Federal University of São Paulo

Science and Technology Institute

Master's Degree em Pure and Applied Mathematics

PHYSICAL LAYER SECURITY IN WIRELESS COMMUNICATION

Júlia Wotzasek Pereira

São José dos Campos - SP - Brazil

2023

Júlia Wotzasek Pereira

PHYSICAL LAYER SECURITY IN WIRELESS COMMUNICATION

Dissertation presented to Federal University of São Paulo – Science and Technology Institute as a partial requirement to obtain a Master's degree in Pure and Applied Mathematics.

Supervisor:
Profa. Dra. Grasiele Cristiane Jorge

Co-supervisor:
Dra. Maiara Francine Bollauf

São José dos Campos - SP - Brazil

2023

Pereira, Júlia

Physical Layer Security in Wireless Communication / Júlia Wotzasek Pereira. – São José dos Campos - SP - Brazil, 2023.

71p.

Dissertation (Master) – Federal University of São Paulo, Science and Technology Institute. Postgraduate Program in Pure and Applied Mathematics.

1. Information Theory. 2. Communication Theory. 3. Wireless Communication. 4. Wiretap Channel.

Federal University of São Paulo

Science and Technology Institute

Postgraduate Program in Pure and Applied Mathematics

Head of Department: Prof. Dr. Marcelo Cristiano Gama

Program Coordinator: Prof. Dr. Tiago Rodrigues Macedo

Júlia Wotzasek Pereira

PHYSICAL LAYER SECURITY IN WIRELESS COMMUNICATION

Chairman of the Examination Committee:

Profa. Dra. Grasiele Cristiane Jorge

Examination Committee:

Prof. Dr. Agnaldo José Ferrari

Profa. Dra. Sara Díaz Cardell

Prof. Dr. Øyvind Ytrehus

I dedicate this to my parents, who never let my supply of coffee, love and chocolate run out.

ACKNOWLEDGEMENTS

First, I would like to express my deepest gratitude to my supervisor Prof. Dra. Grasiele Cristiane Jorge and to my co-supervisor Dra. Maiara Francine Bollauf, whose accept this frenetic journey caused by the change of my research objectives. Without your patience, wisdom, knowledge and insatiable curiosity, I probably would not be able to conclude this text in less than one year!

I am extremely grateful to Prof. Thiago Castilho de Mello, who guided me in my research in algebra since my first year in college. Although I changed the subject, algebra never left its main role in my heart and in this text.

I could not have undertaken this journey without the continuous support of my mother, Maria Emilia Wotzasek Pereira, who never let me give up, and also of my father, Renato Fernandes Pereira, who are always available to discuss my thesis (even if he has no idea what is this much mathematics behind).

Special thanks to Prof. João Guilherme Giudice, from College prep, who took 5 minutes to pay me a coffee to ask (after many trick questions at the classroom done by myself) if I'd ever thought of dabbling in math.

I also thanks Prof. Ana Luisa de Correa Gennare, who never let anyone push me down, and teach me advance math in the meanwhile.

I would like to extend my sincere thanks to Teixeira Júnior. Help people is a very hard task, since you should always respect what the helped person want, not what you think is the right to them. I trusted you in essential points of my professional and personal life, and you support me all the time. My path could have been very different without your sincerity.

- Olf Ivi.

- Olf Hspjl!

- Il jhylmbs hivba doha fvb zhf, P ilsplcl zvtlvul pz spzalupun av bz!

Caesar Ciphered Message [16]

RESUMO

Essa dissertação visa analisar o uso de reticulados para modelar métodos de segurança da informação na camada física em comunicações *wireless*. Em uma comunicação *wireless* é possível que, além do receptor, um ouvinte indesejado possa ter acesso à mensagem enviada. O objetivo da segurança na camada física é maximizar a confusão de terceiros e impedir que estes sejam capazes de interpretar a mensagem. Shannon estabeleceu, em 1948, que a comunicação eficiente pode ser feita com segurança e confiança em um canal ruidoso.Wyner definiu em seu trabalho publicado em 1975 o canal wiretap (canal com escuta), que é uma boa modelagem para comunicação wireless. Métodos utilizando reticulados para prover a segurança na camada física em um canal wiretap gaussiano são apresentados por Forutan e Fischer (2015), Oggier, Solé e Belfiore (2014), e Nazer and Gastpar (2011). Neste trabalho apresentamos as principais definições de reticulados necessárias. Apresentamos também o processo de comunicação e o canal Gaussiano, além do modelo OSI. Estabelecemos a estrutura da comunicação *wireless* em canal *wiretap* com o uso de reticulados. Ilustramos conceitos apresentados por meio de exemplos, além de discutir ataques passivos ao canal, por meio da combinação de métodos proposta por Forutan e Fischer.

Palavras-chave: Teoria da Informação, Teoria da Comunicação, Reticulados, Comunicação Wireless, Canal Wiretap, Segurança da Informação.

ABSTRACT

This dissertation aims to analyse the use of lattices to model wireless communication using physical layer security methods. In wireless communication, it is possible that, in addition to the receiver, an unwanted listener may have access to the sent message. The physical layer security objective is to maximize the confusion and avoid that others can interpret the message. Shannon establishes, in 1948, that the efficient communication can be done reliably and securely in a noisy channel. Wyner defined in his paper published in 1975 the wiretap channel, which is a model for secure communication. Methods using lattices to provide physical layer security over a Gaussian wiretap channel are presented by Forutan and Fischer (2015), Oggier, Solé and Belfiore (2014), and Nazer and Gastpar (2011). In this work we present the main definitions of lattices. We also present the communication process and the Gaussian channel, and the OSI Model. We establish the wireless communication structure in the wiretap channel using lattices. We illustrate the concepts through a set of examples, and also discuss how to manage passive attacks to the channel, using a combination of methods proposed by Forutan and Fischer.

Keywords: Information Theory, Communication Theory, Lattices, Wireless Communication, Wiretap Channel, Information Security.

CONTENTS

Chapter 1

INTRODUCTION

1.1 Context

The *sphere packing problem* asks how to pack equally sized spheres together in the densest way [7]. The already proved *Kepler's conjecture* states that, in the Euclidean three space, the densest packing is the face-centered cubic which coincides with the way oranges are usually pilled in a grocery store, as shown in Figure 1.1 [14].

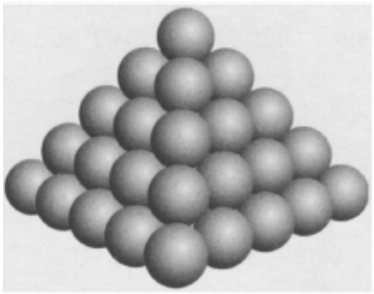


Figure 1.1: The face-centered cubic packing [14].

Although this problem is still open for some dimensions, it has applications in several areas, including information theory [26]. Its connection is established via the sampling theorem, which Shannon states that if a signal f with bandwidth of W hertz and almost all energy concentrated in a interval of T seconds, then f is accurately represented by a vector of $2WT$ samples [25, 26]. If we consider the signals as distinct neighboring billiard balls at the n-dimensional space, then the connection with the sphere packing problem clearly follows [26].

Before Shannon's seminal paper [25], the *communication theory* community used to believe that increasing the transmission rate of information over communication channel should increase the error probability [9]. Shannon started the *information theory* field of knowledge in the moment he proved that it is not true since the communication rate is below the chan-

nel capacity, and also that the capacity can be computed from the noise characteristics of the channel [9]. Then the two fundamental questions of the communication theory are answered by the information theory: What is the higher data compression possible? What is the higher data transmission rate of communication [9]?

Even when the focus is security, those questions are still valid, since we want to know which is the best transmission rate possible that keeps the communication secure. To ensure the confidentiality of communications, there are two approaches, the *information theoretical* and the *complexity-based* one [17].

The *complexity-based* security method assumes that the adversary which would try to eavesdrop a sent message in a communication system has computational limitations, so the idea is to make practically infeasible for the adversary to deduce the corresponding plaintext [17].

The *information-theoretical* approach assumes that the adversary has unlimited computation resources, so the encryption should be done in a way that the adversary can at least randomly guess the message [17].

Both methods deal with the necessity of keys to allow the communication parties to decode the message, which should be kept secret. In wireless communication, however, it is very difficult to have a third party to ensure this security key transmission [17].

A good example of the complexity-based approach is *cryptography*, which is the science of information and communication security [29]. It is used for authentication and encryption at several areas like bank cards and wireless communication, and it can be used to control access of cards and also for payment application [29]. The keys exchange is a problem in this type of method, as we already mentioned.

Furthermore, the post-quantum cryptography is already being studied to consider how to keep the communications secure even when the quantum computers are available [1]. In a context where the most used cryptographic algorithms like the Rivest-Shamir-Adleman (RSA) and Elliptic-curve cryptography (ECC) are broken, several alternatives are being studied [1]. One of the potential solutions for the post-quantum cryptography is a lattice-based one, which is also the mathematical structure underline this dissertation.

There are a lot of lattices applications [35], not only in cryptography, but also in information theory. Consider that the communication is established by layers in which each layer depends on the result of the previous one [32]. In this structure - called *OSI Model* - the presentation and physical layers play a fundamental role in the security, since the encryption occurs in the presentation layer [32] while the physical layer characterizes the physical specifications of the

medium, defining the standards of interface devices, cables and digital signals such as coaxial cables are wireless [24]. The physical layer is where the wiretap communication is established to ensure security without key exchange.

The wiretap model proposed by Wyner [33] models this noisy channel with the objective of encoding the data in such a way that the wiretapper (a.k.a. eavesdropper) level of confusion will be as high as possible. In other words, the wiretap models the situation where Alice (the source) wants to communicate with Bob (the receiver) but there is Eve (the eavesdropper) listening to their message exchange. A simple representation can be seen at Figure 1.2.

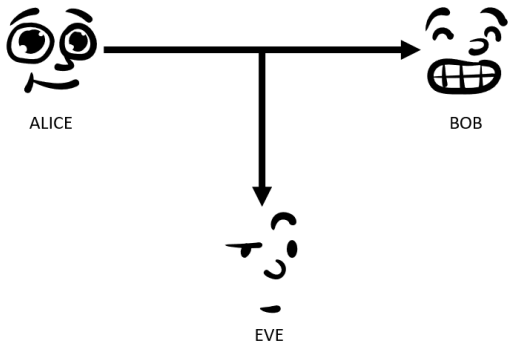


Figure 1.2: Wiretap communication between Alice and Bob and listened by Eve.

By taking advantage of the eavesdropper weaker channel quality, it is possible to inhibit the attacker to obtain the communicated information. Using mostly the stochastic nature of the channel noise and interference, the physical layer security requires no keys shared among network nodes, which is pretty compatible with the information-theoretic perspective [12] and also can be modelled using lattices.

In this dissertation we focus on the physical layer security, particularly on the lattice coding for the wiretap channel.

1.2 Proposed theme

The wireless communication is open to access, since the communication occurs by antennas, which makes the wiretap model vulnerable to this type of attack. We use lattice theory to comprehend and discuss security methods for wiretap channel. In this context, we study physical layer security strategies via lattice coset encoding and connections with compute-and-forward. We will show that it is possible to model and ensure secure communications using lattices.

1.2.1 General objective

The main objective of this dissertation is to investigate how to establish a secure communication in a wireless channel via the physical layer security. To achieve this goal, the mathematical structure underlying the security design is a lattice.

1.2.2 Specific objectives

To achieve the general objective, we tackle the following specific objectives:

1. Study lattice concepts and definitions, understand about main theorems and the important lattices.
2. Understand theta series and the Gaussian channel to be able to define quality metrics to the security schemes.
3. Analyse the cooperative relaying strategies and how to model the wireless communication using lattices.
4. Define the wiretap channel model and the lattice coset coding.
5. Study the compute-and-forward framework.
6. Review the method proposed in [12] combining the wiretap channel communication with the compute-and-forward one.
7. Compare passive and active attack.

1.3 Methodology

The dissertation was done with a top-down methodology. We started by choosing an article to review, an this article was [12]. This article discusses about lattices, Gaussian channels, lattice-based physical layer network coding, compute-and-forward, wiretap channel and the combination of both methods to avoid the cooperative jamming. So these topics become requirements to the understanding of this article and, with an extensive research about this requirement topics, this text was designed. We also point out the following relevant references:

- [23] describes the construction and analysis of a lattice-based communication in a wiretap channel, an important source to understand lattice encoding, secrecy gain, theta series properties and Eve's confusion through error probability.

- [22] is the seminal work on the compute-and-forward method, so this article describes the entire method.

We present the proofs of some theorems when they are relevant or when we believe that the proof is useful to further understanding of the topic. A ★ symbol in the beginning if a proof indicates it is slightly different from the literature.

1.4 Structure of the dissertation

This master's dissertation is structured in the following way:

In Chapter 2, we explain the basic concepts related to lattices and some important lattices. We discuss about the concepts of dual lattice, nested lattices and theta series. We complete with some packing properties and a brief description of Construction A.

In Chapter 3, we elucidate information theoretical concepts required to understand the physical layer security methods. We define the Gaussian channel, mutual information and information channel capacity. The wiretap channel is also introduced. We present the lattice's encoding and decoding, we analyse the eavesdropper confusion by the error probability analysis. We introduce some design criteria related to secrecy and reliability.

In Chapter 4, we explain some cooperative relaying strategies to then introduce the wireless communication with the usage of lattices. Each of the steps of the communication process explained in the Chapter are converted in equations and functions and some examples are presented to clarify the method. We then introduce the method the compute-and-forward method and its respective with lattices concepts of computation rate region is further discussed.

In Chapter 5, the compute-and-forward method and the lattice in coding methods are merged as a way to avoid wiretap passive attacks. We also discuss about the active and general passive attacks.

To conclude, in Chapter 6 we summarize the dissertation, analysing the main covered topics and also present our perspectives for future works.

Chapter 2

LATTICES

This chapter aims to introduce the main lattice definitions and some of the important lattices, which is the mathematical structure that underline this dissertation. This chapter is based on [7], [11], [27], [23], [8] and [28].

2.1 Lattice basic definitions

In this text we always will use the symbol $+$ to denote the usual sum in $\mathbb{R}^n$.

Definition 2.1 (Discrete set)**.** Let $D \subseteq \mathbb{R}^n$ be a set. D is called *discrete* if for each $\mathbf{x} \in D$ there exists an $r > 0$ for which $B(\mathbf{x}, r) \cap D = \{\mathbf{x}\}$.

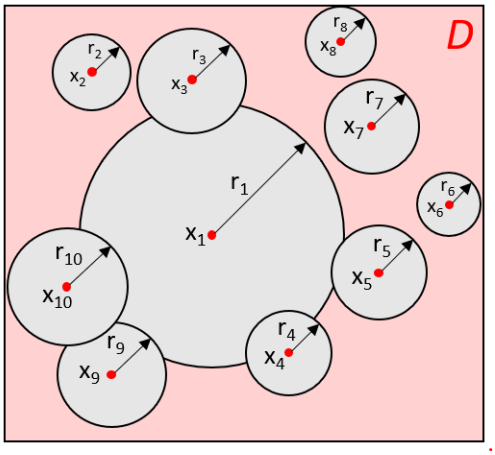


Figure 2.1: Discrete set example.

In the Figure 2.1 one can notice that for all points in D, it is possible to get an $r_i > 0$ and define a ball centered in $\mathbf{x}_i$ with ratio r_i that only contains one point from D, and this point is the center $\mathbf{x}_i$. For Figure 2.1, $1 \leq i \leq 10$.

Definition 2.2 (Lattice)**.** A *lattice* is a discrete additive subgroup of $\mathbb{R}^n$.

Let Λ be a lattice. Since Λ is an additive subgroup of $\mathbb{R}^n$ by definition, it means that for all $\mathbf{x},\mathbf{y} \in \Lambda$, $\mathbf{x}+\mathbf{y} \in \Lambda$ and $-\mathbf{x} \in \Lambda$.

Definition 2.3 (Euclidean norm)**.** Consider $\mathbf{x} = (x_1,\ldots,x_n)$ in $\mathbb{R}^n$. We define the *Euclidean norm* of $\mathbf{x}$ as:

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

The *minimum norm* of $\Lambda \subseteq \mathbb{R}^n$ as:

$$d_{min}(\Lambda) := \inf_{\mathbf{x}\in\Lambda\setminus\{0\}} \|\mathbf{x}\|_2 = \inf_{\mathbf{x},\mathbf{y}\in\Lambda,\mathbf{x}\neq\mathbf{y}} \|\mathbf{x}-\mathbf{y}\|_2.$$

Remark 2.4. At this dissertation, the only norm used will be the Euclidean. Then, for simplicity, we omit the 2 index: $\|\mathbf{x}\| = \|\mathbf{x}\|_2$.

Example 2.5. By Definition 2.3, given $\mathbf{x},\mathbf{y} \in \mathbb{Z}^n$, $\|\mathbf{x}-\mathbf{y}\|^2 = \sum_{i=1}^n (x_i-y_i)^2$. As all x_i, y_i values are integers, we have that, for $\mathbf{x} \neq \mathbf{y}$, $\|\mathbf{x}-\mathbf{y}\|^2 \geq 1$. As this distance is achieved by $\mathbf{x} = (1,0,\ldots,0)$ and $\mathbf{y} = (0,0,\ldots,0)$, for example. Thus, $d_{min}(\mathbb{Z}^n) = 1$. △

Example 2.6. $\mathbb{Z}^n$ is a lattice. Indeed $\mathbb{Z}^n$ is a nonempty subset of $\mathbb{R}^n$ since $\mathbf{0} \in \mathbb{Z}^n$. Let $\mathbf{x} = (x_1,\ldots,x_n), \mathbf{y} = (y_1,\ldots,y_n)$ be arbitrary vectors of $\mathbb{Z}^n$. So $\mathbf{x}-\mathbf{y} = (x_1,\ldots,x_n)-(y_1,\ldots,y_n) = (x_1-y_1,\ldots,x_n-y_n)$. For all components, as $x_i, y_i \in \mathbb{Z}$, we got that $x_i - y_i \in \mathbb{Z}$, thus $\mathbf{x}-\mathbf{y} \in \mathbb{Z}^n$.

To conclude, consider a ball centred at a point of $\mathbb{Z}^n$ with radius equal to $1/2$. Such ball only intercept the others at the border. Thus the set is discrete. Therefore $\mathbb{Z}^n$ is a lattice. △

Example 2.7. Consider the following set:

$$E_8 = \{(x_1,\ldots,x_8) : \text{ all } x_i \in \mathbb{Z} \text{ or all } x_i \in \mathbb{Z}+\frac{1}{2}, \sum x_i \equiv 0 \mod 2\}.$$

E_8 is a subset of $\mathbb{R}^n$ since all entries belongs to $\mathbb{Z}$ or to $\mathbb{Z}+\frac{1}{2}$. E_8 is not empty, since we have that $(2,0,0,0,0,0,0,0) \in E_8$, for example.

1. Consider $\mathbf{x} = (x_1,\ldots,x_8)$ and $\mathbf{y} = (y_1,\ldots,y_8)$ with $\mathbf{x},\mathbf{y} \in \mathbb{Z}^8$:

   - **It is closed by sum and inverse:** We have that $\mathbf{x}-\mathbf{y} = (x_1-y_1,\ldots,x_8-y_8) \in E_8$, since $x_i, y_i \in \mathbb{Z}$ implies that $x_i - y_i \in \mathbb{Z}$ and $\sum_{i=1}^8 (x_i-y_i) = \left(\sum_{i=1}^8 x_i\right) - \left(\sum_{i=1}^8 y_i\right) \equiv 0-0 \mod 2 \equiv 0 \mod 2$.

- **The minimum distance is $\sqrt{2}$:** $\|\mathbf{x}-\mathbf{y}\|^2 = (x_1-y_1)^2+\cdots+(x_8-y_8)^2$. Since all entries are integers and the sum of coordinates should be even, for $\mathbf{x}\neq\mathbf{y}$ we have:

$$\begin{aligned}\|\mathbf{x}-\mathbf{y}\|^2 &= (x_1-y_1)^2+\cdots+(x_8-y_8)^2\\ &\equiv (x_1^2+y_1^2)+\cdots+(x_8^2+y_8^2) \mod 2\\ &\equiv (x_1^2+\cdots+x_8^2)+(y_1^2+\cdots+y_8^2) \mod 2\\ &\equiv 0+0 \mod 2.\end{aligned}$$

  Then $\|\mathbf{x}\|^2 \geq 2$. This distance is achieved by $\mathbf{x}=(2,0,\ldots,0)$ and $\mathbf{y}=(0,0,\ldots,0)$, then $\|\mathbf{x}-\mathbf{y}\|_{min}=\sqrt{2}$.

2. Consider $\mathbf{x}=\left(x_1+\frac{1}{2},\ldots,x_8+\frac{1}{2}\right)$ and $\mathbf{y}=\left(y_1+\frac{1}{2},\ldots,y_8+\frac{1}{2}\right)$ with $\mathbf{x},\mathbf{y}\in\left(\mathbb{Z}+\frac{1}{2}\right)^8$:

   - **It is closed by sum and inverse:** We have that

$$\mathbf{x}-\mathbf{y}=\left(\left(x_1+\frac{1}{2}\right)-\left(y_1+\frac{1}{2}\right),\ldots,\left(x_8+\frac{1}{2}\right)-\left(y_8+\frac{1}{2}\right)\right)\in E_8,$$

     since $x_i+\frac{1}{2}, y_i+\frac{1}{2}\in\mathbb{Z}+\frac{1}{2}$ implies that $x_i-y_i\in\mathbb{Z}$ and $\sum_{i=1}^8\left(\left(x_i+\frac{1}{2}\right)-\left(y_i+\frac{1}{2}\right)\right)=\left(\sum_{i=1}^8 x_i\right)-\left(\sum_{i=1}^8 y_i\right)\equiv 0-0 \mod 2\equiv 0 \mod 2$.
   - **The minimum distance is $\sqrt{2}$:** $\|\mathbf{x}-\mathbf{y}\|^2=(x_1-y_1)^2+\cdots+(x_8-y_8)^2$, cancelling all fractions. Thus, the minimum distance is the same for the previous item. The distance $\sqrt{2}$ is achieved by $\mathbf{x}=\left(\frac{3}{2},\frac{1}{2},\ldots,\frac{1}{2}\right)$ and $\mathbf{y}=\left(\frac{1}{2},\frac{1}{2},\ldots,\frac{1}{2}\right)$.

