to require solution of the closest lattice point problem, which is known to be NP-complete [21], assuring security. The Babai algorithm is used in some public key cryptosystems to attack the communication in order to approximate the closest lattice point (message) that is being transmitted, thus computation of its error probability is of interest also in this context.

4.2 Error analysis

Consider a generic distributed function computation problem in a network of N interconnected sensor/computers and possibly a central computing node, called a fusion center F. Communication links with limited bandwidth interconnect the nodes, which are assumed to have limited processing power. Node i observes real valued random variable X_i.

In the *centralized model* (Figure 15), the objective is to compute a function $f(x_1, x_2, \ldots, x_n)$ at the fusion center by communicating information from the nodes. We also consider the *interactive model* (Figure 16), where the purpose is to compute a function $f(x_1, x_2, \ldots, x_n)$ at each node, and the fusion center is absent. In general, since random variables are real valued, these calculations would require that the system communicate an infinite number of bits. Since the network has finite bandwidth links, the information must be quantized in a suitable manner, but quantization affects the accuracy of the function that we are trying to compute. Thus, the main objective is to manage the tradeoff between communication cost and function computation accuracy.

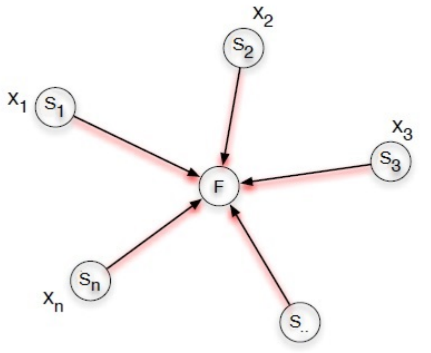

Figure 15 – Centralized model.

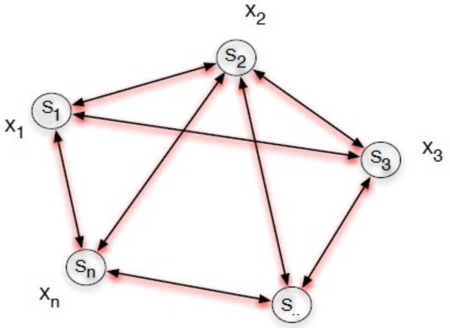

Figure 16 – Interactive model.

The function f to be considered in our study calculates the closest lattice point and our results are regarding to arbitrary lattices in two and three dimensions. The chosen approach to solve the distributed problem was to reproduce the Babai partition by sending a limited number of bits in each model (centralized and interactive) and send it across the network. As the solutions are approximate, we expect errors that will be described in the sequel.

4.2.1 Two dimensional case

We assume that node i observes an independent identically distributed (iid) random process $\{X_i(t), t \in \mathbb{Z}\}$, where t is the time index (suppressed) and that random processes observed at distinct nodes are mutually independent. The random vector $X = (X_1, X_2)$ is obtained by projecting a random process on the basis vectors of an underlying coordinate frame, which is assumed to be fixed.

Consider that the lattice Λ is generated by the scaled generator matrix αV, where V is the generator matrix of the unscaled lattice. Let $\mathcal{V}(\lambda)$ and $\mathcal{B}(\lambda)$ denote the Voronoi and Babai cells, respectively, associated with lattice vector $\lambda \in \Lambda$. The error probability $P_e(\alpha)$, is the probability of the event $\{\lambda_{nl}(X) \neq \lambda_{np}(X)\}$, where λ_{nl} is the exact closest lattice point and λ_{np} is the approximated closest lattice point given by the Babai (np) algorithm. Moreover, $P_e := \lim_{\alpha\to 0} P_e(\alpha) = area(\mathcal{B}(0) \bigcap \mathcal{V}(0)^c)/area(\mathcal{B}(0))$.

Our first remark about the Babai partition is that it is basis dependent, whereas the Voronoi partition is independent of the basis used to represent the lattice, and this has an impact on the error probability. To better illustrate this phenomenon, consider the following example.

Example 26. *Consider a lattice $\Lambda \subseteq \mathbb{R}^2$ with basis $\{(5,0),(3,1)\}$. The probability of error in this case, if we calculate the area inside the Babai partition but outside the Voronoi* *partition, is* $P_e = 0.6$ *(Figure 17), whereas if we start from the basis* $\{(1,2),(-2,1)\}$, *we achieve after the QR decomposition* $\left\{(\sqrt{5},0),(0,\sqrt{5})\right\}$ *and* $P_e = 0$, *since the Babai region associated with an orthogonal basis and the Voronoi region for rectangular lattices coincides.*

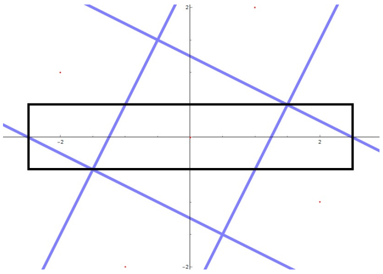

Figure 17 – Voronoi region and Babai partition of the triangular basis $\{(5,0),(3,1)\}$.

Example 26 illustrates the necessity of working with a good basis. In our analysis, we will always consider a Minkowski-reduced basis. As mentioned above, additional motivation comes from the observation that for a Minkowski-reduced basis in two dimensions, the relevant vectors are known.

To see this, we first note that an equivalent condition for a basis $\{v_1, v_2\}$ to be Minkowski-reduced in dimension two is $||v_1|| \leqslant ||v_2|| \leqslant ||v_1 \pm v_2||$ (cf. Proposition 1, Chapter 1) Thus, we can state the following result, which was derived from the two dimensional analysis proposed in [17].

Lemma 2. *[17] (Relevant vectors of a Minkowski-reduced basis) If a Minkowski-reduced basis is particularly given by* $\{(1,0),(a,b)\}$ *then, besides the basis vectors, a third relevant vector is*

$$\begin{cases} (-1+a,b), & \text{if } \pi/3 \leqslant \theta \leqslant \pi/2 \\ (1+a,b), & \text{if } \pi/2 < \theta \leqslant 2\pi/3, \end{cases} \tag{4.1}$$

where θ *is the angle between* $(1,0)$ *and* (a,b).

Note that, if $\{v_1, v_2\}$ is a Minkowski-reduced basis then so it is $\{-v_1, v_2\}$ and hence any lattice has a Minkowski-reduced basis with $\frac{\pi}{2} \leqslant \theta \leqslant \frac{2\pi}{3}$. So, if we consider the Minkowski-reduced basis $\{(1,0),(a,b)\}$, with $a^2+b^2 \geqslant 1$ and $-\frac{1}{2} \leqslant a \leqslant 0$, it is possible to use Lemma 2 to describe the Voronoi region of Λ and determine its intersection with the associated Babai partition. Observe that the area of both regions must be the same and in this specific case, equal to b. This means that the vertices that define the Babai rectangular partition have always in the form $\left(\pm\frac{1}{2}, \pm\frac{b}{2}\right)$.

In addition, $\{(-1-a,-b),(1,0),(a,b)\}$ is an obtuse superbase for Λ, so the relevant vectors that defines the Voronoi region are $\pm(1,0), \pm(a,b)$ and $\pm(-1-a,-b)$. We will admit in the upcoming analysis, without loos of generality, only the relevant vectors in the first quadrant, i.e., $(1,0),(1+a,b),(a,b)$, due to the symmetry that the Voronoi cell has. Therefore, we can state the following result:

Theorem 7. *(Error probability function for an arbitrary 2−dimensional lattice) Consider a lattice $\Lambda \subset \mathbb{R}^2$ with a triangular Minkowski-reduced basis $\beta = \{v_1, v_2\} = \{(1,0),(a,b)\}$ such that the angle θ between v_1 and v_2 satisfies $\frac{\pi}{2} \leqslant \theta \leqslant \frac{2\pi}{3}$. The probability of error P_e for the Babai partition is given by*

$$P_e = F(a,b) = \frac{-a-a^2}{4b^2}. \tag{4.2}$$

Proof. To calculate P_e for the lattice Λ, we compute the ratio between the area of the Babai region which is not overlapped by the Voronoi region $\mathcal{V}(0)$ and the area $|b|$ of the Babai region. In this case, it is twice the error areas given by A_1 and A_2 according to Figure 19, normalized by the $\det(\Lambda)$.

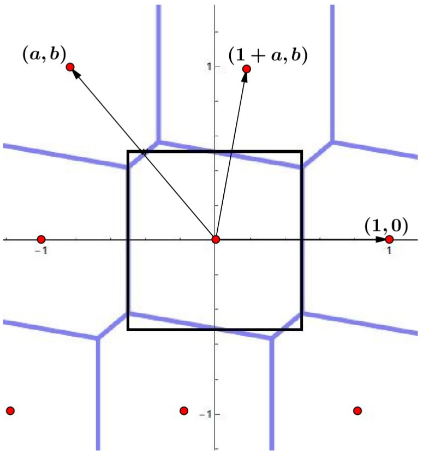

Figure 18 – Voronoi region, Babai partition and three relevant vectors .

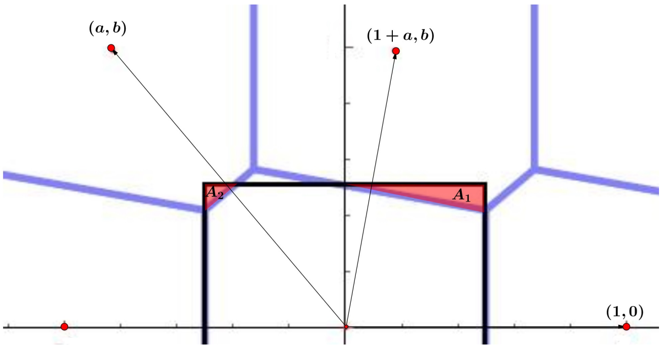

Figure 19 – Error triangles.

