Construction of Capacity Achieving Lattice Gaussian Codes

Thesis by

Wael Alghamdi

In Partial Fulfillment of the Requirements

For the Degree of

Master of Science

King Abdullah University of Science and Technology, Thuwal,

Kingdom of Saudi Arabia

The thesis of Wael Alghamdi is approved by the examination committee

Committee Chairperson: Professor Mohamed-Slim Alouini

Committee Member: Professor Tareq Al-Naffouri

Committee Member: Professor Mikhail Moshkov

ABSTRACT

Construction of Capacity Achieving Lattice Gaussian Codes

Wael Alghamdi

We propose a new approach to proving results regarding channel coding schemes based on construction−A lattices for the Additive White Gaussian Noise (AWGN) channel that yields new characterizations of the code construction parameters, i.e., the primes and dimensions of the codes, as functions of the block-length. The approach we take introduces an averaging argument that explicitly involves the considered parameters. This averaging argument is applied to a generalized Loeliger ensemble [1] to provide a more practical proof of the existence of AWGN-good lattices, and to characterize suitable parameters for the lattice Gaussian coding scheme proposed by Ling and Belfiore [3].

ACKNOWLEDGEMENTS

I express my most sincere appreciation and gratitude to Professor Mohamed-Slim Alouini and Dr. Walid Abediseid for their guidance, support and help during my Masters. They have been a great source of knowledge and have inspired me with precious ideas. Their guidance, encouragement and patience made this work possible. I also thank all my friends at King Abdullah University of Science and Technology, for their encouragement and support.

And, as it always has been and always will be, my deepest love and gratitude is devoted to my family. They are always a source of love, support and encouragement. To them, I dedicate this work.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

SNR	Signal-to-Noise-Ratio
VNR	Volume-to-Noise-Ratio
NN	Nearest Neighbor
Fl	Flatness
LG	Lattice Gaussian

LIST OF SYMBOLS

$\lvert\cdot\rvert$	Cardinality of a set, or magnitude of a complex number
$\mathcal{P}(\cdot)$	Power set
$\lVert\cdot\rVert$	Euclidean norm
σ_w^2	Noise variance
$\mathbb{R}^n$	$n-$dimensional real Euclidean space
Λ	A lattice
Θ_Λ	Theta series of lattice Λ
$\mathcal{V}(\Lambda)$	Voronoi region of lattice Λ
Λ^*	Dual lattice of lattice Λ
μ_L	Lebesgue measure
C	A linear code
p	Prime number
n	Blocklength
k	Rank of a linear code
$\mathbb{F}_p$	Finite field with p elements
$\mathbb{Z}$	Integers
$\mathfrak{p}$	Quadruple of parameters (for a lattice or a lattice ensemble)
$\mathcal{B}_n(q,r)$	$n-$dimensional real Euclidean ball around q of radius r
E_{sp}	Sphere-packing exponent
E_P^{un}	Unexpurgated Poltyrev exponent
$\gamma_\Lambda(\sigma)$	Volume-to-Noise-Ratio (VNR)
ϵ_Λ	Flatness factor of lattice Λ
$W^{(n)}$	$n-$dimensional white Gaussian noise
G	Random matrix over a finite field
$\Lambda(G)$	Lattice ensemble
$\mathbb{E}_X[\cdot]$	Expectation with respect to X
$\mathbb{H}(\cdot)$	Entropy
f_X	Probability density function of X
$(a;q)_m$	Pochhammer symbol

Chapter 1

Introduction

An explicit construction of a structured coding scheme that achieves the capacity of the additive white Gaussian noise (AWGN) channel has been a major problem in coding theory. Much of the recent work towards this goal is motivated by Loeliger's proof that construction$-$A lattices can be made to satisfy a uniformity property similar to a Minkowski-Hlawka-Siegel (MHS) ensemble [1]. This property of construction$-$A lattices was used by Erez and Zamir to show that nested lattices with dithering can achieve the capacity of the AWGN channel [2], and by Ling and Belfiore to show that a lattice Gaussian coding scheme can achieve the capacity of the AWGN channel without the need of dithering [3]. However, practical parameters defining the construction$-$A lattices used in the coding schemes remain missing.

