A Study on the Capacity of Gaussian Channels: From a Lattice Code Perspective

by

Mingxi Nan

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Applied Science
in
Electrical and Computer Engineering

Waterloo, Ontario, Canada, 2011

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

As one of the most significant classes of structure codes, lattice codes are related to various geometric and coding problems, such as sphere packing and covering, quantization, signaling for the additive white Gaussian noise (AWGN) channel, Wyner-Ziv coding, dirty-paper coding, etc. In this thesis, we are especially interested in the construction of lattice codes for the AWGN channel, since from the classical channel coding theory, the capacity-achieving codebooks for the AWGN channel may possess little or no structure, making them ill-suited for applications. Specifically, we investigate the employment of lattice codes into the one-input-two-output AWGN channel to achieve its capacity.

For the one-input-two-output AWGN channel, the receiver decodes jointly with its two observations which are the outputs of the transmitted signal going through two independent AWGN channels. An angle-decoding scheme is proposed, and we prove that under such decoding scheme, the capacity of the one-input-two-output AWGN channel can be achieved using lattice codes, where the bounding region of the lattice code is an n-dimensional ball to preserve the structure and symmetry of the underlying lattices, instead of a "thin" spherical shell as in previous studies.

Moreover, to further preserve the lattice symmetry and to reduce complexity, the nested lattice code with lattice decoding is incorporated into the one-input-two-output AWGN channel, as under the lattice decoding scheme, the receiver decodes to the nearest lattice point, neglecting the effects of bounding region. In contrast, minimum-distance decoding or the proposed angle-decoding aims to find the nearest codeword inside the bounding region. We first transform the one-input-two-output AWGN channel into a modulo-lattice additive noise (MLAN) channel with vanishing information loss, and then apply the nested lattice code on the MLAN channel. Furthermore, we extend the nested lattice code to a general single-input-multiple-output AWGN channel and prove it to be capacity achieving.

Acknowledgements

Firstly and most importantly, I would like to thank my supervisor Professor Liang-Liang Xie for his insightful guidance and continuous support during my two year education at the University of Waterloo and throughout this thesis.

Secondly, I would like to express my sincere gratitude to the readers of this thesis, Professor Pin-Han Ho and Professor Zhou Wang, for taking the time to read my thesis.

Also, I want to thank my fellow student, Mr. Xiugang Wu for his generous help. The discussions with him are invaluable resources for my improvement.

Contents

List of Figures

Chapter 1

Introduction

1.1 Problems and Motivations

Consider the following Gaussian channel, as shown in Fig. 1.1,

$$Y = X + Z, \quad Z \sim \mathcal{N}(0, N)$$

with average power constraint

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

for any codeword $(x_1, x_2, ...x_n)$.

The capacity of this channel is defined as

$$C = \max_{p(x):EX^2 \leq P} I(X;Y)$$

and proved to be

$$C = \frac{1}{2}\log(1 + \frac{P}{N}).$$

The achievability of the capacity on Gaussian channels is based on the random coding argument proposed by Shannon in his revolutionary paper [2], where each codeword X^n is randomly generated according to a normal distribution with variance $P - \epsilon$, i.e., $X_i(\omega) \sim \mathcal{N}(0, P - \epsilon)$ for $i = 1, 2, ..., n$ and $\omega = 1, 2, ..., 2^{nR}$. The

average probability of error over the ensemble of the random codebooks is driven to zero for any $R < C$. Shannon proved the existence of the optimal codebooks. However, one cannot describe the exact structures of the capacity achieving codebooks or how to construct one. Indeed, a capacity achieving codebook that is randomly generated may possess no structure or symmetry. Consequently, the application of random coding theorem on the AWGN channel is quite complicated or even unpractical. Motivated by this, over decades, the minds of the researchers in the communication community have been dedicated to the search for low-complexity and structured encoding and decoding schemes for the AWGN channel.

Specifically, lattices are employed for the construction of structured codes for AWGN channels due to their figures of merit. The development of lattice codes for AWGN channels originated in the work [3], [4] of R.de Buda, which states the following.

(1) For any rate $R < \log \frac{P}{N}$, there exists a lattice code $\mathcal{C}_n$ with arbitrarily small (maximal) probability of error with lattice decoding. Furthermore, the bounding region of the code can be chosen as an n-dimensional ball of radius $\sqrt{nP}$.

(2) By choosing the bounding region as a "thin" spherical shell instead of the whole sphere, the lattice code can achieve the capacity on AWGN channel using maximum-likelihood (ML) decoding.

Lattice decoding amounts to find the nearest lattice point (which may not be a codeword), neglecting the effects of the bounding region. In contrast, ML decoding, i.e., the optimum decoding procedure, requires to find the closest codeword to the received signal.

There are two main gaps between the above results. One is whether the rates

up to capacity can be achieved by setting the bounding regions of lattice codes as an n-dimensional ball as opposed to a spherical shell, so that the structure and symmetry of the underlying lattices can be preserved. The other is to design a capacity-achieving lattice encoding and decoding scheme to further conserve the lattice symmetry and to reduce complexity. Rüdiger Urbanke and Bixio Rimoldi closed the first gap in their paper [9], proving that lattice codes within spherical bounding regions can achieve capacity on the AWGN channel. The proof is from a fundamental geometrical perspective and is significantly simplified under the proposed decoding rule, which will be specified in Chapter 3. The second gab is closed by Uriz Erez and Ram Zamir in [13], where an AWGN channel is first transformed into a modulo-lattice additive noise (MLAN) channel with vanishing information loss as n goes to infinity, and then the capacity of the transformed MLAN channel is achieved with nested lattice codes with lattice encoding and decoding scheme.

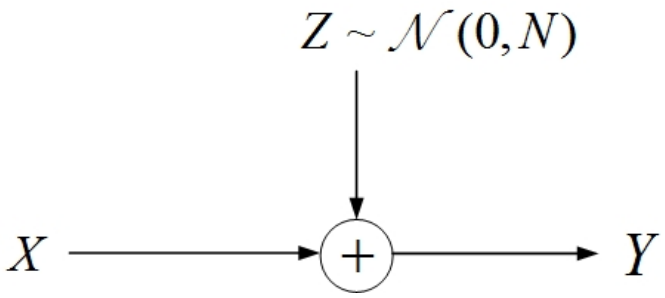

Figure 1.1: Additive white Gaussian noise (AWGN) channel.

Motivated by the application of lattice codes on the AWGN channel, in this thesis, we explore the coding schemes in [9] and [13] and extend them to a more complicated case, the single-input-multiple-output Gaussian channel. Specifically, the following one-input-two-output AWGN channel depicted in Fig. 1.2 is considered,

$$\begin{cases} Y_1 = X + Z_1 \\ Y_2 = X + Z_2 \end{cases}$$

where $Z_1 \sim \mathcal{N}(0, N_1)$, $Z_2 \sim \mathcal{N}(0, N_2)$. X is the channel input with average power

constraint P, and the receiver decodes based on Y_1 and Y_2 jointly.

A suboptimal angle-decoding scheme is proposed, and we prove that under such scheme there exists a sequence of lattices Λ_n achieves the capacity on the one-input-two-output AWGN channel with vanishing probability of error. Also, we transform the one-input-two-output AWGN channel into a single-input-single-output MLAN channel, and prove the existence of a sequence of lattices Λ_n such that the information rate of the transformed MLAN channel approaches the capacity of the original AWGN channel as n goes to infinity. Then the nested lattice code with lattice decoding scheme is exploited into the transformed MLAN channel. Moreover, we extend the nested lattice code to the general single-input-multiple-output AWGN channel to achieve its capacity.

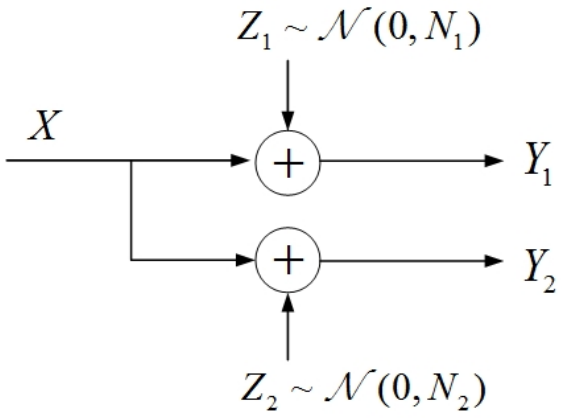

Figure 1.2: One-input-two-output AWGN channel.

1.2 Thesis Outline

The remainder of the thesis is organized as follows.

Chapter 2 presents some background information that supports this thesis. Some fundamental definitions and theorems in information theory are first introduced, e.g., the channel coding theorem and the basic tools to study the Gaussian

channel. And then the Gaussian channel is specified. Also, we give a general introduction to lattices.

In Chapter 3, we study the work in [9] which proves that lattice codes can achieve the capacity on AWGN channels. Inspired by its idea, an angle-decoding scheme for the one-input-two-output AWGN channel is proposed. Furthermore, we prove that under such decoding scheme, the capacity of the one-input-two-output AWGN channel can be achieved using lattice codes with an n-dimensional ball of radius $\sqrt{nP}$ as the boundary region.

In Chapter 4, the nested lattice code, which uses lattice encoding and decoding to preserve the structure of the underlying lattice, is investigated. Again, we employ the nested lattice code approach on the one-input-two-output AWGN channel. Moreover, the nested lattice code is extended to a general single-input-multiple-output AWGN channel and proved to be capacity achieving.

Finally, Chapter 5 concludes this thesis and points out some future work related to our research.

Chapter 2

Preliminaries

2.1 Basics of Information Theory

In this section, we introduce some basic definitions and fundamental theorems [21] developed in information theory.

2.1.1 Entropy and Mutual Information

We start with the concept of entropy, which is the measure of uncertainty of a random variable. Let X be a random variable with alphabet $\mathcal{X}$ and probability mass function $p(x) = \Pr(X = x),\ x \in \mathcal{X}$.

Definition 2.1.1 (Entropy)**.** *The entropy $H(X)$ of a discrete random variable X is defined by*

$$H(X) = -\sum_{x \in \mathcal{X}} p(x) \log p(x).$$

We can easily extend the definition of entropy to a pair of random variables since (X, Y) can be considered as a single vector-valued random variable.

Definition 2.1.2 (Joint entropy)**.** *The joint entropy $H(X, Y)$ of a pair of discrete random variables (X, Y) with a joint distribution $p(x, y)$ is defined as*

$$H(X, Y) = -\sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} p(x, y) \log p(x, y).$$

Furthermore, the conditional entropy is defined as follows.

Definition 2.1.3 (Conditional entropy)**.** *If* $(X, Y) \sim p(x, y)$*, then the conditional entropy* $H(Y|X)$ *is defined as*

$$H(Y|X) = -\sum_{x\in\mathcal{X}} p(x) \sum_{y\in\mathcal{Y}} p(y|x) \log p(y|x).$$

We now introduce mutual information, which is a measure of the amount of information that one random variable contains about another.

Let (X, Y) be a pair of random variables with a joint probability mass function $p(x, y)$ and marginal probability mass functions $p(x)$ and $p(y)$.

Definition 2.1.4 (Mutual information)**.** *The mutual information* $I(X;Y)$ *is defined as*

$$I(X;Y) = \sum_{x\in\mathcal{X}} \sum_{y\in\mathcal{Y}} p(x, y) \log \frac{p(x, y)}{p(x)p(y)}.$$

We can rewrite the mutual information $I(X;Y)$ as

$$I(X;Y) = H(X) - H(X|Y) = H(Y) - H(Y|X).$$

Thus, the mutual information $I(X;Y)$ is the reduction of the uncertainty of one random variable due to the knowledge of the other.

2.1.2 Channel Capacity

One of the most fundamental goals in information theory is to find the highest communication rate at which information can be transmitted with arbitrarily low probability of error. Shannon's channel coding theorem [1] answers this question for single user channels. Before we state the channel coding theorem, first we need the following definitions to obtain a better understanding of a communication system.

Definition 2.1.5. *A discrete channel, denoted by $(\mathcal{X}, p(y|x), \mathcal{Y})$, consists of two finite sets $\mathcal{X}$ and $\mathcal{Y}$ and a collection of probability mass functions $p(y|x)$, one for each $x \in \mathcal{X}$, such that for every x and y, $p(y|x) \geq 0$, and for every x, $\sum_y p(y|x) = 1$, with the interpretation that X is the input and Y is the output of the channel. The channel is said to be memoryless if the probability distribution of the output depends only on the input at that time and is conditionally independent of previous channel inputs or outputs.*

Definition 2.1.6. *The n-th extension of the discrete memoryless channel (DMC) is the channel $(\mathcal{X}^n, p(y^n|x^n), \mathcal{Y}^n)$, where*

$$p(y_k|x^k, y^{k-1}) = p(y_k|x_k), \ k = 1, 2, ..., n.$$

If the channel is used without feedback, then the channel transition function reduces to

$$p(y^n|x^n) = \prod_{i=1}^{n} (y_i|x_i).$$

Definition 2.1.7. *An (M, n) code for the channel $(\mathcal{X}, p(y|x), \mathcal{Y})$ consists of the following:*

1. *An index set $\{1, 2, \ldots, M\}$.*
2. *An encoding function $X^n : \{1, 2, \ldots, M\} \to \mathcal{X}^n$, yielding codewords*

$$X^n(1), X^n(2), \ldots, X^n(M).$$

The set of codewords is called the codebook.