3. Consider $\mathbf{x}=\left(x_1+\frac{1}{2}+,\ldots,x_8+\frac{1}{2}\right)$ and $\mathbf{y}=(y_1,\ldots,y_8)$ with $\mathbf{x}\in\left(\mathbb{Z}+\frac{1}{2}\right)^8$ and $\mathbf{y}\in\mathbb{Z}^8$:

   - **It is closed by sum and inverse:** We have that $\mathbf{x}-\mathbf{y}=\left(x_1+\frac{1}{2}-y_1,\ldots,x_8+\frac{1}{2}-y_8\right)\in E_8$, since $x_i,y_i\in\mathbb{Z}$ implies that $x_i+\frac{1}{2}-y_i\in\mathbb{Z}+\frac{1}{2}$ and $\sum_{i=1}^8\left(x_i+\frac{1}{2}-y_i\right)=\left(\sum_{i=1}^8 x_i+\frac{1}{2}\right)-\left(\sum_{i=1}^8 y_i\right)\equiv 0-0 \mod 2\equiv 0 \mod 2$.
   - **The minimum distance is $\sqrt{2}$:** $\|\mathbf{x}-\mathbf{y}\|^2=\left(x_1+\frac{1}{2}-y_1\right)^2+\cdots+\left(x_8+\frac{1}{2}-y_8\right)^2$. Notice that $\left(x_i+\frac{1}{2}-y_i\right)^2\geq\frac{1}{4}$ for all $i\in\{1,\ldots,8\}$. Thus, $\|\mathbf{x}-\mathbf{y}\|^2\geq 8\cdot\frac{1}{4}=2$. The distance $\frac{1}{\sqrt{2}}$ is achieved by $x=\left(\frac{1}{2},\frac{1}{2},\ldots,\frac{1}{2}\right)$ and $y=(0,0,\ldots,0)$.

Consider a ball centred at any point of E_8 with radius $r=d_{min}(E_8)/2=\frac{\sqrt{2}}{2}$. Such ball only intercept the others at the border. Thus the set is discrete. Therefore, E_8 is a lattice. △

Theorem 2.8. *A subset $\{0\}\neq\Lambda\subseteq\mathbb{R}^n$ is a lattice if, and only if, there are $\boldsymbol{b}_1,\ldots,\boldsymbol{b}_m\in\mathbb{R}^n$ linear independent vectors such that Λ consists of all integer linear combinations of those vectors, i.e.,*

$$\Lambda=\{\alpha_1\boldsymbol{b}_1+\cdots+\alpha_m\boldsymbol{b}_m : \alpha_1,\ldots,\alpha_m\in\mathbb{Z}\}. \tag{2.1}$$

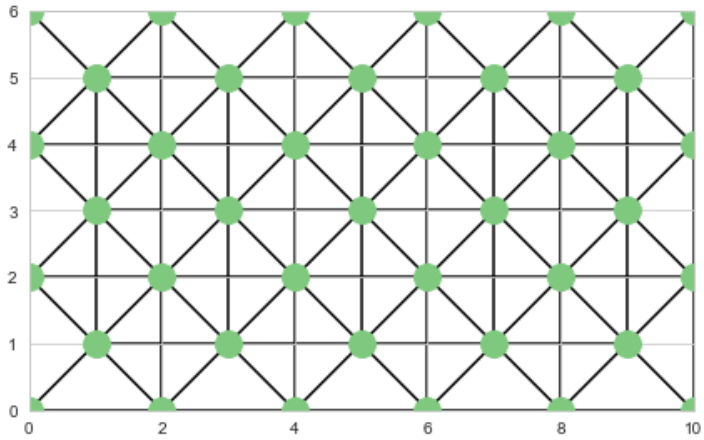
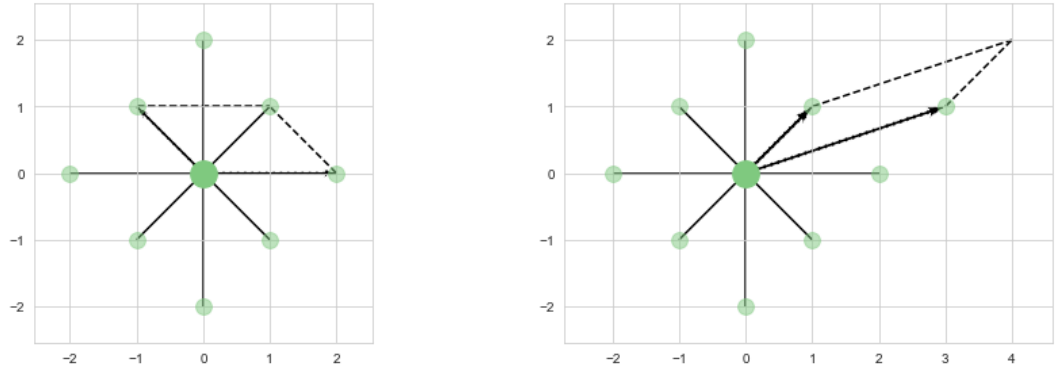


Figure 2.2: Lattice Λ.



(a) Basis $\{(2,0),(-1,1)\}$. **(b)** Basis $\{(3,1),(1,1)\}$.

Figure 2.3: Basis to lattice Λ.

Proof. The proof can be found at [27, Theorem 1.1.2, p.13]. □

Definition 2.9 (Basis)**.** A linear independent set of vectors $\beta = \{\mathbf{b}_1,\ldots,\mathbf{b}_m\}$, $\mathbf{b}_i \in \mathbb{R}^n$, is a *basis* for the lattice $\Lambda \subseteq \mathbb{R}^n$ when (2.1) holds.

By Theorem 2.8, there exists a basis for all lattices. A lattice basis is not unique [27].

Example 2.10. [27] Let $\Lambda \subseteq \mathbb{R}^2$ be the lattice in Figure 2.2.

Both bases ($\{(2,0),(-1,1)\}$ and $\{(3,1),(1,1)\}$) from Figure 2.3a and Figure 2.3b are bases to lattice Λ. △

Definition 2.11 (Gram Matrix)**.** Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice and $\beta = \{\mathbf{b}_1,\ldots,\mathbf{b}_m\}$ be a basis such that $\mathbf{b}_i = (b_{i1},\ldots,b_{in})$, for each $i = 1,\ldots,m$. The matrix

$$B = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1} & b_{m2} & \cdots & b_{mn} \end{pmatrix}$$

is a *generator matrix* to Λ. The matrix $G = BB^t$ is called *Gram matrix* associated to the basis $\{\mathbf{b}_1, \ldots, \mathbf{b}_m\}$.

Example 2.12. Let us use the lattice from Example 2.10 with basis $\{(2,0),(-1,1)\}$.

A generator matrix is:

$$B_1 = \begin{pmatrix} 2 & 0 \\ -1 & 1 \end{pmatrix}.$$

Then the associated Gram matrix is:

$$G_1 = B_1 B_1^t = \begin{pmatrix} 2 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 2 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 4 & -2 \\ -2 & 2 \end{pmatrix}.$$

For the basis $\{(3,1),(1,1)\}$ a generator matrix is:

$$B_2 = \begin{pmatrix} 3 & 1 \\ 1 & 1 \end{pmatrix}.$$

Then the associated Gram matrix is:

$$G_2 = B_2 B_2^t = \begin{pmatrix} 3 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 3 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 10 & 4 \\ 4 & 2 \end{pmatrix}.$$

Notice that $\det(G_1) = 4 \cdot 2 - (-2) \cdot (-2) = 4$ and $\det(G_2) = 10 \cdot 2 - 4 \cdot 4 = 4$, what means that $\det(G_1) = \det(G_2)$. This fact motivates the next theorem. △

Definition 2.13 (Unimodular matrix)**.** Let U be a square matrix with integer entries. We call U as *unimodular matrix* if $\det(U) = \pm 1$.

Theorem 2.14. *[27, Theorem 1.1.5, p.18] The determinant of any Gram matrix of a lattice is invariant under change of basis.*

Proof. Let B_1 and B_2 be generator matrices of Λ. By [27, Theorem 1.1.4, p.17], there is an unimodular matrix U such that $B_2 = UB_1$. Thus, $G_2 = B_2 B_2^t = (UB_1)(UB_1)^t = (UB_1)(B_1^t U^t) =$

$UB_1B_1^tU^t = UG_1U^t$.

Thus, $\det(G_2) = \det(UG_1U^t) = \det(U)\det(G_1)\det(U^t)$.

We know by Definition 2.13 that $\det(U) = \pm 1$. We also know that $\det(U^t) = \det(U)$. So $\det(U)\det(U^t) = (\pm 1)(\pm 1) = 1$. Therefore $\det(G_2) = \det(G_1)$ and the statement holds. □

Definition 2.15 (Determinant)**.** Let $\Lambda \subseteq \mathbb{R}^n$ a lattice and G a Gram matrix of Λ. The *determinant* of Λ is defined as $\det(\Lambda) = \sqrt{\det(G)}$.

Example 2.16. For the lattice Λ of Figure 2.2, we calculated in Example 2.12 that $\det(G_1) = 4$. So, the $\det(\Lambda) = 2$. △

Definition 2.17 (Rank)**.** Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice and $\beta = \{\mathbf{b}_1, \ldots, \mathbf{b}_m\}$ be a basis of Λ. We call the *rank* as the number m of vector at the β basis. If $m = n$, we say that the lattice Λ is *full rank*.

Notice that, if B is full rank, then $\det(G) = \det(B) \cdot \det(B)$ and thus $\det(\Lambda) = |\det(B)|$.

Example 2.18. The basis $\{(2,0),(-1,1)\}$ in Example 2.10 is full rank and $|\det(B_1)| = 2 = \det(\Lambda)$. △

Definition 2.19 (Fundamental Region)**.** Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice with rank m, where B is a generator matrix. A *fundamental region* $\mathscr{F}$ *of* Λ *is* a subset of $span(\beta)$ that covers $span(\beta)$ by translations $\mathbf{v} + \mathscr{F}$ with $\mathbf{v} \in \Lambda$, i.e.,

$$span(B) = \bigcup_{\mathbf{v} \in \Lambda} (\mathbf{v} + \mathscr{F}),$$

and the intersection of $\mathbf{v}_1 + \mathscr{F}$ and $\mathbf{v}_2 + \mathscr{F}$, $\mathbf{v}_1 \neq \mathbf{v}_2$, is at most at the borders.

Example 2.20. Consider the lattice from Figure 2.2.

- **Not a fundamental region**: The red rectangle in Figure 2.4 is not a fundamental region because there is superposition between tiles, represented by the blue rectangle area. It is important to highlight that the entire space could be covered with those rectangles.

  The blue circle in Figure 2.5 also is not a fundamental region since it does not cover the entire space, even if there is no superposition.

- **It is a fundamental region:** In Figure 2.6 we have two different fundamental regions.

  In Figure 2.6a the red squares represents $\mathscr{F}_1 = \{\alpha_1(-1,1) + \alpha_2(1,1); 0 \leq \alpha_1, \alpha_2 \leq 1\}$. Notice that there is no superposition except in the border and that the entire space is covered.

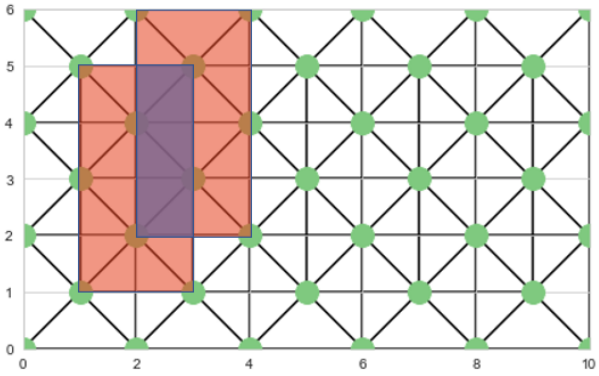


Figure 2.4: Not a fundamental region.

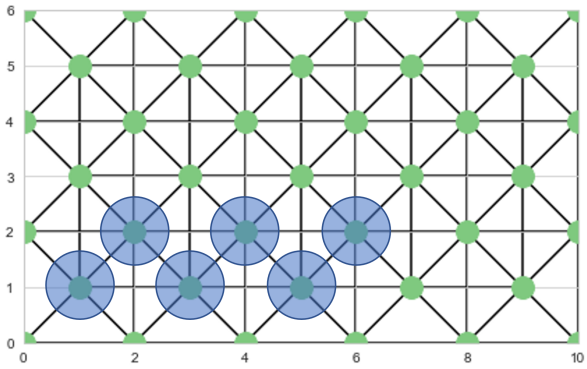
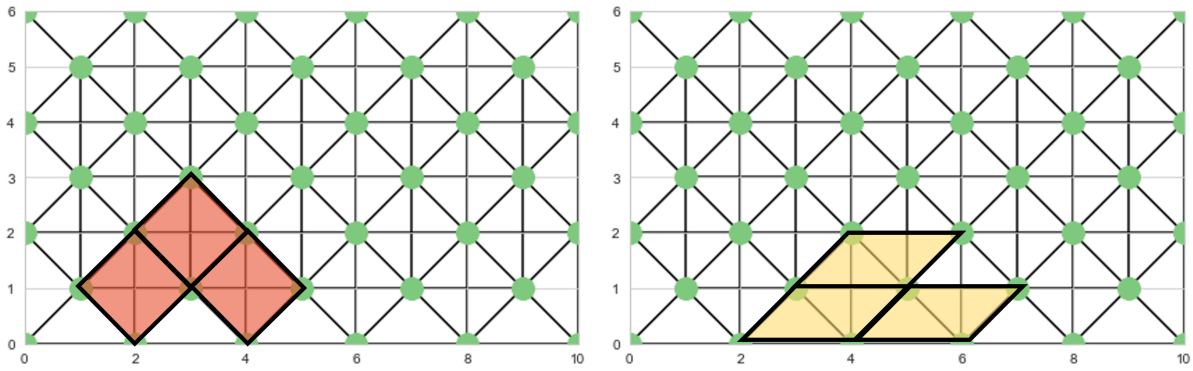


Figure 2.5: Not a fundamental region.



(a) $F_1 = \{\alpha_1(-1,1) + \alpha_2(1,1); 0 \leq \alpha_1, \alpha_2 \leq 1\}$. **(b)** $F_2 = \{\alpha_1(0,2) + \alpha_2(1,1); 0 \leq \alpha_1, \alpha_2 \leq 1\}$.

Figure 2.6: Fundamental regions of a Lattice Λ.

In Figure 2.6b the yellow squares represents $\mathscr{F}_2 = \{\alpha_1(0,2) + \alpha_2(1,1); 0 \leq \alpha_1, \alpha_2 \leq 1\}$. Notice that there is no superposition except in the border and that the entire space is covered. △

Theorem 2.21. *[27, Corollary 1.3.1, p.25] The volume of a fundamental region of a lattice* Λ *of rank m is equal to* $\det(\Lambda)$.

Definition 2.22 (Volume)**.** Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice with rank m. We call the *volume of lattice* Λ,

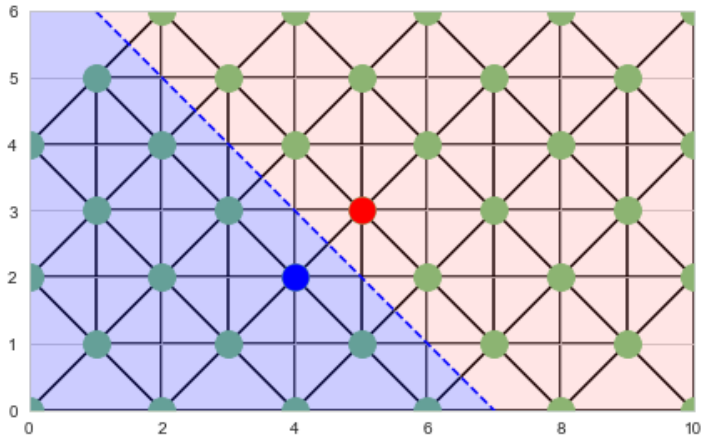
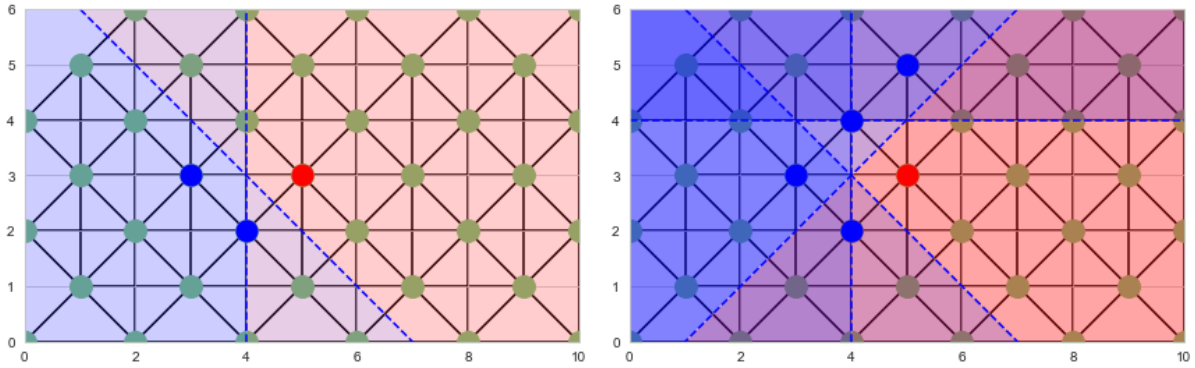


Figure 2.7: Lattice Λ partitioned in two regions: blue (related to point $(4,2)$) and red (related to point $(5,3)$).



(a) Add region partition related to point $(3,3)$. **(b)** Add region partition related to point $(4,4)$ and $(5,5)$.

Figure 2.8: Region partitions at lattice Λ.

$vol(\Lambda)$, as the volume of any fundamental region of Λ.

Example 2.23. In the Figure 2.6a we can notice that, as the square side is equal to $\sqrt{2}$, then the area of the red fundamental region $\mathscr{F}_1$ is equal to $(\sqrt{2})^2 = 2$.

Using the Theorem 2.21 we also find that $vol(\mathscr{F}_1) = \det(\Lambda) = \sqrt{\det G_1} = \sqrt{4} = 2$. △

Definition 2.24 (Voronoi region)**.** Given an element $\mathbf{v} \in \Lambda \subseteq \mathbb{R}^n$, the *Voronoi region* will be defined as:

$$\mathscr{V}(\mathbf{v}) = \{\mathbf{x} \in \mathbb{R}^n; \|\mathbf{x}-\mathbf{v}\| \leq \|\mathbf{x}-\mathbf{u}\|, \forall \mathbf{u} \neq \mathbf{v} \in \Lambda\}.$$

Example 2.25. For the lattice in Example 2.10, we can get its Voronoi region. By Definition 2.24, by fixing two points $\mathbf{x}, \mathbf{y} \in \Lambda$, for all $\mathbf{z} \in \mathbb{R}^2$, if $\|\mathbf{z}-\mathbf{x}\| \leq \|\mathbf{z}-\mathbf{y}\|$, then $\mathbf{z}$ belongs to the region of $\mathbf{x}$, and if $\|\mathbf{z}-\mathbf{x}\| \geq \|\mathbf{z}-\mathbf{y}\|$, then $\mathbf{z}$ be in the region of $\mathbf{y}$. What we can notice from that is that regions intersect at the border and that this is equivalent to draw the perpendicular bisector. We can see that in Figure 2.7:

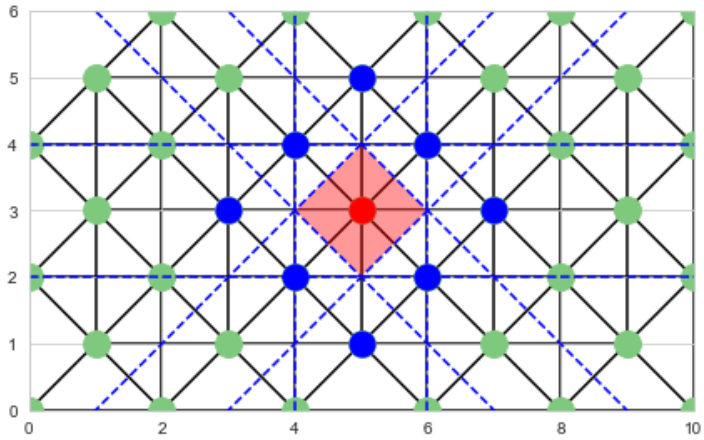


Figure 2.9: Voronoi region to lattice Λ, related to the point $(5,3)$.

If we iterate through the points which are closer to the red point and after all interactions, we got that the Voronoi region related to the red point $(5,3)$ is given by the intersection of red regions. We can see that in the Figure 2.9. △

Remark 2.26. Since lattices are regular and periodic arrangements of points, all Voronoi regions are congruent. It follows from definition that Voronoi region is a fundamental region.

2.2 Important lattices

According to their properties, there are some important lattices that worth to be covered. Lattices from this section are constructed according to [7].

2.2.1 $\mathbb{Z}^n$

Let $\mathbb{Z}$ denote the set of integer numbers. Then,

$$\mathbb{Z}^n = \{(x_1,\ldots,x_n) | x_i \in \mathbb{Z}, i = 1,\ldots,n\}$$

is a lattice. It is also called *n-dimensional cubic* or *integer lattice*. Its generator matrix is given by the identity matrix I_n. See Example 2.6.