The uniformity property of construction$-$A lattices is utilized in the literature for approximating lattice sums (that are averaged over lattice ensembles) as either Riemann or Lebesgue integrals, e.g., using the MHS theorem. Thus, the explicitness of the parameters involved is destroyed or rendered computationally infeasible at best. For instance, the approach of Erez and Zamir requires the prime numbers defining the relevant construction$-$A lattices to be exponential in the block-length [2], while that of Ling and Belfiore does not quantify how large the involved primes should be [3]. Such impracticality is induced by the best, yet loose, existing bounds on the error term in approximating Riemann sums by integrals. The error terms in

such approximations are unknown (for the Lebesgue integral) or polynomial in the mesh size (for the Riemann integral), which translate into unknown large primes or exponentially large primes, respectively. Therefore, the need for a new averaging argument is dire.

This work proposes an averaging argument that transforms averaged lattice sums into lattice sums over the simplest known lattice: the integer lattice $\mathbb{Z}^n$. By refraining from using the MHS theorem, we are not bound to treat the error term of discretized integrals. Instead, we show that asymptotic results regarding a Riemann theta function and a Pochhammer symbol suffice to get stronger versions of the previously known results and new characterizations of the primes and dimensions of the construction$-$A lattices that are used to build capacity-achieving codes. In particular, we show that primes of size comparable to the squared root of the block-length yield capacity-achieving codes for the AWGN channel.

We use the following notations. The symbol log always refers to the natural logarithm, and information is measured in nats. For any set S, $|S|$ denotes the number of elements in S, 1_S the indicator function of S and $\mathcal{P}(S)$ the power set of S. The notation $\|\cdot\|$ will always refer to the $2-$norm. The symbol 0 will refer to either a scalar (in $\mathbb{R}$ or $\mathbb{F}_p$), a vector (in $\mathbb{R}^n$ or $\mathbb{F}_p^n$) or a matrix (over $\mathbb{R}$ or $\mathbb{F}_p$), but it will be clear from context which is the meaning referred to. We will use μ_L to refer to the Lebesgue measure over $\mathbb{R}^n$ for any fixed n, which will be clear from the context. Also, for any natural n, point $q \in \mathbb{R}^n$ and $r > 0$, we will denote by $\mathcal{B}_n(q, r)$ the open ball in $\mathbb{R}^n$ of radius r around q. Throughout, we fix a sequence $\{\sigma_{w,n}\} \subset \mathbb{R}_{>0}$, and for each n, we let $W^{(n)}$ denote a random vector whose components are i.i.d. zero-mean Gaussian random variables of variance $\sigma_{w,n}^2$. We also denote the probability density function of a random variable Z by f_Z. Further, the random variables $(U_{\mathfrak{p}}, U'_{\mathfrak{p}}, u_{\mathfrak{p}}, G, W^{(n)}, X, Z)$ considered in this work are pairwise independent.

For sets S and T, we define $S + T := \{s + t\ ;\ s \in S, t \in T\}$ (the Minkowski sum)

and $ST = \{st \ ; \ s \in S, t \in T\}$, whenever these definitions make sense. If $S = \{s\}$ consists of a single element, we write $s + T := \{s\} + T$ and $sT := \{s\}T$ for short.

Chapter 2

Preliminaries

We review in this chapter the mathematical machinery we need.

2.1 Lattices

One of the central objects in our work, important in virtue of their structured nature, are lattices in real Euclidean spaces. We describe in this section two equivalent definitions of lattices in real Euclidean spaces, and introduce first properties of lattices. We discuss lattices further in the following sections.

2.1.1 Definition

First, we define what a discrete subgroup of a real Euclidean space is.

Definition 2.1.1. For any $n \in \mathbb{N}$, a subgroup $\Lambda \subset \mathbb{R}^n$ is called discrete if $|\Lambda \cap K| < \infty$ for every compact subset $K \subset \mathbb{R}^n$.

Remark 1. *Recall that, by the Heine-Borel theorem, compact subsets of* $\mathbb{R}^n$ *are exactly the closed and bounded ones. Thus, we may equivalently say that a subgroup* $\Lambda \subset \mathbb{R}^n$ *is discrete if and only if* $|\Lambda \cap \mathcal{B}_n(q, r)| < \infty$ *for every* $q \in \mathbb{R}^n$ *and* $r > 0$*, or, if and only if* $\{|\Lambda \cap \mathcal{B}_n(0, r_j)|\}_{j \in \mathbb{N}} \subset \mathbb{N}$ *for some sequence* $0 < r_1 < r_2 < \cdots$ *that increases without bound.*

Remark 2. *Discreteness of a subgroup $\Lambda \subset \mathbb{R}^n$, implies, in view of remark 1, that it contains minimal vectors, i.e., the number*

$$d_{\min}(\Lambda) := \min\{\|x\| \ ; \ x \in \Lambda \setminus \{0\}\} \tag{2.1}$$

is well-defined.