3. *A decoding function $g : \mathcal{Y}^n \to \{1, 2, \ldots, M\}$, which is a deterministic rule which assigns a guess to each possible received vector.*

A DMC channel is illustrated in Figure 2.1, where message W is encoded into an n-bits codeword X^n, and after channel, X^n is mapped to Y^n. The decoder decodes W as $\hat{W}$ based on its observation Y^n.

Definition 2.1.8 (Probability of error)**.** *Let*

$$\lambda_i = \Pr(g(Y^n) \neq i | X^n = X^n(i)) = \sum_{y^n : g(y^n) \neq i} p(y^n|x^n(i))$$

be the conditional probability of error given that index i was sent. The maximal probability of error $\lambda^{(n)}$ for an (M, n) code is defined as

$$\lambda^{(n)} = \max_{i \in \{1,2,\ldots,M\}} \lambda_i.$$

The average probability of error $P_e^{(n)}$ for an (M, n) code is defined as

$$P_e^{(n)} = \frac{1}{M} \sum_{i=1}^{M} \lambda_i.$$

Definition 2.1.9. *The rate R of an (M, n) code is*

$$R = \frac{\log M}{n} \quad \textit{bits per transmission.}$$

Definition 2.1.10 (Achievable rate and capacity)**.** *A rate R is said to be achievable if there exists an sequence of $(2^{nR}, n)$ codes such that the maximal probability of error $\lambda^{(n)}$ tends to 0 as $n \to \infty$. The capacity of a discrete memoryless channel is the supermum of all achievable rates.*

We now formally state Shannon's channel coding theorem.

Theorem 2.1.1 (The Channel Coding Theorem)**.** *All rates below capacity $C = \max_{p(x)} I(X;Y)$ are achievable. Specifically, for every rate $R < C$, there exists a sequence of $(2^{nR}, n)$ codes with maximum probability error $\lambda^{(n)} \to 0$. Conversely, any sequence of $(2^{nR}, n)$ codes with $\lambda^{(n)} \to 0$ must have $R \leq C$.*

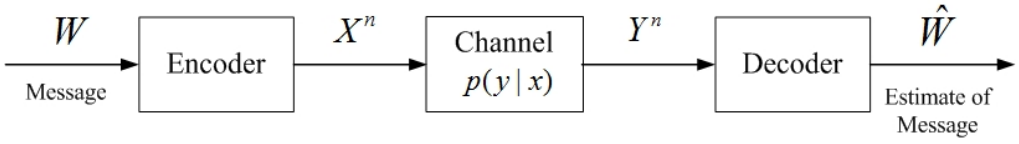

Figure 2.1: DMC channel.

2.1.3 Differential Entropy

Now we introduce the concept of differential entropy, which is the entropy of a continuous random variable.

Definition 2.1.11 (Support set of a continuous random variable)**.** *Let X be a random variable with cumulative distribution function $F(x) = Pr(X \leq x)$. If $F(x)$ is continuous, the random variable is said to be continuous. Let $f(x) = F'(x)$ when the derivative is defined. If $\int_{-\infty}^{\infty} f(x) = 1$, then $f(x)$ is called the probability density function for X. The set where $f(x) > 0$ is called the support set of X.*

Definition 2.1.12 (Differential entropy)**.** *The differential entropy $h(X)$ of a continuous random variable X with density $f(x)$ is defined as*

$$h(X) = -\int_S f(x) \log f(x) dx,$$

where S is the support set of the random variable.

As in the discrete case, we extend the definition of differential entropy of a single random variable to multiple random variables.

Definition 2.1.13 (Joint and conditional differential entropy)**.** *The differential entropy of a set of random variables $X_1, X_2, ..., X_n$ with density $f(x_1, x_2, ..., x_n)$ is defined as*

$$h(X_1, X_2, ..., X_n) = -\int f(x_1, x_2, ..., x_n) \log f(x_1, x_2, ..., x_n) dx_1 dx_2 ... dx_n.$$

If X, Y have a joint density function $f(x, y)$, we can define the conditional differential entropy $h(X|Y)$ as

$$h(X|Y) = -\int f(x, y) \log f(x|y) dx dy.$$

The following theorems will be broadly used in the studying of Gaussian Channels in the sequel.

Theorem 2.1.2 (Entropy of a multivariate normal distribution)**.** *Let $X_1, X_2, ..., X_n$ have a multivariate normal distribution with mean μ and covariance matrix K. (We use $\mathcal{N}(\mu, K)$ to denote this distribution.) Then*

$$h(X_1, X_2, ..., X_n) = \frac{1}{2} \log (2\pi e)^n |K| \quad bits,$$

where $|K|$ denotes the determinant of K.

Theorem 2.1.3. *Let the random vector* $\mathbf{X} \in \mathbb{R}^n$ *have zero mean and covariance* $K = E\mathbf{X}\mathbf{X}^t$, *i.e.,* $K_{ij} = EX_iX_j$, $1 \leq i, j \leq n$. *Then,*

$$h(\mathbf{X}) \leq \frac{1}{2}\log(2\pi e)^n|K|,$$

with equality iff $\mathbf{X} \sim \mathcal{N}(0, K)$.

2.2 The Gaussian Channel

In this section, we introduce the most important continuous alphabet channel, the Gaussian Channel, as shown in Fig. 1.1. This is a time discrete channel with output Y_i at time i, where Y_i is the sum of the inputX_i and noise Z_i. Z_i is independent of X_i and is drawn i.i.d from a Gaussian distribution with variance N. Thus, the channel can be expressed as

$$Y = X + Z, \quad Z \sim \mathcal{N}(0, N). \tag{2.1}$$

We assume an average power constraint on the input X. For any codeword $(x_1, x_2, ..., x_n)$ transmitted over the channel, we require

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

Definition 2.2.1 (Capacity of Gaussian channel)**.** *The information capacity of the Gaussian Channel with power constraint* P *is*

$$C = \max_{p(x):EX^2 \leq P} I(X;Y). \tag{2.2}$$

We can calculate the information capacity as follows,

$$\begin{aligned} I(X;Y) &= h(Y) - h(Y|X) \\ &= h(Y) - h(X+Z|X) \\ &= h(Y) - h(Z). \end{aligned} \tag{2.3}$$

(2.3) follows since Z is independent of X.

Now, with

$$h(Z) = \frac{1}{2}\log 2\pi eN$$

and

$$EY^2 = E(X+Z)^2 \leq P + N,$$

by Theorem. 2.1.3, we have

$$\begin{aligned} I(X;Y) &= h(Y) - h(Z) \\ &\leq \frac{1}{2}\log 2\pi e(P+N) - \frac{1}{2}\log 2\pi eN \\ &= \frac{1}{2}\log(1+\frac{P}{N}). \end{aligned}$$

Hence, the capacity of the Gaussian channel is

$$C = \max_{p(x):EX^2\leq P} I(X;Y) = \frac{1}{2}\log(1+\frac{P}{N}),$$

where the maximum is attained when $X \sim \mathcal{N}(0,P)$. As a result, we have the following theorem.

Theorem 2.2.1. *The capacity of a Gaussian channel with power constraint P and noise variance N is*

$$C = \frac{1}{2}\log(1+\frac{P}{N}) \quad \textit{bits per transmission.} \tag{2.4}$$

An (M,n) code and the achievable rate of the Gaussian channel are defined similarly with the discrete case as follows.

Definition 2.2.2. *An (M,n) code for the Gaussian channel with power constraint P consists of the following:*

1. An index set $\{1,2,\ldots,M\}$.

2. An encoding function $x:\{1,2,\ldots,M\} \to \mathcal{X}^n$, yielding codewords $x^n(1), x^n(2), \ldots, x^n(M)$, satisfying the power constraint P, i.e., for every codeword

$$\sum_{i=1}^{n} x_i^2(w) \leq nP, \quad w = 1,2,...,M.$$

3. A decoding function

$$g : \mathcal{Y}^n \to \{1, 2, \ldots, M\}.$$

Definition 2.2.3. *A rate R is said to be achievable for a Gaussian channel with a power constraint P if there exists a sequence of $(2^{nR}, n)$ codes with codewords satisfying the power constraint such that the maximal probability of error tends to zero. The capacity of the channel is the supremum of the achievable rates.*

2.3 Lattices: Definitions and Figures of Merit

Lattices are related to several geometric problems such as sphere packing, sphere covering and the kissing number problems, as well as other areas of mathematics like number theory and combinatorics. Outside mathematics, the main application of lattices is in engineering, and specifically in channel coding. In the recent years, interesting links were found between lattices and coding schemes for multi-terminal networks. Lattice codes form effective arrangements of points in space for coding problems, e.g., quantization and signaling for the AWGN channel [24], [10]. Good lattices tend to be "perfect" in all aspects as the dimension goes to infinity. In this section, we will introduce some basic definitions and main figures of merit of lattices for the further study of lattices in the area of Gaussian network information theory.

Definition 2.3.1. *An n-dimensional lattice Λ is defined by a set of n basis vectors $\mathbf{g}_1, \mathbf{g}_2, ..., \mathbf{g}_n \in \mathbb{R}^n$. The lattice Λ is composed of all integral combinations of the basis vectors, i.e.,*

$$\Lambda = \{\lambda = G \cdot \mathbf{i} : \mathbf{i} \in \mathbb{Z}^n\},$$

where $\mathbb{Z} = \{0, \pm 1, \pm 2, ...\}$ and the $n \times n$ generator matrix G is given by $G = [\mathbf{g}_1, \mathbf{g}, ..., \mathbf{g}_n]$.

Definition 2.3.2 (Nearest neighbor quantizer and Voronoi region [5])**.** *The nearest neighbor quantizer $Q(\cdot)$ associated with Λ is defined by*

$$Q(\mathbf{x}) = \lambda \in \Lambda, \quad \text{if } \|\mathbf{x} - \lambda\| \leq \|\mathbf{x} - \lambda'\| \ \ \forall \lambda' \in \Lambda,$$

where $\|\cdot\|$ denotes Euclidean norm. The basic Voronoi region associates with $\lambda \in \Lambda$, denoted by $\mathcal{V}_0$, is a set of points in $\mathbb{R}^n$ closest to the zero codeword, i.e.,

$$\mathcal{V}_0 = \{\mathbf{x} : Q(\mathbf{x}) = 0\}.$$

The Voronoi region associated with each $\lambda \in \Lambda$ is the set of points $\mathbf{x}$ such that $Q(\mathbf{x}) = \lambda$ and it is given by a shift of $\mathcal{V}_0$ by λ.

According to the definition of Voronoi region, every $\mathbf{x} \in \mathbb{R}^n$ can be uniquely expressed as

$$\mathbf{x} = \lambda + r,$$

with $\lambda \in \Lambda$, $r \in \mathcal{V}$.

Definition 2.3.3 (Modulo lattice operation)**.** *The modulo lattice operation with respect to a lattice Λ is defined as,*

$$x \mod \Lambda = x - Q(x).$$

It will prove useful to consider more general fundamental regions and quantizers for a lattice Λ.

Definition 2.3.4. *Let Ω be any fundamental region of Λ, i.e., every $\mathbf{x} \in \mathbb{R}^n$ can be uniquely written as $x = \lambda + e$ where $\lambda \in \Lambda$, $e \in \Omega$ and $\mathbb{R}^n = \Lambda + \Omega$. We correspondingly define the quantizer associated with Ω by*

$$Q_\Omega(\mathbf{x}) = \lambda, \quad \textit{if } \mathbf{x} \in \lambda + \Omega.$$

Following, we introduce some important parameters to measure a lattice Λ .

Definition 2.3.5 (Second moment of a lattice)**.** *The second moment σ_Λ^2 associated with Ω of a lattice is defined as*

$$\sigma_\Lambda^2 = \frac{1}{n} E\|\mathbf{U}\|^2 = \frac{1}{n} \frac{\int_\Omega \|\mathbf{x}\|^2 d\mathbf{x}}{V}$$

where U is a random vector uniformly distributed over Ω and $V \triangleq V(\Lambda) = |\Omega|$.

For a fixed lattice, σ_Λ^2 is minimized if Ω is chosen as the Voronoi region $\mathcal{V}$.

A figure of merit of a lattice quantizer with respect to the Mean-square error distortion measure is the normalized second moment defined as follows.

Definition 2.3.6 (Normalized seconde moment)**.** *The normalized second moment of* Λ *is defined as*

$$G(\Lambda) \triangleq \frac{\sigma_\Lambda^2}{V^{2/n}} = \frac{1}{n}\frac{\int_\mathcal{V} \|\mathbf{x}\|^2 d\mathbf{x}}{V^{1+2/n}}. \tag{2.5}$$

The minimum possible value of $G(\Lambda_n)$ over all lattices in R^n is denoted by G_n. It is well known that

$$G_n \geq G_n^* > \frac{1}{2\pi e}$$

where G_n^* is the normalized second moment of an n-dimensional sphere and $\frac{1}{2\pi e}$ is the normalized seconde moment of an infinite-dimensional sphere. A result in [11] states that there exists a sequence of lattices Λ_n with

$$\lim_{n\to\infty} G_n = \frac{1}{2\pi e},$$

i.e., there exists a sequence of "good" lattices Λ_n^* whose Voronoi region $\mathcal{V}$ approaches a sphere in the sense that $G(\Lambda_n^*) = G_n \to G_n^* \to \frac{1}{2\pi e}$ as $n \to \infty$. We say that such lattices are good for quantization [12].