The perpendicular bisector line to the line defined by $(0,0)$ and $(1+a,b)$, passing through the point $\left(\frac{1+a}{2}, \frac{b}{2}\right)$, has equation $y_1 = \frac{-1-a}{b}x + \frac{(1+a)^2}{2b} + \frac{b}{2}$. Based on this fact, we have the vertices which define the triangle with area A_1, that are

$$\left(\frac{1}{2}, \frac{b}{2}\right), \left(\frac{1}{2}, \frac{a+a^2+b^2}{2b}\right) \text{ and } \left(\frac{a+1}{2}, \frac{b}{2}\right). \tag{4.3}$$

Thus, $A_1 = \left| -\frac{a^2(a+1)}{8b} \right| = \frac{a^2(a+1)}{8b}$, for $-1/2 \leqslant a \leqslant 0$ and $b \geqslant \sqrt{3}/2$.

By doing an analogue process to the remaining triangle, the perpendicular bisector line to the line defined by $(0,0)$ and (a,b), passing through the point $\left(\frac{a}{2}, \frac{b}{2}\right)$, have equation $y_2 = -\frac{a}{b}x + \frac{a^2}{2b} + \frac{b}{2}$. Hence, the triangle with area A_2 is defined by

$$\left(-\frac{1}{2}, \frac{b}{2}\right), \left(-\frac{1}{2}, \frac{a+a^2+b^2}{2b}\right) \text{ and } \left(\frac{a}{2}, \frac{b}{2}\right), \tag{4.4}$$

resulting in $A_2 = \left| -\frac{a(a+1)^2}{8b} \right| = -\frac{a(a+1)^2}{8b}$, in the range $-1/2 \leqslant a \leqslant 0$ and $b \geqslant \sqrt{3}/2$.

Therefore, the probability of error is the sum $2A_1 + 2A_2$, normalized by the area of the Voronoi region (same as the area of Babai region) $|\det(V)| = |b| = b$, where V is the generator matrix of Λ. Then,

$$\begin{aligned} F(a,b) &= \frac{2A_1 + 2A_2}{b} = \frac{a^2(a+1)}{4b^2} - \frac{a(a+1)^2}{4b^2} \\ &= \frac{1}{4}\left(\frac{-a-a^2}{b^2}\right), \end{aligned} \tag{4.5}$$

which demonstrates the result. □

Remark 7. *Note that starting from any Minkowski-reduced basis of a two-dimensional lattice $\gamma = \{v_1, v_2\}$, considering $\rho = \frac{\|v_2\|}{\|v_1\|}$ and the angle θ between the basis vectors, the result of Theorem 7 can be rewritten as*

$$P_e = H(\theta, \rho) = \frac{1}{4\rho} \frac{|\cos\theta|}{\operatorname{sen}^2\theta}(1 - \rho|\cos\theta|). \tag{4.6}$$

We obtain the following Corollary, illustrated in Figure 20, from the probability of error $P_e = F(a,b) = \frac{1}{4}\frac{a}{b^2}(1-a) = \frac{1-(1+2a)^2}{16b^2}$ obtained in Theorem 7 with $b \geqslant \sqrt{3}/2$ and $-1/2 \leqslant a \leqslant 0$.

Corollary 5. *For any two-dimensional lattice and a Babai partition constructed from the QR decomposition associated with a Minkowski-reduced basis where $\frac{\pi}{2} \leqslant \theta \leqslant \frac{2\pi}{3}$, it follows that*

$$0 \leqslant P_e \leqslant \frac{1}{12}, \tag{4.7}$$

and

a) $P_e = 0 \Longleftrightarrow a = 0$, i.e., the lattice is orthogonal.

b) $P_e = \frac{1}{12} \Longleftrightarrow (a,b) = \left(-\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$, i.e., the lattice is equivalent to hexagonal lattice.

c) the level curves of P_e are described as ellipsoidal arcs in the region $a^2 + b^2 \geqslant 1$ and $-\frac{1}{2} \leqslant a \leqslant 0$.

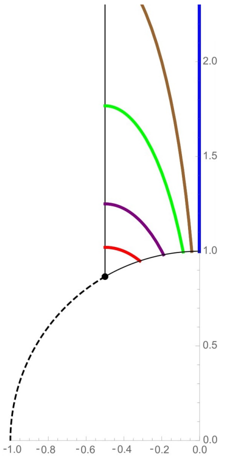

Figure 20 – Level curves of $P_e = k$, in right-left ordering, for $k = 0, k = 0.01, k = 0.02, k = 0.04, k = 0.06$ and $k = 1/12 \approx 0.0833$. a is represented in the horizontal axis and b in the vertical axis.

4.2.2 Three dimensional case

To analyse the error in the three dimensional case, we developed and implemented an algorithm in the software *Mathematica* [53] (Appendix A) which calculates the error probability of any three dimensional lattice, given an obtuse superbase. We assume, as we did in the two dimensional analysis, an initial upper triangular lattice basis given by $\{(1,0,0),(a,b,0),(c,d,e)\}$, where $a, b, c, d, e \in \mathbb{R}$. It can be accomplished by performing a QR decomposition and a multiplication by a scalar factor in the original basis.

It is important to remark that the error probability is, in the general case, dependent on the basis ordering. Our algorithm searches over all orderings and determines the best one. As an example, the performance of the BCC lattice is invariant over basis ordering, due to its symmetries. On the other hand, for the FCC lattice, depending on how the basis is ordered, we can find two different error probabilities, 0.1505 and 0.1667, but only 0.1505 is tabulated.

A detailed description of the algorithm is presented below and the complete program implemented in *Mathematica* is in Appendix A.

Algorithm: Error probability of the closest lattice point problem in a distributed system (three dimensional case)

Voronoi region: Provided an obtuse superbase, the vertices and faces that define the Voronoi region of Λ are determined by Equations (1.32) and (1.33), following the method proposed by Conway and Sloane [17]. In this stage, we determine, generate and classify the correspondent Voronoi region of Λ into one of five possibilities described in Figure 7.

Babai partition: Determine the vertices of the Babai cell. Since we have assumed a generator matrix in upper triangular form, $\{(1,0,0),(a,b,0),(c,d,e)\}$, the vertices are:

$$\begin{gathered}\left(\frac{1}{2},-\frac{b}{2},\frac{e}{2}\right),\left(\frac{1}{2},\frac{b}{2},\frac{e}{2}\right),\left(-\frac{1}{2},-\frac{b}{2},\frac{e}{2}\right),\left(-\frac{1}{2},\frac{b}{2},\frac{e}{2}\right),\\ \left(\frac{1}{2},-\frac{b}{2},-\frac{e}{2}\right),\left(\frac{1}{2},\frac{b}{2},-\frac{e}{2}\right),\left(-\frac{1}{2},-\frac{b}{2},-\frac{e}{2}\right),\left(-\frac{1}{2},\frac{b}{2},-\frac{e}{2}\right).\end{gathered} \tag{4.8}$$

Intersection: In this stage, using a function in Mathematica [53], we calculate the intersection between the Voronoi and Babai regions obtained previously. This function runs through all points that define both solids and select the coincident ones, providing in the end of the process, the vertices that determine the intersection region. We calculate then the volume of the intersection normalized by the volume of the lattice Λ. The algorithm determines first the format of each type of Voronoi cell (Figure 7) to simplify the calculations of the error probability. To be more specific, if all conorms $p_{ij}, (0 \leqslant i < j \leqslant 3)$ are nonzero (truncated octahedron) or if only one conorm is zero (hexa-rhombic dodecahedron) or if two collinear conorms are zero (rhombic dodecahedron), we implement the general intersection algorithm, defined as: let v_1, e_1, f_1 be, respectively, the set of vertices, edges and faces that define the Babai region of Λ and v_2, e_2, f_2, be, respectively, the set vertices, edges and faces that define the Voronoi region of Λ. Thus, we solve:

$$\texttt{Solve \{Or } \{x,y,z\} \in e_1 \texttt{ and } \{x,y,z\} \in f_2 \texttt{ Or } \{x,y,z\} \in e_2 \texttt{ and } \{x,y,z\} \in f_1\texttt{\}.}$$

The union of points (x, y, z) resulting from the previous system will define the intersection of Voronoi and Babai regions of Λ. For the two remaining cases, i.e., when we have two non-collinear zeros (hexagonal prism) we only calculate the intersection between the hexagonal basis and the rectangular basis of both prisms and when we have four zeros, the error probability is zero.

Packing density: Finally, we calculate the packing density Δ_3.

We present, in whats follows, results obtained by applying Algorithm 1 to some known lattices. In Fig. 21 we have

- in **red**, the cubic lattice $\mathbb{Z}^3$ with basis $\{(1,0,0),(0,1,0),(0,0,1)\}$;

- in green, the lattice with basis $\{(1,0,0),\ (-\frac{1}{2},-\frac{\sqrt{3}}{2},0),(0,0,1)\}$, Voronoi region: hexagonal prism;
- in blue, the body-centered cubic (BCC) lattice, with basis $\{(1,0,0),(-\frac{1}{3},\frac{2\sqrt{2}}{3},0),(-\frac{1}{3},-\frac{\sqrt{2}}{3},\sqrt{\frac{2}{3}})\}$, Voronoi region: truncated octahedron;
- in **black**, the face-centered cubic (FCC) lattice, with basis $\{(1,0,0),(0,1,0),(-\frac{1}{2},-\frac{1}{2},\frac{1}{\sqrt{2}})\}$; Voronoi region: rhombic dodecahedron;
- in purple, lattice with basis $\{(1,0,0),\ (-\frac{1}{2},-\frac{\sqrt{5}}{2},0),(0,\frac{1}{\sqrt{5}},\frac{2}{\sqrt{5}})\}$, Voronoi region: hexa-rhombic dodecahedron.