Example 2.27. Let $n = 2$ and so a generator matrix be I_2. Then, the lattice $\mathbb{Z}^2$ is the one showed in Figure 2.10. △

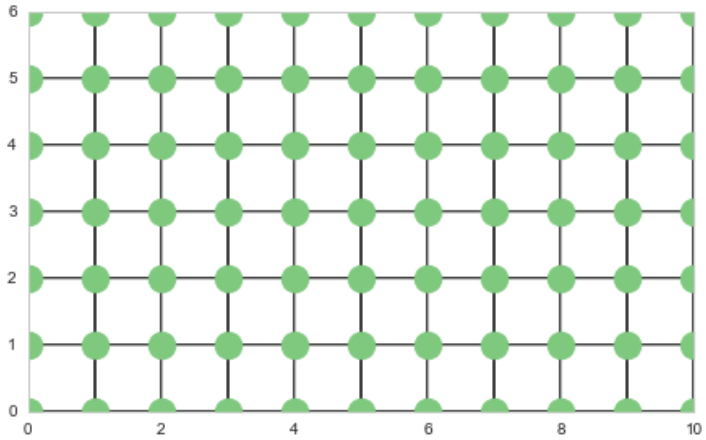


Figure 2.10: Lattice $\mathbb{Z}^2$.

2.2.2 A_n

For $n \geq 1$, then the A_n lattice is defined as the following:

$$A_n = \{(x_0, x_1, \ldots, x_n) \in \mathbb{Z}^{n+1} : x_0 + \cdots + x_n = 0\}.$$

It means that the A_n lattice is in an hyperplane of $\mathbb{Z}^{n+1}$. A generator matrix can be given by:

$$B = \begin{pmatrix} -1 & 1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & -1 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & -1 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \ldots & -1 & 1 \end{pmatrix}.$$

Example 2.28. Let $n = 2$ and so a generator matrix be

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

Then, the lattice A_2 is the one showed in Figure 2.11. △

2.2.3 D_n

Lattice D_n can be written, for $n \geq 3$, as:

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

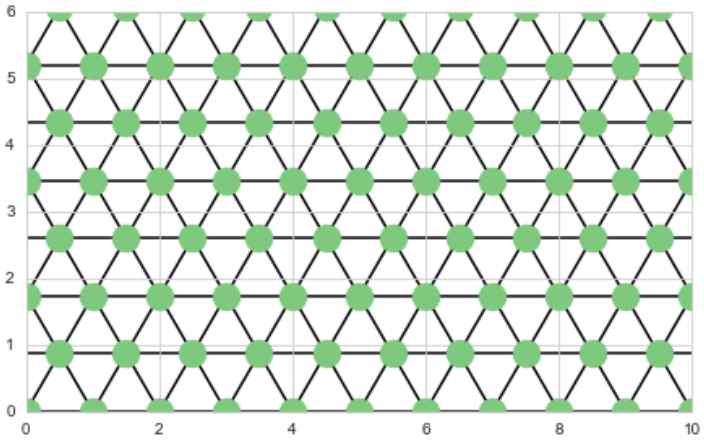


Figure 2.11: Lattice A_2.

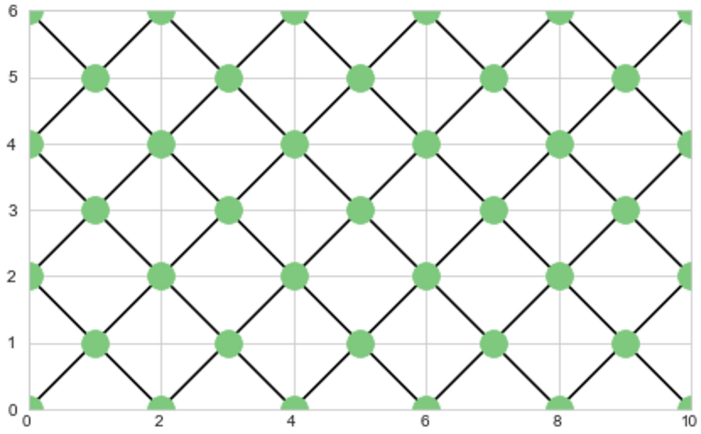


Figure 2.12: Lattice D_2.

It is also called as *checkerboard lattice*. A generator matrix is given by

$$B = \begin{pmatrix} -1 & -1 & 0 & 0 & \dots & 0 & 0 \\ 1 & -1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & -1 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & -1 & 1 \end{pmatrix}.$$

Example 2.29. Let $n = 2$ and so a generator matrix be

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

Then, the lattice D_2 is the one showed in Figure 2.12. △

2.2.4 E_8

Lattice E_8 consists of the points

$$E_8 = \{(x_1,\ldots,x_8) : x_i \in \mathbb{Z}\ \forall i \text{ or } x_i \in \mathbb{Z}+\frac{1}{2}\ \forall i, \sum x_i \equiv 0 \mod 2\}.$$

A generator matrix of E_8 is given by:

$$B = \begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \\ 1/2 & 1/2 & 1/2 & 1/2 & 1/2 & 1/2 & 1/2 & 1/2 \end{pmatrix}.$$

The E_8 represents the most efficient way of packing spheres in 8 dimensions [30]. See Example 2.7.

2.2.5 Leech Λ_{24}

A generator matrix of the Leech lattice Λ_{24} is given by:

$$B = \frac{1}{\sqrt{8}} \begin{pmatrix} 8 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 4 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 4 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 4 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 4 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 4 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 4 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 2 & 2 & 2 & 0 & 0 & 0 & 0 & 2 & 2 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 2 & 0 & 2 & 0 & 0 & 2 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 2 & 2 & 2 & 0 & 0 & 2 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 2 & 2 & 0 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 2 & 2 & 2 & 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 \\ -3 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

It is important to highlight that the Leech lattice is the densest packing of congruent spheres in twenty-four dimensions and that it is the unique optimal periodic packing [5].

2.3 Dual lattice

Definition 2.30 (Usual Inner product)**.** Let $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_n)$ be vectors in $\mathbb{R}^n$. We define the *usual inner product in* $\mathbb{R}^n$ as:

$$\mathbf{x} \cdot \mathbf{y} = \sum_{i=1}^{n} x_i y_i.$$

In particular,

$$\mathbf{x} \cdot \mathbf{x} = \|\mathbf{x}\|^2.$$

Definition 2.31 (Integral lattice)**.** A lattice Λ is called *integral if* $\boldsymbol{x} \cdot \boldsymbol{x}$ *is an integer for all* $\boldsymbol{x} \in \Lambda$. *If* $\boldsymbol{x} \cdot \boldsymbol{x}$ *is an even integer for all* $\boldsymbol{x} \in \Lambda$*, then* Λ *is called even, otherwise odd.*

Definition 2.32 (Dual lattice)**.** Let $\Lambda, \Lambda^* \subseteq \mathbb{R}^n$ be lattices. Λ and Λ^* are called *dual* if the inner products of their points are integers, i.e.,

$$\langle \boldsymbol{\lambda}, \boldsymbol{\lambda}^* \rangle \in \mathbb{Z}, \ \forall\, \boldsymbol{\lambda} \in \Lambda, \boldsymbol{\lambda}^* \in \Lambda^*.$$

Example 2.33. Let D_2 be the checkerboard lattice from Subsection 2.2.3 and Example 2.29. So a generator matrix B is given by:

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

The generated lattice can be seen at Figure 2.13.

By definition, the lattice D_2^* has generator matrix $B^* = (B^{-1})^T$. Thus B^* is given by:

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

The generated lattice can be seen at Figure 2.14, with the same dimensions of 2.13. △

Proposition 2.34. *Let* Λ *be a full rank lattice and* Λ^* *its dual. Then,*

$$vol(\Lambda) = \frac{1}{vol(\Lambda^*)}. \tag{2.2}$$

Proof. By definition, if B is the full rank generator matrix for Λ, then $B^* = (B^{-1})^T$ is a generator matrix for Λ^*. So we have that $vol(\Lambda) = |\det(B)|$ and $vol(\Lambda^*) = |\det((B^{-1})^T)| = |\det(B^{-1})|$.

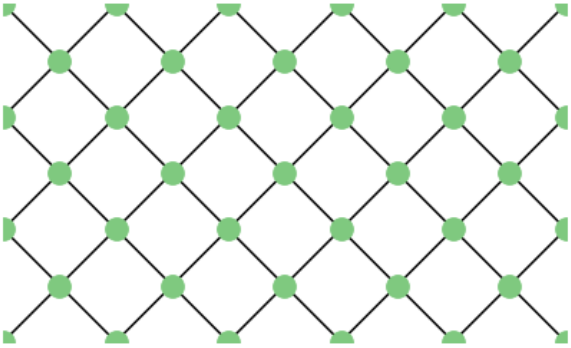


Figure 2.13: Checkerboard lattice D_2.

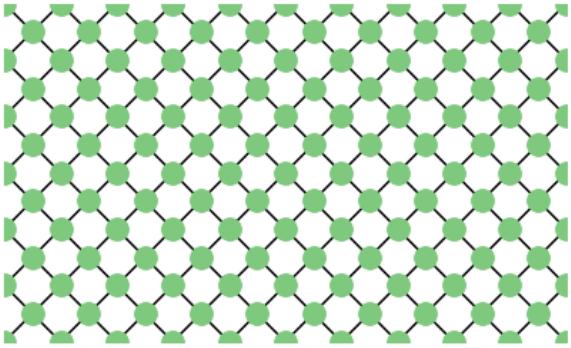


Figure 2.14: Dual of the checkerboard lattice D_2.

Then,

$$\frac{1}{\det(\Lambda^*)} = \frac{1}{|\det(B^{-1})|} = |\det(B)| = vol(\Lambda),$$

since $1 = \det(B)\det(B^{-1})$. □

A lattice Λ is *integral* if one of its Gram matrix G has only integer entries. Equivalently, a lattice Λ is integral if and only if $\Lambda \subseteq \Lambda^*$.

Definition 2.35 (Unimodular lattice)**.** An integral lattice is called *unimodular* if $\Lambda = \Lambda^*$.

Remark 2.36. Let Λ be a unimodular lattice, i.e., $\Lambda^* = \Lambda$, with generator matrix B. We get:

$$vol(\Lambda) = \frac{1}{vol(\Lambda^*)} \Leftrightarrow vol(\Lambda)^2 = 1 \Leftrightarrow \det(BB^t) = 1 \Leftrightarrow |\det(B)| = 1.$$

So the Definition 2.35 can include this fact about the generator B, even if it does not restrict the definition of unimodular lattices.

Example 2.37. The Gosset E_8 lattice is unimodular [7]. △

Definition 2.38 (Isodual lattice)**.** A lattice Λ is *isodual* if it can be obtained from its dual by (possibly) a rotation or reflection.

Remark 2.39. All unimodular lattices are isodual.

2.4 Nested lattices

Definition 2.40 (Sublattice)**.** [8] Let Λ and Λ' be lattices such that $\Lambda' \subseteq \Lambda$. Λ' is said to be a *sublattice* of Λ. A subset of a lattice is a sublattice if and only if it is an additive subgroup.

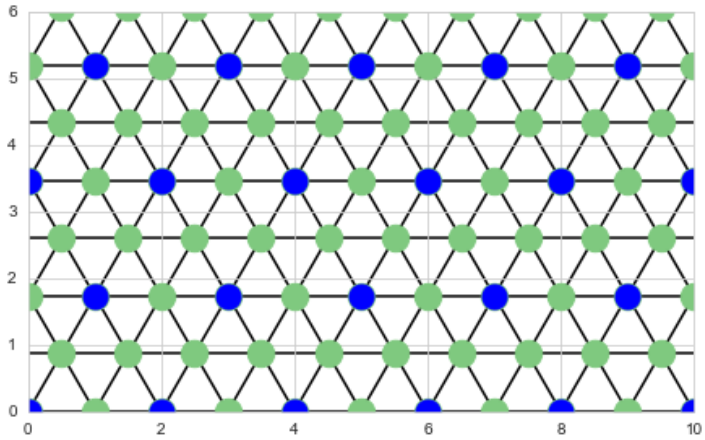


Figure 2.15: Lattice Λ with basis $\beta = \{(1,0),(1/2,\sqrt{3},2)\}$ (represented by blue and green points) and lattice Λ' with basis $\beta' = \{(2,0),(1,\sqrt{3})\}$ (represented only by the blue points).

Example 2.41. Let $\Lambda \subseteq \mathbb{R}^n$ be the lattice shown in Figure 2.15 with generator matrix B defined as:

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

Now let $\Lambda' \subseteq \mathbb{R}^n$ be the lattice generated by B':

$$B' = \begin{pmatrix} 2 & 0 \\ 1 & \sqrt{3} \end{pmatrix}.$$

Notice that $B' = 2B$, thus $\Lambda' \subseteq \Lambda$. △

Definition 2.42 (Nested lattices)**.** Let $\Lambda, \Lambda' \subseteq \mathbb{R}^n$. If Λ' is a sublattice of Λ, then we call (Λ, Λ') a *nested lattice pair*, where Λ is the *fine lattice* while Λ' is the *coarse lattice*.

Remark 2.43. [35] Let B and B' be generator matrices for Λ and Λ' respectively. It follows from Definition 2.42 that each basis vector $\mathbf{b}'_i$ of Λ' is a integer combination:

$$\mathbf{b}'_i = \sum_{k=1}^{n} m_{i,k}\mathbf{b}_k$$

of the basis vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$ of Λ. Thus the corresponding generator matrices B and B' satisfy:

$$B' = M \cdot B,$$

with the *nesting matrix* $M = (m_{i,k})$ an $n \times n$ integer matrix whose module of the determinant is greater or equal to 1, being equal if and only if the two lattices are identical (refer to Theorem 2.14).

Proposition 2.44 (Diagonal nesting)**.** *[35, Proposititon 8.1.1, p.181] Let $\Lambda' \subseteq \Lambda$ be a nested lattice pair. There exist generator matrices B and B' of Λ and Λ', respectively, such that:*

$$B' = diag(m_1, \ldots, m_n) \cdot B, \tag{2.3}$$

where the m_i are positive integers. That is, each basis vector of Λ' is an integer multiple of a single basis vector of Λ.

Proof. Suppose that B and $B' = MB$ are arbitrary generator matrices of the lattices Λ and Λ', respectively, where M is a general integer matrix. By the Smith normal form [6, Theorem 4, p.322], M can be decomposed as:

$$M = Q_1 diag(m_1, \ldots, m_n) Q_2, \tag{2.4}$$

where Q_1, Q_2 are $n \times n$ unimodular matrices, and m_i are positive integers.

Since $B' = MB$, with (2.4) we got:

$$\begin{aligned} B' = MB = (Q_1 diag(m_1, \ldots, m_n) Q_2) B \Leftrightarrow \\ Q_1^{-1} B' = (Q_1^{-1} Q_1) diag(m_1, \ldots, m_n)(Q_2 B) = diag(m_1, \ldots, m_n)(Q_2 B) \end{aligned} \tag{2.5}$$

Since Q_1 and Q_2 are unimodular, then both are invertible and also we can write $C = Q_2 B$ and $C' = Q_1^{-1} B'$ which are also generators matrices to Λ and Λ', respectively. Thus we can complete the proof by replacing $C = Q_2 B$ and $C' = Q_1^{-1} B'$ at the last row of (2.5):

$$C' = diag(m_1, \ldots, m_n) C.$$

which is the desired diagonal form of (2.3). □

Example 2.45. Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice with generator matrix B defined as:

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

Let $\Lambda' \subseteq \mathbb{R}^n$ be a lattice with generator matrix B' defined as:

$$B' = \begin{pmatrix} -13 & -\sqrt{3} \\ 18 & 2\sqrt{3} \end{pmatrix}.$$

We can see both Λ and Λ' in Figure 2.16. Observe that $B' = MB$, where:

$$M = \begin{pmatrix} -12 & -2 \\ 16 & 4 \end{pmatrix}.$$

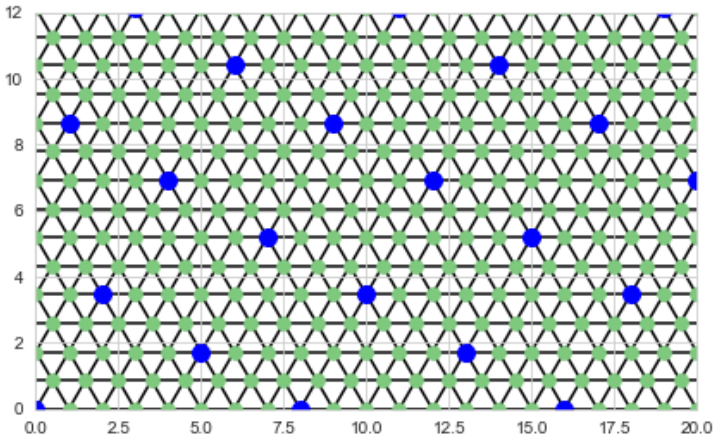


Figure 2.16: Lattice Λ with basis $B = \{(1,0),(1/2,\sqrt{3},2)\}$ and lattice Λ' with basis $B' = \{-13,-\sqrt{3}),(18,2\sqrt{3})\}$ represented by the blue points.

Using the Smith decomposition [6, Theorem 4, p.322], M can be decomposed as [8]:

$$M = \begin{pmatrix} -12 & -2 \\ 16 & 4 \end{pmatrix} = \begin{pmatrix} -1 & -1 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 8 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ -1 & 0 \end{pmatrix}.$$

Thus,

$$C = \begin{pmatrix} 2 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1/2 & \sqrt{3}/2 \end{pmatrix} = \begin{pmatrix} 5/2 & \sqrt{3}/2 \\ -1 & 0 \end{pmatrix},$$

and

$$C' = \begin{pmatrix} 1 & 1 \\ -2 & -1 \end{pmatrix} \begin{pmatrix} -13 & -\sqrt{3} \\ 18 & 2\sqrt{3} \end{pmatrix} = \begin{pmatrix} -5 & -\sqrt{3} \\ -8 & 0 \end{pmatrix}.$$

The generated lattices with the new generator matrices are the same from Figure 2.16. △

Definition 2.46 (Lattice's cosets and coset leader)**.** [8] Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice and $\Lambda' \subset \Lambda$ be a sublattice of Λ. Since $\Lambda' \subseteq \Lambda$ is a subgroup, then Λ can be partioned into a set of cosets of Λ' which form a finite *quotient group* Λ/Λ'.

Each of these cosets can be identified using a *coset leader* (or *coset representative*) in the fundamental region of lattice Λ.

Example 2.47. Consider the lattices from Example 2.41. We can see also that Λ' partitioned the lattice Λ in 4 cosets, as in Figure 2.17:

At this example, we can take $(0,0)$, $(1,0)$, $(\frac{1}{2},\frac{\sqrt{3}}{2})$ and $(\frac{3}{2},\frac{\sqrt{3}}{2})$ as the coset leaders, where the colors of coordinates corresponds to the colors in Figure 2.17

△

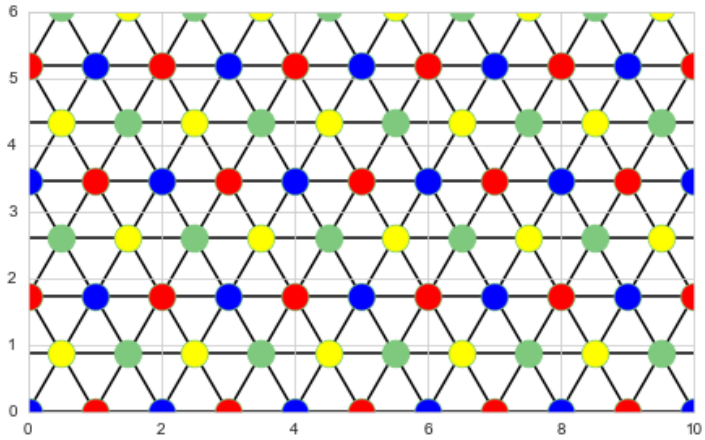


Figure 2.17: Λ' partition the lattice Λ in 4 cosets.

Proposition 2.48. *[8, p.18] Let B and $B' = MB$ be the generator matrices for Λ and Λ' respectively, where both B and B' full rank lattices. The number of elements of Λ/Λ' is given by:*

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

In this case, we can choose a set of elements $S = \{\lambda_1, \ldots, \lambda_{|\det(M)|}\} \subset \Lambda$ such that

$$\Lambda = \bigcup_{\lambda_i \in S} \Lambda' + \lambda_i.$$

Moreover, S can be obtained from the intersection of Λ with any fundamental region of Λ'.

2.5 Theta series

Definition 2.49 (Theta series of a lattice)**.** Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice. The *theta series of* Λ is defined as:

$$\Theta_\Lambda(q) = \sum_{\mathbf{x}\in\Lambda} q^{\mathbf{x}\cdot\mathbf{x}} = \sum_{\mathbf{x}\in\Lambda} q^{\|\mathbf{x}\|^2}$$

where $\mathbf{x}\cdot\mathbf{x}$ is the inner product of $\mathbf{x}$ and $\mathbf{x}$, $q = e^{i\pi z}$, with $z \in \mathbb{C}$ and $Im(z) > 0$.

It can also be rewritten as:

$$\Theta_\Lambda(z) = \sum_{m:N(m)>0} N(m)q^m,$$

where $q = e^{i\pi z}$, $A_m = \{\mathbf{x} \in \Lambda : \mathbf{x}\cdot\mathbf{x} = m\}$ and $N(m) = |A_m|$.

Remark 2.50. $N(m)$ counts the number of vectors that has norm equal to $\sqrt{m}$.

Remark 2.51. The powers of q are the sum all squared norms achievable by lattice points.

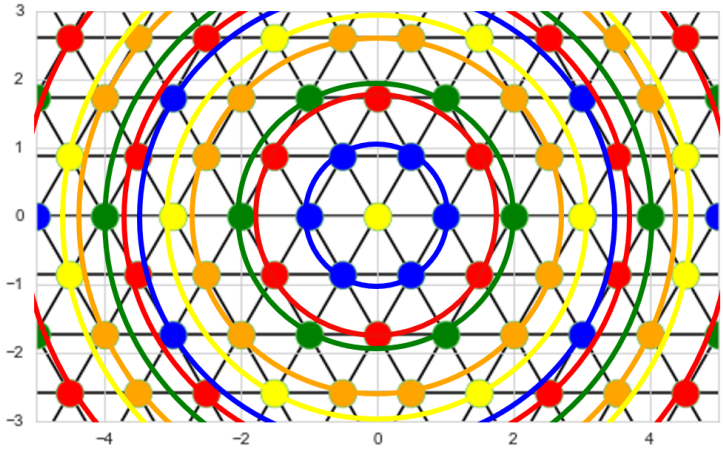


Figure 2.18: Theta Series of Lattice Λ.