Chapter 3

A Geometric Approach to the Capacity of AWGN Channels Using Lattice Codes

Reconsider the following AWGN channel with power constraint P,

$$Y = X + Z, \quad Z \sim \mathcal{N}(0, N).$$

As mentioned in the previous chapter, the capacity of this channel is $C = \frac{1}{2}\log(1 + \frac{P}{N})$. However, from a classical information theoretic perspective, the achievability of the capacity is based on a random coding argument, hence, the capacity achieving codebooks may exhibit little or no structure, making them ill-suited for practical applications. This inspires the investigation into the maximal reliable transmission rates achievable by structured codes, in other words, the search for low-complexity, structured codes with rates approaching capacity for the AWGN channel.

An important class of structured codes is the class of lattice codes. In [9], the authors proved that lattice codes with spherical bounding region can achieve the channel capacity of AWGN channels from a geometric approach. In this chapter, we will first introduce the work in [9] and then modify and extend it to the AWGN

channel with one input and two outputs.

3.1 Lattice Codes Can Achieve Capacity on the Single-Input-Single-Output AWGN Channel

A lattice code $\mathcal{C}_n$ is defined as the intersection of an (possibly translated) n-dimensional lattice Λ_n with a region $\mathcal{B}_n$ of bounded support.

The main result in [9] is summarized by the following theorem.

Theorem 3.1.1. *Let P, N and $\epsilon > 0$ be given. If*

$$R < \frac{1}{2}\log(1 + \frac{P}{N})$$

then there exists a lattice code $\mathcal{C}_n$ for the AWGN channel with power constraint P and noise variance N, where $\mathcal{B}_n$ is the n-dimensional ball of radius $\sqrt{nP}$, such that $\mathcal{C}_n$ has rate lower-bounded by R and average probability of error of a minimum-distance decoder upper-bounded by ϵ.

For the consistency of our work on the extension to the one-input-two-output AWGN channel, here the proof of the above theorem is outlined.

Let P be the signal power constraint per dimension and N be the noise variance. R is given such that

$$R < \frac{1}{2}\log(1 + \frac{P}{N}).$$

There exist R' and P' such that

$$R < R' < \frac{1}{2}\log(1 + \frac{P'}{N}) < \frac{1}{2}\log(1 + \frac{P}{N}).$$

Let T_n be the n-dimensional ball of radius $\sqrt{nP}$ and volume

$$V_n = \frac{(\pi nP)^{\frac{n}{2}}}{\Gamma(n/2+1)}\ , \tag{3.1}$$

where $\Gamma(x)$ is the well-known Gamma function. For $P' < P$, let T'_n be the n-dimensional ball of radius $\sqrt{nP'}$ and volume

$$V'_n = \frac{(\pi n P')^{\frac{n}{2}}}{\Gamma(n/2+1)}. \tag{3.2}$$

Further, define $T_n^{\triangle} = T_n \backslash T'_n$ with volume $V_n^{\triangle} = V_n - V'_n$.

Given a lattice Λ_n with fundamental region Ω_n and $s \in \Omega_n$, define the lattice code

$$\mathcal{C}_n = (\Lambda_n + s) \cap T_n$$

and the subcodes

$$\mathcal{C}'_n = (\Lambda_n + s) \cap T'_n,$$

$$\mathcal{C}_n^{\triangle} = (\Lambda_n + s) \cap T_n^{\triangle}.$$

Let $M_n = M_n(\Lambda_n, s)$, $M'_n = M'_n(\Lambda_n, s)$ and $M_n^{\triangle} = M_n^{\triangle}(\Lambda_n, s)$ be the cardinalities of these codes respectively.

For an arbitrary code $\mathcal{C}$, let $P^{\mathcal{C}}$ denote the average probability of error under minimum-distance decoding. Let $\pi : \mathbb{R}^n \backslash \{0\} \to \partial T'_n$ be the mapping defined by $\pi(x) = (\sqrt{nP'}/\|x\|)x$. The mapping radially projects a nonzero point onto the sphere of radius $\sqrt{nP'}$. Then we have the following lemmas.

Lemma 3.1.1.

$$P^{\mathcal{C}_n} \leq \frac{M'_n}{M_n} + P^{\mathcal{C}_n^{\triangle}}.$$

Lemma 3.1.2.

$$P^{\mathcal{C}_n^{\triangle}} \leq P^{\pi(\mathcal{C}_n^{\triangle})}.$$

Combining Lemma 3.1.1 and Lemma 3.1.2, we get

$$P^{\mathcal{C}_n} \leq \frac{M'_n}{M_n} + P^{\pi(\mathcal{C}_n^{\triangle})}. \tag{3.3}$$

Next, we will bound $P^{\pi(\mathcal{C}_n^{\triangle})}$ by defining a suitable suboptimum decoder.

For $y \in \mathbb{R}^n$ and $0 < \theta < \frac{\pi}{2}$, let $B_\theta(y)$ be the n-dimensional closed circular cone with apex at 0, axis passing through y and half angle θ. For each $x \in \pi(\mathcal{C}_n^\triangle)$ the associated decoding region $A_\theta(x)$ is defined as

$$A_\theta(x) = B_\theta(x) \setminus \bigcup_{x' \in \pi(\mathcal{C}_n^\triangle)\setminus\{x\}} B_\theta(x'). \tag{3.4}$$

In words, the decoding region of a codeword consists of those parts of its associated cone which do not overlap with any cone associated to another codeword. Note that

$$A_\theta^c(x) = B_\theta^c(x) \bigcup_{x' \in \pi(\mathcal{C}_n^\triangle)\setminus\{x\}} B_\theta(x').$$

Let $P_\theta^{\pi(\mathcal{C}_n^\triangle)}$ denote the probability of error for the proposed suboptimum decoder and $x_0 = (\sqrt{nP'}, 0, ..., 0)$. For any $x \in \mathcal{C}_n^\triangle$, we have

$$\begin{aligned}
P_\theta^{\pi(\mathcal{C}_n^\triangle)} &= Pr(\pi(x) + Z \in A_\theta^c(\pi(x))) \\
&\leq Pr(\pi(x) + Z \in B_\theta^c(\pi(x))) + \sum_{x' \in \mathcal{C}_n^\triangle \setminus \{x\}} Pr(\pi(x) + Z \in B_\theta(\pi(x'))) \\
&= Pr(x_0 + Z \notin B_\theta(x_0)) + \sum_{x' \in \mathcal{C}_n^\triangle \setminus \{x\}} Pr(\pi(x) + Z \in B_\theta(\pi(x'))) \\
&= Pr(x_0 + Z \notin B_\theta(x_0)) + \sum_{x' \in \mathcal{C}_n^\triangle \setminus \{x\}} Pr(\pi(x') + Z \in B_\theta(\pi(x))) \\
&= Pr(x_0 + Z \notin B_\theta(x_0)) + \sum_{x' \in \mathcal{C}_n^\triangle \setminus \{x\}} p_\theta(x, x') \\
&= Pr(x_0 + Z \notin B_\theta(x_0)) + \sum_{g \in \Lambda_n \setminus \{0\}} p_\theta(g + x, x) \mathcal{X}_{T_n^\triangle}(g + x),
\end{aligned} \tag{3.5}$$

where

$$p_\theta(x, x') := Pr(\pi(x') + Z \in B_\theta(\pi(x)))$$

and

$$\mathcal{X}_{T_n^\triangle}(x) = \begin{cases} 1, & \text{if } x \in T_n^\triangle \\ 0, & \text{if } x \notin T_n^\triangle. \end{cases}$$

Lemma 3.1.3. *Given $d_n \in \mathbb{R}^+$ there exists a lattice Λ_n^* with determinant $det(\Lambda_n^*) = d_n$ and an $s^* \in P_n^*$ such that*

$$\frac{1}{M_n^{\triangle}(\Lambda_n^*, s^*)} \sum_x \in \mathcal{C}_n^{\triangle}(\Lambda_n^*, s^*) \sum_{g \in \Lambda_n \setminus \{0\}} p_\theta(g+x, x) \mathcal{X}_{T_n^{\triangle}}(g+x)$$
$$\leq \frac{2\sqrt{nP}(n-1)\pi^{n-1/2}(nP')^{n/2}}{d_n \Gamma(\frac{n+1}{2})} \int_0^\theta (\sin x)^{n-2} dx.$$

Moreover, s^* can be chosen in such a way that

$$\frac{M_n'(\Lambda_n^*, s^*)}{M_n^(\Lambda_n^*, s^*)} \leq 4 \frac{V_n'}{V_n}$$

and

$$M_n^{\triangle}(\Lambda_n^*, s^*) \geq \frac{V_n^{\triangle}}{4 d_n}.$$

Applying Lemma 3.1.3 and (3.5) to (3.3), we get

$$\begin{aligned}
P^{\mathcal{C}_n(\Lambda_n^*, s^*)} &\leq \frac{M_n'(\Lambda_n^*, s^*)}{M_n^(\Lambda_n^*, s^*)} + \frac{1}{M_n^{\triangle}} \sum_{x \in \mathcal{C}_n^{\triangle}(\Lambda_n^*, s^*)} P^{\pi(\mathcal{C}_n^{\triangle}(\Lambda_n^*, s^*))}(\pi(x)) \\
&\leq \frac{M_n'(\Lambda_n^*, s^*)}{M_n^(\Lambda_n^*, s^*)} + \frac{1}{M_n^{\triangle}} \sum_{x \in \mathcal{C}_n^{\triangle}(\Lambda_n^*, s^*)} P_\theta^{\pi(\mathcal{C}_n^{\triangle}(\Lambda_n^*, s^*))}(\pi(x)) \\
&\leq \frac{M_n'(\Lambda_n^*, s^*)}{M_n^(\Lambda_n^*, s^*)} + Pr(x_0 + Z \notin B_\theta(x_0)) \\
&+ \frac{1}{M_n^{\triangle}(\Lambda_n^*, s^*)} \sum_x \in \mathcal{C}_n^{\triangle}(\Lambda_n^*, s^*) \sum_{g \in \Lambda_n \setminus \{0\}} p_\theta(g+x, x) \mathcal{X}_{T_n^{\triangle}}(g+x) \\
&\leq 4 \frac{V_n'}{V_n} + Pr(x_0 + Z \notin B_\theta(x_0)) + \frac{2\sqrt{nP}(n-1)\pi^{n-1/2}(nP')^{n/2}}{d_n \Gamma(\frac{n+1}{2})} \int_0^\theta (\sin x)^{n-2} dx.
\end{aligned} \tag{3.6}$$

Choose $d_n = 2^{-nR'} V_n^{\triangle}$, then the rate $\frac{1}{n} \log M_n(\Lambda_n^*, s^*)$ is lower bounded by

$$\begin{aligned}
\frac{1}{n} \log M_n(\Lambda_n^*, s^*) &\geq \frac{1}{n} \log M_n^{\triangle}(\Lambda_n^*, s^*) \\
&\geq \frac{1}{n} \log \frac{V_n^{\triangle}}{4 d_n} \\
&= \frac{1}{n} \log 2^{nR'-2} \\
&= R' - \frac{2}{n}
\end{aligned}$$

$$> R - \frac{2}{n}.$$

To upper bound the average probability of error $P^{\mathcal{C}_n(\Lambda_n^*, s^*)}$, we let $\sin\theta = 2^{-R'}$, then the last term on the right side of (3.6) can be also bounded to zero as $n \to \infty$. And by Lemma 3.2.2 in Section 3.2.3, it follows that

$$Pr(x_0 + Z \notin B_\theta(x_0)) \to 0$$

as $n \to \infty$. This proves Theorem 3.1.1.

Here we give an interpretation of the proof above. Although the decoding region is defined as

$$A_\theta(x) = B_\theta(x) \backslash \bigcup_{x' \in \pi(\mathcal{C}_n^\triangle) \backslash \{x\}} B_\theta(x')$$

for each $x \in \pi(\mathcal{C}_n^\triangle)$, as $n \to \infty$, by letting $\sin\theta = 2^{-R'}$, we have

$$\sum_{x' \in \mathcal{C}_n^\triangle \backslash \{x\}} Pr(\pi(x) + Z \in B_\theta(\pi(x'))) \to 0,$$

that is, with θ properly set, $B_\theta(x)$ tends to be non-overlapping as the dimension n goes to infinity, i.e., $A_\theta(x) \to B_\theta(x)$ as $n \to \infty$. Consequently, codewords $x \in \pi(\mathcal{C}_n^\triangle)$ are separated well enough that after the channel, the received signal is still closest to the transmitted one. And the minimum distance between any two codewords becomes $2\sqrt{nP'} \cdot \sin\theta$ and approaches $2\sqrt{\frac{NP}{P+N}}$ when we let $R' \to R$ and $P' \to P$ to achieve the channel capacity as $n \to \infty$.

Inspired by this interpretation, in the following section, we apply lattice codes to a more complex case, the one-input-two-output AWGN channel, and prove that lattice codes can achieve the capacity of this channel from a geometric approach.

3.2 An Extension to the One-Input-Two-Output AWGN Channel

We consider the following Gaussian channel with one input X and two outputs Y_1 and Y_2 as depicted in Fig.1.2.

$$\begin{cases} Y_1 = X + Z_1, \\ Y_2 = X + Z_2. \end{cases} \tag{3.7}$$

where $Z_1 \sim \mathcal{N}(0, N_1)$ and $Z_2 \sim \mathcal{N}(0, N_2)$. The receiver decodes jointly with Y_1 and Y_2.