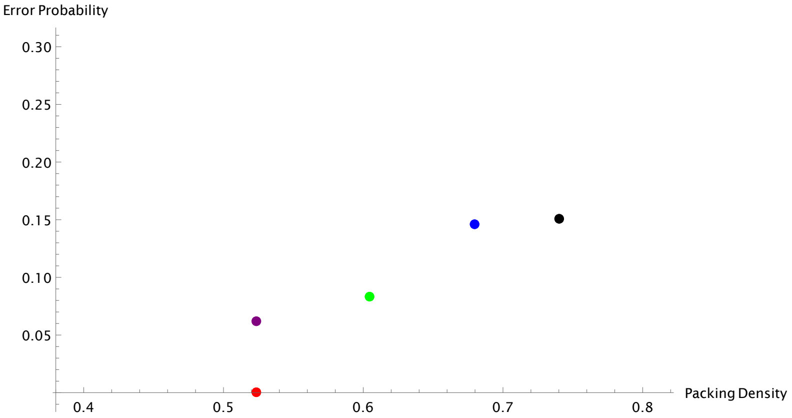

Figure 21 – Performance of known lattices.

Table 3 below presents some lattice performances when we run Algorithm 1.

Table 3 – Performance (Algorithm 1) for known lattices.

Lattice/Voronoi cell	Notation Table 15.6, [18]	Conorms $(\alpha,\beta,\gamma,a,b,c)$	Δ_3	P_e
Cubic/ Cuboid	111	$(-1,-1,-1,0,0,0)$	0.5235	0
Hexa-rhombic dodecahedron	$2_1 3_1 2$	$(-\frac{1}{2},-\frac{1}{2},-\frac{1}{2},0,-\frac{1}{2},-\frac{1}{2})$	0.5235	0.0617
Hexagonal prism (corresp. A_2 lattice)	$2_{-1}22$	$(-\frac{1}{2},-\frac{1}{2},-1,0,0,-\frac{1}{2})$	0.6046	0.0833
BCC/ Truncated octahedron	$3_1 3_1 3_{-1}$	$(-1,-,1-,1,-1,-1,-1)$	0.6801	0.1459
FCC/ Rhombic dodecahedron	$2_1 2_1 2$	$(-\frac{1}{2},-\frac{1}{2},0,-\frac{1}{2},-\frac{1}{2},0)$	0.7404	0.1505

We remark that the error probability for the hexagonal prism is identical to the two dimensional case (see Theorem 7) and cuboids have a null error probability (when aligned to the coordinate axes). We also see that the face-centered cubic lattice, which has the best packing density for lattices in three dimensions, is the worst case when one considers its error probability.

Now, we will apply Algorithm 1 to lattices whose basis was chosen randomly. Specifically, we start by considering a basis at random, with the format $\{(1,0,0), (a,b,0), (c,d,e)\}$, where a, b, c, d, e are real numbers in the range $[-4, 4]$. Then, the program tests if this basis is both an obtuse superbase and Minkowski-reduced according to Theorem 3. If this condition is false, another random basis is selected, until a suitable one is found. At the end of this stage, we will have a randomly chosen obtuse, Minkowski-reduced superbase for the lattice Λ.

In Figure 22, we have plotted the known points already seen in Figure 21, together with orange points that are associated with lattices having a packing density greater than 0.4 randomly chosen as above. Note that with overwhelming probability, a randomly chosen basis will have a truncated octahedron as a Voronoi region (the most general Voronoi region in three dimensions).

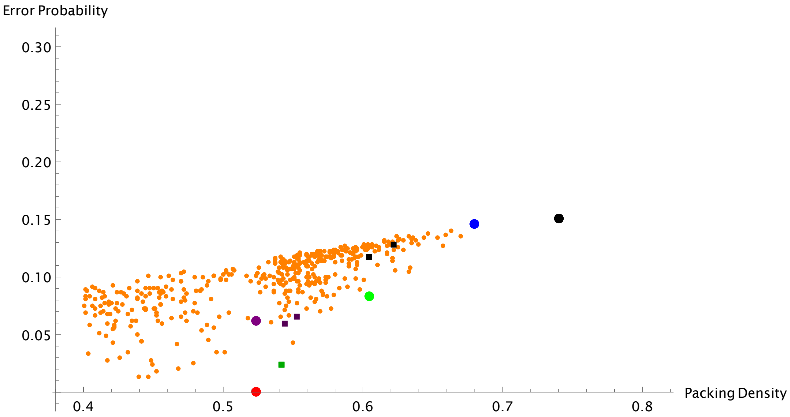

Figure 22 – Comparison between random and known performances.

However, by considering conorms that are approximately zero, we can identify cases that are ‘almost’ like one of the degenerate polyhedra. These cases are presented in Table 4, illustrated as square points in Figure 22, where the color characterizes the cell type, following the notation of Figure 21.

Table 4 – Performance (Algorithm 1) for random lattices.

(Aproximate) Voronoi cell	Conorms $(\alpha, \beta, \gamma, a, b, c)$	Δ_3	P_e
Hexa-rhombic dodecahedron	$(-0.4447, -0.7089, -0.7596, -0.0007, -0.3055, -0.2903)$	0.5441	0.0592
Hexa-rhombic dodecahedron	$(-0.3128, -0.7110, -0.6812, -0.0005, -0.4535, -0.2884)$	0.5527	0.0652
Rhombic-dodecahedron	$(-0.0574, -0.5159, -0.7771, -0.0041, -0.4708, -0.4798)$	0.6044	0.1169
Rhombic-dedecahedron	$(-0.5280, -0.05218, -0.6273, -0.4968, -0.0650, -0.4509)$	0.6220	0.1280
Hexagonal prism	$(-0.5246, -0.9048, -0.6788, -0.0201, -0.4024, -0.0750)$	0.5417	0.0237

After 5000 trials and computationally evidences, we conjecture that:

Conjecture 1. *For any three dimensional lattice and a Babai partition constructed from the QR decomposition associated with an obtuse superbase which is also Minkowski-reduced,*

$$0 \leqslant P_e \leqslant 0.1505. \tag{4.9}$$

Compared with the two dimensional case, we have an increase of 7.32% in the conjectured bound for the error probability and we expect this number to grow more as the dimension increases.

We also conjecture, assuming a more "spherical shape" for Voronoi regions of densest lattices the following

Conjecture 2. *The worst error probability for a lattice in dimension n is achieved by the densest lattice and it tends to one when n goes to infinity.*

4.3 Rate computation for constructing a Babai partition for arbitrary $n > 1$

Communication protocols are presented for the centralized and interactive model along with associated rate calculations in the limit as $\alpha \to 0$.

4.3.1 Centralized model

We now describe the transmission protocol Π_c by which the nearest plane lattice point can be determined at the fusion center F. Let $v_{ml}/v_{mm} = p_{ml}/q_{ml}$ where p_{ml} and $q_{ml} > 0$ are relatively prime. Note that we are assuming that the generator matrix is such that the aforementioned ratios are rational, for $l > m$. Let $q_m = l.c.m\ \{q_{ml}, l > m\}$, where $l.c.m$ denotes the least common multiple of its argument. By definition $q_n = 1$ (n is the lattice dimension).

Protocol 1. *(Transmission, Π_c). Let $s(m) \in \{0, 1, \ldots, q_m - 1\}$ be the largest s for which $[x_m/v_{mm} - s/q_m] = [x_m/v_{mm}]$. Then node m sends $\tilde{b}_m = [x_m/v_{mm}]$ and $s(m)$ to F, $m = 1, 2, \ldots, n$ (by definition $s(n) = 0$).*

Let $\bar{b} = (b_1, b_2, \ldots, b_n)$ be the coefficients of λ_{np}, the Babai point.

Theorem 8. *The coefficients of the Babai point $\bar{b}$ can be determined at the fusion center F after running transmission protocol Π_c.*

Proof. Observe that each coefficient of $\bar{b}$ is given by

$$b_m = \left[\frac{x_m - \sum_{l=m+1}^{n} b_l v_{m,l}}{v_{mm}}\right], \qquad m = 1, 2, \ldots, n, \tag{4.10}$$

which is written in terms of $\{z\}$ and $\lfloor z \rfloor$, the fractional and integer parts of real number z, respectively, ($z = \lfloor z \rfloor + \{z\}$, $0 \leqslant \{z\} < 1$) and also $[z]$ represents the integer closest to z. Then,

$$b_m = \left[\frac{x_m}{v_m} - \left\{ \frac{\sum_{l=m+1}^{n} b_l v_{ml}}{v_{mm}} \right\} \right] - \left\lfloor \frac{\sum_{l=m+1}^{n} b_l v_{ml}}{v_{mm}} \right\rfloor, \qquad m = 1, 2, \ldots, n. \tag{4.11}$$

Since the fractional part in the above equation is of the form s/q_m, $s \in \{0, 1, \ldots, q_m - 1\}$, where q_m is defined above, it follows that $0 \leqslant s/q_m < 1$. Thus

$$b_m = \begin{cases} \tilde{b}_m - \left\lfloor \frac{\sum_{l=m+1}^{n} b_l v_{ml}}{v_{mm}} \right\rfloor, & s \leqslant s(m), \\ \tilde{b}_m - \left\lfloor \frac{\sum_{l=m+1}^{n} b_l v_{ml}}{v_{mm}} \right\rfloor - 1, & s > s(m). \end{cases} \tag{4.12}$$

can be computed in the fusion center F in the order $m = n, n-1, \ldots, 1$. □

Corollary 6. *The rate required to transmit $s(m)$, $m = 1, 2, \ldots, n-1$ is no larger than $\sum_{i=1}^{n-1} \log_2(q_i)$ bits.*

Therefore, the total rate for computing the Babai point at the fusion center F under the centralized model is no larger than

$$\sum_{i=1}^{n} h(p_i) - \log_2 |\det V| - n \log_2(\alpha) + \sum_{i=1}^{n-1} \log_2(q_i) \text{ bits}, \tag{4.13}$$

where $h(p_i)$ is the differential entropy of random variable X_i, and scale factor α is small. Thus the incremental cost due to the $s(m)$'s does not scale with α. However, when α is small, this incremental cost can be considerable, if the lattice basis is not properly chosen as we will see in further examples.