Example 2.52. [28] Considering the lattice Λ from Example 2.41, with basis

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

the theta series is:

$$\Theta_\Lambda(z) = \sum_{\mathbf{x}\in\Lambda} q^{\mathbf{x}\cdot\mathbf{x}} = 1+6q+6q^4+12q^7+6q^9+6q^{12}+\ldots,$$

which can be visualized by the the Figure 2.18. △

Definition 2.53 (Jacobi Theta Series)**.** The Jacobi Theta Series are given by:

$$\vartheta_1'(z) = \Theta_1'(0|z) = \sum_{m=-\infty}^{\infty} (-1)^m (2m+1) q^{(m+1/2)^2}$$

$$\vartheta_2(z) = \sum_{m=-\infty}^{\infty} q^{(m+1/2)^2}$$

$$\vartheta_3(z) = \Theta_3(0|z) = \sum_{m=-\infty}^{\infty} q^{m^2}$$

$$\vartheta_4(z) = \Theta_3\left(\frac{\pi}{2}|z\right) = \Theta_3(z+1) = \sum_{m=-\infty}^{\infty} (-q)^{m^2}$$

Proposition 2.54. *[7, Equation 47, p.108] For the $\mathbb{Z}^n$ lattice,*

$$\Theta_{\mathbb{Z}^n}(z) = \vartheta_3(z)^n.$$

Theorem 2.55. *Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice. Then $\Theta_\Lambda(z) = \sum_{x\in\Lambda} e^{\pi i z x\cdot x}$ converges uniform and absolutely for all $z \in \mathbb{C}$, with $Im(z) > 0$.*

Proof. ★ Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice and $\beta = \{\mathbf{b}_1,\ldots,\mathbf{b}_n\}$ be its basis. By Theorem 2.8, for all

$\mathbf{x} \in \Lambda$, $\mathbf{x}$ can be written as:

$$\mathbf{x} = y_1\mathbf{b}_1 + \cdots + y_n\mathbf{b}_n, \tag{2.6}$$

where $y_i \in \mathbb{Z}$ and $i = \{1,\ldots,n\}$. Thus, for all $\mathbf{x} \in \Lambda$, there exists $\mathbf{y} = (y_1,\ldots,y_n) \in \mathbb{Z}^n$ such that $\mathbf{x} = \mathbf{y}B$.

By definition, a series $\sum_{n=0}^{\infty} a_n(x)$ is called *uniformly absolutely-convergent* if $\sum_{n=0}^{\infty} |a_n(x)|$ is uniformly convergent.

So let us analyse the convergence of $\sum_{\mathbf{x}\in\Lambda} |e^{\pi i z\mathbf{x}\cdot\mathbf{x}}|$. By (2.6), we get:

$$\sum_{\mathbf{x}\in\Lambda} |e^{\pi i z\mathbf{x}\cdot\mathbf{x}}| = \sum_{\mathbf{y}\in\mathbb{Z}^n} |e^{\pi i z\mathbf{y}B\cdot\mathbf{y}B}|. \tag{2.7}$$

Notice that $|e^{\pi i z\mathbf{y}B\cdot\mathbf{y}B}| = |e^{\pi i(Re(z)+iIm(z))\mathbf{y}B\cdot\mathbf{y}B}| = |e^{\pi i Re(z)\mathbf{y}B\cdot\mathbf{y}B}||e^{-\pi Im(z)\mathbf{y}B\cdot\mathbf{y}B}| = e^{-\pi Im(z)\mathbf{y}B\cdot\mathbf{y}B}$, since

$$\begin{aligned} |e^{\pi i Re(z)\mathbf{y}B\cdot\mathbf{y}B}| &= |\cos(\pi Re(z)\mathbf{y}B\cdot\mathbf{y}B) + i\sin(\pi Re(z)\mathbf{y}B\cdot\mathbf{y}B)| \\ &= \cos^2(\pi Re(z)\mathbf{y}B\cdot\mathbf{y}B) + \sin^2(\pi Re(z)\mathbf{y}B\cdot\mathbf{y}B) = 1 \end{aligned}$$

and $e^{-\pi Im(z)\mathbf{y}B\cdot\mathbf{y}B}$ is a real and positive number, so then we can disregard its absolute value.

In (2.7), we get:

$$\sum_{\mathbf{x}\in\Lambda} |e^{\pi i z\mathbf{x}\cdot\mathbf{x}}| = \sum_{\mathbf{y}\in\mathbb{Z}^n} |e^{\pi i z\mathbf{y}B\cdot\mathbf{y}B}| = \sum_{\mathbf{y}\in\mathbb{Z}^n} e^{-\pi Im(z)\mathbf{y}B\cdot\mathbf{y}B}.$$

By hypodissertation, $Im(z) > 0$. Thus, exists $\delta > 0$ such that $Im(z) \geq \delta > 0$. Thus,

$$\sum_{\mathbf{x}\in\Lambda} |e^{\pi i z\mathbf{x}\cdot\mathbf{x}}| \leq \sum_{\mathbf{y}\in\mathbb{Z}^n} e^{-\pi\delta\mathbf{y}B\cdot\mathbf{y}B}. \tag{2.8}$$

We have that $\mathbf{y}B\cdot\mathbf{y}B = \|\mathbf{y}B\|^2$. Consider the inducted matrix norm as $\|B\| = \max_{\|\mathbf{y}\|=1} \|\mathbf{y}B\|$. By definition, $\|B\| > 0$ and

$$\|\mathbf{y}B\| \leq \|\mathbf{y}\|\|B\|.$$

Considering $x = yB$, we get:

$$\begin{aligned} \|\mathbf{x}B^{-1}\| &\leq \|\mathbf{x}\|\|B^{-1}\| \\ \Rightarrow \|\mathbf{y}BB^{-1}\| &\leq \|\mathbf{y}B\|\|B^{-1}\| \\ \Rightarrow \|\mathbf{y}B\| &\geq \frac{1}{\|B^{-1}\|}\|\mathbf{y}\| = \varepsilon\|\mathbf{y}\|. \end{aligned}$$

Thus, in (2.8), we can say that there exists an $\varepsilon > 0$ such that

$$\sum_{\mathbf{y}\in\mathbb{Z}^n} e^{-\pi\delta\mathbf{y}B\cdot\mathbf{y}B} \leq \sum_{\mathbf{y}\in\mathbb{Z}^n} e^{-\pi\delta\varepsilon\mathbf{y}\cdot\mathbf{y}}. \tag{2.9}$$

Since $\mathbf{y}\cdot\mathbf{y} = \|\mathbf{y}\|^2$, let us call $\|\mathbf{y}\| = r$. In (2.9), by using Proposition 2.54:

$$\sum_{\mathbf{y}\in\mathbb{Z}^n} e^{-\pi\delta\varepsilon\mathbf{y}\cdot\mathbf{y}} = \left(\sum_{r\in\mathbb{Z}} e^{-\pi\delta\varepsilon r^2}\right)^n.$$

By the ratio test,

$$\lim_{r\to\infty} \frac{e^{-\pi\delta\varepsilon(r+1)^2}}{e^{-\pi\delta\varepsilon r^2}} = \lim_{r\to\infty} \frac{e^{-\pi\delta\varepsilon(r^2+2r+1)}}{e^{-\pi\delta\varepsilon r^2}}$$
$$= \lim_{r\to\infty} \frac{(e^{-\pi\delta\varepsilon r^2})(e^{-\pi\delta\varepsilon 2r})(e^{-\pi\delta\varepsilon})}{e^{-\pi\delta\varepsilon r^2}} = \lim_{r\to\infty} (e^{-\pi\delta\varepsilon 2r})(e^{-\pi\delta\varepsilon}) = 0 < 1.$$

Thus, $\left(\sum_{r=-\infty}^{\infty} e^{-\pi\delta\varepsilon r^2}\right)^n \leq \infty$ converges and since $\sum_{\mathbf{x}\in\Lambda} |e^{\pi i z\mathbf{x}\cdot\mathbf{x}}| \leq \left(\sum_{r=-\infty}^{\infty} e^{-\pi\delta\varepsilon r^2}\right)^n$, then it also converges by the comparison criteria. □

At Table 2.1 we can find the theta series for some of the important lattices, described as combination of Jacobi theta series.

Lattice Λ	**Theta Series Θ_Λ**
Cubic lattice $\mathbb{Z}^n$	ϑ_3^n
Checkerboard lattice D_n	$\frac{1}{2}(\vartheta_3^n + \vartheta_4^n)$
Gosset E_8	$\frac{1}{2}(\vartheta_2^8 + \vartheta_3^8 + \vartheta_4^8)$
Leech Λ_{24}	$\frac{1}{8}(\vartheta_2^8 + \vartheta_3^8 + \vartheta_4^8)^3 - \frac{45}{16}(\vartheta_2\vartheta_3\vartheta_4)^8$

Table 2.1: Theta series for some of the important lattices from Section 2.2 [23].

Proposition 2.56. *[23, Equation 12, p.5695] Let ϑ_2, ϑ_3 and ϑ_4 be the Jacobi theta series. The following equations hold:*

$$\vartheta_2(e^{-\pi}) = \vartheta_4(e^{-\pi})$$
$$\vartheta_3(e^{-pi}) = \sqrt[4]{2}\vartheta_4(e^{-\pi}).$$

2.6 Packing properties

Definition 2.57 (Packing and packing radius)**.** Let $\Lambda \subset \mathbb{R}^n$ be a lattice and let $r \in \mathbb{R}$, $r > 0$, be a radius. Let $\mathscr{B}_r = \{\mathbf{x} \in \mathbb{R}^n; \|\mathbf{x}\| \leq r\}$. The set $\Lambda + \mathscr{B}_r$ is a packing if for all distinct points

$\lambda, \lambda' \in \Lambda$, the sets $\lambda + \mathscr{B}_r$ and $\lambda' + \mathscr{B}_r$ either do not intersect or only intersect at the border.

The *packing radius* $r_{\text{pack}}(\Lambda)$ of the lattice is defined by the largest balls the lattice can pack:

$$r_{\text{pack}}(\Lambda) = \sup\{r : \Lambda + \mathscr{B}_r \text{ is a packing}\}.$$

Definition 2.58 (Effective radius)**.** [35] The *effective radius of a lattice* Λ is defined as the radius of a sphere having the same volume at the lattice cells:

$$r_{\text{eff}}(\Lambda) = \left[\frac{vol(\Lambda)}{V_n}\right]^{1/n},$$

where $V_n = \frac{\pi^{n/2}}{(n/2)!}$.

Definition 2.59 (Packing efficiency)**.** [35] The *packing efficiency* of a lattice Λ is defined as:

$$\rho_{\text{pack}}(\Lambda) = \frac{r_{\text{pack}}(\Lambda)}{r_{\text{eff}}(\Lambda)}.$$

Remark 2.60. [35] Since the packing efficiency is normalized by the effective radius, it guarantees that the packing efficiency is *invariant to scaling*, i.e., $\rho_{pack}(\alpha\Lambda) = \rho_{pack}(\Lambda)$. Thus, it is possible to use the ρ_{pack} is to express the proportion of space taken up by the spheres. This is known as *packing density*:

$$\Delta(\Lambda) = \frac{\text{volume of packed spheres}}{\text{volume of space}} = \frac{vol(\mathscr{B}_{r_{\text{pack}}(\Lambda)})}{vol(\Lambda)} = \rho^n_{\text{pack}}(\Lambda).$$

2.7 Construction A

The Construction A is defined to be applied in section 3.14.

Definition 2.61 (Linear code)**.** [15] Let $\mathbb{F}_q^n$ be a finite field of q elements. A *q-ary linear code* $\mathscr{C}$, for q prime, is a vector subspace of $\mathbb{F}_q^n$.

Linear codes in $\mathbb{F}_q^n$ can be extended for lattices in $\mathbb{Z}^n$ via *Construction A*, defined by Proposition 2.62.

Proposition 2.62. *[15] Consider the surjective function:*

$$\Phi : \mathbb{Z}^n \to \mathbb{F}_q^n$$
$$(x_1, \ldots, x_n) \mapsto (\bar{x_1}, \ldots, \bar{x_n}),$$

where $\bar{x_i}$ is obtained by the reduction module q of x_i for all $i = \{1, \ldots, n\}$. The code $\mathscr{C} \subseteq \mathbb{F}_q^n$ is a linear code if, and only if, $\Phi^{-1}(\mathscr{C}) \subseteq \mathbb{Z}^n$ is a lattice in $\mathbb{R}^n$. It is also true that $q\mathbb{Z}^n \subseteq \Phi^{-1}(\mathscr{C})$.

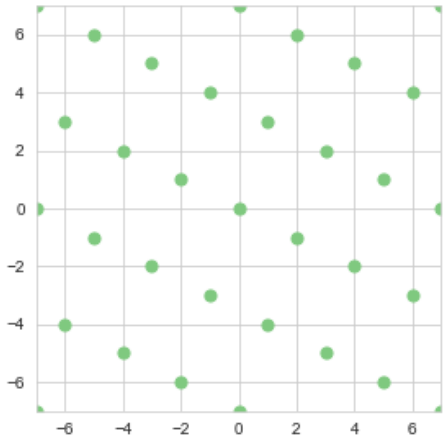


Figure 2.19: Lattice generated by Construction A for code $\mathscr{C} = \langle(\bar{1},\bar{3})\rangle$.

Example 2.63. [15] The Figure 2.19 shows the lattice generated by code $\mathscr{C}$ defined as:

$$\mathscr{C} = \langle(\bar{1},\bar{3})\rangle = \{(\bar{0},\bar{0}),(\bar{1},\bar{3}),(\bar{2},\bar{6}),(\bar{3},\bar{2}),(\bar{4},\bar{5}),(\bar{5},\bar{1}),(\bar{6},\bar{4})\} \subset \mathbb{F}_7^2.$$

△

Chapter 3

WIRETAP CHANNEL COMMUNICATION

Information Theory is the quantitative study of signal transmission [20]. The main problem of communication is to reproduce at one point the exact or approximate the content of a message sent from another point. It is important to consider that this message is one in a set of possible messages. [25].

Is this chapter we introduce the main concepts of Information Theory relevant to this work, explaining the general communication system and the Gaussian channel. Using the lattice concepts we have presented in the previous chapter, it is possible to discuss about the lattice encoding method and also about the metrics which measure the security.

3.1 Communication process

Claude Elwood Shannon wrote the seminal paper *A Mathematical Theory of Communication* [25], which is considered as the starting point of the Information Theory [21]. In this paper he establishes that information could be quantified and delivered reliably even if the channel has its imperfections [21].

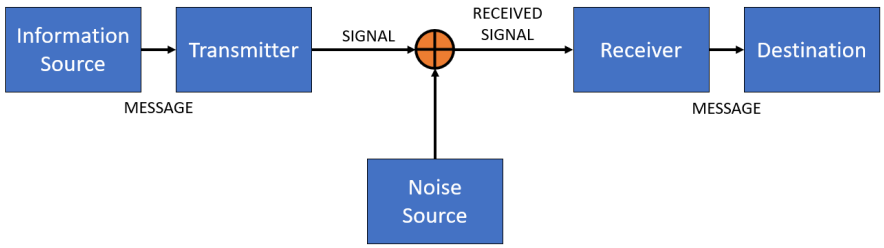


Figure 3.1: Schematic Diagram of a general communication system (based on [25]).

Following the steps proposed by Shannon in his paper, the communication process consists

basically on the steps showed in Figure 3.1.

Information source: It is the one which produces the message or a sequence of messages to be communicated to the receiving terminal.

Transmitter: It is responsible to convert the message in signals which can be transmitted over the channel.

Channel: It is the medium in which the signal is communicated. It is designed with a *noise source* which models the real noise of the channel.

Receiver: It does exactly the same task of the transmitter, but in the opposite way, reconstructing the message from the signal.

Destination: It is the target of the message.

3.2 Gaussian channel

Definition 3.1 (Discrete and memoryless channel)**.** [9] A *discrete channel* is a system consisting of an input alphabet $\mathscr{X}$ and an output alphabet $\mathscr{Y}$ and a probability transition matrix $p(y|x)$ that is the probability to get an y output given an x symbol in the input. It is also call *memoryless* if this probability does not depend on the time.

Example 3.2. [9] Suppose a binary channel without noise, in which the output reproduces the input. In that case, $\mathscr{X} = \{0,1\}$ and $\mathscr{Y} = \{0,1\}$, and $p(x) = \left(\frac{1}{2}, \frac{1}{2}\right)$. △

Definition 3.3 (Mutual information)**.** [9] Consider two random variables X and Y with a joint probability mass function $p(x,y)$ and marginal probability mass functions $p(x)$ and $p(y)$. The *mutual information* $I(X;Y)$ is given by:

$$I(X;Y) := \sum_{x\in\mathscr{X}} \sum_{y\in\mathscr{Y}} p(x,y) \log_2 \frac{p(x,y)}{p(x)p(y)}.$$

Definition 3.4 (Information channel capacity)**.** [9] Given a discrete memoryless channel, the *information channel capacity* is given by

$$C = \max_{p(x)} I(X;Y),$$

with the max taken over all possible input distributions $p(x)$.

Example 3.5. In the Example 3.2, the capacity $C = \max I(X;Y) = 1$, which is achieved by using $p(x) = \left(\frac{1}{2}, \frac{1}{2}\right)$. △

Remark 3.6. Note that the Definition 3.4 states that the capacity is achieved by the maximization over $p(x)$, which is something that the code designer can control.

Definition 3.7 (Gaussian channel)**.** [9] Let a time-discrete channel **C**. As an time-discrete channel, it has an output y_i at time i, where y_i is the sum of the input x_i with a noise z_i, where z_i is a Gaussian distribution with variance σ^2 and mean 0. Thus,

$$y_i = x_i + z_i,\ z_i \sim \mathcal{N}(0, \sigma^2).$$

It is assumed that the noise z_i and the signal x_i are independent.

The graphic representation of the Gaussian channel can be seen in Figure 3.2.

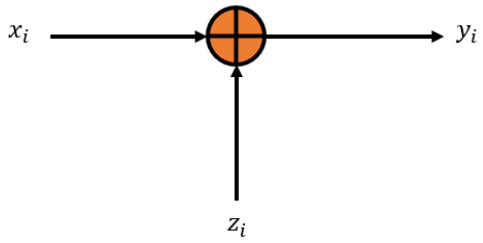


Figure 3.2: Gaussian channel [9].

Remark 3.8. When the noise that the channel model assumes is Gaussian distributed, it is called an *Additive White Gaussian Noise (AWGN)*. So a channel defined accordingly to Definition 3.7 is also called *AWGN channel* [35].

Remark 3.9. [9] The Gaussian channel is a good model for common communication channels, such as satellite links and wired and wireless telephone channels.

Notice that, with variance zero, the receiver receives the transmitted symbol with no error. It is usual to assume some energy or power limitations [9].

Definition 3.10 (Power constraint for Gaussian channel)**.** Let **G** be a Gaussian channel and P a power constraint value. Assume that all input $\mathbf{X} \subseteq \mathbb{F}^n$, where $\mathbb{F}$ is a field. So for any vector $\mathbf{X} = (x_1, \ldots, x_n)$ - which we call *codeword* - transmitted over the channel, it is required that:

$$\frac{1}{n}\sum_{i=1}^{n} x_i^2 \leq P.$$

Remark 3.11. Without the power constraint for Gaussian channels, it would be possible to choose the signal power as large as we want. In a way, this is equivalent to "choosing" the noise variance as small as we want, since both scenarios amount to making the SNR (*Signal-to-noise*

ratio) as large as we want. This in turn would make the channel capacity as large as we want. This approach is not realistic, since real channels have power limitations [9].

3.3 Wiretap channel

A *wiretap* is when someone listens to or monitor a telephone, telegraph, cellular, fax or internet communications with or without the consent of the communication parties. It can be done with programs, and tools, such as wiretap Trojans [31].

Definition 3.12 (Wiretap channel)**.** First introduced by Wyner in [33] as *Wire-tap channel*, a *Wiretap channel* is a discrete and memoryless channel (Definition 3.1) which is subject to a wiretap at the receiver.

The following is presumed in the original context:

- The eavesdropper views the channel output via a second discrete and memoryless channel.
- It is permitted to the transmitter to encode and to the receiver to decode.
- The eavesdropper knows the codebooks used in the operations.

Figure 3.3 represents the fact that the eavesdropper listen to the y_i words in that representation in general. It is usual to consider Gaussian channel in that context when considering lattice encoding, which will be our approach from now on.

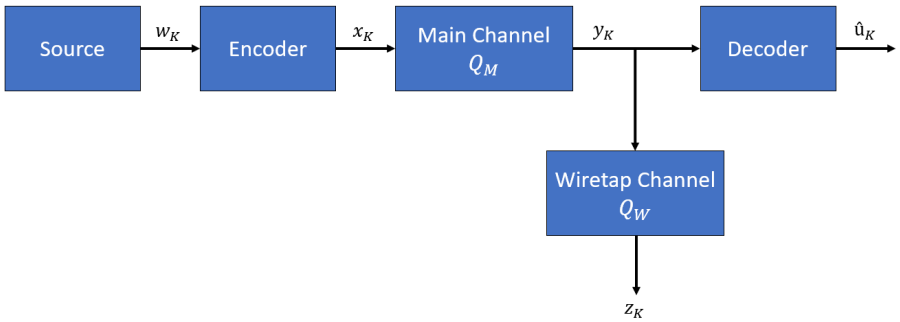


Figure 3.3: Wiretap channel (based on [33]).