3.2.1 Channel Capacity

For the above AWGN channel, let $X \sim \mathcal{N}(0, P)$ to achieve the channel capacity. Accordingly, Y_1 and Y_2 are both normally distributed with mean 0 and variance $P + N_1$, $P + N_2$ respectively. Furthermore, the vector (Y_1, Y_2) has a multivariate normal distribution, since any linear combination of its components has a univariate normal distribution. We denote

$$(Y_1, Y_2) \sim \mathcal{N}(\mu_Y, K_Y),$$

where

$$\mu_Y = (EY_1, EY_2) = (0, 0)$$

is the mean vector, and K_Y is the covariance matrix with value

$$K_Y = \begin{pmatrix} \sigma_{Y_1}^2 & \rho_{Y_1,Y_2}\sigma_{Y_1}\sigma_{Y_2} \\ \rho_{Y_2,Y_1}\sigma_{Y_2}\sigma_{Y_1} & \sigma_{Y_2}^2 \end{pmatrix}.$$

ρ_{Y_1,Y_2} is the correlation between Y_1 and Y_2, defined as

$$\rho_{Y_1,Y_2} = \frac{E(Y_1 - \mu_{Y_1})E(Y_2 - \mu_{Y_2})}{\sigma_{Y_1}\sigma_{Y_2}}.$$

Thus,

$$\begin{aligned}\rho_{Y_1,Y_2} &= \frac{E(Y_1Y_2 - \mu_{Y_1}Y_2 - Y_1\mu_{Y_2} + \mu_{Y_1}\mu_{Y_2})}{\sigma_{Y_1}\sigma_{Y_2}} \qquad (3.8)\\ &= \frac{EY_1Y_2}{\sigma_{Y_1}\sigma_{Y_2}} \\ &= \frac{E(X+Z_1)(X+Z_2)}{\sigma_{Y_1}\sigma_{Y_2}} \\ &= \frac{EX^2 + EXEZ_1 + EXEZ_2 + EZ_1EZ_2}{\sigma_{Y_1}\sigma_{Y_2}} \\ &= \frac{P}{\sqrt{(P+N_1)(P+N_2)}}. \qquad (3.9)\end{aligned}$$

And

$$K_Y = \begin{pmatrix} P+N_1 & P \\ P & P+N_2 \end{pmatrix}.$$

Similarly, $(Z_1, Z_2) \sim \mathcal{N}(\mu_Z, K_Z)$, where

$$\mu_Z = (0,0)$$

and

$$K_Z = \begin{pmatrix} N_1 & 0 \\ 0 & N_2 \end{pmatrix}.$$

Therefore, the channel capacity is

$$\begin{aligned}I(X;Y_1,Y_2) &= h(Y_1,Y_2) - h(Y_1,Y_2|X) \\ &= h(Y_1,Y_2) - h(Z_1,Z_2) \\ &= \frac{1}{2}\log(2\pi\mathrm{e})^2|K_Y| - \frac{1}{2}\log(2\pi\mathrm{e})^2|K_Z| \\ &= \frac{1}{2}\log\frac{|K_Y|}{|K_Z|} \\ &= \frac{1}{2}\log\frac{(P+N_1)(P+N_2)-P^2}{N_1N_2} \\ &= \frac{1}{2}\log(1+\frac{P(N_1+N_2)}{N_1N_2}) \\ &= \frac{1}{2}\log(1+\frac{P}{\frac{N_1N_2}{N_1+N_2}}). \qquad (3.10)\end{aligned}$$

We can interpret such channel as a single-input-single-output AWGN channel with noise $N \sim \mathcal{N}(0, \frac{N_1N_2}{N_1+N_2})$.

3.2.2 Basics of Spherical Trigonometry

Before we move to the proof of the achievability of capacity on the one-input-two-output AWGN channel using lattice codes, we give a brief introduction to some basic definitions and theorems in spherical trigonometry [23], which will support our proof in the sequel.

Definition 3.2.1 (Circle and great circle)**.** *If a plane cuts a sphere, its intersection is a circle. Circles whose centers coincide with the center of the sphere are great circles.*

Definition 3.2.2 (Arc and spherical triangle)**.** *As with a line segment in a plane, an arc of a great circle (subtending less than* $180°$*)on a sphere is the shortest path lying on the sphere between its two endpoints.*
When the arcs of three great circles intersect on the surface of a sphere, the lines enclose an area known as a spherical triangle.

As their name implies, the great circles are the largest circles of intersection one can obtain by passing a straight plane through a sphere. To measure an arc on the great circle and the relationship between two arcs, respectively, we use central angle and spherical angle defined as follows.

Definition 3.2.3 (Central angle)**.** *A central angle is an angle whose vertex is the center of a circle, and whose sides pass through a pair of points on the circle, thereby subtending an arc between those two points whose angle is (by definition) equal to the central angle itself.*

Definition 3.2.4 (Spherical angle)**.** *A spherical angle is the angle formed by the intersection of the arcs of two great circles. If we draw tangents to the arcs at their point of intersection, than the angle formed by the two tangents is said to be the measure of the spherical angle.*

For example, in Fig.3.1, arcs $\widehat{ABC}$ and $\widehat{ADC}$ form the spherical angle $\angle A$ and $\angle C$. If we draw the tangents to the arcs $\widehat{ABC}$ and $\widehat{ADC}$ at C, then $\angle QCP$ is

said to be the measure of the spherical angle $\angle C$. And arc $\widehat{BD}$ is measured by its central angle $\angle BOD$.

We point out that a spherical triangle is specified as usual by its spherical angles and its sides, and the sides are given not by their lengths, but by their central angles.

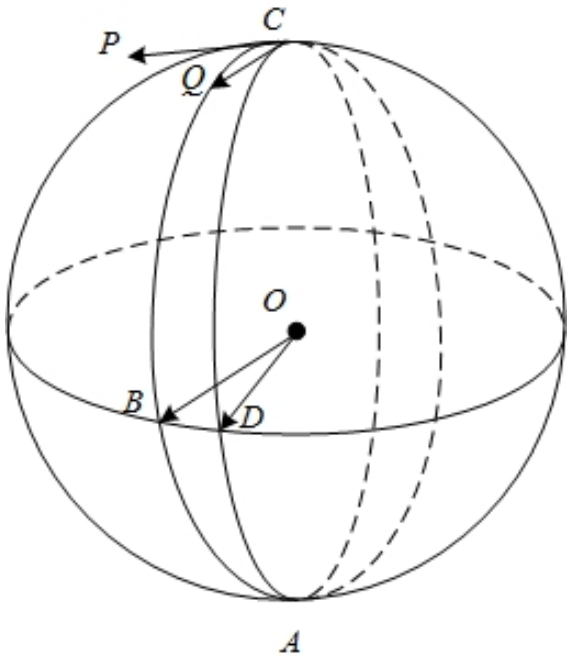

Figure 3.1: Spherical angle and its measure.

Given a spherical triangle, we can utilize the Law of Sines and the Law of Cosines to calculate its unknown angles.

Theorem 3.2.1 (Law of Sines and Law of Cosines)**.** *Given a spherical triangle $\triangle ABC$ as shown in Fig. 3.2, with central angles a, b and c associated with arcs BC, AC and AB respectively. By the Law of Sines, we have*

$$\frac{\sin a}{\sin A} = \frac{\sin b}{\sin B} = \frac{\sin c}{\sin C}.$$

And by the Law of Cosines,

$$\cos a = \cos b \cos c + \sin b \sin c \cos A.$$

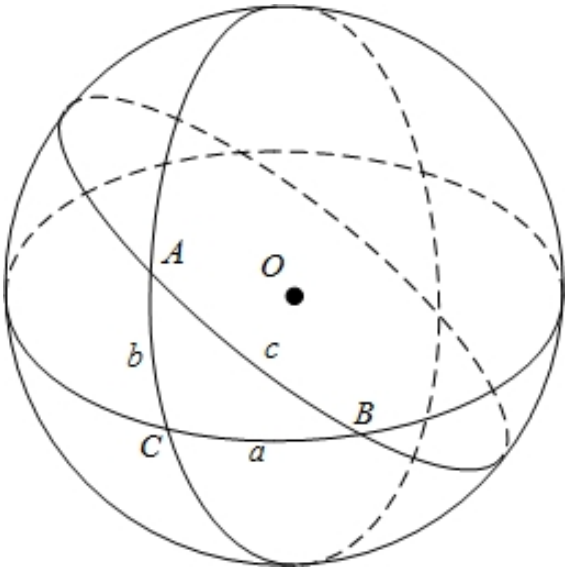

Figure 3.2: Spherical triangle.

3.2.3 Achievability of the Channel Capacity

For the one-input-two-output AWGN channel with power constraint P, each codeword x of an n-dimensional lattice code must satisfy

$$\|x\| \leq nP,$$

where $\|\cdot\|$ is the Euclidean norm. Still, the signal space is set as an n-dimensional ball of radius $\sqrt{nP}$.

T_n, T'_n, V_n, V'_n, $T_n^{\triangle}$, $\mathcal{C}_n$, $\mathcal{C}'_n$, $\mathcal{C}_n^{\triangle}$, $M_n, M'_n, M_n^{\triangle}$ are defined in the same way as in Section 3.1 for some $P' < P$. Specifically, for an arbitrary code $\mathcal{C}$, let $P^{\mathcal{C}}$ denote the average probability of error under an angle-decoding scheme defined as follows.

For $y \in \mathbb{R}^n$ and $0 < \theta < \frac{\pi}{2}$, let $B_\theta(y)$ be the n-dimensional closed circular cone with apex at 0, axis passing through y and half angle θ. Upon receiving y_1 and y_2, the decoding area is defined as

$$A_{\theta_1,\theta_2}(y_1, y_2) = B_{\theta_1}(y_1) \cap B_{\theta_2}(y_2) \cap T_n^{\triangle}, \tag{3.11}$$

where θ_1 and θ_2 will be determined later. If there is one and only one codeword x' in $A_{\theta_1,\theta_2}(y_1, y_2)$, we decodes the transmitted signal x as x'. Otherwise, an error is claimed.

Lemma 3.2.1.

$$P^{\mathcal{C}_n} \leq \frac{M'_n}{M_n} + P^{\mathcal{C}_n^{\triangle}}.$$

Proof.

$$\begin{aligned}
P^{\mathcal{C}_n} &= \frac{1}{M_n} \sum_{x \in \mathcal{C}_n} P^{\mathcal{C}_n}(x) \\
&= \frac{1}{M_n} \sum_{x \in \mathcal{C}'_n} P^{\mathcal{C}_n}(x) + \frac{1}{M_n} \sum_{x \in \mathcal{C}_n^{\triangle}} P^{\mathcal{C}_n}(x) \\
&= \frac{M'_n}{M_n} + \frac{1}{M_n} \sum_{x \in \mathcal{C}_n^{\triangle}} P^{\mathcal{C}_n}(x) \\
&\leq \frac{M'_n}{M_n} + \frac{1}{M_n^{\triangle}} \sum_{x \in \mathcal{C}_n^{\triangle}} P^{\mathcal{C}_n}(x) \\
&= \frac{M'_n}{M_n} + P^{\mathcal{C}_n^{\triangle}}.
\end{aligned}$$

□

By Lemma 3.1.3, for any $\epsilon > 0$, there exists a sufficiently large n, such that

$$\begin{aligned}
\frac{M'_n}{M_n} &\leq \frac{4V'_n}{V_n} \\
&= 4\frac{(\pi n P')^{\frac{n}{2}}}{\Gamma(n/2+1)} \Big/ \frac{(\pi n P)^{\frac{n}{2}}}{\Gamma(n/2+1)} \\
&= 4(\frac{P'}{P})^{\frac{n}{2}} \\
&\leq \epsilon.
\end{aligned}$$

Thus, to upper bound the average probability of error $P^{\mathcal{C}_n}$, now we only need to consider the codewords in the n-dimensional sphere shell $T_n^{\triangle}$, that is the sub-codebook $\mathcal{C}_n^{\triangle}$.

Suppose codeword $x \in \mathcal{C}_n^{\triangle}$ is transmitted, the decoder receives y_1 and y_2. The premiss of successful decoding is that

$$x \in B_{\theta_1}(y_1) \quad \text{and} \quad x \in B_{\theta_2}(y_2),$$

$$\text{i.e.,} \quad x \in A_{\theta_1,\theta_2}(y_1, y_2).$$

Lemma 3.2.2. *For the following AWGN channel,*

$$Y_i = X_i + Z_i$$

where each n-dimensional codeword $x = (x_1, x_2, ..., x_n)$ *satisfies* $\|x\| = nS$ *and* $Z_i \sim \mathcal{N}(0, N)$*, we have*

$$\sin \angle(x + Z, x) \to \sqrt{\frac{N}{S+N}} \qquad as \quad n \to \infty.$$

Proof.

$$\begin{aligned} \cos \angle(x + Z, x) &= \frac{(x+Z) \cdot x}{\|x+Z\|\|x\|} \\ &= \frac{\|x\|^2 + x \cdot Z}{\|x+Z\|\|x\|} \end{aligned}$$

Since x and the Gaussian noise Z are independent, we have

$$x \perp Z, \quad \text{i.e.,} \quad x \cdot Z = 0.$$

Also,

$$\begin{aligned} E\|x+Z\|^2 &= E(x^2 + 2x \cdot Z + Z^2) \\ &= S^2 + N^2 \end{aligned}$$

Hence,

$$\begin{aligned} \cos \angle(x + Z, x) &\to \frac{S}{\sqrt{S+N}\sqrt{S}} \quad \text{as} \quad n \to \infty \\ &= \sqrt{\frac{S}{S+N}}. \end{aligned}$$

And

$$\sin \angle(x + Z, x) \to \sqrt{\frac{N}{S+N}} \quad \text{as} \quad n \to \infty.$$

□

According to the above lemma, we let $\sin\theta_1 = \sqrt{\frac{N_1}{P'+N_1}}$ and $\sin\theta_2 = \sqrt{\frac{N_2}{P'+N_2}}$ so that

$$x \in A_{\theta_1,\theta_2}(y_1, y_2)$$

with probability approaching to 1 as n goes to infinity.