This rate computation can be visualized geometrically and under the light of the decoding in orthogonal lattices. Consider a lattice $\Lambda \subset \mathbb{R}^n$ generated by $\{v_1, v_2, \ldots, v_n\}$, where we want to decode under the constraints proposed by the centralized model, a real vector $x = (x_1, x_2, \ldots, x_n)$. We construct an associated orthogonal lattice $\Lambda' \subseteq \mathbb{R}^n$ whose basis vectors are $\{\underbrace{(v_{11}, 0, \ldots, 0)}_{v_1'}, \ldots, \underbrace{(0, 0, \ldots, v_{nn})}_{v_n'}\}$, where $v_{ii}, 1 \leqslant i \leqslant n$ are the diagonal elements from the original generator matrix of Λ. Observe that the Voronoi region of Λ' corresponds to the Babai partition not aligned achieved without sending any extra bit in this model.

The idea is to decode in the orthogonal associated lattice Λ', which is a simple process and after that, recover the original approximate closest lattice point in Λ. In the end, we aim to prove that this process is equivalent to sending the extra bits and with this information, decide between the cases described in Equation (4.12).

Initially, we can notice that these Babai partitions in the space follow a cyclic behavior, i.e., after exactly $\prod_{m=1}^{n-1} q_m$, where $q_m = l.c.m\ \{q_{ml}, l > m\}$ shifts, it comes back to the original setting. This number, when calculated as a rate, corresponds precisely to the upper bound we have for the extra bits, introduced in Corollary 6.

Example 27. *Consider a lattice Λ generated by $\{(1,0),(2/5,2)\}$ and Λ' generated by $\{(1,0),(0,2).\}$ In this case, $q_1 = 5$ and there are q_1 distinct settings in the plane one need to analyze. After q_1 shifts, the Voronoi aligned partition around lattice points in the form $(0,\kappa)$, $\kappa \in \mathbb{Z}$, starts to be repeated, as illustrated in Figure 23.*

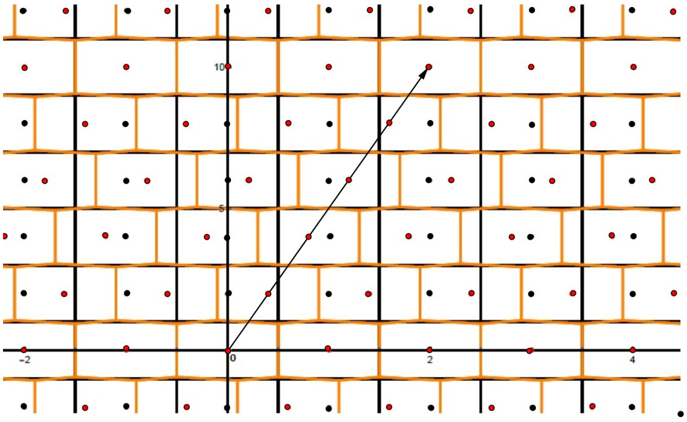

Figure 23 – Voronoi partition of Λ in orange and Voronoi partition of Λ' (Babai) in black.

This situation can be seen as a "modulo q_m" operation, where each class is represented uniquely in the space.

The vector $\tilde{b} = (\tilde{b}_1, \ldots, \tilde{b}_n)$, with $\tilde{b}_i = \lfloor x_i/v_{ii} \rceil$, is such that $||x - V'\tilde{b}||$ is minimum, where V' has the vectors $v_1', \ldots, v_2'$ on its columns. It means that $\tilde{b}$ decodes $x \in \mathbb{R}^n$ in the associated lattice Λ' and we want to use this information to decode approximately in Λ. Clearly, $\tilde{b}_n = b_n$ always.

In a general two dimensional case, for a matrix in the form $V = \begin{pmatrix} v_{11} & v_{12} \\ 0 & v_{22} \end{pmatrix}$, we consider $\tilde{b}_2 = b_2$. Indeed, this fact is always true because essentially, we want to write the vector (x_1, x_2) in terms of the basis $\{v_1, v_2\}$. So,

$$\begin{pmatrix} v_{11} & v_{12} \\ 0 & v_{22} \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}. \tag{4.14}$$

To recover the aligned Babai partition, one aims to find:

$$\begin{aligned} b_2 &= \left[\frac{x_2}{v_{22}}\right], \\ v_{11}b_1 + v_{12}b_2 = x_1 \Rightarrow b_1 &= \left[\frac{x_1}{v_{11}} - \frac{v_{12}}{v_{11}}b_2\right] = \left[\frac{x_1}{v_{11}} - \frac{p_{12}}{q_{12}}b_2\right] \\ &= \left[\underbrace{\left[\frac{x_1}{v_{11}}\right]}_{\tilde{b}_1} + \overline{x}_1 - \left\{\frac{p_{12}}{q_{12}}b_2\right\}\right] - \underbrace{\left\lfloor\frac{p_{12}}{q_{12}}b_2\right\rfloor}_{(b_2p_{12} \mod q_1)}, \end{aligned} \tag{4.15}$$

where $-\frac{1}{2} < \overline{x}_1 < \frac{1}{2}$. Geometrically, this operation means that we are bringing the analysis in each case to one of the $\{0, 1, \dots, q_1 - 1\}$ classes and correcting it by a factor of $(b_2p_{12} \mod q_1)$, which represents the translation occurred to the lattice point.

Example 28. *Figure 23 has represented in black the lattice points of Λ' and in red the lattice points of Λ, which are the ones we want to recover at the end of the process. We can immediately notice that the correction we need to take in account depends on where x_1 is located in the plane. For example, if $\tilde{b}_2 = 3 = b_2$ and $-\frac{1}{2} < x_1 < \frac{1}{2}$, then*

$$b_1 = \begin{cases} \tilde{b}_1 - 1, & \textit{if } -\frac{1}{2} + \frac{1}{5} = -\frac{3}{10} < x_1 - [x_1] < \frac{1}{2} \\ (\tilde{b}_1 - 1) - 1, & \textit{if } -\frac{1}{2} < x_1 - [x_1] \leqslant -\frac{3}{10}. \end{cases} \tag{4.16}$$

In a more general setting, according to Equation (4.15), we have that:

$$b_1 = \begin{cases} \tilde{b}_1 - (b_2p_{12} \mod q_1), & \textit{if } -\frac{v_{11}}{2} + \left\{\frac{p_{12}}{q_{12}b_2}\right\} < \frac{x_m}{v_{mm}} - \left[\frac{x_m}{v_{mm}}\right] < \frac{v_{11}}{2} \\ \tilde{b}_1 - (b_2p_{12} \mod q_1) - 1, & \textit{if } -\frac{v_{11}}{2} < \frac{x_m}{v_{mm}} - \left[\frac{x_m}{v_{mm}}\right] \leqslant -\frac{v_{mm}}{2} + \left\{\frac{p_{12}}{q_{12}b_2}\right\}. \end{cases} \tag{4.17}$$

This analysis can be also described for the $n-$dimensional case, where we aim to find the Babai point $\overline{b} = (b_1, \dots, b_n)$, as

$$b_m = \begin{cases} \tilde{b}_m - (\sum\limits_{l=m+1}^{n} b_lp_{ml}\hat{q}_{ml} \mod q_m), & \text{if } -\frac{v_{mm}}{2} + \left\{\frac{\sum_{l=m+1}^{n} b_lv_{ml}}{v_{mm}}\right\} < \frac{x_m}{v_{mm}} - \left[\frac{x_m}{v_{mm}}\right] < \frac{v_{mm}}{2} \\ \tilde{b}_m - (\sum\limits_{l=m+1}^{n} b_lp_{ml}\hat{q}_{ml} \mod q_m) - 1, & \text{if } -\frac{v_{mm}}{2} < \frac{x_m}{v_{mm}} - \left[\frac{x_m}{v_{mm}}\right] \leqslant -\frac{v_{mm}}{2} + \left\{\frac{\sum_{l=m+1}^{n} b_lv_{ml}}{v_{mm}}\right\}, \end{cases} \tag{4.18}$$

where $\hat{q}_{ml} = q_m/q_{ml}$. Therefore, the cost of analyzing all the classes is no larger than $\sum\limits_{m=1}^{n-1} \log_2(q_m)$, as stated in Corollary 6.

The following example illustrates how the method proposed in Theorem 8 works in two and three dimensions and also explore a case where this cost could be large.

Example 29. *Consider the hexagonal A_2 lattice generated by*

$$V = \begin{pmatrix} 1 & \frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} \end{pmatrix}.$$

The basis vectors are already Minkowski-reduced and applying what we described above we have that the coefficients b_2 and b_1 are given respectively by

$$b_2 = \left[\frac{x_2}{v_{22}}\right] = \left[\frac{2}{\sqrt{3}}x_2\right] \tag{4.19}$$

and

$$\begin{aligned} b_1 &= \left[\frac{x_1}{v_{11}} - \left\{\frac{b_2 v_{21}}{v_{11}}\right\}\right] - \left\lfloor\frac{b_2 v_{21}}{v_{11}}\right\rfloor && (4.20) \\ &= \left[x_1 - \left\{\left[\frac{2}{\sqrt{3}}x_2\right]\frac{1}{2}\right\}\right] - \left\lfloor\left[\frac{2}{\sqrt{3}}x_2\right]\frac{1}{2}\right\rfloor. && (4.21) \end{aligned}$$

Hence, for any real vector $x = (x_1, x_2)$ we have $\left\{\left[\frac{2}{\sqrt{3}}x_2\right]\frac{1}{2}\right\} = \frac{s}{q}$, with $q = 2$ and $s \in \{0, 1\}$. Node one must then send the largest integer $s(1)$ in the range $\{0, 1\}$ for which $\left[x_1 - \frac{s(1)}{q_1}\right] = [x_1]$ and $s(1) = 0$ or $s(1) = 1$ depending on the value that x_1 assumes.