Definition 3.13 (Gaussian wiretap channel)**.** [23] The *Gaussian wiretap channel* is a broadcast channel where the source (Alice) sends a signal to a legitimate receiver (Bob), while an illegitimate eavesdropper (Eve) can listen to the transmission. The Figure 3.4 illustrates the model.

Considering that the variance at Bob's channel is σ_b^2 and at the Eve's channel is σ_e^2, we can write that:

$$\mathbf{y}_b = \mathbf{x} + \mathbf{z}_b,$$
$$\mathbf{y}_e = \mathbf{x} + \mathbf{z}_e,$$

where $\mathbf{x}$ is the message sent by Alice and $\mathbf{z}_b, \mathbf{z}_e$ denotes the Gaussian noise at Bob and Eve, respectively, with both zero mean and variances σ_b^2 and σ_e^2.

It is also supposed that Alice knows Bob's channel (σ_b^2) as well as Eve's channel (σ_e^2).

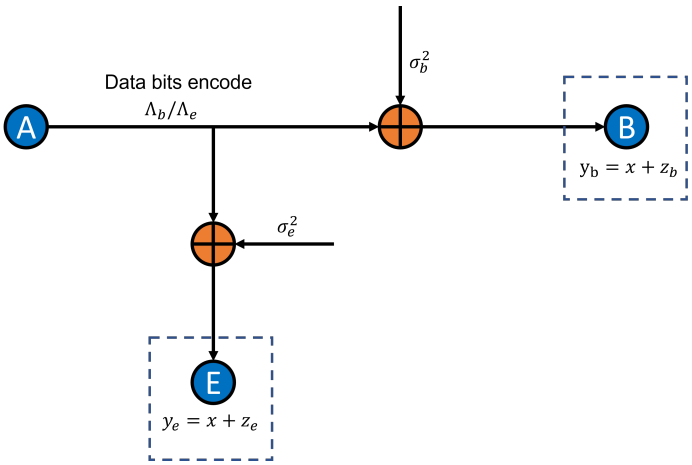


Figure 3.4: Gaussian wiretap channel, where z_b, z_e denotes the Gaussian noise at Bob and Eve, both with zero mean and variances σ_b^2 and σ_e^2. The lattice part is discussed on section 3.4.

Considering the wiretap channel over a Gaussian channel, the objective of the wiretap channel designer should be to maximize the message rate R_ℓ and as well as maximizing the confusion of the eavesdropper [33].

Notice that this is a suitable model to describe the communication between Alice and Bob while Eve is listening, as we introduced at the Chapter 1. If we recap to Figure 1.2, it is possible to understand Eve as the eavesdropper, listening and trying to decode what Bob is receiving.

3.4 Lattice coset encoding

The *coset encoding* is performed with two nested lattices. The following explanation in based on [23].

Definition 3.14 (Coset encoding)**.** The *coset encoding* is a method used to encode together both data and random bits to confuse the eavesdropper. The wiretap lattice code used is described as a pair of nested lattices $\Lambda_e \subseteq \Lambda_b$.

Λ_b - lattice designed to ensure reliability for Bob.

Λ_e - sublattice of Λ_b whose role is to increase Eve's confusion.

Definition 3.15 (Alice's encoding)**.** The Alice's encoder maps ℓ bits $s_1,\ldots,s_\ell$ from $S=\{0,1\}$ (i.e., binary code) to a codeword $\mathbf{x}=(x_1,\ldots,x_n)\in\mathbb{R}^n$.

$$\begin{aligned}\varepsilon : (\{0,1\})^\ell &\to \mathbb{R}^n\\ (s_1,\ldots,s_\ell) &\mapsto (x_1,\ldots,x_n).\end{aligned}$$

So we get that:

$$\begin{aligned}\mathbf{y}_b &= \mathbf{x}+\mathbf{z}_b\\ \mathbf{y}_e &= \mathbf{x}+\mathbf{z}_e,\end{aligned}$$

where $\mathbf{x}\in\Lambda_b\subseteq\mathbb{R}^n$.

A natural selection of $\Lambda_e\subseteq\Lambda_b$ considered in [23] is $\Lambda_e=2\mathbb{Z}^n$ and $\Lambda_b=\Lambda$ generated via Construction A (Section 2.7).

Definition 3.16 (Coset encoding method)**.** Considering the Alice's encoding of Definition 3.15, the vector of ℓ information bits is mapped to $\mathbf{x}\in\Lambda_b$,

$$\mathbf{s}=(s_1,\ldots,s_\ell)\in\{0,1\}^\ell \mapsto \mathbf{x}=(x_1,\ldots,x_n)\in\Lambda_b,$$

this vector of information is mapped to a set of codewords, concretely a coset, after which the point to be actually transmitted is chosen randomly inside the coset.

Consequently, k bits ($k\leq\ell$) of $s\in\{0,1\}^\ell$ will carry the information and $\ell-k$ bits will carry the randomness.

The lattice Λ_b is partitioned into a union of disjoint cosets

$$\Lambda_e+\mathbf{c},$$

with $\Lambda_e\subseteq\Lambda_b$ and $\mathbf{c}$ and n-dimensional vector.

Definition 3.17 (Coset encoding restriction)**.** To encode the words, it is necessary to have 2^k cosets to be labeled by the information vector $\mathbf{s}_d\in\{0,1\}^k$ (to get only bits of information):

$$\Lambda_b=\bigcup_{j=1}^{2^k}(\Lambda_e+\mathbf{c}_j)$$

which means that the number $|\Lambda_b/\Lambda_e|$ is

$$|\Lambda_b/\Lambda_e| = 2^k = \frac{vol(\Lambda_e)}{vol(\Lambda_b)}.$$

So the mapping is done with Alice choosing a point $x \in \Lambda_e + \mathbf{c}_{j(s_d)}$ and sending it over the wiretap channel:

$$\mathbf{s}_d \mapsto \Lambda_e + \mathbf{c}_{j(sd)}.$$

A random vector $\mathbf{r} \in \Lambda_e$ is also chosen. The transmitter lattice point $\mathbf{x} \in \Lambda_b$ is finally of the form:

$$\mathbf{x} = \mathbf{r} + \mathbf{c} \in \Lambda_e + \mathbf{c}.$$

Example 3.18. Let Λ_b be the lattice generated by $\begin{pmatrix} 1 & 0 \\ 1/2 & \sqrt{3}/2 \end{pmatrix}$ and Λ_e be the lattice generated by $\begin{pmatrix} 4 & 0 \\ 2 & 2\sqrt{3} \end{pmatrix}$.

For Λ_b we have:

$$\begin{aligned} vol(\Lambda_b) = \det(BB^T)^{\frac{1}{2}} &= \det\left(\begin{pmatrix} 1 & 0 \\ 1/2 & \sqrt{3}/2 \end{pmatrix}\begin{pmatrix} 1 & 1/2 \\ 0 & \sqrt{3}/2 \end{pmatrix}\right)^{\frac{1}{2}} \\ &= \det\begin{pmatrix} 1 & 1/2 \\ 1/2 & 1 \end{pmatrix}^{\frac{1}{2}} = (1-1/4)^{\frac{1}{2}} = \frac{\sqrt{3}}{2}. \end{aligned}$$

For Λ_e we have:

$$vol(\Lambda_e) = \det(M_e M_e^T)^{\frac{1}{2}} = \det(4^2 MM^T)^{\frac{1}{2}} = 4\det(MM^T)^{\frac{1}{2}} = 4\frac{\sqrt{3}}{2}.$$

Thus $|\Lambda_b/\Lambda_e| = \frac{vol(\Lambda_e)}{vol(\Lambda_e)} = \frac{4\frac{\sqrt{3}}{2}}{\frac{\sqrt{3}}{3}} = 4 = 2^2$.

In that example, $k = 2$. So the information correspond only to two bits. △

Remark 3.19. The sublattice Λ_e is used to encode the random bits that are there to increase Eve's confusion and is then intended for Eve.

Since the lattice encoding considers to send the k information bits and $\ell - k$ random bits to confuse Eve, the total rate can be written as:

$$R = R_s + R_e,$$

where R_s is the rate of information bits rate to Bob and R_e is the random bits rate.

Given that rates, it is possible to establish how much information and random bits are sent, according to Table 3.1, for complex and real channels:

Complex channel	**Real channel**
$R_s = \frac{2k}{n} \Leftrightarrow k = \frac{nR_s}{2}$	$R_s = \frac{k}{n} \Leftrightarrow k = nR_s$
$R_e = \frac{2r}{n} \Leftrightarrow r = \frac{nR_e}{2}$	$R_e = \frac{r}{n} \Leftrightarrow r = nR_e$
$\ell = k+r = \frac{n}{2}(R_s+R_e)$	$\ell = k+r = n(R_s+R_e)$

Table 3.1: Rates for complex and real channels.

Assume that the channel between Alice and Eve is corrupted by an additive uniform noise. Given a fine lattice Λ_b, consider that Alice sends one point $\mathbf{x} \in \Lambda_b$ and that Eve receives over coarse lattice Λ_e, with $\Lambda_e \subset \Lambda_e$:

$$\mathbf{y} = \mathbf{x} + \mathbf{z}$$

with $\mathbf{z} \sim \mathcal{N}(\mathbf{0}, \sigma^2)$.

With the objective of confusing Eve, Alice performs the coset encoding as follows:

1. She performs the quotient:

$$\mathbf{r} = \mathbf{x} \mod \Lambda_e,$$

   where r carries the data and random symbols goes to the quotient.

2. She encodes random symbols in Λ_e while data symbols are mapped to cosets of Λ_b/Λ_e (this is well defined, since Λ_e is a subgroup of Λ_b as in Definition 2.46).

With this approach, Eve will detect the random symbols with error free, and the data symbols with maximal confusion.

To maximize the probability of Bob to decode correctly, it is necessary that Λ_b is *AWGN-good*. To minimize the probability of Eve doing the right choice, it is necessary that Λ_e has a small *flatness factor* [19] or a higher secrecy gain [23], concepts that will be explored later in this chapter. We will explore this later in this chapter. We proceed now with an example of application.

Example 3.20. Considering the lattices of Example 2.47, that is:

$$\Lambda_e = \{(2x+y, \sqrt{3}y) | x, y \in \mathbb{Z}\}$$

and its cosets:

$$\begin{aligned}
\Lambda_e + (0,0) &= \{(2x+y, \sqrt{3}y) | x,y \in \mathbb{Z}\} \\
\Lambda_e + (1,0) &= \{(2x+y+1, \sqrt{3}y) | x,y \in \mathbb{Z}\} \\
\Lambda_e + \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right) &= \left\{\left(2x+y+\frac{1}{2}, \sqrt{3}y+\frac{\sqrt{3}}{2}\right) \middle| x,y \in \mathbb{Z}\right\} \\
\Lambda_e + \left(\frac{3}{2}, \frac{\sqrt{3}}{2}\right) &= \left\{\left(2x+y+\frac{3}{2}, \sqrt{3}y+\frac{\sqrt{3}}{2}\right) \middle| x,y \in \mathbb{Z}\right\}.
\end{aligned}$$

Note that:

$$\begin{aligned}
\Lambda_b &= \left\{\left(x+\frac{y}{2}, \frac{\sqrt{3}y}{2}\right) \middle| x,y \in \mathbb{Z}\right\} \\
&= (\Lambda_e + (0,0)) \cup (\Lambda_e + (1,0)) \cup \left(\Lambda_e + \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)\right) \cup \left(\Lambda_e + \left(\frac{3}{2}, \frac{\sqrt{3}}{2}\right)\right).
\end{aligned}$$

This fact can be viewed at Example 2.47.

Alice wants to communicate a message to Bob using the Gaussian wiretap channel. Assume that she can use 2 bits per channel use, so then it is possible to label any of the above 4 cosets. As an example:

$$\begin{aligned}
00 &\mapsto (\Lambda_e + (0,0)) \\
01 &\mapsto (\Lambda_e + (1,0)) \\
10 &\mapsto \left(\Lambda_e + \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)\right) \\
11 &\mapsto \left(\Lambda_e + \left(\frac{3}{2}, \frac{\sqrt{3}}{2}\right)\right)
\end{aligned}$$

This example is shown at Figure 3.5 - 3.8.

The Figure 3.5 shows how is the lattice Λ_b/Λ_e view for Bob. So then Alice decides to transmit the point 00, so then she randomly picks a point in the coset $\Lambda_e + (0,0)$, for example, $((6, 2\sqrt{3})$ in Figure 3.7) and can send this point over the wiretap channel.

Since Alice knows Bob's variance σ_b^2, Alice chosen a Λ_b for which the signal sent falls in the right Voronoi region for decoding in Figure 3.7. On the other hand, Eve is in trouble with her lattice, since her variance σ_e^2 is greater then Bob's one, what makes the point falls outside the right region, so Eve does not know how to decode it correctly in Figure 3.8.

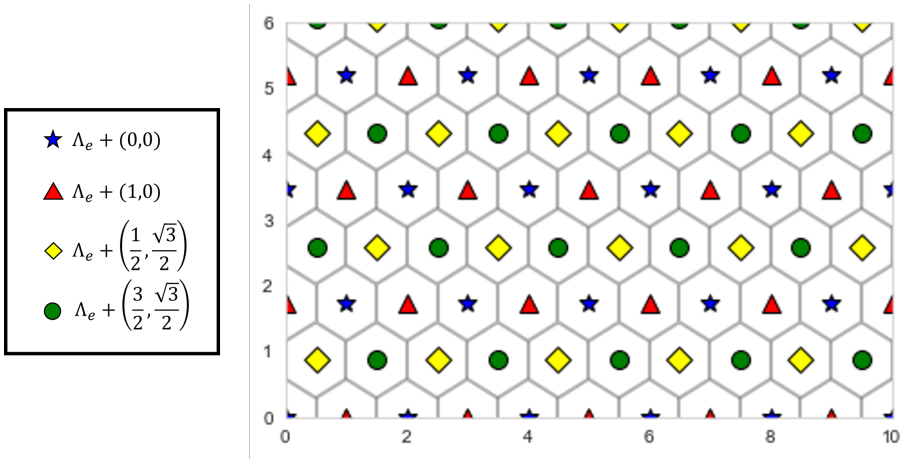


Figure 3.5: Lattice view for Bob of Λ_b/Λ_e.

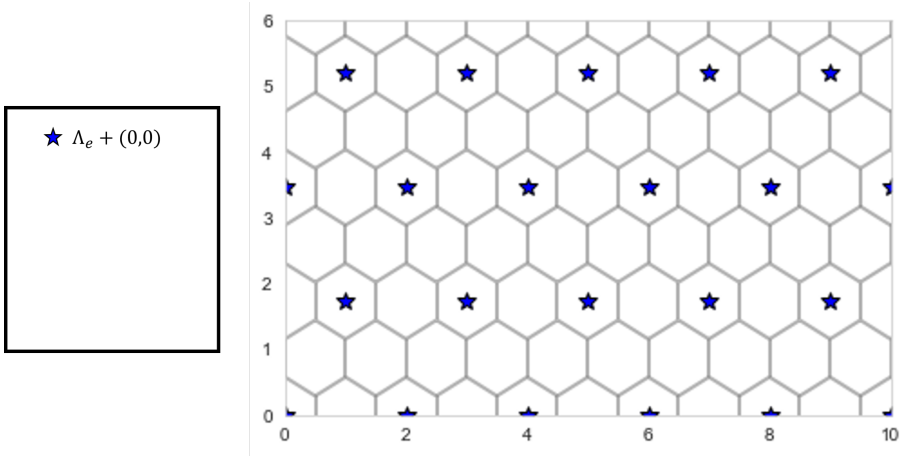


Figure 3.6: One point is chosen randomly from Λ_b/Λ_e.

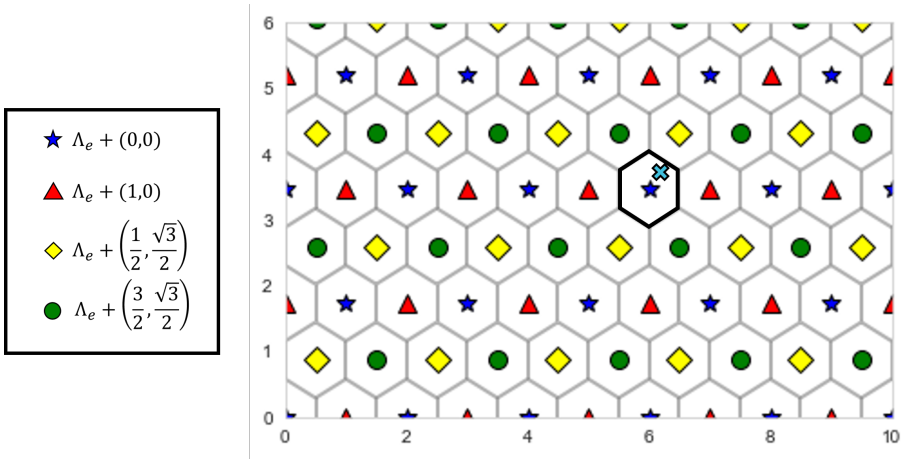


Figure 3.7: For Bob the signal is on the correct Voronoi section, so he decodes it.

△

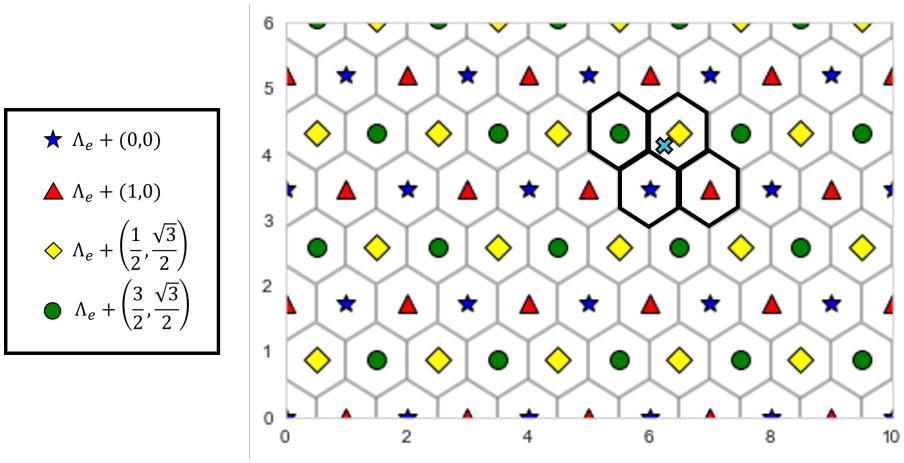


Figure 3.8: For Eve the signal is noisier, and she does not know the correct coset to decode.

3.5 Lattice coset decoding

After the transmission over the Gaussian wiretap channel, Bob and Eve receive respectively:

$$\mathbf{y}_b = \mathbf{x} + \mathbf{z}_b = \mathbf{r} + \mathbf{c} + \mathbf{z}_b,$$
$$\mathbf{y}_e = \mathbf{x} + \mathbf{z}_e = \mathbf{r} + \mathbf{c} + \mathbf{z}_e.$$

Remember that $r \in \Lambda_e$ is used to encode the random bits created to Eve, c is the coset representative of the information bits.

The goal of the coset decoding is that both Bob and Eve are interested in decoding the information bits, i.e., in finding the correct coset that was sent.

The method for both Bob and Eve is to find the closest lattice point in Λ_b to their respective signal y_b and y_e from which they deduce the coset to which the signal corresponds.

Definition 3.21 (Gaussian distribution)**.** For $\sigma > 0$ and $\mathbf{c} \in \mathbb{R}^n$, the *Gaussian distribution* of variance σ^2 centered at $\mathbf{c}$ is, for all $\mathbf{x} \in \mathbb{R}^n$,

$$f_{\sigma,\mathbf{c}}(\mathbf{x}) = \frac{1}{(\sqrt{2\pi\sigma^2})^n} e^{-\frac{\|\mathbf{x}-\mathbf{c}\|^2}{2\sigma^2}}.$$

Definition 3.22 (Λ-periodic)**.** Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice. The quotient $\mathbb{R}^n/\Lambda$ can be represented by any fundamental region of Λ. Then a function is called to be Λ-*periodic* if it repeats over the fundamental regions.

Definition 3.23 (Gaussian Distribution over Λ)**.** Let Λ be a lattice. We define the Λ-periodic

function for all $\mathbf{x} \in \mathbb{R}^n$,

$$f_{\sigma,\Lambda}(\mathbf{x}) = \sum_{\boldsymbol{\lambda}\in\Lambda} f_{\sigma,\boldsymbol{\lambda}}(\mathbf{x}) = \frac{1}{(\sqrt{2\pi\sigma^2})^n} \sum_{\boldsymbol{\lambda}\in\Lambda} e^{-\frac{\|\mathbf{x}-\boldsymbol{\lambda}\|^2}{2\sigma^2}}.$$

Remark 3.24. [19] $f_{\sigma,\Lambda(\mathbf{x})}$ restricted to the fundamental region $\mathbb{R}^n/\Lambda$ is a probability density.

Definition 3.25 (Discrete Gaussian distribution over Λ centered at c)**.** Let Λ be a lattice, σ^2 be the variance and $\boldsymbol{c} \in \mathbb{R}^n$. The following discrete distribution taking $\boldsymbol{\lambda} \in \Lambda$ is

$$D_{\Lambda,\sigma,\boldsymbol{c}}(\boldsymbol{\lambda}) = \frac{f_{\sigma,c}(\boldsymbol{\lambda})}{f_{\sigma,\Lambda}(\boldsymbol{c})}, \forall \boldsymbol{\lambda} \in \Lambda.$$

Definition 3.26 (Decoder)**.** Let $\mathbf{x} \in \Lambda \subseteq \mathbb{R}^n$ be a transmitted codeword with Voronoi cell $\mathscr{V}_\Lambda(\mathbf{x})$ over the AWGN channel with noise variance σ^2. Thus the decoder makes the correct decision if and only if the noise vector $\mathbf{y}$ is in $\mathscr{V}_\Lambda(\mathbf{x})$, what is a event of probability:

$$P_c(\mathbf{x},\sigma) = \frac{1}{(\sigma\sqrt{2\pi})^n} \int_{\mathscr{V}_\Lambda(\mathbf{x})} e^{-\frac{\|\mathbf{y}-\mathbf{x}\|^2}{2\sigma^2}} dy,$$

Remark 3.27. [23] P_c value concerns not just a point but a coset, and thus the probability that the received signal lies in the union of the Voronoi regions of Λ_b, translated by points of Λ_e.