As illustrated in Fig.3.3, let O be the center of T_n and $\overline{OX}, \overline{XY_1}$, and $\overline{XY_2}$ represent x, Z_1 and Z_2 respectively. θ_1', θ_2' are the angles between x and y_1, y_2. The shadowed area represents $B_{\theta_1}(y_1)$, where θ_1 is chosen slightly greater than θ_1' with high probability, so that $x \in B_{\theta_1}(y_1)$ almost surely.

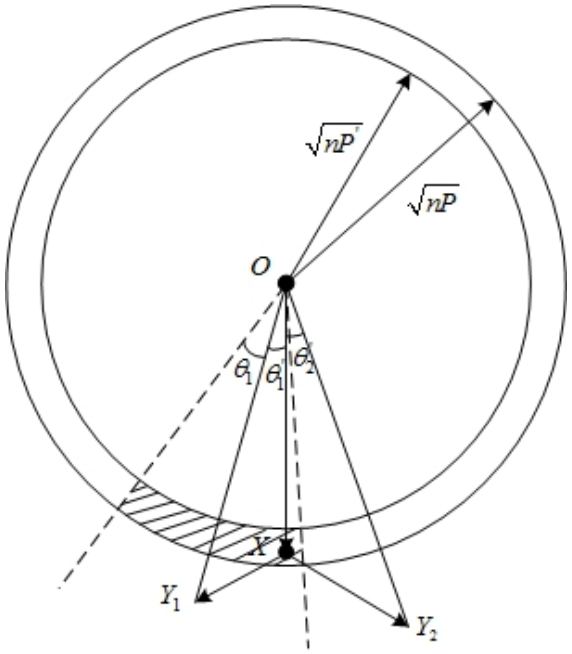

Figure 3.3: The angle-decoding scheme for the AWGN channel.

Next, we will upper bound the probability that there are other codewords besides the true codeword x lying in the decoding area $A_{\theta_1,\theta_2}(y_1, y_2)$ by properly setting the fundamental region Ω_n of the lattice Λ_n. Specifically, we will make sure that Ω_n is large enough that no two codewords can exist in $A_{\theta_1,\theta_2}(y_1, y_2)$ simultaneously .

Denote $\partial T_n(x)$ as the sphere of radius $\sqrt{nP_x}$ and center O, where $P_x = \|x\|$. First, let's look at the projection of $B_{\theta_1}(y_1)$ and $B_{\theta_2}(y_2)$ on $\partial T_n(x)$, represented by the outer circles of the two rings in Fig.3.4, while the inner circles stand for the projection of $B_{\theta_1'}(y_1)$ and $B_{\theta_2'}(y_2)$ on $\partial T_n(x)$. Hence, the shadowed part is the projection of decoding area $A_{\theta_1,\theta_2}(y_1, y_2)$ on the sphere $\partial T_n(x)$. Let the intersection points of axis OY_1 and OY_2 with $\partial T_n(x)$ be O_1 and O_2 respectively. Obviously, the edges of the projection of $B_{\theta_1'}(y_1)$ and $B_{\theta_2'}(y_2)$ on $\partial T_n(x)$ intersect at X and its symmetrical point X'. By symmetrical, we mean that X and X' are symmetrical with respect to the great circle OO_1O_2. Also, as in the *Proof of the Capacity Theorem* in [22], for any point $y \in A_{\theta_1,\theta_2}(y_1, y_2)$, y is contained in the n-dimensional ball centered at H and of radius $\frac{1}{2}XX'$ with probability approaching to 1, if we let P' arbitrarily close to P with n goes to infinity. In another word, if we set the fundamental region Ω_n of Λ_n as an n-dimensional ball of radius $\frac{1}{2}XX'$, then with high probability, no other codeword is in $A_{\theta_1,\theta_2}(y_1, y_2)$.

In the following, we will calculate XX' with the knowledge of spherical trigonometry which still holds in the n-dimensional space. All the discussion is based on the sphere $\partial T_n(x)$.

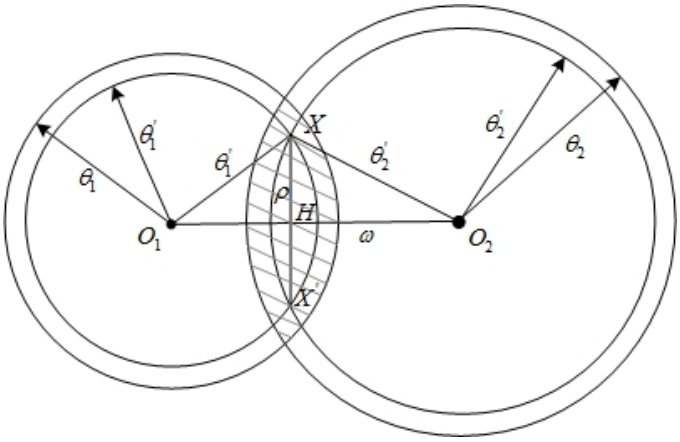

Figure 3.4: The projection of the decoding area on the sphere $\partial T_n(x)$.

In Fig.3.3, $XY_1 \perp OXY_2$, since the channel input x and the noise Z_1, Z_2 are

mutually independent, i.e., $Z_1 \perp x$ and $Z_1 \perp Z_2$.

Similarly, $XY_2 \perp OXY_1$.

Thus, $OXY_1 \perp OXY_2$. Since the great circle OO_1X and OO_2X are on the planes OXY_1 and OXY_2 respectively, we have

$$\widehat{O_1X} \perp \widehat{O_2X}.$$

Also, $XX' \perp OO_1O_2$. Therefore, $\widehat{XX'} \perp \widehat{O_1O_2}$ at point H. To sum up, $\triangle XO_1O_2$ is a right spherical triangle with height $\widehat{XH}$, and the central angles of $\widehat{O_1X}$ and $\widehat{O_2X}$ are θ_1' and θ_2' respectively, as shown in Fig.3.4. Let ρ be the central angle of $\widehat{XH}$ and ω be the central angle of $\widehat{O_1O_2}$. By the spherical Law of Sines, we have

$$\frac{\sin\theta_1'}{\sin O_2} = \frac{\sin\theta_2'}{\sin O_1} = \sin\omega,$$

and

$$\frac{\sin\theta_1'}{\sin\angle O_1HX} = \frac{\sin\rho}{\sin O_1}$$

i.e.,

$$\sin\theta_1' = \frac{\sin\rho}{\sin O_1}$$

since $\angle O_1HX = \frac{\pi}{2}$.

Thus,

$$\sin\omega = \sin\theta_2' \cdot \frac{\sin\theta_1'}{\sin\rho}. \tag{3.12}$$

Also, by the spherical Law of Cosines, we have

$$\begin{aligned}\cos\omega &= \cos\theta_1'\cos\theta_2' + \sin\theta_1'\sin\theta_2'\cos\angle O_1XO_2 \\ &= \cos\theta_1'\cos\theta_2'.\end{aligned} \tag{3.13}$$

Combining (3.12) and (3.13), we have

$$\begin{aligned}\sin^2\rho &= \frac{\sin^2\theta_1'\sin^2\theta_2'}{\sin^2\omega} \\ &= \frac{\sin^2\theta_1'\sin^2\theta_2'}{1-\cos^2\omega} \\ &= \frac{\sin^2\theta_1'\sin^2\theta_2'}{1-\cos^2\theta_1'\cos^2\theta_2'}\end{aligned} \tag{3.14}$$

As $n \to \infty$, let $P' \to P$, then

$$\sin\theta_1, \ \ \sin\theta_1' \to \sqrt{\frac{N_1}{P+N_1}}, \tag{3.15}$$

and

$$\sin\theta_2, \ \ \sin\theta_2' \to \sqrt{\frac{N_2}{P+N_2}}. \tag{3.16}$$

Inserting (3.15) and (3.16) into (3.14), we have

$$\begin{aligned}
\sin^2\rho &\to \frac{\frac{N_1}{P+N_1}\cdot\frac{N_2}{P+N_2}}{1-\frac{P}{P+N_1}\cdot\frac{P}{P+N_2}} \\
&= \frac{N_1N_2}{P(N_1+N_2)+N_1N_2} \\
&= \frac{\frac{N_1N_2}{N_1+N_2}}{P+\frac{N_1N_2}{N_1+N_2}}.
\end{aligned}$$

And

$$\begin{aligned}
\frac{1}{2}XX' &= \sqrt{nP_x}\cdot\sin\rho \\
&\to \sqrt{nP}\cdot\sqrt{\frac{\frac{N_1N_2}{N_1+N_2}}{P+\frac{N_1N_2}{N_1+N_2}}}.
\end{aligned} \tag{3.17}$$

We denote $r_n(P,N_1,N_2) = \sqrt{nP}\cdot\sqrt{\frac{\frac{N_1N_2}{N_1+N_2}}{P+\frac{N_1N_2}{N_1+N_2}}}$, and let Ω_n be the n-dimensional ball of radius $r_n(P,N_1,N_2)$. Hence, the minimum distance between any two codewords is $2r_n(P,N_1,N_2)$.

Codeword $X \in \mathcal{C}_n^{\triangle}$ is random selected and transmitted, then for any $\epsilon > 0$, under our proposed angle-decoding scheme, where θ_1 and θ_2 are set as

$$\sin\theta_1 = \sqrt{\frac{N_1}{P'+N_1}}$$

and

$$\sin\theta_2 = \sqrt{\frac{N_2}{P'+N_2}}.$$

Then the average probability of error under the proposed angle-decoding scheme can be upper bounded as,

$$\begin{aligned}
P^{\mathcal{C}_n} &\leq \frac{M'_n}{M_n} + P^{\mathcal{C}_n^{\triangle}} \\
&\leq \epsilon + P^{\mathcal{C}_n^{\triangle}} \\
&= \epsilon + P\{X \notin A_{\theta_1,\theta_2}(y_1,y_2) \text{ or } \exists X' \neq X \text{ s.t. } X, X' \in A_{\theta_1,\theta_2}(y_1,y_2)\} \\
&\leq \epsilon + P\{X \notin A_{\theta_1,\theta_2}(y_1,y_2)\} + P\{\exists X' \neq X \text{ s.t. } X, X' \in A_{\theta_1,\theta_2}(y_1,y_2)\} \\
&\leq \epsilon + P\{X \notin A_{\theta_1,\theta_2}(y_1,y_2)\} + P\{\exists X', X'' \text{ s.t. } X', X'' \in A_{\theta_1,\theta_2}(y_1,y_2)\} \quad (3.18) \\
&\leq \epsilon + \epsilon + \epsilon \\
&= 3\epsilon
\end{aligned}$$

when $P' \to P$ as $n \to \infty$, where (3.18) follows that the probability of $X, X' \in A_{\theta_1,\theta_2}(y_1,y_2)$ is less than or equal to the probability that there exist any pair of codewords (X', X'') such that $X', X'' \in A_{\theta_1,\theta_2}(y_1,y_2)$.

And with $P^{\mathcal{C}_n}$ upper bounded as $n \to \infty$, the achievable rate is

$$\begin{aligned}
R &= \frac{1}{n}\log\frac{V_n}{vol(\Omega_n)} \\
&= \frac{1}{n}\log\left(\frac{(\pi nP)^{\frac{n}{2}}}{\Gamma(n/2+1)} \Big/ \frac{(\pi r_n^2(P,N_1,N_2))^{\frac{n}{2}}}{\Gamma(n/2+1)}\right) \\
&= \frac{1}{n}\cdot\frac{n}{2}\log\frac{\pi nP}{\pi nP\cdot\frac{\frac{N_1N_2}{N_1+N_2}}{P+\frac{N_1N_2}{N_1+N_2}}} \\
&= \frac{1}{2}\log\frac{P+\frac{N_1N_2}{N_1+N_2}}{\frac{N_1N_2}{N_1+N_2}} \\
&= \frac{1}{2}\log\left(1+\frac{P}{\frac{N_1N_2}{N_1+N_2}}\right).
\end{aligned}$$

Finally, we reach the following theorem.

Theorem 3.2.2. *For the one-input-two-output AWGN channel, with any $\epsilon > 0$, there exists a sequence of n-dimensional lattice Λ_n with fundamental region Ω_n, such that its rate R defined as*

$$R = \frac{1}{n}\log\frac{vol(T_n)}{vol(\Omega_n)}$$

approaches C with the average decoding error probability P_e upper bounded by 3ϵ for sufficiently large n, where $C = \frac{1}{2}\log\left(1 + \frac{P}{\frac{N_1 N_2}{N_1+N_2}}\right)$ is channel capacity, $vol(\cdot)$ denotes the volume of an n-dimensional space, and T_n is the n-dimensional ball of radius $\sqrt{nP}$.