The cost of this procedure, according to Corollary 6, is no larger than $\log_2 q_1 = 1$ bit. Thus the cost of constructing the nearest plane partition for the hexagonal lattice is at most one bit.

Nevertheless, this rate could be potentially large as the next example illustrates.

Example 30. *Suppose a lattice generated by*

$$V = \begin{pmatrix} 1 & \frac{311}{1000} \\ 0 & \frac{101}{100} \end{pmatrix}.$$

One can notice that the basis vectors are already Minkowski-reduced. Using the theory developed above we have that

$$b_2 = \left[\frac{x_2}{v_{22}}\right] = \left[\frac{100}{101}x_2\right] \tag{4.22}$$

and

$$\begin{aligned} b_1 &= \left[\frac{x_1}{v_{11}} - \left\{\frac{b_2 v_{21}}{v_{11}}\right\}\right] - \left\lfloor\frac{b_2 v_{21}}{v_{11}}\right\rfloor && (4.23) \\ &= \left[x_1 - \left\{\left[\frac{100}{101}x_2\right]\frac{311}{1000}\right\}\right] - \left\lfloor\left[\frac{100}{101}x_2\right]\frac{311}{1000}\right\rfloor. && (4.24) \end{aligned}$$

Consider, for example, $x = (1,1)$ *then we have that* $\left\{\left[\frac{100}{101}x_2\right]\frac{311}{1000}\right\} = \frac{311}{1000} = \frac{s}{q}$. *In this purpose, node one sends the largest integer* $s(1)$ *in the range* $\{0, 1, \ldots, 999\}$ *for which* $\left[x_1 - \frac{s(1)}{q_1}\right] = [x_1]$ *and we get* $s(1) = 500$.

This procedure will cost no larger than $\log_2 q_1 = \log_2 1000 \approx 9.96$ *and in the worst case, we need to send almost* 10 *bits to achieve Babai partition in the centralized model.*

Example 31. *Consider the three dimensional body centered cubic (BCC) lattice with generator matrix given by*

$$V = \begin{pmatrix} 1 & -\frac{1}{3} & -\frac{1}{3} \\ 0 & \frac{2\sqrt{2}}{3} & -\frac{\sqrt{2}}{3} \\ 0 & 0 & \sqrt{\frac{2}{3}} \end{pmatrix}, \tag{4.25}$$

which is the upper triangular matrix obtained after applying QR decomposition in the original basis considered in Example 9. In order to align this Voronoi region with Babai partition in its best way, we need to calculate the Babai point given by (b_1, b_2, b_3) *described below.*

$$b_3 = \left[\sqrt{\frac{3}{2}}x_3\right], \tag{4.26}$$

$$\begin{aligned} b_2 &= \left[\frac{3}{2\sqrt{2}}x_2 + \left\{\frac{1}{2}b_3\right\}\right] + \left\lfloor\frac{1}{2}b_3\right\rfloor \\ &= \left[\frac{3}{2\sqrt{2}}x_2 + \left\{\frac{1}{2}\left[\sqrt{\frac{3}{2}}x_3\right]\right\}\right] + \left\lfloor\frac{1}{2}\left[\sqrt{\frac{3}{2}}x_3\right]\right\rfloor, \end{aligned} \tag{4.27}$$

and

$$b_1 = \left[x_1 + \left\{\frac{1}{3}b_2 + \frac{1}{3}b_3\right\}\right] + \left\lfloor\frac{1}{3}b_2 + \frac{1}{3}b_3\right\rfloor, \tag{4.28}$$

where b_2 *and* b_3 *are integers previously defined in Equations (4.26) and (4.27), respectively.*

Hence, for any real vector $x = (x_1, x_2, x_3)$ *we have two nodes that should send extra information, nodes* 2 *and* 1, *according to the following description*

$$\begin{cases} \textit{Node 2: } \left\{\frac{1}{2}b_3\right\} = \frac{s(2)}{q(2)}, \ q(2) = 2 \textit{ then } s(2) = 0 \textit{ or } 1 \\ \textit{Node 1: } \left\{\frac{1}{3}b_2 + \frac{1}{3}b_3\right\} = \frac{s(1)}{q(1)}, \ q(1) = 3 \textit{ then } s(1) = 0, 1 \textit{ or } 2. \end{cases} \tag{4.29}$$

Observe that the values of $s(1)$ *and* $s(2)$ *are calculated here in a general way, however, they exact values depend on* x_1 *and* x_2, *respectively. Therefore, the total rate to send* $s(1)$ *and* $s(2)$ *to the fusion center is*

$$\log_2 2 + \log_2 3 \approx 2.5859 \approx 3 \textit{ bits}. \tag{4.30}$$

The analysis here points to the importance of the number-theoretic structure of the generator matrix V in determining the communication requirements for computing x_{np}.

4.3.2 Interactive model

For $i = n, n-1, \ldots, 1$, node S_i sends $U_i = \left\lceil (X_i - \sum_{j=i+1}^{n} \alpha v_{ij} U_j)/\alpha v_{ii} \right\rfloor$ to all other nodes. The total number of bits communicated is given by $R = (n-1)\sum_{i=1}^{n} H(U_i|U_{i+1}, U_{i+2}, \ldots, U_n)$. For α suitably small, and under the assumption of independent X_i, this rate can be approximated by $R = (n-1)\sum_{i=1}^{n} h(p_i) - \log_2(\alpha v_{ii})$. Normalizing so that V has unit determinant we get $R = (n-1)\sum_{i=1}^{n} h(p_i) - n(n-1)\log_2(\alpha)$.

In this chapter, we have investigated the closest lattice point problem in a distributed network, under two communication models, centralized and interactive. By exploring the nearest plane (Babai) partition for a given Minkowski-reduced basis, we have determined a closed form for the error probability in two dimensions. For the three dimensional case, using an obtuse superbase, we have estimated computationally the worst error probability for random lattices and also conjectured bounds for it. Based on our analysis, we expect that the worst error probability in an $n-$dimensional lattice is achieved by the densest lattice and goes to one as n goes to infinity. The number of bits that nodes need to send in both models (centralized and interactive) to achieve the rectangular nearest plane partition was also computed. The communication cost/error tradeoff of refining the nearest-plane estimate in an interactive setting is addressed in the companion papers [50, 51].

Chapter 5

Summary of contributions and future work

The main contributions of this thesis are:

Construction C: we present counterexamples to show that for 3 levels and up, Construction C is not geometrically uniform in general (Examples 10 and 11), describe two different ways of producing geometrically uniform constellations (Theorem 4 and Corollary 1), which provided an alternative proof for the geometric uniformity of 2−level Construction C (Corollary 2).

Construction $C^{\star}$: we define a new multilevel constellation that we call Construction $C^{\star}$ (Definition 29), inspired by the bit-interleaved coded modulation, demonstrate that a 2−level Construction $C^{\star}$ is geometrically uniform (Theorem 5) and for three levels and up it is not necessarily geometrically uniform. Necessary and sufficient conditions that guarantee the latticeness of Construction $C^{\star}$ (Theorem 6) are provided as well as a detailed description of the computation of the minimum distance of this construction (Section 3.3.3.1) and also comparisons with the associated Construction C. The average minimum distance in the presence of a random interleaver is also determined (Section 3.3.3.2) and used to show that a hybrid Construction $C^{\star}/C$ has potentially a better packing efficiency than Construction C (Figure 14) in a scenario where the codes that define both constructions are Gilbert-Varshamov achieving.

Approximate closest lattice point in a distributed system: we derive a function to compute the error probability of solving the approximate closest point in a distributed system considering the Babai partition for two dimensions (Theorem 7), showing that the worst error probability happens with the hexagonal A_2 lattice (Corollary 5) and we estimate computationally lower and upper bounds for the error probability for three dimensional lattices (Figure 22). From this analysis, we could conjecture that also for dimension three, the worst error probability happens when we consider the densest lattices (Conjecture 1) and we expect this to happen also for larger dimensions (Conjecture 2). We also calculate the rate for achieving the Babai partition in a distributed system which is centralized (Theorem 8) and in an interactive (Section 4.3.2).

We enumerate in what follows, promising research topics that we aim to explore in future works:

Hybrid Construction C/D for multi-terminal coding

Multi-terminal lattice coding theory is being an interesting topic of study in recent years, e.g., for side information problems, network coding and interference alignment ([39], [44], [57]). Some of the new coding schemes are motivated by the insight provided by the lattice structure, while others really hinge upon the Euclidean-space linearity of the lattice. Multi-terminal codes commonly use a nested pair of codes, where one of the codes should be closed under real addition (i.e., a lattice) while the other code can have a non-linear structure. As multilevel codes are natural candidates for nesting, it would be interesting to explore the potential of a hybrid Construction C/D nested coding scheme for efficient multi-terminal coding.

Construction $C^{\star}$ with Gray map

In our work, we defined Construction $C^{\star}$ under the natural labeling in order to compare it with Construction C, nevertheless, in the original definition of the bit-interleaved coded modulation, from where Construction $C^{\star}$ was inspired, the mapping used is the Gray map, determined as

The Gray map is a mapping from $\mathbb{Z}_4$ to $\mathbb{Z}_2^2$ defined by

$$0 \rightarrow (0,0), \quad 1 \rightarrow (0,1), \quad 2 \rightarrow (1,1), \quad 3 \rightarrow (1,0), \tag{5.1}$$

which can be coordinate wisely extended to a mapping from $\mathbb{Z}_4^n$ to $\mathbb{Z}_2^{2n}$.