Remark 3.28. [23] Suppose that the lattice point $\mathbf{x} = \mathbf{r} + \mathbf{c} \in \Lambda_b$ has been transmitted, with $\mathbf{r} \in \Lambda_e \cap \mathscr{V} \subseteq \Lambda_b$, where $\mathscr{V}$ is the Voronoi region of the code. The probability P_c of finding the correct coset is thus,

$$P_c(\mathscr{V},\mathbf{x},\sigma) = \frac{1}{(\sigma\sqrt{2\pi})^n} \sum_{\mathbf{t}\in\Lambda_e\cap\mathscr{V}} \int_{\mathscr{V}_{\Lambda_b}(\mathbf{x}+\mathbf{t})} e^{-\frac{\|\mathbf{y}-\mathbf{x}\|^2}{2\sigma^2}} dy. \tag{3.1}$$

Since all terms in (3.1) are positive, we can upper bound it by extending the summation over the whole lattice Λ_e, which gives:

$$P_c \leq \frac{1}{(\sigma\sqrt{2\pi})^n} \sum_{\mathbf{t}\in\Lambda_e} \int_{\mathscr{V}_{\Lambda_b}(\mathbf{x}+\mathbf{t})} e^{-\frac{\|\mathbf{y}-\mathbf{x}\|^2}{2\sigma^2}} dy.$$

Taking M codewords from Λ_b and mapping $\mathbf{u} = \mathbf{y} - \mathbf{x} - \mathbf{t}$, we get:

$$P_c \leq \frac{1}{(\sigma\sqrt{2\pi})^n} \sum_{\mathbf{t}\in\Lambda_e} \int_{\mathscr{V}(\Lambda_b)} e^{-\frac{\|\mathbf{u}+\mathbf{t}\|^2}{2\sigma^2}} du.$$

Since the vector received by Bob is most likely to lie in the Voronoi region of Λ_b around the transmitted point (Alice chooses Λ_b to fit Bob's channel), then the term in $t \neq 0$ are negligible for Bob, which yields:

$$P_{c,b} \leq \frac{1}{(\sigma_b\sqrt{2\pi})^n} \int_{\mathscr{V}(\Lambda_b)} e^{-\frac{\|\mathbf{u}\|^2}{2\sigma^2}} du.$$

And this is the case of transmitting lattice points over the Gaussian channel, for which we know that Λ_b should have a good Hermite parameter to get a good coding gain [7].

3.6 Eve's confusion analysis

By analysing the probability of correct decision for Eve we get:

$$P_{c,e} \leq \frac{1}{(\sigma_e\sqrt{2})^n} vol(\mathscr{V}(\Lambda_b)) \sum_{\mathbf{t}\in\Lambda_e} e^{-\frac{\|\mathbf{t}\|^2}{2\sigma_e^2}}. \tag{3.2}$$

Maximize Eve's confusion is equivalent to minimize the probability $P_{c,e}$ of Eve making a correct decision, while keeping $P_{c,b}$ unchanged. This is equivalent to minimize (3.2), that is to find a lattice Λ_b which is as good as possible for the Gaussian channel, and which contains a sublattice Λ_e such that:

$$\text{minimize w.r. } \Lambda_e \sum_{\mathbf{t}\in\Lambda_e} e^{-\frac{\|\mathbf{t}\|^2}{2\sigma_e^2}}$$

$$\text{under the constraint } \log_2|\Lambda_b/\Lambda_e| = k.$$

And thus to minimize Eve's probability of correct decision is equivalent to minimize $\Theta_{\Lambda_e}(z)$ in $z = i/(2\pi\sigma_e^2)$, under the constraint that $log_2|\Lambda_b/\Lambda_e| = k$, which is the motivation to the secrecy gain definition, so we formally presented next. In summary, the best Λ_e is the sublattice of Λ_b with the larger secrecy gain [23].

3.7 Secrecy gain

The secrecy gain quantifies how much confusion a specific lattice provides compared to using the $\mathbb{Z}^n$ lattice. [23]

Recall from Definition 2.49 that the theta series of a lattice Λ is given by:

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

We can rewrite this a function of the complex value z:

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

Now set $y = -iz$ and restrict to real positive values of y [23]. With this we restrict the theta

series to real values in the equation:

$$\Theta_\Lambda(y) = \sum_{\mathbf{t}\in\Lambda} q^{\|\mathbf{t}\|^2},\ q = e^{-\pi y},\ y > 0.$$

Definition 3.29 (Secrecy function)**.** [23] Let Λ be an n-dimensional lattice of volume κ^n. The secrecy function of Λ is given by:

$$\Xi_\Lambda(y) = \frac{\Theta_{\kappa\mathbb{Z}^n}(y)}{\Theta_\Lambda(y)},\ y > 0.$$

Definition 3.30 (Strong secrecy gain)**.** [23]

$$\chi_{\Lambda,\text{strong}} = \sup_{y>0} \Xi_\Lambda(y).$$

Calculate the strong secrecy gain is expensive. So consider that we can consider a symmetry point y_0 such that $\Xi_\Lambda(y_0 \cdot y) = \Xi_\Lambda(y_0/y)$. Then it is possible to relax the definition [23]:

Definition 3.31 (Weak secrecy gain)**.** [23] Let Λ be an n-dimensional lattice, whose secrecy function has a symmetry point y_0. Then the *weak secrecy gain* χ_Λ of Λ is given by:

$$\chi_\Lambda = \Xi_\Lambda(y_0) = \frac{\Theta_{\kappa\mathbb{Z}^n}(y_0)}{\Theta_\Lambda(y_0)},$$

where $\kappa = vol(\Lambda)^{1/n} = |det(B)|^{\frac{1}{n}}$.

Proposition 3.32. *[23] Let Λ be a lattice with generator matrix B and λ^* its dual. The following holds for the theta series:*

$$\Theta_\Lambda(y) = |\det(B)|^{-1} \left(\frac{1}{\sqrt{y}}\right)^n \Theta_{\Lambda^*}(1/y).$$

Proposition 3.33. *[23, Proposition 1, p.5963] The secrecy function of an isodual lattice has multiplicative symmetry point at $y = 1$.*

Proof. The secrecy function of an isodual lattice Λ and the secrecy function of its dual Λ^* are the same:

$$\Xi_\Lambda(y) = \frac{\Theta_{\mathbb{Z}^n}(y)}{\Theta_\Lambda(y)} = \frac{\Theta_{\mathbb{Z}^n}(y)}{\Theta_{\Lambda^*(y)}} = \Xi_{\Lambda^*}(y).$$

Since $\mathbb{Z}^n$ and Λ are isodual and we have the volume 1 in Proposition 3.32, then:

$$\Theta_{\mathbb{Z}^n}(y) = y^{-\frac{n}{2}} \Theta_{\mathbb{Z}^n}\left(\frac{1}{y}\right),$$
$$\Theta_\Lambda(y) = y^{-\frac{n}{2}} \Theta_{\Lambda^*}\left(\frac{1}{y}\right).$$

and

$$\Xi_\Lambda(y) = \frac{\Theta_{\mathbb{Z}^n}(y)}{\Theta_\Lambda(y)} = \frac{y^{-\frac{n}{2}}\Theta_{\mathbb{Z}^n}\left(\frac{1}{y}\right)}{y^{-\frac{n}{2}}\Theta_{\Lambda^*}\left(\frac{1}{y}\right)} = \frac{\Theta_{\mathbb{Z}^n}\left(\frac{1}{y}\right)}{\Theta_{\Lambda^*}\left(\frac{1}{y}\right)} = \Xi_\Lambda\left(\frac{1}{y}\right).$$

This shows that $y_0 = 1$ is a multiplicative symmetry point for the secrecy function. □

Example 3.34. [23] Let us use $\Lambda = E_8$ and $y = 1$. Using Table 2.1 and Proposition 2.56, we get:

$$\begin{aligned}
\Xi_{E_8}(1) = \frac{\Theta_{\mathbb{Z}^8}(1)}{\Theta_{E_8}(1)} &= \frac{\vartheta_3(e^{-\pi})^8}{\frac{1}{2}(\vartheta_2(e^{-\pi})^8 + \vartheta_2(e^{-\pi})^3 + \vartheta_4(e^{-\pi})^8)} \\
&= \frac{\sqrt[4]{2}^8\,\vartheta_4(e^{-\pi})^8}{\frac{1}{2}[\vartheta_4(e^{-\pi})^8 + \sqrt[4]{2}^8\vartheta_4(e^{-\pi})^8 + \vartheta_4(e^{-\pi})^8]} \\
&= \frac{4\vartheta_4(e^{-\pi})^8}{\frac{1}{2}[\vartheta_4(e^{-\pi})^8 + 4\vartheta_4(e^{-\pi})^8 + \vartheta_4(e^{-\pi})^8]} \\
&= \frac{4}{\frac{1}{2}[1+4+1]} = \frac{4}{3}.
\end{aligned}$$

Thus, $\chi_{E_8} = \Xi_{E_8}(1) = \frac{4}{3} = 1.33$. △

Example 3.35. [23] Let us use the Leech lattice $\Lambda = \Lambda_{24}$ and $y = 1$. Using Table 2.1 and Proposition 2.56, we get:

$$\begin{aligned}
\Xi_{\Lambda_{24}} = \frac{\Theta_{\mathbb{Z}_{24}}(1)}{\Theta_{\Lambda_{24}}(1)} &= \frac{\vartheta_3(e^{-\pi})^{24}}{\frac{1}{8}(\vartheta_2(e^{-\pi})^8 + \vartheta_3(e^{-\pi})^8 + \vartheta_4(e^{-pi})^8)^3 - \frac{45}{16}(\vartheta_2(e^{-\pi})\cdot\vartheta_3(e^{-\pi})\cdot\vartheta_4(e^{\pi}))^8} \\
&= \frac{(\sqrt[4]{2}\vartheta_4(e^{-\pi}))^{24}}{\frac{1}{8}[\vartheta_4(e^{-\pi})^8 + (\sqrt[4]{2}\vartheta_4(e^{-\pi}))^8 + \vartheta_4(e^{-\pi})^8] - \frac{45}{16}[\vartheta_4(e^{-\pi})(\sqrt[4]{2}\vartheta_4(e^{-\pi}))\vartheta_4(e^{-\pi})]^8} \\
&= \frac{64\vartheta_4(e^{-\pi})^{24}}{\frac{1}{8}[\vartheta_4(e^{-\pi})^{24}[1+4+1]^3 - \frac{45}{16}\vartheta_4(e^{-\pi})^{24}\cdot 4} \\
&= \frac{64}{\frac{1}{8}6^3 - \frac{45}{4}} = \frac{256}{63} = 4.0635.
\end{aligned}$$

△

In [23] an asymptotic analysis of the secrecy gain was made to prove that there exists a family of even unimodular lattices whose secrecy gains exponentially grows up with the dimension.

It was proved in [3] that it is possible to generalize this analysis to the *formally unimodular lattices*, i.e., lattices such that $\Theta_\Lambda(z) = \Theta_{\Lambda^*}(z)$, to improve on the secrecy gain.

Improvements on the secrecy gain can also be achieved when using lattices obtained via Construction A from codes over $\mathbb{Z}_4$ instead of binary codes [2].

3.8 Other secrecy criteria

Definition 3.36 (Perfect secrecy capacity)**.** The *perfect secrecy capacity* is the maximum amount of information that Alice can send to Bob while ensuring that Eve gets a not relevant quantity of information.

Definition 3.37 (Flatness Factor)**.** For a lattice Λ and for a parameter σ, the *flatness factor* is defined by:

$$\varepsilon_{\Lambda}(\sigma) \triangleq \max_{\mathbf{x}\in\mathscr{F}} \left| \frac{f_{\sigma,\Lambda}(\mathbf{x})}{1/vol(\Lambda)} - 1 \right|,$$

where $\mathscr{F}$ is a fundamental region of Λ.

Proposition 3.38. *[19, Proposition 2, p. 5] It is also possible to define the flatness factor in terms of theta series:*

$$\varepsilon_{\Lambda}(\sigma) = \left(\frac{\gamma_{\Lambda}(\sigma)}{2\pi}\right)^{\frac{n}{2}} \Theta_{\Lambda}\left(\frac{1}{2\pi\sigma^2}\right) - 1,$$

where $\gamma_{\Lambda}(\sigma) = \frac{vol(\Lambda)^{\frac{2}{n}}}{\sigma^2}$ *is the volume-to-noise ratio (VNR) .*

Definition 3.39 (Secrecy-good)**.** A sequence of lattices $\Lambda^{(n)}$ is *secrecy-good* if

$$\varepsilon_{\Lambda}^{(n)} = e^{-\Omega(n)}, \ \forall \gamma_{\Lambda}^{(n)} < 2\pi,$$

where $\Omega(n)$ is a function asymptotically larger than n or larger as n.

In [19] it was shown that if the flatness factor is small, then a discrete Gaussian distribution over the fine lattice results in almost uniformly distributed cosets, and vice versa [19].

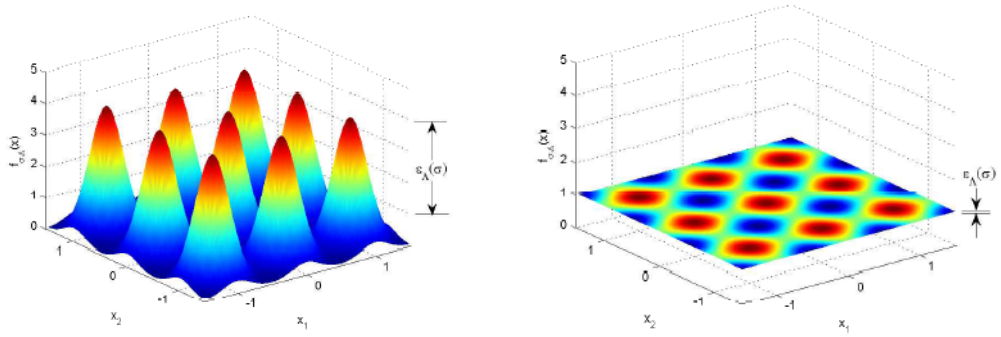
In Figure 3.9 it is possible to see in the Figure 3.9a, if the flatness factor is large, then we can see clearly the peaks, facilitating the decoding. In Figure 3.9b we can see that, with a small flatness factor, the distribution are almost uniformly distributed, making a random guessing the best option.

3.9 Reliability criteria

Definition 3.40 (Error probability for AWGN)**.** The *error probability* for decoding a lattice Λ in the presence of AWGN with noise $\mathbf{z}$ with variance σ^2 is defined as:

$$P_e(\Lambda, \sigma^2) = Pr\{\mathbf{z} \in \mathscr{V}(0)\},$$

where $\mathscr{V}(0)$ is the fundamental Voronoi cell of Λ.



(a) $\gamma_\Lambda(\sigma) = 8\pi$, $\varepsilon_\Lambda(\sigma) = 3$ [19]. **(b)** $\gamma_\Lambda(\sigma) = \pi$, $\varepsilon_\Lambda(\sigma) = 0.0075$ [19].

Figure 3.9: Flatness factor Gaussian distribution [19].

In the Definition 3.40, notice that what is analysed is the probability of the noisy signal to fall inside the Voronoi cell.

Definition 3.41 (Hermite parameter)**.** Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice. The *Hermite parameter* measures the packing efficiency:

$$\delta(\Lambda) = \frac{d^2_{min}(\Lambda)}{vol^{2/n}(\Lambda)}.$$

For some target error probability $0 < \varepsilon < 1$, let $\sigma^2(\varepsilon) = value$ of σ^2 such that P_e is equal to ε.

Definition 3.42 (Normalized volume to noise ratio)**.** [35] The *normalized volume-to-noise ratio* (NVNR) of a lattice Λ, at a target error probability $0 < Pr\{\mathbf{z} \notin \mathscr{V}(0)\} < 1$, is defined as:

$$\mu(\Lambda, P_e) = \mu(\Lambda, \sigma^2(P_e)) = \frac{vol^{2/n}(\Lambda)}{\sigma^2(P_e)}$$

Definition 3.43 (AWGN-good)**.** A sequence of lattices $\Lambda^{(n)}$ will be *AWGN-good* if the following holds:

$$\lim_{n\to\infty} \frac{vol(\Lambda_n)^{\frac{2}{n}}}{2\pi\sigma^2} = e$$
$$\lim_{n\to\infty} Pr\{\mathbf{z} \notin \mathscr{V}(0)\} = 0.$$

Notice that the Definition 3.43 is the asymptotic analysis of Definition 3.42. For a given target P_e, the objective is to find the densest lattice, i.e., the lattice with the lowest NVNR. This would imply the largest coding rate per unit volume [35]. Thus, the NVNR can measure the possible performance advantages [35].

Another important issue of Definition 3.43 is that it analyses the NVNR asymptotically for a family of lattices, what make it harder to do practical lattice choices for decoding. That is why

is more useful to look for the Hermite parameter instead.

Definition 3.44 (Coding gain)**.** [35] The coding gain of a lattice Λ relative to the cubic lattice $\mathbb{Z}^n$, at some error probability P_e in the presence of AWGN, is defined as:

$$\Gamma_e(\Lambda, P_e) = \frac{\mu(\mathbb{Z}^n, P_e)}{\mu(\Lambda, P_e)}.$$

3.10 Method analysis

In summary, to implement a lattice encoding, it is necessary to have:

- a lattice Λ_b that is good for reliability, it is, with good coding gain or Hermite parameter;
- a sublattice $\Lambda_e \subseteq \Lambda_b$ that is good for secrecy, it is, with good secrecy gain or flatness factor;
- the restriction of $\log_2 |\Lambda_b/\Lambda_e| = k$.

Example 3.45. Let us consider an 8-dimensional nested lattice code construction. Alice communicates to Bob using an 8-dimensional lattice.

Define $\Lambda_b = E_8$, since it has the best coding gain (Hermite Constant) in dimension 8 ([7]) and it is unimodular. Alice also knows that Bob's SNR is $\gamma_b = \frac{E_s}{\sigma_b^2}$.

Define Λ_e as a sublattice of E_8, which first optimize the secrecy gain. Since E_8 is an extremal ([23]) lattice, all its scaled versions reach the lower bound on the maximal secrecy gain χ_8 and consequently we can pick $\Lambda_e = 2^m E_8$.

Observes that:

$$|E_8/(2^m E_8)| = 2^{8m}.$$

Thus $R_s = \frac{2(8m)}{8} = 2m$.

Considering that $R_s = R - \log_2 \frac{\gamma_e}{2\pi}$, we can calculate that:

$$R - R_s = R_e = \log_2(\gamma_e) - \log_2(2\pi) = \frac{\gamma_e(dB)}{10}\log_2 10 - \log_2(2\pi) \cong \frac{\gamma_e(dB)}{10}3.32 - 2.65.$$

Considering that Alice knows Eve's SNR, she can decide how many of random bits are necessary to be sent: $\gamma_e = 10dB \Rightarrow R_e \cong 0.67$.
$\gamma_e = 20dB \Rightarrow R_e \cong 4$.

So the better Eve's SNR is, the more random bits are needed. If $R = 6$ bits, Eve's SNR is 20 dB, then Alice can send $R_s = 2$ bits per complex channel use, which means that $\Lambda_e = 2E_8$.

The encoding can be done via Construction A. For E_8, we have:

$$E_8 = \sqrt{2}\mathbb{Z}^8 + \frac{1}{\sqrt{2}}(8,4,4)$$

where $C = (8,4,4)$ is the Reed-Müller code of length 8 and dimension 4 and since $\mathbb{Z}^8 = 2\mathbb{Z}^8 + (8,8,1)$, we have

$$E_8 = \sqrt{2}\mathbb{Z}^8 + \frac{1}{\sqrt{2}}(8,8,1) + \frac{1}{\sqrt{2}}(8,4,4).$$

△

Chapter 4

COMPUTE-AND-FORWARD

The physical layer is the responsible for the hardware part of the networks, such as cabling and relays. Although the cabling part can seems as bit pipes - real cables -, the cabling can also be wireless, thought antennas, Bluetooth and others [24].

When we assume a wireless communication, then a transmission from a single node can be heard by all the nearby nodes, not only the intended receiver, and any receiver can capture signals from all the nearby transmitters [22].

Naturally, this "easy to access" signals seems, at a first sight, as a highly undesirable characteristic. To defeat that, a lot of algorithms has been considered to transform the physical layer as a set of reliable bit pipes again, i.e., a set of links which can accommodate a specific number of bits per time unit [22].

This kind of strategy is implemented to avoid interference results in diminishing rates as the network size increases [22]. Thus, this chapter aims to explain some cooperative strategies and establish a set of definitions about how to see the wireless communication in a lattice scenario. Observe that this is a reliability method, different from the previous chapter in which we've presented a security method.

4.1 Cooperative relaying strategies

Definition 4.1 (Relay channel)**.** [9] A *relay channel* is a channel in which there is one sender and one receiver with a number of intermediate nodes which acts as relays to help the communication from the sender to the receiver.

Considering a relay channel, here are some of the relaying cooperative strategies:

- **Decode-and-Forward:** Each relay should decode at least a part of the message transmitted. Then, the recovered bits are re-encoded for collaborative transmission to the next relay. A potential problem is that the relay interference increases with the message size [22].

- **Compress-and-Forward:** Also called *estimate-and-forward*, this strategy takes the observed signal at the relay and quantize this information to pass to the destination. The destination receives information from multiple relays, treating the network as a multiple-input multiple-output (MIMO) channel. Since there is no decoding in the intermediate nodes, the noise builds up as the message traverse the network [22].

- **Amplify-and-Forward:** Each relay repeats and transmits a scaled version of its observation. It also deals with the networks as it is MIMO, and also make possible to add a beam forming gain [13], but the noise also adds up with transmissions [22].