Chapter 4

Nested Lattice Code Approach to the Capacity of AWGN Channels

The central line of development in the application of lattices for the AWGN channel originated in the work of De Buda. De Buda's theorem [4] states that a spherical lattice code with second moment P, which is the intersection of a lattice with a sphere, can approach arbitrarily closely the AWGN channel capacity. To achieve the best error exponent of the AWGN channel, a "thin" spherical shell is taken instead of a full sphere. This result has been corrected and refined by several authors [6], [7], [8] including [9] that we exploited in the last chapter.

However, when a lattice code is defined in this manner, much of the underlying lattice's structure and symmetry, the key factors that we apply a lattice code to AWGN channels to replace a random code, are lost. In addition, the optimality of such schemes relies on maximum-likelihood (ML) decoding, i.e., minimum distance decoding when the codewords are uniformly distributed. Thus, the decoding regions are not fundamental regions of the lattices and are unbounded, resulting a further lost of the lattice symmetry. In contrast, lattice decoding amounts to find the nearest lattice point (which might not be a codeword), neglecting the effects of the bounding region, to take full advantage of the underlying lattice structure and

to deduce decoding complexity [15], [7].

Therefore, Uri Erez and Ram Zamir [13] proposed a new scheme with lattice encoding and decoding, the nested lattice code defined in the whole sphere, and proved it to be capacity achieving for AWGN channels. In this chapter, we will investigate the nested lattice code, and again, extend it to the one-input-two-output AWGN channel, further, to the general single-input-multiple-output AWGN channel.

4.1 Achieving Capacity on the AWGN Channel with Lattice Encoding and Decoding

Recall the AWGN channel defined in 2.1 with average power constraint P.

In [13], an AWGN channel is first transformed to a modulo-lattice additive noise (MLAN) channel, and then a nested lattice code is used in the MLAN channel to achieve its capacity, where the coarse lattice is used for shaping so that it is a good quantizer, and the fine lattice defines the codewords so that it is a good channel code.

4.1.1 Transformation from AWGN Channels to MLAN Channels

In this section, we describe a technique derived in [14] to transform a block of n uses of the AWGN channel $Y = X + Z$ to an n-dimensional MLAN channel. The input alphabet of this channel is a fundamental region Ω of a lattice Λ, which we call the shaping lattice. Such transformation is not strictly information lossless, however, for a "good" lattice, the information loss goes to zero as the dimension of

the lattice goes to infinity.

Let U be a random variable uniformly distributed over Ω. We employ U as a dither signal that is assumed to known to both transmitter and receiver, and is independent of the channel. The following property will be extensively used in the sequel.

Lemma 4.1.1. *For any random variable $X \in \Omega$, statistically independent of U, we have that the sum $Y = X + U \mod_{\Omega} \Lambda$ is uniformly distributed over Ω, and is statistically independent of X.*

Given $t \in \Omega$ and the dither U, the output of the transmitter is given by a modulo lattice operation

$$X_t = [t - U] \mod_{\Omega} \Lambda. \tag{4.1}$$

After the AWGN channel, the received signal $Y = X_t + Z$ is multiplied by some attenuation factor $0 < \alpha < 1$, which will be specified later, and the dither U is added. Finally, the decision signal is defined as

$$Y' = [\alpha Y + U] \mod_{\Omega} \Lambda. \tag{4.2}$$

Lemma 4.1.2. *The channel from t to Y' defined by (2.1), (4.1) and (4.2), is equivalent in distribution to the channel*

$$Y' = [t + Z'] \mod_{\Omega} \Lambda \tag{4.3}$$

where Z' is independent of t and is distributed as

$$Z' = [\alpha Z + (1 - \alpha)U] \mod_{\Omega} \Lambda$$

where U is a random variable uniformly distributed over Ω and is statistically independent of Z.

Proof.

$$\begin{aligned} Y' &= [\alpha Y + U] \mod_{\Omega} \Lambda \\ &= [\alpha(X_t + Z) + U] \mod_{\Omega} \Lambda \\ &= [X_t + U + (\alpha - 1)X_t + \alpha Z] \mod_{\Omega} \Lambda \\ &= [(t - U) \mod_{\Omega} \Lambda + U + (\alpha - 1)X_t + \alpha Z] \mod_{\Omega} \Lambda \\ &= [t - (1 - \alpha)X_t + \alpha Z] \mod_{\Omega} \Lambda \end{aligned} \tag{4.4}$$

where (4.4) follows the distributive law of the modulo operation. And the lemma follows, since by Lemma 4.1.1, X_t is independent of t and has the same distribution as U. □

For an input power constraint, let Ω be the Voronoi region $\mathcal{V}$ of the lattice. Since $\mathcal{V} = -\mathcal{V}$, we have

$$Z' = [(1 - \alpha)U + \alpha Z] \mod \Lambda$$

where $\mod \Lambda$ denotes $\mod_{\mathcal{V}} \Lambda$.

Moreover, the lattice is scaled so that the second moment of $\mathcal{V}$ is P. Hence, by Lemma 4.1.1, the average transmitted power is

$$\frac{1}{n} E\|X_t\|^2 = \frac{1}{n} E\|U\|^2 = P, \tag{4.5}$$

satisfying the power constraint of the AWGN channel.

Next, we will calculate the capacity of the MLAN channel.

For the equivalent channel (4.3), take $\Omega = \mathcal{V}$, so that the input $T \sim \text{Unif}(\mathcal{V})$ to achieve the capacity. Thus, the output Y' is also uniformly distributed over the Voronoi region $\mathcal{V}$. The resulting information rate is

$$\frac{1}{n} I(T; Y') = \frac{1}{n} h(Y') - \frac{1}{n} h(Y'|T)$$

$$
\begin{aligned}
&= \frac{1}{n}\log V - \frac{1}{n}h(Z') \\
&= \frac{1}{2}\log\frac{P}{G(\Lambda)} - \frac{1}{n}h(Z') \qquad (4.6)
\end{aligned}
$$

where V is the volume of $\mathcal{V}$ and (4.6) follows the definition of normalized second moment (2.5).

We are still left with the choice of α. Suppose $\alpha = 1$, then $Z' = Z \mod \Lambda$. When $P \gg N$ and Λ is a "good" lattice in the sense that $G(\Lambda) \approx \frac{1}{2\pi e}$, it can be shown that the effect of the modulo operation on the noise entropy becomes negligible. As a result, we have

$$\frac{1}{n}h(Z') \approx \frac{1}{n}h(Z) = \frac{1}{2}\log 2\pi eN$$

and the information rate tends to $\frac{1}{2}\log\frac{P}{N}$, the rate previously conjectured to be the greatest achievable with lattice decoding [3], [7].

Nevertheless, in order to maximize $\frac{1}{n}I(T;Y')$, we search for an α to minimize $\frac{1}{n}h(Z')$.

By Lemma 2.1.3,

$$\frac{1}{n}h(Z') \le \frac{1}{n}\cdot\frac{1}{2}\log((2\pi e)^n \cdot \frac{1}{n}E\|Z'\|^2). \qquad (4.7)$$

And we know that

$$
\begin{aligned}
\frac{1}{n}E\|Z'\|^2 &\le \frac{1}{n}E\|(1-\alpha)U + \alpha Z\|^2 \\
&= (1-\alpha)^2 P + \alpha^2 N \\
&\ge \frac{P}{P+N}\cdot N \qquad (4.8)
\end{aligned}
$$

where (4.8) meets equality when α is chosen as the MMSE coefficient $\frac{P}{P+N}$ [16].

Hence, with $\alpha = \frac{P}{P+N}$,

$$\frac{1}{n}h(Z') \leq \frac{1}{2}(2\pi e \frac{PN}{P+N}).$$

Now consider a sequence of lattices Λ_n with $\lim_{n\to\infty} G(\Lambda_n) = \frac{1}{2\pi e}$.

Theorem 4.1.1 (Capacity of MLAN channel)**.** *For the MLAN channel, if we choose* $T \sim$ *Unif*$(\mathcal{V})$, $\alpha = \frac{P}{P+N}$, *and if the sequence of lattices* Λ_n *satisfies* $\lim_{n\to\infty} G(\Lambda_n) = \frac{1}{2\pi e}$, *then*

$$\lim_{n\to\infty} \frac{1}{n} I(T; Y') = \frac{1}{2}\log(1 + SNR).$$

Proof. Since the capacity of the original AWGN channel is $C = \frac{1}{2}\log(1 + \frac{P}{N})$, on the one hand, it follows from the data processing inequality that

$$\frac{1}{n} I(T; Y') \leq \frac{1}{2}\log(1 + \frac{P}{N}). \tag{4.9}$$

On the other hand, from (4.6), (4.7) and (4.8), we get

$$\begin{aligned} \frac{1}{n} I(T; Y') &\geq \frac{1}{2}\log\frac{P}{G(\Lambda_n)} - \frac{1}{2}\log(2\pi e \frac{PN}{P+N}) && (4.10) \\ &= \frac{1}{2}\log(\frac{P+N}{PN} \cdot \frac{P}{2\pi e G(\Lambda_n)}) \\ &\to \frac{1}{2}\log(1 + \frac{P}{N}) && (4.11) \end{aligned}$$

as $G(\Lambda_n) \to \frac{1}{2\pi e}$ with $n \to \infty$. □

4.1.2 Nested Lattice Codes for Shaping and Coding

Before applying the nested lattice code into the modulo transformation scheme in the previous section, we formally define nested lattices and some related notations.

Definition 4.1.1 (Nested Lattices, nesting ratio and coset leaders)**.** *A pair of n-dimensional lattices* (Λ_1, Λ_2) *is called nested if* $\Lambda_2 \subset \Lambda_1$, *i.e., there exists corresponding generator matrices* G_1 *and* G_2 *such that*

$$G_2 = G_1 \cdot J,$$

where J is an $n \times n$ integer matrix whose determinant is greater than one. Denote the Voronoi regions of Λ_1 and Λ_2 as $\mathcal{V}_1$ and $\mathcal{V}_2$, and their volumes as V_1 and V_2 respectively. We call $\sqrt[n]{det(J)} = \sqrt[n]{\frac{V_2}{V_1}}$ the nesting ratio. The points of the set

$$C = \Lambda_1 \mod \Lambda_2 \triangleq \Lambda_1 \cap \mathcal{V}_2$$

are called the coset leaders of Λ_2 relative to Λ_1.

A nested lattice code is a lattice code whose bounding region is the Voronoi region of a sublattice. This can be visualized as in Fig.4.1, where a pair of two-dimensional ratio-three nested lattices is depicted.

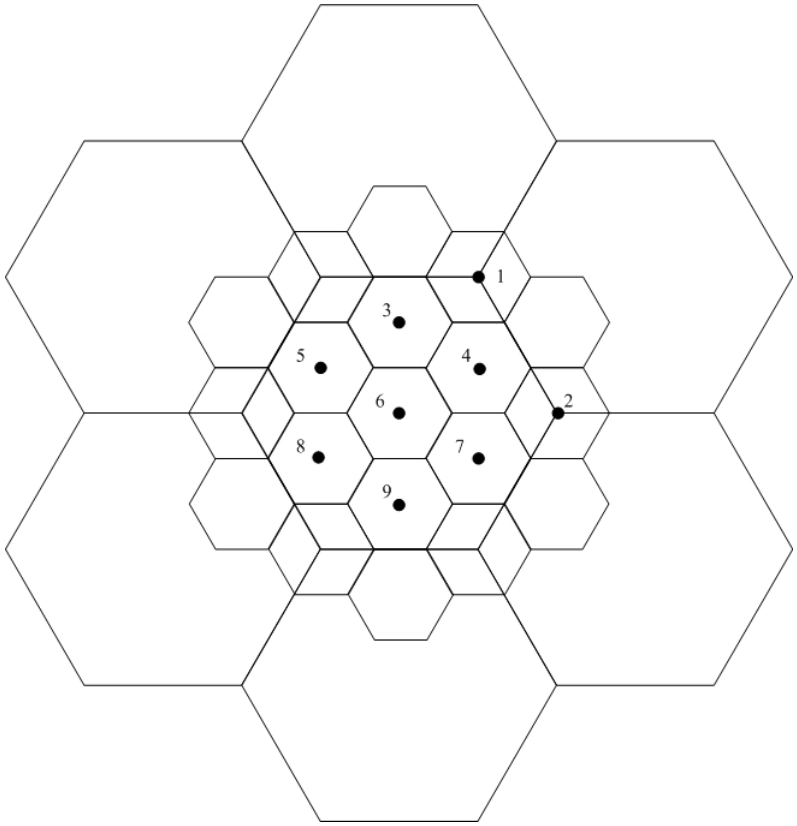

Figure 4.1: Nested lattices of ratio three.

And the coding rate of the nested lattice code is defined as

$$R = \frac{1}{n} \log \|\mathcal{C}\| = \frac{1}{n} \log \frac{V_2}{V_1}.$$

Let (Λ_1, Λ) be a rate-R nested lattice code with $\sigma^2(\mathcal{V}) = P$. Following, we incorporate the nested lattice code into the MLAN transformation scheme of an AWGN channel.

Message selection: Associate a message with each member of coset leaders $\mathcal{C} = \{c\}$.

Encoding: Let $U \sim \text{Unif}(\mathcal{V})$ be the dither. Given the message $c \in \mathcal{C}$, the encoder sends

$$X = [c - U] \mod \Lambda.$$

Consequently, by Lamma 4.1.1 and (4.5), X is uniform over $\mathcal{V}$ with average transmitted power P.

Decoding: Let $\alpha = \frac{P}{P+N}$. The decoder decodes c as

$$\hat{c} = Q_{\mathcal{V}_1}(\alpha Y + U) \mod \Lambda$$

This lattice encoding and decoding scheme is depicted in Fig.4.2.