Thus, we aim to study the properties of a constellation generated with the Gray map instead of the natural labeling and relate the results associated to $4-$ary codes to what we have already done for Construction $C^{\star}$. The extension of Construction $C^{\star}$ to general $q-$ary codes is also a topic of interest.

Decoding algorithm for Construction $C^{\star}$

When we talk about multilevel construction, it is implicit the use of multistage decoding. However, for Construction $C^{\star}$ this method is not efficient due to the dependence imposed by the assumption of a main code $\mathcal{C} \subset \mathbb{F}_2^{nL}$. Hence, one of our goals is to find an efficient decoding method for Construction $C^\star$, which takes advantage of the structure of the main code.

Error probability for a $n-$dimensional lattice

Regarding the study of the error probability, we aim to find (if possible) a closed formula to calculate the error probability for general three dimensional lattices and prove Conjecture 1 and somehow to approach Conjecture 2 under certain restrictions. Further problems include to generalize the results presented here to families A_n and D_n lattices, for which reduced form bases and algorithms that searches for the closest lattice point are already available [2]. We also want to investigate the closest lattice point in a distributed system for Voronoi's first kind lattices, inspired by [36].

Bibliography

[1] E. Agrell and T. Eriksson, *Optimization of Lattice for Quantization.* IEEE Transactions on Information Theory 44(5), pp. 1814-1828, 1998.

[2] E. Agrell, T. Eriksson, A. Vardy and K. Zeger, *Closest Point Search in Lattices.* IEEE Transactions on Information Theory 48(8), pp. 2201-2214, 2002.

[3] M. Ajtai, *Generating hard instances of lattice problems.* In Complexity of computations and proofs, vol. 13 of Quad. Mat., pages 132. Dept. Math., Seconda Univ. Napoli, Caserta, 2004. Preliminary version in STOC 1996.

[4] M. Ajtai, *The Shortest Vector Problem in L2 is NP-hard for Randomized Reductions (Extended Abstract).* Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing, pp. 10–19, 1998.

[5] O. Amrani, Y. Be'ery, A. Vardy, F.-W. Sun, and H. C. A. van Tilborg, *The Leech Lattice and the Golay Code: Bounded-Distance Decoding and Mu1tilevel Constructions.* IEEE Transactions on Information Theory 40(4), 1030-1043. 1994.

[6] O. Ayaso, D. Shah and M. A. Dahleh, *Information Theoretic Bounds for Distributed Computation Over Networks of Point-to-Point Channels.* IEEE Transactions on Information Theory 56(12), pp. 6020-6039, 2010.

[7] L. Babai, *On Lovász lattice reduction and the nearest lattice point problem.* Combinatorica, 6(1), pp. 1-13, 1986.

[8] T. Berger, *Rate distortion theory: A mathematical basis for data compression.* Prentice-Hall, Englewood Cliffs, NJ, 1971.

[9] M. F. Bollauf, V. Vaishampayan and S. I. R. Costa, *On the Communication Cost of Determining an Approximate Nearest Lattice Point.* 2017 IEEE International Symposium on Information Theory (ISIT), Aachen, pp. 1838-1842, 2017.

[10] M. F. Bollauf, V. Vaishampayan and S. I. R. Costa, *Communication-Efficient Search for an Approximate Closest Lattice Point.* https://arxiv.org/abs/1801.09796 [it], Jan. 2018.

[11] M. F. Bollauf and R. Zamir, *Uniformity properties of Construction C.* 2016 IEEE International Symposium on Information Theory (ISIT), Barcelona, pp. 1516-1520, 2016.

[12] M. F. Bollauf, R. Zamir and Sueli. I. R. Costa, *Construction $C^\star$: an interlevel coded version of Construction C.* 2018 International Zurich Seminar, Zurich, pp. 118–122, 2018.

[13] M. F. Bollauf, R. Zamir and Sueli. I. R. Costa, *Multilevel constructions: coding, packing and geometric uniformity.* https://arxiv.org/abs/1806.05715 [it], Jun. 2018.

[14] R. de Buda, *Fast FSK signals and their demodulation.* Can. Electron. Eng. Journal, 1, pp. 28–34, 1972.

[15] R. de Buda, *Coherent demodulation of frequency-shift keying with low deviation ratio.* IEEE Trans. Commun., COM-20, pp. 429–435, 1972.

[16] H. Cohn, A. Kumar, S. Miller, D. Radchenko, and M. Viazovska, *The sphere packing problem in dimension 24.* Ann. of Math., vol. 185, pp. 1017–1033, 2017.

[17] J. H. Conway and N. J. A. Sloane, *Low-dimensional lattices. VI. Voronoi reduction of three-dimensional lattices.* Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences, vol. 436, no. 1896, pp. 55-68. The Royal Society, 1992.

[18] J. H. Conway and N.J. A. Sloane, *Sphere Packings, Lattices and Groups*, 3rd ed. New York, USA: Springer, 1999.

[19] M. Costa, *Writing on dirty paper.* IEEE Trans. Information Theory, vol. IT-29, pp. 439–441, 1983.

[20] D. Deblercq, M. Fossorier and E. Biglieri, *Channel Coding: Theory, Algorithms, and Applications.* Oxford, UK: Academic Press, 2014.

[21] P. van Emde Boas, *Another NP-Complete Problem and the Complexity of Computing Short Vectors in a Lattice.* Report 81-04, Mathematische Institut, Universiry of Amsterdam, Amsterdam, 1981.

[22] G. D. Forney, *Coset codes-part I: introduction and geometrical classification.* IEEE Transactions on Information Theory 34(5), pp. 1123-1151, 1988.

[23] G. D. Forney, *Coset codes-part II: binary lattices and related codes.* IEEE Transactions on Information Theory 34(5), pp. 1152-1187, 1988.

[24] G. D. Forney, *Geometrically uniform codes.* IEEE Trans. on Inf. Th. 37(5), pp. 1241-1260, 1991.

[25] G. D. Forney, M. D. Trott and S. Chung, *Sphere-Bound-Achieving Coset Codes and Multilevel Coset Codes.* IEEE Transactions on Information Theory 46(3), pp. 820-850, 2000.

[26] S.D. Galbraith. *Mathematics of Public Key Cryptography.* Cambridge University Press, 2012.

[27] G. H. Golub and C. F. Van Loan, *Matrix Computations.* The Johns Hopkins University Press, 4 ed, 2013.

[28] V. Guruswami. (2010), *Gilbert-Varshamov bound [Class notes].* Pittsburgh, PA: Carnegie Mellon University, Introduction to Coding Theory.

[29] T. Hales, *A Proof of the Kepler Conjecture.* Ann. Math. 162, pp. 1065-1185, 2005.

[30] J. Hoffstein, J. Phiper and J.H. Silverman, *An Introduction to Mathematical Cryptography.* Springer, 2008.

[31] R. Keralapura, G. Cormode, and J. Ramamirtham, *Communication-efficient distributed monitoring of thresholded counts.* Proceedings of the 2006 ACM SIGMOD international conference on Management of data, ACM, 2006.

[32] W. Kositwattanarerk and F. Oggier, *Connections between Construction D and related constructions of lattices.* Designs, Codes and Cryptography, v.73, pp. 441-455. Norwell, USA: Kluwer Academic Publishers, 2014.

[33] E. Kushilevitz and N. Nissan, *Communication Complexity.* Cambridge University Press, 1997.

[34] A. K. Lenstra, H. W. Lenstra and L. Lovász, *Factoring polynomials with rational coefficients.* Mathematische Annalen 261(4), 515â, 1982.

[35] N. Ma, and P. Ishwar, *Some results on distributed source coding for interactive function computation*, IEEE Transactions on Information Theory, vol. 57, No. 9, pp. 6180-6195, 2011.

[36] R. G. McKilliam, A. Grant and I. V. L. Clarkson, *Finding a closest point in a lattice of Voronoi's first kind.* Siam J. Discrete Math 28(3), pp. 1405-1422, 2014.

[37] D. Micciancio and S. Goldwasser, *Complexity of lattice problems: a cryptographic perspective.* Vol. 671. Springer Science & Business Media, 2012.

[38] H. Minkowski, *On the positive quadratic forms and on continued fractions algorithms (Über die positiven quadratischen formen undüber kettenbruchähnliche algorithmen).* J. Reine und Angewandte Math., vol. 107, pp. 278–297, 1891.

[39] B. Nazer and M. Gastpar, *Compute-and-Forward: Harnessing Interference Through Structured Codes.* IEEE Transactions on Information Theory 57(10), pp. 6463 - 6486, 2011.

[40] J. Neukirch and N. Schappacher, *Algebraic Number Theory.* Springer Berlin Heidelberg, 1999.

[41] A. Orlitsky and J. R. Roche, *Coding for Computing*, IEEE Trans. on Inf. Th., vol. 47, no. 3, pp. 903-917, 2001.

[42] C. Peikert. *A Decade of Lattice Cryptography.* 2016.

[43] M. Pohst, *On the computation of lattice vectors of minimal length, successive minima and reduced bases with applications.* ACM SIGSAM Bulletin 15(1), pp. 37-44, 1981.

[44] S. S. Pradhan and K. Ramchandran, *Distributed source coding using syndromes (discus): design and construction.* Proc. IEEE Data Compression Conference, Snowbird, UT, 1999.

[45] S. A. Ramprashad and G. Caire and H. C. Papadopoulos, *Cellular and Network MIMO architectures: MU-MIMO spectral efficiency and costs of channel state information.* Conference Record of the Forty-Third Asilomar Conference on Signals, Systems and Computers, pp. 1811-1818, 2009.