Now, we are ready to define what lattices in real Euclidean spaces are.

Definition 2.1.2 (Lattice)**.** For any $n \in \mathbb{N}$, a lattice in $\mathbb{R}^n$ is a discrete subgroup of rank n.

Intuitively, discreteness of a lattice ensures the well-spacing of the elements in the lattice. More precisely, discreteness amounts to the fact that no element of the lattice is a limit point of other elements in the lattice. Being a subgroup reflects the symmetrical (around the origin) and the translational invariance natures of a lattice. Finally, being of full-rank (see theorem 2.1.3) amounts to having the lattice be non-degenerate, i.e., not lying entirely on a hyperplane.

For problems in coding theory, an equivalent definition of lattices in real Euclidean spaces is usually made use of, which we introduce next. First, we mention a well-known theorem that yields the equivalence of the two definitions.

Theorem 2.1.3. *For any $n \in \mathbb{N}$, a nonzero subgroup $\Lambda \subset \mathbb{R}^n$ is discrete if and only if there is an integer $1 \leq \ell \leq n$ and a full-rank matrix $B \in \mathbb{R}^{n \times \ell}$ such that $\Lambda = \{Bx \ ; \ x \in \mathbb{Z}^\ell\}$.*

Remark 3. *When $1 \leq \ell \leq n$ and $B \in \mathbb{R}^{n \times \ell}$ is full-rank, the mapping $x \mapsto Bx$ is an isomorphism of groups $\mathbb{Z}^\ell \longrightarrow \{Bx \ ; \ x \in \mathbb{Z}^\ell\}$, hence $\{Bx \ ; \ x \in \mathbb{Z}^\ell\}$ has rank ℓ.*

We may now introduce the following equivalent definition of lattices in real Euclidean spaces.

Definition 2.1.4 (Lattice)**.** For any $n \in \mathbb{N}$, a lattice in $\mathbb{R}^n$ is a subgroup $\Lambda = \{Bx \ ; \ x \in \mathbb{Z}^n\}$, where $B \in \mathbb{R}^{n \times n}$ is full-rank. We say that Λ is generated by B.

A natural question is whether lattice generators are unique. It is clear that $-B$ is a generator if B is. It is also true that only a unimodular transformation preserves generators. A matrix T is called unimodular if it is an invertible integer matrix whose inverse is also an integer matrix. Clearly, T^{-1} is unimodular if T is. Thus, if $T \in \mathbb{Z}^{n \times n}$ is unimodular, then $T\mathbb{Z}^n = \mathbb{Z}^n$. Thus, $BT\mathbb{Z}^n = B\mathbb{Z}^n$, i.e., BT is a generator if B is. The converse is also true.

Theorem 2.1.5. *Let Λ be a lattice generated by B. Then, generators of Λ are exactly the matrices BT where T is any unimodular matrix.*

Proof. That matrices BT, where T is unimodular, generate Λ follows from the discussion before the theorem. So, assume that D generates Λ, and we will show that $B^{-1}D$ is unimodular.

Suppose that $\Lambda \subset \mathbb{R}^n$. Then, $D\mathbb{Z}^n = \Lambda = B\mathbb{Z}^n$. For each integer $1 \leq j \leq n$, let $x_j, y_j \in \mathbb{Z}^n$ be such that $De_j = Bx_j$ and $Dy_j = Be_j$. Then, for each j, $(B^{-1}De_j, D^{-1}Be_j) = (x_j, y_j) \in \mathbb{Z}^n \times \mathbb{Z}^n$. Hence, $B^{-1}D, D^{-1}B \in \mathbb{Z}^{n \times n}$, as desired. $\square$

Note that, if T is unimodular, then $|\det(T)| = 1$. Indeed,

$$1 = \det(I) = \det(TT^{-1}) = \det(T)\det(T^{-1})$$

implies that $\det(T) \mid 1$, i.e., $|\det(T)| = 1$.

Hence, for any lattice, the absolute value of the determinant of a generator is the same for all generators.

Definition 2.1.6 (Lattice Determinant)**.** Let Λ be a lattice. We define the determinant of Λ by $\det(\Lambda) := |\det(B)|$, where B is any generator of Λ.