It follows from Lemma 4.1.2 that

$$\begin{aligned} \hat{c} &= Q_{\mathcal{V}_1}([\alpha Y + U] \mod \Lambda) \mod \Lambda \\ &= Q_{\mathcal{V}_1}(Y') \mod \Lambda \\ &= Q_{\mathcal{V}_1}([c + Z'] \mod \Lambda) \mod \Lambda \end{aligned}$$

where $Z' = (1 - \alpha)U + \alpha Z \mod \Lambda$.
The equivalent channel from c to $\hat{c}$ is illustrated in Fig.4.3.

Since the channel is modulo additive and Λ is nested in Λ_1, the decoding error probability for any codeword c is given by

$$P_e = Pr(Z' \notin \mathcal{V}_1).$$

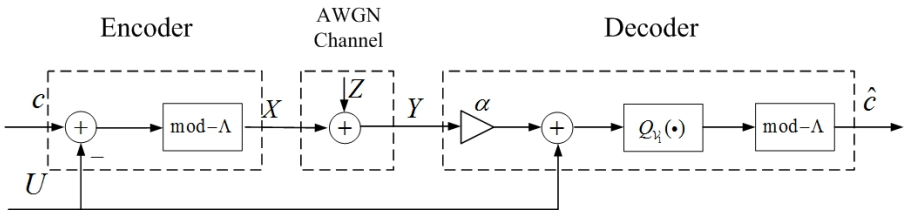

Figure 4.2: Lattice encoding/decoding scheme.

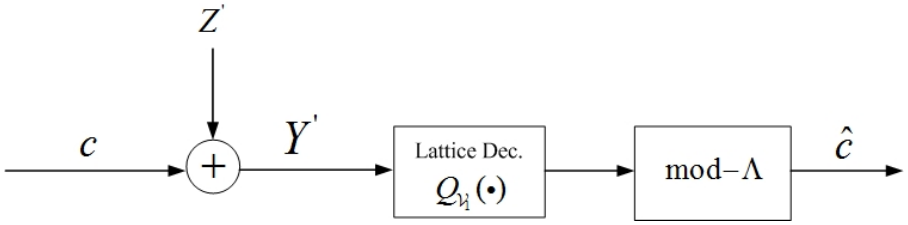

Figure 4.3: Equivalent MLAN channel.

By Theorem 3 in [13], there exists a sequence of n-dimensional nested lattice pairs $(\Lambda_1^{(n)}, \Lambda^{(n)})$ whose rate R approaches the capacity of the AWGN channel with error probability P_e goes to zero as $n \to \infty$.

4.2 Incorporation of Nested Lattice Codes into One-Input-Two-Output AWGN Channels

Recall the one-input-two-outputs AWGN channel defined in (3.7) with power constraint P and noise variances N_1 and N_2 , to employ nested lattice codes on such channel, as in Section 4.1.2, we first transform it into an MLAN channel.

Given $t \in \mathcal{V}$ and the dither U, the transmitter sends

$$X = [t - U] \mod \Lambda. \tag{4.12}$$

Upon receiving $Y_1 = X + Z_1$ and $Y_2 = X + Z_2$, the receiver computes

$$Y' = (\alpha Y_1 + \beta Y_2 + U) \mod \Lambda. \tag{4.13}$$

This results the MLAN channel from t to Y'. Similarly, we have the following lemma and theorem.

Lemma 4.2.1. *The channel from t to Y' defined by (3.7), (4.12) and (4.13) is equivalent in distribution to the channel*

$$Y' = (t + N_{eff}) \mod \Lambda \tag{4.14}$$

where N_{eff} is independent of t and is distributed as

$$N_{eff} = [(1-\alpha-\beta)U + \alpha Z_1 + \beta Z_2] \mod \Lambda. \tag{4.15}$$

where U is a random variable uniformly distributed over $\mathcal{V}$ and is independent of Z_1 and Z_2.

Proof.

$$\begin{aligned} Y' &= [\alpha(X+Z_1) + \beta(X+Z_2) + U] \mod \Lambda \\ &= [X + U + (\alpha+\beta-1)X + \alpha Z_1 + \beta Z_2] \mod \Lambda \\ &= [(t-U) \mod \Lambda + U + (\alpha+\beta-1)X + \alpha Z_1 + \beta Z_2)] \mod \Lambda \\ &= [t - (1-\alpha-\beta)X + \alpha Z_1 + \beta Z_2] \mod \Lambda. \end{aligned}$$

According to Lemma 4.1.1, X is independent of t and has the same distribution as U. In addition, we have $\mathcal{V} = -\mathcal{V}$. Consequently,

$$N_{eff} = [(1-\alpha-\beta)U + \alpha Z_1 + \beta Z_2] \mod \Lambda.$$

□

Theorem 4.2.1. *For the MLAN channel defined in (4.14) and (4.15), if we choose $T \sim$ Unif($\mathcal{V}$), $\alpha = \frac{PN_2}{(N_1+N_2)P+N_1N_2}$ and $\beta = \frac{PN_1}{(N_1+N_2)P+N_1N_2}$, and if the sequence of lattices Λ_n satisfies $\lim_{n\to\infty} G(\Lambda_n) = \frac{1}{2\pi e}$, then*

$$\lim_{n\to\infty} \frac{1}{n} I(T;Y') = \frac{1}{2}\log(1+SNR),$$

where $SNR = \frac{P}{\frac{N_1N_2}{N_1+N_2}}$ with respect to (3.10).

Proof. With the choice of $T \sim \text{Unif}(\mathcal{V})$, the output Y' is also uniformly distributed over $\mathcal{V}$. Hence,

$$\frac{1}{n}I(T;Y') = \frac{1}{n}h(Y') - \frac{1}{n}h(Y'|T) \tag{4.16}$$

$$= \frac{1}{2}\log\frac{P}{G(\Lambda)} - \frac{1}{n}h(N_{eff}). \tag{4.17}$$

Again, we choose α and β as MMSE coefficients to minimize $h(N_{eff})$ as follows.

$$P_{eff} \triangleq \frac{1}{n}E\|N_{eff}\|^2 \leq \frac{1}{n}E\|(1-\alpha-\beta)U + \alpha Z_1 + \beta Z_2\|^2 \tag{4.18}$$

$$= (1-\alpha-\beta)^2 P + \alpha^2 N_1 + \beta^2 N_2. \tag{4.19}$$

Let

$$\frac{\partial P_{eff}}{\partial \alpha} = \frac{\partial P_{eff}}{\partial \beta} = 0$$

to minimize P_{eff}. We get

$$\alpha = \frac{PN_2}{(N_1+N_2)P + N_1N_2} \tag{4.20}$$

and

$$\beta = \frac{PN_1}{(N_1+N_2)P + N_1N_2}. \tag{4.21}$$

Therefore,

$$\begin{aligned} P_{eff} &= (\frac{N_1N_2}{(N_1+N_2)P + N_1N_2})^2 P + (\frac{PN_2}{(N_1+N_2)P + N_1N_2})^2 N_1 \\ &\quad + (\frac{PN_1}{(N_1+N_2)P + N_1N_2})^2 N_2 \\ &= \frac{N_1N_2P[N_1N_2 + P(N_1+N_2)]}{[(N_1+N_2)P + N_1N_2]^2} \\ &= \frac{P}{1+\frac{P}{\frac{N_1N_2}{N_1+N_2}}} \\ &= \frac{P}{1+SNR}. \end{aligned}$$

With the same deduction in (4.9), (4.10) and (4.11), the theorem follows. □

The one-input-two-output AWGN channel is transformed into a single-input-single-output MLAN channel with noise N_{eff} instead of N' compared with the

corresponding MLAN channel of the single-input-single-output AWGN channel. Thus, the nested lattice code for such AWGN channel is also quite similar, with minor changes.

Still, let (Λ_1, Λ) be a rate-R nested lattice code. The message selection and encoding stay the same where the encoder sends

$$X = [c - U] \mod \Lambda.$$

Upon reception, the decoder computes

$$\hat{c} = Q_{\mathcal{V}_1}(\alpha Y_1 + \beta Y_2 + U) \mod \Lambda.$$

Hence,

$$\begin{aligned} \hat{c} &= Q_{\mathcal{V}_1}[(\alpha Y_1 + \beta Y_2 + U) \mod \Lambda] \mod \Lambda \\ &= Q_{\mathcal{V}_1}[(c + N_{eff}) \mod \Lambda] \mod \Lambda. \end{aligned}$$

where $N_{eff} = (1 - \alpha - \beta)U + \alpha Z_1 + \beta Z_2 \mod \Lambda$. The decoding error probability is given by

$$P_e = Pr(N_{eff} \notin \mathcal{V}_1)$$

and by Theorem 3 in [13], approaches zero with n goes to infinity.

4.3 An extension to the Single-Input-Multiple-Output AWGN Channel

In the previous section, we exploited nested lattice codes for the one-input-two-output AWGN channel to achieve the channel capacity. Following this idea, now we further extend nested lattice codes to a more general case, the single-input-multiple-output AWGN channel.

Consider the following AWGN channel with input X and n outputs $Y_1, Y_2, ..., Y_n$.

$$\begin{cases} Y_1 = X + Z_1 \\ Y_2 = X + Z_2 \\ \quad ... \quad ... \quad ... \\ Y_n = X + Z_n \end{cases} \tag{4.22}$$

where Z_i are mutually independent and $Z_i \sim \mathcal{N}(0, N_i)$ for $i = 1, 2, ..., n$.

4.3.1 Channel Capacity

First, we calculate the channel capacity of the multiple-output AWGN channel in (4.22). Similarly with the two-output case in Section. 3.2.1, Y_i is normally distributed with mean 0 and variance $P + N_i$, and the vector $(Y_1, Y_2, ..., Y_n)$ has a multivariate normal distribution, denoted by

$$(Y_1, Y_2, ..., Y_n) \sim \mathcal{N}(\mu_Y, K_Y),$$

where

$$\mu_Y = (EY_1, EY_2, ..., EY_n) = (0, 0, ..., 0)$$

and

$$K_Y = \begin{pmatrix} \sigma_{Y_1}^2 & \rho_{Y_1,Y_2}\sigma_{Y_1}\sigma_{Y_2} & \rho_{Y_1,Y_3}\sigma_{Y_1}\sigma_{Y_3} & ... & ... & \rho_{Y_1,Y_n}\sigma_{Y_1}\sigma_{Y_n} \\ \rho_{Y_2,Y_1}\sigma_{Y_2}\sigma_{Y_1} & \sigma_{Y_2}^2 & \rho_{Y_2,Y_3}\sigma_{Y_2}\sigma_{Y_3} & ... & ... & \rho_{Y_2,Y_n}\sigma_{Y_2}\sigma_{Y_n} \\ ... & ... & ... & ... & ... & ... \\ ... & ... & ... & ... & ... & ... \\ \rho_{Y_n,Y_1}\sigma_{Y_n}\sigma_{Y_1} & \rho_{Y_n,Y_2}\sigma_{Y_n}\sigma_{Y_2} & \rho_{Y_n,Y_3}\sigma_{Y_n}\sigma_{Y_3} & ... & ... & \sigma_{Y_n}^2 \end{pmatrix}.$$

Note that ρ_{Y_i,Y_j} is the correlation between Y_i and Y_j for $i, j = 1, 2, ..., n$. As computed in (3.8) and (3.9), we get

$$\rho_{Y_i,Y_j} = \frac{P}{\sqrt{(P + N_i)(P + N_j)}}.$$

Therefore, we have

$$K_Y = \begin{pmatrix} P+N_1 & P & P & ... & ... & P \\ P & P+N_2 & P & ... & & P \\ ... & ... & ... & ... & ... & ... \\ ... & ... & ... & ... & ... & ... \\ P & P & P & ... & ... & P+N_n \end{pmatrix}. \tag{4.23}$$

Also, it's obvious that

$$(Z_1, Z_2, ..., Z_n) \sim \mathcal{N}(\mu_Z, K_Z)$$

with

$$\mu_Z = (0, 0, ..., 0)$$

and

$$K_Z = \begin{pmatrix} N_1 & 0 & 0 & ... & 0 \\ 0 & N_2 & 0 & ... & 0 \\ ... & ... & ... & ... & ... \\ ... & ... & ... & ... & ... \\ 0 & 0 & 0 & ... & N_n \end{pmatrix}. \tag{4.24}$$

Follows from (4.23) and (4.24), we have

$$\begin{aligned} I(X; Y_1, Y_2, ..., Y_n) &= h(Y_1, Y_2, ..., Y_n) - h(Y_1, Y_2, ..., Y_n|X) \\ &= h(Y_1, Y_2, ..., Y_n) - h(Z_1, Z_2, ..., Z_n) \\ &= \frac{1}{2}\log(2\pi e)^n|K_Y| - \frac{1}{2}\log(2\pi e)^n|K_Z| \\ &= \frac{1}{2}\log\frac{|K_Y|}{|K_Z|} \\ &= \frac{1}{2}\log\frac{\sum_{i=1}^n \frac{\prod_{k=1}^n N_k}{N_i} P + \prod_{k=1}^n N_k}{\prod_{k=1}^n N_k} \qquad (4.25) \\ &= \frac{1}{2}\log(1 + P\sum_{i=1}^n \frac{1}{N_i}) \qquad (4.26) \end{aligned}$$

The calculation of $|K_Y|$ in (4.25) can be easily done by deduction and hence is omitted here. Next, we will apply nested lattice codes to the general multiple-output AWGN channel to achieve its capacity (4.26).