[46] C.E. Shannon, *A Mathematical Theory of Communication.* Bell System Technical Journal, 27(3), pp. 379-423, 1948.

[47] L. Szczecinski and A. Alvarado, *Bit-interleaved coded modulation : fundamentals, analysis, and design.* John Wiley & Sons, 2015.

[48] A. S. Tanenbaum and M.n van Steen, *Distributed Systems Principles and Paradigms.* Createspace Independent Publishing Platform, 2 ed., 2016.

[49] L. Fejes Tóth, *On the densest packing of circles in a convex domain.* Norske Vid. Selsk. Fordhl., Trondheim, 21, pp. 68-76, 1948.

[50] V. A. Vaishampayan and M. F. Bollauf, *Communication Cost of Transforming a Nearest Plane Partition to the Voronoi Partition*, Proc. 2017 IEEE Int. Symp. Inform. Th., Aachen, Germany, pp. 1843-1847, July 2017.

[51] V. A. Vaishampayan and M. F. Bollauf, *On the Interactive Communication Cost of the Distributed Nearest Lattice Point Problem.* https://arxiv.org/abs/1801.10491 [it], Jan. 2018.

[52] M. S. Viazovska, *The sphere packing problem in dimension 8.* Ann. of Math., vol. 185, pp. 991–1015, 2017.

[53] Wolfram Research, Inc., Mathematica, Version 11.2, Champaign, IL, 2017.

[54] A. C. Yao, *Some Complexity Questions Related to Distributive Computing(Preliminary Report)*. Proceedings of the Eleventh Annual ACM Symposium on Theory of Computing, STOC '79, pp. 209-213, 1979.

[55] R. Zamir, *Lattice Coding of Signals and Networks: A Structured Coding Approach to Quantization, Modulation and Multi-user Information Theory.* Cambridge University Press, 2014.

[56] R. Zamir, *Lattices are everywhere.* Information Theory and Applications Workshop, San Diego-CA, pp. 392–421, 2009.

[57] R. Zamir, S. Shamai, and U. Erez, *Nested linear/lattice codes for structured multiterminal binning.* IEEE Transactions on Information Theory 48, pp. 1250–1276, 2002.

[58] E. Zehavi, *8-PSK trellis codes for a Rayleigh channel.* IEEE Trans. Commun., 40 (3), pp. 873–884, 1992.