In the next section, we give a geometrical interpretation of the determinant of a lattice.

2.1.2 Fundamental Region

A fundamental region of a lattice $\Lambda \subset \mathbb{R}^n$ is any subset $S \subset \mathbb{R}^n$ such that the collection $\{\lambda + S\}_{\lambda \in \Lambda}$ of translates forms a partition of $\mathbb{R}^n$. One example of a fundamental region for a lattice is the fundamental parallelepiped of a generator for the lattice.

Definition 2.1.7 (Fundamental Parallelepiped)**.** Let $B \in \mathbb{R}^{n \times n}$ be invertible. The fundamental parallelepiped of B is defined as $\mathcal{P}(B) := B[0,1)^n$.

It is clear that $\mathcal{P}(B)$ forms a fundamental region for a lattice generated by B, but it is not uniquely so. Nevertheless, one can show that all fundamental regions of a lattice have the same Lebesgue measure, and it is equal to the determinant of the lattice.

Let S and S' be two fundamental regions of a lattice Λ. Then, for any $\lambda \in \Lambda$,

$$S \cap (\lambda + S') = (-\lambda + S) \cap S' + \lambda.$$

Also, by translation-invariance of the Lebesgue measure,

$$\mu_L\left((-\lambda + S) \cap S' + \lambda\right) = \mu_L\left((-\lambda + S) \cap S'\right).$$

Thus,

$$\begin{aligned}
\mu_L(S) &= \mu_L\left(\bigcup_{\lambda \in \Lambda} S \cap (\lambda + S')\right) = \mu_L\left(\bigcup_{\lambda \in \Lambda} ((-\lambda + S) \cap S' + \lambda)\right) \\
&= \sum_{\lambda \in \Lambda} \mu_L\left((-\lambda + S) \cap S' + \lambda\right) = \sum_{\lambda \in \Lambda} \mu_L\left((-\lambda + S) \cap S'\right) \\
&= \mu_L\left(\bigcup_{\lambda \in \Lambda} (-\lambda + S) \cap S'\right) = \mu_L\left(S'\right).
\end{aligned}$$

Thus, all fundamental regions of Λ have the same Lebesgue measure. Finally, if $\Lambda \subset \mathbb{R}^n$, one may compute (using the substitution $x = By$)

$$\mu_L(\mathcal{P}(B)) = \int_{\mathbb{R}^n} 1_{B[0,1)^n}(x)\, d\mu_L(x) = |\det(B)| \int_{\mathbb{R}^n} 1_{[0,1)^n}(y)\, d\mu_L(y) = |\det(B)|.$$

2.1.3 Voronoi Region

The fundamental Voronoi region of a lattice is a fundamental region that is most useful in lattice decoding. Let $\Lambda \subset \mathbb{R}^n$ be a lattice, and consider the collection $\{\tilde{\mathcal{V}}_\lambda(\Lambda)\}_{\lambda\in\Lambda}$ defined by

$$\tilde{\mathcal{V}}_\lambda(\Lambda) = \left\{ y \in \mathbb{R}^n \,;\, \|y-\lambda\| < \min_{\lambda\neq\nu\in\Lambda} \|y-\nu\| \right\}.$$

Note that the $\tilde{\mathcal{V}}_\lambda(\Lambda)$ are pairwise disjoint, and that, for each $\lambda \in \Lambda$, $\tilde{\mathcal{V}}_\lambda(\Lambda) = \lambda + \tilde{\mathcal{V}}_0(\Lambda)$. However, $\tilde{\mathcal{V}}_0(\Lambda)$ is not a fundamental region for Λ, since $\bigcup_{\lambda\in\Lambda} \tilde{\mathcal{V}}_\lambda(\Lambda) \subsetneq \mathbb{R}^n$. Nevertheless, $\mathbb{R}^n \setminus \bigcup_{\lambda\in\Lambda} \tilde{\mathcal{V}}_\lambda(\Lambda)$, being a countable union of sets of measure 0, is also a set of measure 0. So, one may extend $\tilde{\mathcal{V}}_0(\Lambda)$ to be a fundamental region (which we will call the fundamental Voronoi region of Λ), as follows.