4.2 Compute-and-Forward definitions

For this set of definitions, we are considering that the channel is Gaussian and composed by relays.

Definition 4.2 (Message)**.** [22] Assume that each transmitter (indexed by $\ell = 1, 2, \ldots, L$) has a *message vector* $\mathbf{w}_\ell \in \mathbb{F}_p^{k_\ell}$, where p is prime, $\mathbb{F}_p$ is a finite field and k_ℓ is the message length. It is also assumed the messages as independently and uniformly chosen.

Remark 4.3. Without loss of generality, we sort the transmitters ascending by the message length.

Remark 4.4. All messages should be *zero-pad*, it means that we add zeros at the left of the message to get them at a common length $k \triangleq \max_\ell k_\ell$.

Example 4.5. Suppose a network $\mathbf{N}$ with 3 transmitters $\{t_1, t_2, t_3\}$ and binary words:

- $\mathbf{w}_1 = 1100$, where $\mathbf{w}_1 \in \mathbb{F}_2^4$.
- $\mathbf{w}_2 = 10$, where $\mathbf{w}_2 \in \mathbb{F}_2^2$.
- $\mathbf{w}_3 = 101$, where $\mathbf{w}_3 \in \mathbb{F}_2^3$.

As stated at Remark 4.3, we should order those transmitters at ascending order. So define $t_1' = t_2$, $t_2' = t_3$ and $t_3' = t_1$.

Finally, as stated at Remark 4.4, $k = \max_\ell k_\ell = \max\{2,3,4\} = 4$. Thus, our final set of messages are $\{0010, 0101, 1100\}$. △

Definition 4.6 (Encoder)**.** [22] A *encoder* is a function that maps the k-length message over the finite field to n-length real-valued codeword.

The function of the encoder is generally expressed as:

$$\varepsilon_\ell : \mathbb{F}_p^k \to \mathbb{R}^n.$$

The obtained real valued word will be represented by the letter x_ℓ:

$$\mathbf{x}_\ell = \varepsilon_\ell(\mathbf{w}_\ell).$$

Finally, each codeword is subject to a power constraint, which is a channel characteristic:

$$\|\mathbf{x}_\ell\|^2 \leq nP.$$

Remark 4.7. It is possible to incorporate asymmetric power constraints by scaling the channel coefficients, but this approach is out of the scope of this text. For more details, see [22].

Example 4.8. With the same conditions of the Example 4.5, let's analyse the encoders.

By the power constraint requisite, we have:

$$\|\mathbf{x}_\ell\|^2 \leq nP \Rightarrow \frac{1}{n}\sum_{i=1}^{k}(x_\ell^i)^2 \leq P,$$

where i is the entry.

Define $n = k$, $\varepsilon(\mathbf{w}_\ell) = \mathbf{w}_\ell$, and $P = \frac{1}{2}$. In fact,

$$\varepsilon(\mathbf{w}_1) = \varepsilon(0010) = 0010, \text{ and } \frac{1}{4}\sum_{i=1}^{4}(w_1^i)^2 = \frac{1}{4}(0+0+1+0) = \frac{1}{4} \leq P.$$

$$\varepsilon(\mathbf{w}_2) = \varepsilon(0101) = 0101, \text{ and } \frac{1}{4}\sum_{i=1}^{4}(w_2^i)^2 = \frac{1}{4}(0+1+0+1) = \frac{1}{2} \leq P.$$

$$\varepsilon(\mathbf{w}_3) = \varepsilon(1100) = 1100, \text{ and } \frac{1}{4}\sum_{i=1}^{4}(w_3^i)^2 = \frac{1}{4}(1+1+0+0) = \frac{1}{2} \leq P.$$

△

Definition 4.9 (Message Rate)**.** [22] The *message rate* R_ℓ of each transmitter is the length of its message (measured in bits) normalized by the size of channel used:

$$R_\ell = \frac{k_\ell}{n}\log p,$$

where log operation is respect to base 2.

Remark 4.10. Since we order by ascending k_ℓ according to Remark 4.3 and p and n are fixed, then $R_1 \leq R_2 \leq \ldots \leq R_L$.

Example 4.11. Continuing the Example 4.8, our channel is binary, so $p = 2$. We define $n = 4$. Then:

- $\mathbf{w}_1 = 0010 \rightarrow \mathbf{x}_1 = 0010 \rightarrow R_1 = \frac{2}{4}\log 2 = \frac{2}{4} = \frac{1}{2}$.
- $\mathbf{w}_2 = 0101 \rightarrow \mathbf{x}_2 = 0101 \rightarrow R_2 = \frac{3}{4}\log 2 = \frac{3}{4}$.
- $\mathbf{w}_3 = 1100 \rightarrow \mathbf{x}_3 = 1100 \rightarrow R_3 = \frac{4}{4}\log 2 = \frac{4}{4} = 1$.

△

Definition 4.12 (channel model)**.** [22] It is a Gaussian channel, so each relay (indexed by $m = 1, 2, \ldots, M$) observes a noisy linear combination of the transmitted signals through the channel:

$$\mathbf{y}_m = \sum_{\ell=1}^{L} h_{m\ell}\mathbf{x}_\ell + \mathbf{z}_m,$$

where $h_{m\ell} \in \mathbb{R}$ are the channel coefficients between the ℓ^{th} transmitter and the receiver, $\mathbf{z}$ is a Gaussian noise, where $\mathbf{z} \sim \mathcal{N}(0, \sigma^2)$.

For the relay m, let $\mathbf{h}_m = [h_{m1} \ldots h_{mL}]^t$ be the channel coefficients for that relay. $\mathbf{H} = \{h_{m\ell}\}$ denotes the entire channel matrix. For that convention, the m^{th} row if $\mathbf{H}$ is h_m^t.

Example 4.13. Given the same assumptions as in Examples 4.8 and 4.11, suppose that we have $M = 2$ relays. So:

$$\mathbf{h}_1 = \begin{pmatrix} 1 & 0 & 1/2 \end{pmatrix}, \mathbf{h}_2 = \begin{pmatrix} 0 & -1 & 1 \end{pmatrix}$$

Thus:

$$\mathbf{H} = \begin{pmatrix} 1 & 0 & 1/2 \\ 0 & -1 & 1 \end{pmatrix}.$$

Consider also that the noise is given by $z = \begin{pmatrix} 0.5 & 0.5 \\ 0.5 & 0.5 \\ 0.5 & 0.5 \end{pmatrix}$.

Thus, we can calculate y_1 and y_2:

$$\begin{aligned}\mathbf{y}_1 &= \sum_{\ell=1}^{3} h_{1\ell}\mathbf{x}_\ell + \mathbf{z}_1 \\ &= \begin{pmatrix} 1 & 0 & 1/2 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} + \begin{pmatrix} 0.5 \\ 0.5 \\ 0.5 \end{pmatrix} \\ &= \mathbf{x}_1 + \frac{\mathbf{x}_3}{2} + \begin{pmatrix} 0.5 \\ 0.5 \\ 0.5 \end{pmatrix}\end{aligned}$$

$$\begin{aligned}\mathbf{y}_2 &= \sum_{\ell=1}^{3} h_{2\ell}\mathbf{x}_\ell + \mathbf{z}_2 \\ &= \begin{pmatrix} 0 & -1 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} + \begin{pmatrix} 0.5 \\ 0.5 \\ 0.5 \end{pmatrix} \\ &= -\mathbf{x}_2 + \mathbf{x}_3 + \begin{pmatrix} 0.5 \\ 0.5 \\ 0.5 \end{pmatrix}\end{aligned}$$

△

Definition 4.14 (Desired equations)**.** [22] Each relay should be able to recover a linear combination of the messages:

$$\mathbf{u}_m = \bigoplus_{\ell=1}^{L} q_{m\ell}\mathbf{w}_\ell.$$

where the $q_{m\ell}$ coefficients are taken in $\mathbb{F}_p$. Although the desired equations are evaluated over the finite field $\mathbb{F}_p$, the channel operates over the reals $\mathbb{R}$. It is a requirement to Definition 4.16.

Each relay has a *decoder*:

$$\mathscr{D}_m : \mathbb{R}^n \to \mathbb{F}_p^k,$$

which maps the channel output $\mathbf{y}_m$ to an estimate $\hat{\boldsymbol{u}}_m = \mathscr{D}_m(\mathbf{y}_m)$ of the equation $\boldsymbol{u}_m$.

Remark 4.15. Decoders do the exact opposite of the encoders - while encoders transform the data from the field to real values (to be sent through the channel), the decoders convert those real values back to the field space.

In Figure 4.1, we have a summary of the process, where each word $\mathbf{w}_\ell$ passes through an

encoder ε_ℓ to become a real codeword $\mathbf{x}_\ell$. After that, it passes throughout the relays (the $\mathbf{H}$ matrix) and then the noise is added in each of the relays ($\mathbf{z}_m$), resulting the real word $\mathbf{y}_m$. Thus this word is decoded by $\mathscr{D}_m$ and then we got an estimated word $\hat{u}_m$.

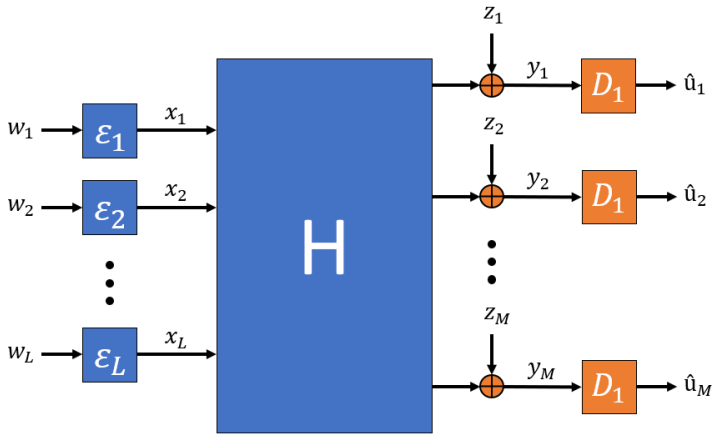


Figure 4.1: Gaussian Network in a lattices view (based on [22]).

Definition 4.16 (Coefficient Vector)**.** The equation with coefficient vector $\mathbf{a}_m = [a_{m1}, \ldots, a_{mL}]^T$ in $\mathbb{Z}^L$ is the linear combination of the transmitted messages u_m with coefficients given by

$$q_{m\ell} = \pi^{-1}([a_{m\ell}] \mod p).$$

where π^{-1} maps elements of $\{0, 1, \ldots, p-1\}$ to the corresponding element in $\mathbb{F}_p$.

Definition 4.17 (Probability of Error)**.** The equations with coefficient vectors $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_M \in \mathbb{Z}^L$ are decoded with *average probability of error* ε if

$$P_e = Pr\left(\bigcup_{m=1}^{M} \{\hat{u}_m \neq u_m\}\right) < \varepsilon.$$

Definition 4.18 (Computational Rate Region)**.** The *computation rate region* $\mathscr{R}(\mathbf{h}_m, \mathbf{a}_m)$ is achievable for any $\varepsilon > 0$ and n large enough, there exists encoders and decoders, $\varepsilon_1, \ldots, \varepsilon_L, \mathscr{D}_1, \ldots, \mathscr{D}_M$, such that all relays can recover their desired equations with average probability of error ε so long as the underlying message rates $R_1, \ldots, R_L$ satisfy

$$R_\ell < \min_{m:a_{m\ell}\neq 0} \mathscr{R}(\mathbf{h}_m, \mathbf{a}_m).$$

4.3 Compute-and-Forward method

The *Compute-and-Forward (C&F)* method was introduced by Nazer and Gastpar in [22]. This strategy enables relays to decode linear equations of the transmitted messages using the

noisy linear combinations provided by the channel. It means that if a destination receives enough linear combinations, then it is able to decode the desired messages reliability [22].

The C&F strategy relies on nested lattices, using their linear structure to ensure that integer combinations of codewords are themselves codewords. It is also possible for the relay to determine any equation, but it is easier to recover at higher rates the ones closer to the channel's coefficients [22].

Different from the *Decode-and-Forward*, *Compress-and-Forward* and the *Amplify-and-Forward* strategies which were discussed in Section 4.1, the C&F strategy stop looking for *bits* and start looking to *equations of bits*, taking more advantages of the modular structure of the network stack [22].

Considering Gaussian channels, in this chapter we will present the lattice assumptions, how this strategy works and finalize this with an example.

The structure of the method can be seen in Figure 4.2.

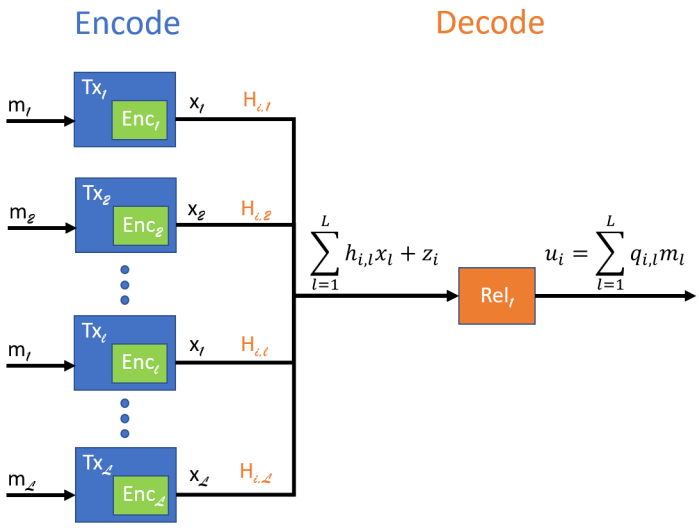


Figure 4.2: Compute and Forward method.

So given $\ell = \{1,\ldots,L\}$ transmitters, and a channel matrix H, at the i^{th} relay we have:

$$\mathbf{y}_i = \sum_{\ell=1}^{L} h_{i,\ell}\mathbf{x}_\ell + \mathbf{z}_i, \tag{4.1}$$

where $h_{i,\ell} \in \mathbb{R}$, the power constraint is given by $\frac{1}{n}E\{\|\mathbf{x}_\ell\|^2\} \leq P$ and $\mathbf{z} \sim \mathcal{N}(\mathbf{0},\sigma^2)$, i.e., an AWGN. At the decoding of the linear combination, we have:

$$\mathbf{u}_i = \bigoplus_{\ell=1}^{L} q_{i,\ell}\mathbf{m}_\ell,$$

with the coefficients $q_{i,\ell} \in \mathbb{F}_p$. We can rewrite (4.1) as the following:

$$\mathbf{y}_i = \sum_{\ell=1}^{L} a_{i,\ell}\mathbf{x}_\ell + \sum_{\ell=1}^{L} (h_{i,\ell} - a_{i,\ell})\mathbf{x}_\ell + \mathbf{z}_i. \tag{4.2}$$

With (4.2) we have two parts:

Linear combination: The first part of (4.2) (represented at (4.3)) is a linear combination of codewords with integer coefficients $a_{i,\ell} \in \mathbb{Z}$

$$\sum_{\ell=1}^{L} a_{i,\ell}\mathbf{x}_\ell. \tag{4.3}$$

Effective noise: The second part of the (4.2) is the noise that remains after the decoding coefficients are chosen:

$$\sum_{\ell=1}^{L} (h_{i,\ell} - a_{i,\ell})\mathbf{x}_\ell + \mathbf{z}_i.$$

With that approach, the coefficients $a_i = (a_{i,\ell})$ are the ones used to decode the words properly.

Definition 4.19 (Compute and Forward lattice conditions)**.** [12]

1. The codebook must be closed under linear combination to ensure that $\sum_\ell a_{i,\ell}\mathbf{x}_\ell$ results in a valid codeword. This way the noise is also independent of this sum.
2. The codebook must be isomorphic to the message space $\mathbb{F}_p$.

Nested lattices match the conditions from Definition 4.19 [22]. Thus, the codewords $\mathbf{x}_\ell$ are basically points from n-dimensional lattice partition Λ/Λ'.

Theorem 4.20. *[22, Theorem 1, p.5] For real-valued AWGN networks with channel coefficient vectors $\boldsymbol{h}_m \in \mathbb{R}^L$ and equation coefficients $\boldsymbol{a}_m \in \mathbb{Z}^L$, the following computation rate region is achievable:*

$$\mathscr{R}(h_i, a_i) = \max_{\alpha_i \in \mathbb{R}} \frac{1}{2} \log^+ \left(\frac{P}{\alpha_i^2 + P\|\alpha_i \boldsymbol{h}_i - \boldsymbol{a}_i\|} \right), \tag{4.4}$$

where $\log^+ = \max(0, \log)$.

Proposition 4.21. *[12, Equation 4, p.3] The unknown integer coefficients $\boldsymbol{a}_i = [a_{i1}, \ldots, a_{iL}]$ could be found maximizing the computational rate $\mathscr{R}(\boldsymbol{h}_i, \boldsymbol{a}_i)$. The maximum region is given by:*

$$\mathscr{R}(\boldsymbol{h}_i, \boldsymbol{a}_i) = \frac{1}{2} \log^+ \left(\left(\|\boldsymbol{a}_i\|^2 - \frac{P(\boldsymbol{h}_i^T \boldsymbol{a})_i^2}{1 + P\|\boldsymbol{h}_i\|^2} \right)^{-1} \right). \tag{4.5}$$

Proof. Let $f(\alpha_i)$ be the denominator of (4.4):

$$f(\alpha_i) = \alpha_i^2 + P \cdot (\alpha_i \mathbf{h}_i - a_i)^T (\alpha_i \mathbf{h}_i - \mathbf{a}_i). \tag{4.6}$$

How (4.6) is quadratic on α_i, we can minimize by setting first derivative to zero:

$$\frac{df}{d\alpha_i} = 2\alpha_i + 2P\|\mathbf{h}_i\|^2 \alpha_i - 2P(\mathbf{h}_i^T \mathbf{a}_i) = 0. \tag{4.7}$$

Thus by isolating α_i in (4.7), we got:

$$\alpha_{MMSE} = \frac{P\mathbf{h}_i^T \mathbf{a}_i}{1 + P\|\mathbf{h}_i\|^2}. \tag{4.8}$$

By replacing (4.8) in (4.6), we got:

$$\begin{aligned} f(\alpha_{MMSE}) &= \alpha_{MMSE}^2 (1 + P\|\mathbf{h}_i\|^2) - 2P\mathbf{h}_i^T \mathbf{a}_i \alpha_{MMSE} + P\|\mathbf{a}_i\|^2 \\ &= \left(\frac{P\mathbf{h}_i^T \mathbf{a}_i}{1 + P\|\mathbf{h}_i\|^2} \right)^2 (1 + P\|\mathbf{h}_i\|^2) - 2P\mathbf{h}_i^T \mathbf{a}_i \left(\frac{P\mathbf{h}_i^T \mathbf{a}_i}{1 + P\|\mathbf{h}_i\|^2} \right) + P\|\mathbf{a}_i\|^2 \\ &= \frac{P^2 (\mathbf{h}_i^T \mathbf{a}_i)^2}{1 + P\|\mathbf{h}_i\|^2} - 2\frac{P^2 (\mathbf{h}_i^T \mathbf{a}_i)^2}{1 + P\|\mathbf{h}_i\|^2} + P\|\mathbf{a}_i\|^2 \\ &= P\left(\|\mathbf{a}_i\|^2 - \frac{P(\mathbf{h}_i^T \mathbf{a}_i)^2}{1 + P\|\mathbf{h}_i\|^2} \right). \end{aligned} \tag{4.9}$$

With (4.9) in (4.4):

$$\begin{aligned} \mathscr{R}(\mathbf{h}_i, \mathbf{a}_i) &= \frac{1}{2} \log^+ \left(\frac{P}{f(\alpha_{MMSE})} \right) \\ &= \frac{1}{2} \log^+ \left(\frac{P}{P\left(\|\mathbf{a}_i\|^2 - \frac{P(\mathbf{h}_i^T \mathbf{a}_i)^2}{1 + P\|\mathbf{h}_i\|^2} \right)} \right) \\ &= \frac{1}{2} \log^+ \left(\left(\|\mathbf{a}_i\|^2 - \frac{P(\mathbf{h}_i^T \mathbf{a}_i)^2}{1 + P\|\mathbf{h}_i\|^2} \right)^{-1} \right). \end{aligned}$$

□

Example 4.22. Suppose in Proposition 4.21 that we have a *perfect match*, i.e., $\mathbf{h}_i = \mathbf{a}_i$. So we have in (4.5):

$$\begin{aligned} \mathscr{R}(\mathbf{a}_i, \mathbf{a}_i) &= \frac{1}{2} \log^+ \left(\left(\|\mathbf{a}_i\|^2 - \frac{P(\mathbf{a}_i^T \mathbf{a}_i)^2}{1 + P\|\mathbf{a}_i\|^2} \right)^{-1} \right) = \frac{1}{2} \log^+ \left(\left(\|\mathbf{a}_i\|^2 - \frac{P\|\mathbf{a}_i\|^4}{1 + P\|\mathbf{a}_i\|^2} \right)^{-1} \right) \\ &= \frac{1}{2} \log^+ \left(\left(\frac{\|\mathbf{a}_i\|^2 + P\|\mathbf{a}_i\|^4 - P\|\mathbf{a}_i\|^4}{1 + P\|\mathbf{a}_i\|^2} \right)^{-1} \right) = \frac{1}{2} \log^+ \left(\frac{1 + P\|\mathbf{a}_i\|^2}{\|\mathbf{a}_i\|^2} \right) \\ &= \frac{1}{2} \log^+ \left(P + \frac{1}{\|\mathbf{a}_i\|^2} \right). \end{aligned}$$

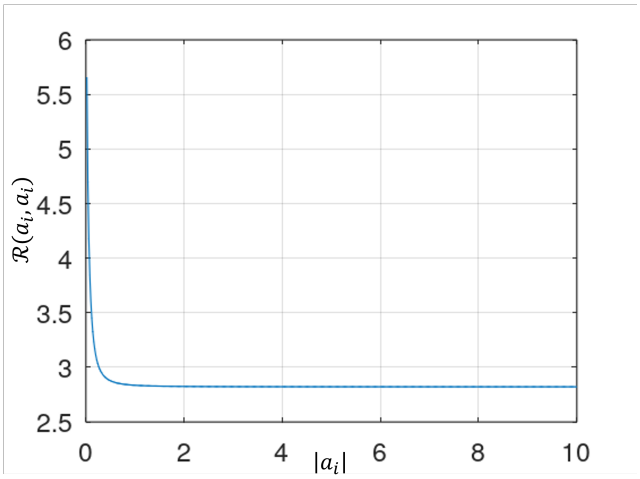


Figure 4.3: Computational rate for a perfect match in compute-and-forward method for power constraint $P = 50$.