Appendix

APPENDIX A

Mathematica program to estimate the closest lattice point in a distributed network (three dimensional case)

```
Result = Table[
  g[a1_, b1_, c1_, d1_, e1_] := Module[{f},

  (*Function f produces an obtuse superbase and identify the Voronoi region*)
     f[a2_, b2_, c2_, d2_, e2_] := Module[{a = a2, b = b2, c = c2, d = d2, e = e2},
      v1 = {1, 0, 0};
      v2 = {a, b, 0};
      v3 = {c, d, e};
      v0 = -v1 - v2 - v3;
      p01 = v0.v1;
      p02 = v0.v2;
      p03 = v0.v3;
      p12 = v1.v2;
      p13 = v1.v3;
      p23 = v2.v3; {p01, p02, p03, p12, p13, p23}];

     {a, b, c, d, e} = {RandomReal[{-1, 1}], RandomReal[{-4, 4}], RandomReal[{-4, 4}], RandomReal[{-4, 4}], RandomReal[{-4, 4}]}; {p01, p02, p03, p12, p13, p23} = f[a, b, c, d, e];

    (*Test if the triangular basis is an obtuse superbase (and
      also Minkowski, according to Theorem 3)*)
  While[(p12 <= 0 && p13 <= 0 && p23 <= 0 && p01 <= 0 && p02 <= 0
     && p03 <= 0 && Norm[v1] <= Norm[v2] && Norm[v2] <= Norm[v3]
     && Norm[v3] <= Norm[v0] && Norm[v3] <= Norm[v2 + v3] && Norm[
     v3] <= Norm[v1 + v3] && Norm[v2] <= Norm[v1 + v2]) == False,
    {a, b, c, d, e} = {RandomReal[{-4, 4}], RandomReal[{-4, 4}],
      RandomReal[{-4, 4}], RandomReal[{-4, 4}], RandomReal[{-4,
      4}]};
     f[a, b, c, d, e] == {p01, p02, p03, p12, p13, p23}];
     {p,q,r,s,t}={a,b,c,d,e};

     (**** TESTING PARAMETERS****)
      (*Truncated Octahedron*)
      (*{p,q,r,s,t}={-1/3,2Sqrt[2]/3,-1/3,-Sqrt[2]/3,Sqrt
         [2/3]};*)
      (*Rhombic Dodecahedron*)
      (*{p,q,r,s,t}={0,1,-1/2,-1/2,1/Sqrt[2]};*)
      (*{p,q,r,s,t}={-1/2,-Sqrt[3]/2,0,1/Sqrt[3],2/Sqrt[6]};*)
      (*Hexagonal Prism*)
      (*{p,q,r,s,t}={-1/2,-Sqrt[3]/2,0,0,1};*)
      (*Elongated Dodecahedron*)
      (*{p,q,r,s,t}={0,1,-1/2,-1/2,2/Sqrt[3]};*)
      (*{p,q,r,s,t}={-1/2,-Sqrt[5]/2,0,1/Sqrt[5],2/Sqrt[5]};*)
      (*Cuboid*)
      (*{p,q,r,s,t}={0,1,0,0,1};*)

    p01 = v[1].v[2];
    p02 = v[1].v[3];
    p03 = v[1].v[4];
    p12 = v[2].v[3];
    p13 = v[2].v[4];
    p23 = v[3].v[4];

    (*Constructing Voronoi region via Coway&Sloane method*)
    Clear[p01, p02, p03, p12, p13, p23];
    v[2] = {1, 0, 0};
    v[3] = {p, q, 0};
    v[4] = {r, s, t};
    v[1] = -v[2] - v[3] - v[4];

    p01 = Chop[N[v[1].v[2]]];
    p02 = Chop[N[v[1].v[3]]];
    p03 = Chop[N[v[1].v[4]]];
    p12 = Chop[N[v[2].v[3]]];
    p13 = Chop[N[v[2].v[4]]];
    p23 = Chop[N[v[3].v[4]]];

    ap = Permutations[{1, 2, 3, 4}];
    P = Table[Dot[v[i], v[j]], {i, 1, 4}, {j, 1, 4}];
    y = {0, 0, 0, 0};
    A = Table[{{i, j, k, l} = ap[[ll]],
       y[[i]] = 1/2 (-P[[i, j]] - P[[i, k]] - P[[i, l]]),
       y[[j]] = 1/2 (P[[i, j]] - P[[j, k]] - P[[j, l]]),
       y[[k]] = 1/2 (P[[i, k]] + P[[j, k]] - P[[k, l]]),
       y[[l]] = 1/2 (P[[i, l]] + P[[j, l]] + P[[k, l]])};
      y, {ll, 1, 24}];

    S = Table[LinearSolve[{v[1], v[2], v[3], v[4]}, {A[[i, 1]], A
       [[i, 2]],
        A[[i, 3]], A[[i, 4]]}], {i, 1, 24}];
        Vol = Abs[q*t];

    (*Constructing the Babai region (error paralelephiped)*)
     vr = {{1/2, -q/2, t/2}, {1/2, q/2, t/2}, {-1/2, -q/2, t/2},
        {-1/2,q/2, t/2}, {1/2, -q/2, -t/2}, {1/2, q/2, -t/2},
        {-1/2, -q/2, -t/2}, {-1/2, q/2, -t/2}};
         f1= {{8,4,2,6},{8,6,5,7},{8,7,3,4},{4,3,1,2},
         {1,3,7,5},{2,1,5,6}};
     R = Graphics3D@GraphicsComplex[vr, Polygon /@ f1];

    (*Calculating the probability of correctness for each special
        Voronoi region*)
    (*Truncated Octahedron*)
    If[(p01 != 0 && p02 != 0 && p03 != 0 && p12 != 0 && p13 != 0
       && p23 != 0),

     ff1 = Complement[f1, {{8, 7, 3, 4}, {2, 1, 5, 6}}];
     f2 = {{2, 1, 3, 4, 6, 5}, {8, 7, 9, 10, 12, 11}, {14, 13,
        15, 16,18, 17}, {20, 19, 21, 22, 24, 23}, {2, 1, 7, 8},
        {4, 3, 13, 14}, {6, 5, 19, 20}, {10, 9, 15, 16}, {12, 11,
        21, 22}, {18, 17, 23, 24}, {20, 6, 4, 14, 17, 23}, {12,
        22, 24, 18, 16, 10}, {21, 19, 5, 2, 8, 11}, {15, 13, 3, 1,
         7, 9}};

     ff2 = Complement[f2, {{8, 7, 9, 10, 12, 11}}, {{20, 6, 4,
        14, 17, 23}}];
     V = Graphics3D@GraphicsComplex[S, Polygon /@ f2];
     P1 = Cases[S, {x_ /; x == 1/2, _, _}];
     P2 = Cases[S, {x_ /; x == -1/2, _, _}];
     Clear[x, y, z];
     Func[v1_, v2_, f1_, f2_] := Module[{fC = Append[#, #[[1]]] &
         /@ f1}, {x, y, z} /.
     NSolve[Or @@ ({x, y, z} \[Element] # & /@ MeshPrimitives[
        MeshRegion[v1, Line /@ fC], 1] ) && Or @@ ({x, y, z} \[
        Element] # & /@ MeshPrimitives[MeshRegion[v2, Polygon /@
        f2], 2])]];

     Intersect[v1_, v2_, f1_, f2_, ff1_, ff2_] := Union[Func[v1,
        v2, f1, ff2], Func[v2, v1, f2, ff1]];

     points = Intersect[vr, S, f1, f2, ff1, ff2] // Chop;
     pts = Union[points, P1, P2];
     B = ConvexHullMesh[pts];
     Vc = Volume[B];
     Pc = Vc/Vol;
     Pc,

     (*Hexa-Rhombic Dodecahedron*)
     If[(p01 != 0 && p02 != 0 && p03 != 0 && p12 != 0 && p13 == 0
         && p23 != 0) || (p01 != 0 && p02 != 0 && p03 != 0 && p12
        != 0 && p13 != 0 && p23 == 0) || (p01 == 0 && p02 != 0 &&
        p03 != 0 && p12 != 0 && p13 != 0 && p23 != 0) || (p01 != 0
         && p02 == 0 && p03 != 0 && p12 != 0 && p13 != 0 && p23 !=
         0) || (p01 != 0 && p02 != 0 && p03 == 0 && p12 != 0 &&
        p13 != 0 && p23 != 0),

      ff1 = Complement[f1, {{8, 7, 3, 4}, {2, 1, 5, 6}}];
      f2 = {{2, 1, 3, 6}, {8, 7, 9, 10, 12, 11}, {14, 15, 16,
         17}, {20, 19, 21, 22, 24, 23}, {2, 1, 7, 8}, {6, 5, 19,
         20}, {10, 9, 15, 16}, {18, 17, 23, 24}, {20, 6, 4, 14,
         17, 23}, {22, 24, 18, 10}, {19, 5, 8, 11}, {15, 13, 3, 1,
          7, 9}};

      ff2 = Complement[f2, {{8, 7, 9, 10, 12, 11}}, {{20, 6, 4,
         14, 17, 23}}];
      V = Graphics3D@GraphicsComplex[S, Polygon /@ f2];
```

```
      P1 = Cases[S, {x_ /; x == 1/2, _, _}];
      P2 = Cases[S, {x_ /; x == -1/2, _, _}];
      Clear[x, y, z];
      Func[v1_, v2_, f1_, f2_] := Module[{fC = Append[#, #[[1]]]
         & /@ f1}, {x, y, z} /.
      NSolve[Or @@ ({x, y, z} \[Element] # & /@ MeshPrimitives[
         MeshRegion[v1, Line /@ fC], 1] ) && Or @@ ({x, y, z} \[
         Element] # & /@ MeshPrimitives[MeshRegion[v2, Polygon /@
         f2], 2])]];

      Intersect[v1_, v2_, f1_, f2_, ff1_, ff2_] := Union[Func[v1,
          v2, f1, ff2], Func[v2, v1, f2, ff1]];

      points = Intersect[vr, S, f1, f2, ff1, ff2] // Chop;
      pts = Union[points, P1, P2];
      B = ConvexHullMesh[pts];
      Vc = Volume[B];
      Pc = Vc/Vol;
      Pc,

      (*Case 1: Rhombic Dodecahedron*)
      If[p01 == 0 && p02 != 0 && p03 != 0 && p12 != 0 && p13 != 0
          && p23 == 0,
       ff1 = Complement[f1, {{8, 7, 3, 4}, {2, 1, 5, 6}}];
       f2 = {{2, 3, 4, 5}, {8, 9, 10, 11}, {14, 15, 16, 17}, {20,
           21, 22, 23}, {4, 3, 13, 14}, {6, 5, 19, 20}, {10, 9,
          15, 16}, {12, 11, 21, 22}, {20, 4, 14, 23}, {22, 18, 16,
           10}, {21, 5, 2, 11}, {15, 3, 1, 9}};

       ff2 = Complement[f2, {{8, 9, 10, 11}}, {{20, 4, 14, 23}}];
       V = Graphics3D@GraphicsComplex[S, Polygon /@ f2];
       P1 = Cases[S, {x_ /; x == 1/2, _, _}];
       P2 = Cases[S, {x_ /; x == -1/2, _, _}];
       Clear[x, y, z];
       Func[v1_, v2_, f1_, f2_] := Module[{fC = Append[#, #[[1]]]
           & /@ f1}, {x, y, z} /.
       NSolve[Or @@ ({x, y, z} \[Element] # & /@ MeshPrimitives[
          MeshRegion[v1, Line /@ fC], 1] ) && Or @@ ({x, y, z} \[
          Element] # & /@ MeshPrimitives[MeshRegion[v2, Polygon /@
           f2], 2])]];

       Intersect[v1_, v2_, f1_, f2_, ff1_, ff2_] := Union[Func[v1
```

```
          , v2, f1, ff2], Func[v2, v1, f2, ff1]];

       points = Intersect[vr, S, f1, f2, ff1, ff2] // Chop;
       pts = Union[points, P1, P2];
       B = ConvexHullMesh[pts];
       Vc = Volume[B];
       Pc = Vc/Vol;
       Pc,

       (*Case 2: Rhombic Dodecahedron*)
       If [p01 != 0 && p02 == 0 && p03 != 0 && p12 != 0 && p13 ==
           0 && p23 != 0,
        ff1 = Complement[f1, {{8, 7, 3, 4}, {2, 1, 5, 6}}];
        f2 = {{1, 3, 6, 5}, {8, 9, 10, 12}, {14, 15, 16, 17},
           {19, 21,24, 23}, {2, 1, 7, 8}, {6, 5, 19, 20}, {10, 9,
           15, 16}, {18, 17, 23, 24}, {6, 4, 17, 23}, {22, 24, 18,
            10}, {19, 5, 8, 11}, {15, 3, 1, 9}};


        ff2 = Complement[f2, {{8, 9, 10, 12}}, {{6, 4, 17, 23}}];
        V = Graphics3D@GraphicsComplex[S, Polygon /@ f2];
        P1 = Cases[S, {x_ /; x == 1/2, _, _}];
        P2 = Cases[S, {x_ /; x == -1/2, _, _}];
        Clear[x, y, z];
        Func[v1_, v2_, f1_, f2_] := Module[{fC = Append[#,
           #[[1]]] & /@ f1}, {x, y, z} /.
        NSolve[Or @@ ({x, y, z} \[Element] # & /@ MeshPrimitives[
           MeshRegion[v1, Line /@ fC], 1] ) && Or @@ ({x, y, z} \[
           Element] # & /@ MeshPrimitives[MeshRegion[v2, Polygon /
           @ f2], 2])]];

        Intersect[v1_, v2_, f1_, f2_, ff1_, ff2_] := Union[Func[
           v1, v2, f1, ff2], Func[v2, v1, f2, ff1]];

        points = Intersect[vr, S, f1, f2, ff1, ff2] // Chop;
        pts = Union[points, P1, P2];
        B = ConvexHullMesh[pts];
        Vc = Volume[B];
        Pc = Vc/Vol;
        Pc,

        (*Case 3: Rhombic Dedecahedron & Special case of Hexa-
        Rhombic Dodecahedron*)
        If[(p01 != 0 && p02 != 0 && p03 == 0 && p12 == 0 && p13 != 0 && p23 != 0) || (p01 != 0 && p02 != 0 && p03 != 0 && p12 == 0 && p13 != 0 && p23 != 0),
         P1 = Cases[S, {_, _, x_ /; x >= t/2}];
         B = ConvexHullMesh[P1];
         Vc = 2*Volume[B];
         Pc = 1 - (Vc/Vol);
         Pc,

         (*Hexagonal Prism*)
         If[(p01 != 0 && p02 != 0 && p03 != 0 && p12 == 0 && p13 == 0 && p23 != 0) || (p01 != 0 && p02 != 0 && p03 != 0 && p12 == 0 && p13 != 0 && p23 == 0) || (p01 == 0 && p02 == 0 && p03 != 0 && p12 != 0 && p13 != 0 && p23 != 0) || (p01 != 0 && p02 != 0 && p03 != 0 && p12 != 0 && p13 == 0 && p23 == 0) || (p01 != 0 && p02 != 0 && p03 == 0 && p12 != 0 && p13 == 0 && p23 != 0) || (p01 == 0 && p02 != 0 && p03 != 0 && p12 == 0 && p13 != 0 && p23 != 0) || (p01 != 0 && p02 == 0 && p03 != 0 && p12 == 0 && p13 != 0 && p23 != 0) || (p01 != 0 && p02 != 0 && p03 == 0 && p12 != 0 && p13 != 0 && p23 == 0) || (p01 == 0 && p02 != 0 && p03 == 0 && p12 != 0 && p13 != 0 && p23 != 0) || (p01 != 0 && p02 == 0 && p03 == 0 && p12 != 0 && p13 != 0 && p23 != 0) || (p01 == 0 && p02 != 0 && p03 != 0 && p12 != 0 && p13 == 0 && p23 != 0) || (p01 != 0 && p02 == 0 && p03 != 0 && p12 != 0 && p13 != 0 && p23 == 0),

          pp = { Part[S[[3]], {1, 2}] , Part[S[[1]], {1, 2}], Part[S[[7]], {1, 2}], Part[S[[9]], {1, 2}], Part[S[[15]], {1, 2}], Part[S[[14]], {1, 2}]};
          qq = {Part[vr[[6]], {1, 2}], Part[vr[[5]], {1, 2}], Part[vr[[7]], {1, 2}], Part[vr[[8]], {1, 2}]};
          m1 = Polygon[pp];
          m2 = Polygon[qq];
          Rd = RegionIntersection[m1, m2];
          Vc = Area[Rd];
          Pc = N[Vc/Vol];
          Pc,

          (*Cuboid*)
        Pc = 1]]]]]]];
                g[a, b, c, d, e];

n = {Norm[v[2]], Norm[v[3]], Norm[v[4]], Norm[v[2] + v[3]], Norm[v[2] + v[4]], Norm[v[3] + v[4]], Norm[v[2] + v[3] + v[4]]};
n1 = (Min[n])/2;
Pd = N[(4/3*Pi*((n1)^{3}))/Vol];
{Pd, 1 - Pc}, {i, 1}]
```