4.3.2 Design of Nested Lattice Codes for the Single-Input-Multiple-Output AWGN Channel

Given a general multiple-output AWGN channel (4.22), here we focus on the transformation of this channel to its corresponding MLAN channel, the rest of the work is quite similar to the two-output Gaussian case and therefore will not be detailed.

With $t \in \mathcal{V}$ and the dither U, the transmitter sends

$$X = (t - U) \mod \Lambda. \tag{4.27}$$

And upon receiving $(Y_1, Y_2, ..., Y_n)$, the receiver computes

$$Y' = (\sum_{i=1}^{n} \alpha_i Y_i + U) \mod \Lambda \tag{4.28}$$

as its decision signal.

This results in the MLAN channel from t to Y' and the following lemma and theorem can be derived accordingly.

Lemma 4.3.1. *The channel from t to Y' defined by (4.22), (4.27) and (4.28) is equivalent in distribution to the channel*

$$Y' = (t + N_{eff}^{(n)}) \mod \Lambda \tag{4.29}$$

where $N_{eff}^{(n)}$ is independent of t and is distributed as

$$N_{eff}^{(n)} = [(1 - \sum_{i=1}^{n} \alpha_i)U + \sum_{i=1}^{n} \alpha_i Z_i] \mod \Lambda. \tag{4.30}$$

where U is a random variable uniformly distributed over $\mathcal{V}$ and is independent of Z_i for $i = 1, 2, ..., n$.

The proof of Lemma.4.3.1 is quite similar to that of Lemma. 4.2.1, thus is omitted here.

Theorem 4.3.1. *For the MLAN channel defined in (4.29) and (4.30), if we choose* $T \sim$ *Unif*$(\mathcal{V})$, $\alpha_i = \frac{P}{P(1+\sum_{j\neq i}\frac{N_i}{N_j})+N_i}$ *for* $i, j \in \{1, 2, ..., n\}$, *and if the sequence of lattices* Λ_n *satisfies* $\lim_{n\to\infty} G(\Lambda_n) = \frac{1}{2\pi e}$, *then*

$$\lim_{n\to\infty} \frac{1}{n} I(T; Y') = \frac{1}{2}\log(1 + SNR),$$

where $SNR = P\sum_{i=1}^{n}\frac{1}{N_i}$ *with respect to the channel capacity (4.26) of the multiple-output Gaussian channel.*

Proof. Here we only need to prove that

$$P_{eff}^{(n)} = \frac{P}{1 + SNR} \tag{4.31}$$

where $P_{eff}^{(n)}$ is the average power of $N_{eff}^{(n)}$ per dimension.

With the same deduction in (4.17) and (4.19), it follows

$$\frac{1}{n} I(T; Y') = \frac{1}{2}\log\frac{P}{G(\Lambda)} - \frac{1}{n}h(N_{eff}^{(n)}),$$

and

$$P_{eff}^{(n)} = \frac{1}{n}E\|N_{eff}^{(n)}\|^2 \leq (1 - \sum_{i=1}^{n}\alpha_i)^2 P + \sum_{i=1}^{n}\alpha_i^2 N_i. \tag{4.32}$$

Let

$$\frac{\partial P_{eff}^{(n)}}{\partial \alpha_i} = 0$$

for $i = 1, 2, ..., n$, to minimize $P_{eff}^{(n)}$, we get the following n equations,

$$(\sum_{i=1}^{n}\alpha_i - 1)P + \alpha_i N_i = 0. \tag{4.33}$$

Thus,

$$\alpha_i N_i = \alpha_j N_j$$

for any $i, j = 1, 2, ..., n$, i.e.,

$$\alpha_j = \frac{N_i}{N_j}\alpha_i \tag{4.34}$$

Inserting (4.34) into (4.33) for each $j \neq i$, we have

$$P(1 + \sum_{j \neq i} \frac{N_i}{N_j})\alpha_i + N_i\alpha_i = P.$$

Hence,

$$\begin{aligned}\alpha_i &= \frac{P}{P(1 + \sum_{j \neq i} \frac{N_i}{N_j}) + N_i} \\ &= \frac{P}{P\sum_j \frac{N_i}{N_j} + N_i}.\end{aligned}$$

Also, we can express α_i in another way, which facilitate the calculation of $P_{eff}^{(n)}$ though seems more complicated, as follows,

$$\alpha_i = \frac{\frac{P}{N_i}\prod_k N_k}{\prod_k N_k + \sum_j \frac{\prod_k N_k}{N_j} P}. \tag{4.35}$$

Combining (4.32) and (4.35), we get

$$\begin{aligned}P_{eff}^{(n)} &= (1 - \sum_{i=1}^{n} \alpha_i)^2 P + \sum_{i=1}^{n} \alpha_i^2 N_i \\ &= (1 - \frac{\sum_i \frac{P}{N_i}\prod_k N_k}{\prod_k N_k + \sum_j \frac{\prod_k N_k}{N_j} P})^2 P + \sum_i (\frac{\frac{P}{N_i}\prod_k N_k}{\prod_k N_k + \sum_j \frac{\prod_k N_k}{N_j} P})^2 N_i \\ &= (\frac{\prod_k N_k}{\prod_k N_k + \sum_j \frac{\prod_k N_k}{N_j} P})^2 P + \frac{P^2 \prod_k N_k \sum_i \frac{\prod_k N_k}{N_i}}{(\prod_k N_k + \sum_j \frac{\prod_k N_k}{N_j} P)^2} \\ &= \frac{\prod_k N_k P(\prod_k N_k + P\sum_i \frac{\prod_k N_k}{N_i})}{(\prod_k N_k + \sum_j \frac{\prod_k N_k}{N_j} P)^2} \\ &= \frac{\prod_k N_k P}{\prod_k N_k + \sum_j \frac{\prod_k N_k}{N_j} P} \\ &= \frac{P}{1 + P\sum_j \frac{1}{N_j}} \\ &= \frac{P}{1 + SNR}.\end{aligned}$$

□

Chapter 5

Conclusion and Future Work

5.1 Conclusion

As the most important continuous alphabet channel, the Gaussian channel relates to many practical problems. However, from the classical random coding perspective, the capacity-achieving codebooks for the Gaussian channel may not preserve any structures, hence are complicated and inefficient for real applications. Motivated by this, we investigated lattice codes for AWGN channels.

Our work mainly consists of two parts.

First, we studied the proof of lattice codes being capacity achieving for AWGN channels in [9]. We gave an intuitive interpretation of the proof, based on which an angle-decoding scheme is proposed for the one-input-two-output AWGN channel. And we proved that lattice codes can achieve the capacity of the one-input-two-output AWGN channel using the proposed decoding scheme.

Secondly, the nested lattice code is explored since it uses lattice coding and decoding to preserve the symmetry of the underlying lattices, and therefore, turns

out to be advantageous in practice. Still, we extended the nested lattice code to the one-input-two-output AWGN channel and proved it to be capacity-achieving. Further, a general multiple-output AWGN channel is considered and the nested lattice codes is employed to achieve its capacity.

5.2 Future Work

Multiple input multiple output (MIMO) systems has attracted great attention as a method to achieve high data rates over wireless networks. The capacity of single user MIMO Gaussian networks was first studied in [17] and [18]. And this work has been extended to MIMO multiple-access channels [19] as well as MIMO broadcast channels [20].

Our research solves the lattice coding for the single-input-multiple-output AWGN channel. In the short run, we would like to study its dual channel, the single user multiple-input-single-output Gaussian channel. First, we will focus on a special case, the two-input-one-output AWGN channel as shown in Fig.5.1, where X_1 and X_2 are jointly encoded and transmitted over an AWGN channel with noise $Z \sim \mathcal{N}(0, N)$. Upon receiving Y, the decoder tries to decode the codeword vector (X_1, X_2). We hope to extend the proposed angle-coding scheme and the nested lattice code to this two-input-one-output AWGN channel to achieve its capacity, and then, to the general multiple-input-single-output case.

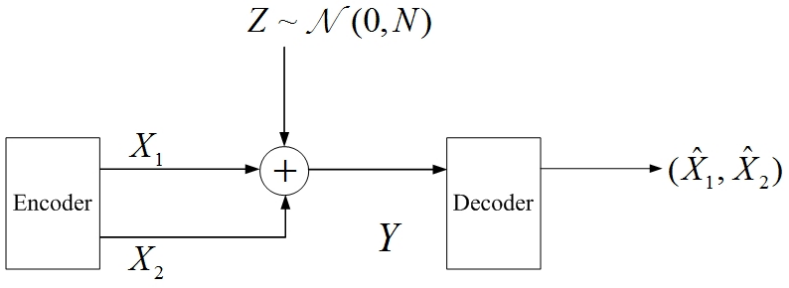

Figure 5.1: Single user two-input-one-output AWGN channel.

In the long run, we hope to incorporate lattice codes into the single user MIMO Gaussian channel, where the transmitter and the receiver communicate both with multiple antennas, to facilitate the application of structured codes in wireless networks.

Bibliography

[1] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, pt. I, pp. 379–423, 1948; pt. II, pp. 623–656, 1948. 7

[2] C. E. Shannon, "Probability of error for optimal codes in a Gaussian channel," *Bell Syst. Tech. J.*, vol. 38, pp. 611–656, May. 1959; pt. II, pp. 623–656, 1948. 1

[3] R. de Buda, "The upper error bound of a new near-optimal code," *IEEE Trans. Inform. Theory*, vol. IT-21, pp. 441–445, July. 1975. 2, 39

[4] R. de Buda, "Some optimal codes have structure," *IEEE Trans. Inform. Theory*, vol. 7, pp. 893–899, Aug. 1989. 2, 35

[5] J. H. Conway and N. J. A. Sloane, "Voronoi regions of lattices, second moments of polytopes, and quantization," *IEEE Trans. Inform. Theory*, vol. IT-28, pp. 211–226, Mar. 1982. 13

[6] T. Linder, C. Schlegel and K. Zeger, "Corrected proof of de Buda's theorem," *IEEE Trans. Inform. Theory*, vol. 39, pp. 1735–1737, Sept. 1993. 35

[7] G. Poltyrev, "On coding without restrictions for the AWGN channel," *IEEE Trans. Inform. Theory*, vol. 40, pp. 409–417, Mar. 1994. 35, 36, 39

[8] G. D. Forney Jr., "Approaching the capacity of the AWGN channel with coset codes and multilevel coset codes," preprint, 1997. 35

[9] R. Urbanke and B. Rimoldi, "Lattice codes can achieve capacity on the AWGN channel," *IEEE Trans. Inform. Theory*, vol. 44, pp. 273–278, Jan. 1998. 3, 5, 16, 17, 35, 52

[10] G. D. Forney Jr., "On the duality of coding and quantizing," *DIMACS Ser. Discr. Math. Theory Comp. Sci.*, vol. 14, 1993. 13

[11] R. Zamir and M. Feder, "On lattice quantization noise," *IEEE Trans. Inform. Theory*, vol. 42, pp. 1152–1159, July. 1996. 15

[12] R. Zamir, S. Shamai (Shitz) and U. Erez, "Nested linear/lattice codes for structured multiterminal binning," *IEEE Trans. Inform. Theory*, vol. 48, pp. 1250–1276, June, 2002. 15

[13] U. Erez and R. Zamir, "Achieving $\frac{1}{2}\log(1+SNR)$ on the AWGN channel with lattice encoding and decoding," *IEEE Trans. Inform. Theory*, vol. 50, pp. 2293–2314, Oct. 2004. 3, 36, 43, 46

[14] U. Erez, S. Shamai (Shitz) and R. Zamir, "Capacity and lattice strategies for cancelling known interference," *IEEE Trans. Inform. Theory*, vol. 51, pp. 3820–3833, Oct. 2005. 36

[15] E. Agrell, T. Eriksson, A. Vardy and K. Zeger, "Closest point search in lattices," *IEEE Trans. Inform. Theory*, vol. 42, pp. 1152–1159, Jan. 1998. 36

[16] E. Telatar, "Shannon meets Wiener II: On MMSE estimation in successive decoding schemes," *42nd Annual Allerton Conference on Communication, Control and Computing, Allteron House, Monticello Illinois*, Oct. 2004. 39

[17] G. D. Forney Jr., "Capacity of multi-antenna Gaussian channels," *European Trans. on Telecomm. ETT*, 10(6):585-596, November 1999. 53

[18] G.J. Foschini and M.J. Gans, A. Vardy and K. Zeger, "On limits of wireless communications in a fading environment when using multiple antennas," *Wireless Personal Communications*, vol.6, pp. 311–335, 1998. 53

[19] W. Yu, W. Rhee, S. Boyd and J. Cioffi, "Iterative water-filling for vector multiple access channels," *Proc. IEEE Int. Symp. Inf. Theory*, pp. 322, ashington DC, June 24-29, 2001. 53

[20] G. Caire and S. Shamai, "On achievable rates in a multi-antenna broadcast downlink," *38th Annual Allerton Conference on Commun., Control and Computing*, Monticello, IL, Oct. 4 - 6, 2000. 53

[21] T. Cover and J. Thomas, *Elements of Information Theory*, New York, Wiley, 1991. 6

[22] J. M. Wozencraft and Irwin Mark Jacobs, *Principles of Communication Engineering*, 1965. 30

[23] F. M. Morgan, *Plane and Spherical Trigonometry*, 1945. 24

[24] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*. New York, Springer-Verlag, 1988. 13