In this case, if $P = 50$ as an example, we have the graph result in Figure 4.3. It means that the blue line at the graph shows the maximum rate that is achievable for each of the norms $\|\boldsymbol{a}_i\|$. △

Since the codebook is isomorphic to $\mathbb{F}_p$, we calculate $q_{i,\ell} = a_{i,\ell} \mod p$. Then the relays recovers u_i with coefficients $q_{i,\ell}$ to the receivers or retransmit $\mathscr{X}_i = \sum_\ell a_{i,\ell} \boldsymbol{x}_\ell$ as a new codeword for the next relays. How the codebook is closed by integer combinations, $\mathscr{X}_i$ exists, at that is true since codewords are chosen from points of the nested lattices Λ/Λ'. [12]

4.4 Method limitation

All relays can successfully recover an integer linear combination of the transmitted codewords if their message rate $R_\ell < \mathscr{R}(\mathbf{h}_i, \mathbf{a}_i)$, according to (4.5) [12]. Observe that this is a constraint to this method, since we can not overtake the maximum rate value.

Since $\mathbf{h}_i$ is given by the channel and $\mathbf{a}_i$ tries to mimic $\mathbf{h}_i$, it is natural to conclude that the limitation is related to the channel characteristics to deal with this method. So after defining $\mathbf{h}_i$ and $\mathbf{a}_i$, we got a clear limitation to (4.9). However, it can be extended to a slow fading scenario under an outage formulation [22].

Chapter 5

COMPUTE-AND-FORWARD WITH LATTICE ENCODING

In Chapter 3 we explained how to use codeword space in coset coding for Gaussian wiretap channels. In Chapter 4 we explained how to construct a framework for physical-layer network coding PNC.

In the article *On the Security of Lattice-based Physical-layer Network Coding Against Wiretap Attacks* [12], Forutan and Fischer described how to apply C&F relaying strategy in a wiretap channel while avoiding wiretap attacks.

5.1 Network coding attacks

Definition 5.1 (Entropy attack)**.** [34] The *entropy attack* is a replay attack, in which malicious nodes create non-innovation and linearly dependent coded packets from the nodes stored at the downstream node. These packets waste resources since they induce useless information to increase the workload of receivers in the process of decoding original packets.

Definition 5.2 (Byzantine attack)**.** [34] The *byzantine attack* is an attack in which the byzantine nodes act as traitor nodes, operating with a hidden intent to disable or impair the network. As they are trusted nodes, they locate along the multi-hop paths between source and destination nodes, so they have complete access to the information and the network resources. Thus this attack is imperceptible.

Definition 5.3 (Pollution attack)**.** [34] The *pollution attack* is usually started by a unauthorized node which inject polluted packets into the information flow. As wireless network is open, the malicious nodes can launch it from arbitrary point in network.

Definition 5.4 (Eavesdropping attack)**.** [34] The *eavesdropping attack* is the attack in which the eavesdropper can either wiretap one or more links in the wired network, or use the high frequency antenna to acquire information within certain range of the intermediate node in the wireless network.

Definition 5.5 (Active attack)**.** [10] When the hacker actively acts at the network modifying messages, it is called a *active attack*.

From Definitions 5.1-5.4, we can notice that the Entropy, Byzantine and Pollution attacks are active attacks. Those attacks can be simply represented by Figure 5.1, in which the malicious active attacker Mallory [4] intercept the communication between Alice and Bob and actively modify it.

Figure 5.1: Active attack from Mallory at the communication between Alice and Bob.

Definition 5.6 (Passive attack)**.** [10] When the hacker only observes the messages, it is called a *passive attack*.

From Definitions 5.1-5.4, we can notice that only the Eavesdropping attack is a passive attack. This attack can be simply represented by Figure 1.2, in which the eavesdropper Eve listen to the communication between Alice and Bob without any modification.

The wiretap channel discussed at Chapter 3 models a passive attack. We reiterate the wiretap channel considers that Eve is able to listen to Alice and Bob communications and that the objective of the wiretap channel designer should be maximize her confusion, making the message barely impossible to be decoded by her.

That being said, the method proposed in [12] analyse only the passive attack of eavesdropping. Although all the following analysis regards to eavesdropping attacks, it is important to highlight that a cooperative jamming is possible, i.e., more than one eavesdropper can collaborate to decode Alice's message [12].

5.2 Application of Compute-and-Forward with lattice encoding

According to [12], let us keep the assumptions of Compute-and-Forward, in which we have L transmitters in the network, indexed by ℓ going from 1 to L. We also consider that each transmitter receives a word $\boldsymbol{w}_\ell$ which is encoded into a length-n codeword $\boldsymbol{x}_\ell$ under the average power constraint $\frac{1}{n}E\{\|\boldsymbol{x}_\ell\|^2\}$. We also assume that both the network nodes and potential attackers are able to receive the signal transmission wherever it occurs.

5.2.1 One isolated attack

The *one isolated attack* is when there is an eavesdropper who seeks the data from a particular transmitter or a subset of them.

Suppose that the eavesdropper Eve tries to obtain the signal from $\boldsymbol{x}_k$ from the k^{th} relay where $k \in \{1,\dots,L\}$, without loss of generality. Consider that the $\boldsymbol{h}_\ell$ vectors correspond to the channel coefficients between the transmitters and the attacker. Thus, according to (4.2), we get:

$$\boldsymbol{y}_k = \sum_{\ell=1}^{L} a_{k,\ell}\boldsymbol{x}_\ell + \sum_{\ell=1}^{L}(h_{k,\ell} - a_{k,\ell})\boldsymbol{x}_\ell + \boldsymbol{z}_k. \tag{5.1}$$

Let $a_k = (0,\dots,0,1,0,\dots,0)$ the integer coefficient vector for the k^{th} relay, with a 1 at the k^{th} position of the vector. Thus in (5.1):

$$\begin{aligned}
\boldsymbol{y}_k &= \boldsymbol{x}_k + \sum_{\substack{\ell=1\\ \ell\neq k}}^{L} h_{\ell,k}\boldsymbol{x}_\ell + (h_{k,k}-1)\boldsymbol{x}_k + \boldsymbol{z}_k \\
&= \boldsymbol{x}_k + \sum_{\substack{\ell=1\\ i\neq k}}^{L} h_{\ell,k}\boldsymbol{x}_\ell + h_{k,k}\boldsymbol{x}_k - \boldsymbol{x}_k + \boldsymbol{z}_k \\
&= \sum_{\substack{\ell=1\\ i\neq k}}^{L} h_{\ell,k}\boldsymbol{x}_\ell + h_{k,k}\boldsymbol{x}_k + \boldsymbol{z}_k \\
&= \sum_{\ell=1}^{L} h_{\ell,k}\boldsymbol{x}_\ell + \boldsymbol{z}_k.
\end{aligned}$$

So then we got, for the k^{th} relay the y_k:

$$\boldsymbol{y}_k = \sum_{\ell=1}^{L} h_{\ell,k}\boldsymbol{x}_\ell + \boldsymbol{z}_k. \tag{5.2}$$

How we want this result for Eve's perception, we rewrite (5.2) considering that $\boldsymbol{y}_e = \boldsymbol{y}_k$ is

respected to Eve and that her noise is described as $\boldsymbol{z}_e \sim \mathcal{N}(\mathbf{0}, \sigma_e^2)$. So Eve's is described as:

$$\boldsymbol{y}_e = \sum_{\ell=1}^{L} h_{\ell,k}\boldsymbol{x}_\ell + \boldsymbol{z}_E.$$

Let's analyse the rate region for this case. According to (4.5):

$$\begin{aligned}
R_k < \mathscr{R}(\boldsymbol{h}_k, \boldsymbol{a}_k) &= \frac{1}{2}\log^+\left(\left(\|\boldsymbol{a}_k\|^2 - \frac{P(\boldsymbol{h}_k^T\boldsymbol{a}_k)^2}{1+P\|\boldsymbol{h}_k\|^2}\right)^{-1}\right) \\
&= \frac{1}{2}\log^+\left(\left(1 - \frac{P\boldsymbol{h}_k^2}{1+P\boldsymbol{h}_k^2+P\left(\sum_{\substack{\ell=1\\ i\neq k}}\boldsymbol{h}_\ell^2\right)}\right)^{-1}\right) \\
&= \frac{1}{2}\log^+\left(\left(\frac{1+P\boldsymbol{h}_k^2+P\left(\sum_{\substack{\ell=1\\ i\neq k}}\boldsymbol{h}_\ell^2\right) - P\boldsymbol{h}_k^2}{1+P\boldsymbol{h}_k^2+P\left(\sum_{\substack{\ell=1\\ i\neq k}}\boldsymbol{h}_\ell^2\right)}\right)^{-1}\right) \\
&= \frac{1}{2}\log^+\left(\frac{1+P\boldsymbol{h}_k^2+P\left(\sum_{\substack{\ell=1\\ i\neq k}}\boldsymbol{h}_\ell^2\right)}{1+P\left(\sum_{\substack{\ell=1\\ i\neq k}}\boldsymbol{h}_\ell^2\right)}\right) \\
R_k < \mathscr{R}(\boldsymbol{h}_k, \boldsymbol{a}_k) &= \frac{1}{2}\log^+\left(1 + \frac{P\boldsymbol{h}_k^2}{1+P\left(\sum_{\substack{\ell=1\\ i\neq k}}\boldsymbol{h}_\ell^2\right)}\right)
\end{aligned} \tag{5.3}$$

We have defined that $\boldsymbol{z}_e \sim \mathcal{N}(0, \sigma_e^2)$. Considering that $\sigma_e \in [0,1]$, then we can rewrite the rate region of (5.3) considering this fact:

$$R_k < \mathscr{R}(\boldsymbol{h}_k, \boldsymbol{a}_k) = \frac{1}{2}\log^+\left(1 + \frac{P\boldsymbol{h}_k^2}{\sigma_e^2+P\left(\sum_{\substack{\ell=1\\ i\neq k}}\boldsymbol{h}_\ell^2\right)}\right) \tag{5.4}$$

The interpretation of (5.4) is that all transmitted signals other than $\boldsymbol{x}_k$ appear as interference to Eve [12]. Thus the attacker is able to recover $\boldsymbol{x}_k$ successfully if the message rate R_k falls under the limit of (5.4).

On the other hand, when we analyse this with the compute-and-forward strategy, we know that only a combination of the messages has the rate under this limit, so Eve will only obtain a mix of the information of the users. In that case, Eve cannot obtain the user's data she intends to [12].

5.2.2 Multiple isolated attacks

The *multiple isolated attacks* is when there are several **non collaborating** eavesdroppers, each interested in the data from a specific transmitter.

Since the eavesdroppers do not collaborate, the restrictions of how to obtain the data remains the same from the only one isolated attack. So the security is also guarantee in that case.

5.2.3 Coordinated attacks

The *coordinated attacks* is when several **collaborative** eavesdroppers capture data of a transmitter or a subsets of transmitters and share between them.

As described in the subsection 5.2.1, Eve is capable of recovering a linear combination of the original transmitted codewords. So suppose that there are at least L eavesdroppers which are collaborating and sharing their recovery information, so then they can solve the linear system.

5.2.3.1 Compute-and-Forward with lattice encoding

Considering the compute-and-forward implementation in the cooperative case (subsection 5.2.3), [12] propose to use the lattice encoding at the compute-and-forward method when choosing the lattices. At the table 5.1 we can verify the main differences.

C&F	**C&F with lattice encoding**
Lattices are AWGN-good	Fine lattice Λ is AWGN-good and coarse lattice Λ' is secrecy-good
Codewords are distributed uniformly at random within the nested lattices Λ/Λ'	Messages encoded into codewords over Λ/Λ' according to coset encoding
	The transmitters select their codewords as lattice points that are conformed to a discrete Gaussian distribution $D_{\Lambda,\sigma,0}$ over the nested lattices Λ/Λ' with $\sigma^2 = P$

Table 5.1: C&F and C&F with lattice encoding comparison (based on [12]).

As discussed in the Definition 3.39, when we change the coarse lattice (the one that refers to Eve's communication system) to have a small flatness factor, then it becomes hard for Eve to detect the peaks and decode the codewords. Also, how it is Gaussian distributed, the communication can achieve higher rates compared to the case where the codebook consists of uniformly distributed codewords [12, 18]. Also the security is granted to the network when applying the lattice coset encoding [12](Section 3.7 and Section 3.8).

Definition 5.7 (C&F with lattice encoding method)**.** Let $\mathscr{C}$ be a communication system. Suppose that:

1. The codebook is n-dimensional nested lattice Λ/Λ'.
2. The fine lattice Λ is partitioned into p^k cosets $\Lambda' + \lambda_m$, with λ_m the coset leader to the message $m \in \mathbb{F}_p^k$.
3. Over each coset $\Lambda' + \lambda_m$ a discrete Gaussian distribution $D_{\Lambda',\sigma,-\lambda_m}$ is defined over $\sigma^2 = P$. Now we are assuming nonlinear messages, different than what was described in the section about coset encoding.
4. Moreover Λ' has a small flatness factor, i.e., $\varepsilon'_\Lambda(\sigma_E) < \frac{1}{2}$.
5. For all transmitter, the encoder $\varepsilon : \mathbb{F}_p^k \to \Lambda/\Lambda'$ maps the message m to a coset $\lambda_m \in \Lambda/\Lambda'$.
6. A transmitter upon sending a rate-R message m selects a lattice point through sampling $D_{\Lambda',\sigma,\lambda_m}$

Since the cosets $\Lambda' + \lambda_m$ will be almost uniformly distributed at random if the distribution of the lattice points in $\Lambda' + \lambda_m$ comply with a discrete Gaussian distribution $D_{\Lambda',\sigma,-\lambda_m}$, the conclusion is that Eve will be confused in distinguishing the cosets [12].

Chapter 6

CONCLUSION

This dissertation has showed that is possible to model communication methods using lattices to guarantee the security and reliability in a wireless channel. Being the lattice encoding, the compute-and-forward or even a combination of both, it is possible to guarantee confidentiality without sharing keys. Although an eavesdropper can listen to the conversation, it is very hard for them to decode correctly due to the confusion generated via the encoding schema and channel characteristics.

We covered all the specific objectives proposed:

1. we presented the lattice concepts and definitions with their main theorems in Chapter 2;
2. we presented the theta series in Chapter 2, the Gaussian channel in Chapter 3 and discussed about the main design criteria in Chapter 3;
3. the cooperative relaying strategies and how to model the wireless communication using lattices were presented in Chapter 4;
4. lattice encoding and wiretap channel were defined in Chapter 3;
5. the compute-and-forward method was presented in Chapter 4;
6. the combined method was presented in 5;
7. the passive and active attacks, in Chapter 5.

To better understand the methods, future studies could address more examples for the combination of lattice encoding and compute-and-forward methods to assess if this is the best approach for the security in a combined eavesdropping attack. It is also possible to analyze the Example 3.45 in this context. Since the rate region is a limitation to the compute-and-forward

method, it would be important to proceed with more studies about the rate regions and how to maximize them to get better usage of the method.

In the future, it would be beneficial to delve deeper into the design criteria and assess the practicality of each method in real-world network communication scenarios. It would also be interesting to calculate how efficient is to apply those methods. This approach can lead to improved outcomes within the telecommunications industry.

REFERENCES

[1] BERNSTEIN, D. J., AND LANGE, T. Post-quantum cryptography. *Nature 549*, 7671 (2017), 188–194.

[2] BOLLAUF, M. F., LIN, H.-Y., AND YTREHUS, Ø. On the secrecy gain of formally unimodular Construction A_4 lattices. In *2022 IEEE International Symposium on Information Theory (ISIT)* (2022), IEEE, pp. 3226–3231.

[3] BOLLAUF, M. F., LIN, H.-Y., AND YTREHUS, Ø. Formally unimodular packings for the Gaussian wiretap channel. *To appear in IEEE Transactions on Information Theory* (2023).

[4] BRUCE, S. *Applied cryptography: protocols, algorithms, and source code in C.-2nd*. john wiley & sons, 1996.

[5] COHN, H., KUMAR, A., MILLER, S., RADCHENKO, D., AND VIAZOVSKA, M. The sphere packing problem in dimension 24. *Annals of Mathematics 185*, 3 (2017), 1017–1033.

[6] COHN, P. Classic algebra. *The Mathematical Gazette 86*, 505 (2002), 175–175.

[7] CONWAY, J. H., AND SLOANE, N. J. A. *Sphere packings, lattices and groups*, vol. 290. Springer Science & Business Media, 1999.

[8] COSTA, S. I., OGGIER, F., CAMPELLO, A., BELFIORE, J.-C., AND VITERBO, E. *Lattices applied to coding for reliable and secure communications*. Springer, 2017.

[9] COVER, T. M., AND THOMAS, J. A. *Elements of Information Theory, Second Edition*, vol. 1. Wiley-Interscience, 2006.

[10] Difference between Active attack and Passive attack. https://www.javatpoint.com/active-attack-vs-passive-attack.

[11] FISCHER, R. F. H. Appendix C: Introduction to lattices. In *Precoding and Signal Shaping for Digital Transmission*. John Wiley & Sons, Inc., Hoboken, NJ, USA, Jan. 2005, pp. 421–437.

[12] FORUTAN, V., AND FISCHER, R. F. On the security of lattice-based physical-layer network coding against wiretap attacks. In *SCC 2015; 10th International ITG Conference on Systems, Communications and Coding* (2015), VDE, pp. 1–6.

[13] GILLIS, A. S. What is beamforming? | Definition from TechTarget. https://www.techtarget.com/searchnetworking/definition/beamforming.

[14] HALES, T. C. A proof of the Kepler conjecture. *Annals of mathematics* (2005), 1065–1185.

[15] JORGE, G. C. *Reticulados q-ários e algébricos*. PhD thesis, Tese de Doutorado, Imecc-Unicamp, 2012.

[16] KARLEIGH MOORE, SATYABRATA DASH, E. R. Caesar Cipher | Brilliant Math & Science Wiki. https://brilliant.org/wiki/caesar-cipher/.

[17] LI, Z., YATES, R., AND TRAPPE, W. Secrecy Capacity of Independent Parallel Channels. In *Securing Wireless Communications at the Physical Layer*, R. Liu and W. Trappe, Eds. Springer US, Boston, MA, 2010, pp. 1–18.

[18] LING, C., AND BELFIORE, J. Achieving the AWGN channel capacity with lattice Gaussian distribution. *CoRR abs/1302.5906* (2013).

[19] LING, C., LUZZI, L., BELFIORE, J.-C., AND STEHLE, D. Semantically secure lattice codes for the Gaussian wiretap channel. *IEEE Transactions on Information Theory 60*, 10 (2014), 6399–6416.

[20] LITTLEJOHN, S. W., AND FOSS, K. A. *Encyclopedia of communication theory*, vol. 1. Sage, 2009.

[21] MIYAMOTO, H. K. Claude E. Shannon | IEEE Information Theory Society. https://www.itsoc.org/about/shannon.

[22] NAZER, B., AND GASTPAR, M. Compute-and-forward: Harnessing interference through structured codes. *IEEE Transactions on Information Theory 57*, 10 (2011), 6463–6486.

[23] OGGIER, F., SOLÉ, P., AND BELFIORE, J.-C. Lattice codes for the wiretap Gaussian channel: Construction and analysis. *IEEE Transactions on Information Theory 62*, 10 (2016), 5690–5708.

[24] ROUSE, M. OSI protocols, May 2020. https://www.techopedia.com/definition/24961/osi-protocols.

[25] SHANNON, C. E. A mathematical theory of communication. *The Bell System Technical Journal 27*, 3 (1948), 379–423.

[26] SLOANE, N. J. A. The sphere-packing problem. *Documenta Mathematika, Vol. III (1998), 387-396* (2002).

[27] STREY, E. *Construções de reticulados a partir de códigos q-ários*. PhD thesis, Tese de Doutorado, Imecc-Unicamp, 2017.

[28] STREY, G. R. D. A. S. *A série teta e a função de sigilo de um reticulado*. PhD thesis, Dissertação de Mestrado, Imecc-Unicamp, 2016.

[29] VAUDENAY, S. *A classical introduction to cryptography: Applications for communications security*. Springer Science & Business Media, 2005.

[30] VIAZOVSKA, M. The sphere packing problem in dimension 8. *Annals of Mathematics 185*, 3 (2017), 991–1015.

[31] What is wiretapping? | Definition from TechTarget. https://www.techtarget.com/whatis/definition/wiretapping.

[32] WILLIAMS, L. OSI model layers and protocols in computer network, Jan. 2020.

[33] WYNER, A. D. The wire-tap channel. *Bell System Technical Journal 54*, 8 (1975), 1355–1387.

[34] YAO, S., CHEN, J., DU, R., DENG, L., AND WANG, C. A survey of security network coding toward various attacks. In *2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications* (2014), pp. 252–259.

[35] ZAMIR, R. Lattices are everywhere. In *2009 Information Theory and Applications Workshop* (2009), pp. 392–421.

GLOSSARY

AWGN – *Additive White Gaussian Noise*

C&F – *Compute and Forward*

ECC – *Elliptic-curve cryptography*

MIMO – *Multiple-Input Multiple-Output*

MMSE – *Minimum mean square error*

NVNR – *Normalized volume-to-noise ratio*

PNC – *Physical-Layer Network Coding*

RSA – *Rivest-Shamir-Adleman*

SNR – *Signal-to-noise ratio*

VNR – *Volume-to-noise ratio*