For any $\lambda \in \Lambda$, let

$$D_\lambda(\Lambda) := \left\{ y \in \mathbb{R}^n \,;\, \|y\| = \|y-\lambda\| = \min_{\nu\in\Lambda} \|y-\nu\| \right\},$$

and $\mathcal{D}(\Lambda) = \bigcup_{\lambda\in\Lambda} D_\lambda(\Lambda)$. Consider

$$\mathcal{S}(\Lambda) := \{ S \subset \mathcal{D}(\Lambda) \,;\, \Lambda \cap \{x-y \,;\, x,y \in S\} \subset \{0\} \}$$

as a partially ordered set, ordered by set inclusion. If $M \in \mathcal{S}(\Lambda)$ is maximal, then $\tilde{\mathcal{V}}_0(\Lambda) \cup M$ is a fundamental region of Λ (by linearity of Λ and $\mathcal{D}(\Lambda) \cap \bigcup_{\lambda\in\Lambda} \tilde{\mathcal{V}}_\lambda(\Lambda) = \emptyset$).

Lemma 2.1.8. *If $\Lambda \subset \mathbb{R}^n$ is a lattice, then $\mathcal{S}(\Lambda)$ contains a maximal element.*

Proof. For any ascending chain $S_1 \subset S_2 \subset \cdots$ in $\mathcal{S}(\Lambda)$, the element $\bigcup_j S_j$ is an upper bound in $\mathcal{S}(\Lambda)$. Thus, Zorn's lemma yields a maximal element in $\mathcal{S}(\Lambda)$. □

Let $M \in \mathcal{S}(\Lambda)$ be maximal, and denote $\mathcal{V}_0(\Lambda) := \tilde{\mathcal{V}}_0(\Lambda) \cup M$. We call $\mathcal{V}_0(\Lambda)$ a fundamental Voronoi region for Λ, and set $\mathcal{V}_\lambda(\Lambda) := \lambda + \mathcal{V}_0(\Lambda)$ for any $\lambda \in \Lambda$. Denote $\mathcal{V}_0(\Lambda) = \mathcal{V}(\Lambda)$ for short.

2.1.4 Dual Lattice

If $B \in \mathbb{R}^{n\times n}$ is invertible, then it is clear that the two lattices $\Lambda_1 := \{Bx \ ; \ x \in \mathbb{Z}^n\}$ and $\Lambda_2 := \{(B^T)^{-1}x \ ; \ x \in \mathbb{Z}^n\}$ satisfy a duality: $\langle \lambda_1, \lambda_2 \rangle \in \mathbb{Z}$ for any $(\lambda_1, \lambda_2) \in \Lambda_1 \times \Lambda_2$. Further, if $y \in \mathbb{R}^n$ satisfies $\langle \lambda_1, y \rangle \in \mathbb{Z}$ for every $\lambda_1 \in \Lambda_1$, then $y \in \Lambda_2$; indeed, writing $y = (B^T)^{-1}x_2$ where $x_2 \in \mathbb{R}^n$, we see that $\mathbb{Z} \ni \langle Be_j, y \rangle = \langle e_j, x_2 \rangle$ for every $1 \le j \le n$, i.e., $x_2 \in \mathbb{Z}^n$. We call Λ_2 the dual lattice of Λ_1.

Definition 2.1.9. Fix $n \in \mathbb{N}$, and let $\Lambda \subset \mathbb{R}^n$ be a lattice. The lattice

$$\{x \in \mathbb{R}^n \ ; \ \langle \lambda, x \rangle \in \mathbb{Z} \text{ for every } \lambda \in \Lambda\}$$

is called the dual of Λ and denoted Λ^*. The lattice Λ is called self-dual if $\Lambda = \Lambda^*$.

Remark 4. *As $\mathbb{Z}^n$ is generated by the identity matrix, it is self-dual.*

2.2 Lattice Theta Series

The lattice theta series encodes the norm information of a lattice, and inherently lends itself to the Gaussian distribution. Thus, it has found its way in applications relating to coding for the AWGN channel.

2.2.1 Functional Equation

We begin with a definition.

Definition 2.2.1 (Lattice Theta Series)**.** Let $\Lambda \subset \mathbb{R}^n$ be a lattice. We define its theta series to be the function $\Theta_\Lambda : \mathbb{R}_{>0} \longrightarrow \mathbb{R}_{>0}$ given, for every $\tau > 0$, by

$$\Theta_\Lambda(\tau) = \sum_{\lambda \in \Lambda} e^{-\pi\tau\|\lambda\|^2} \tag{2.2}$$

Remark 5. *The sum in 2.2 is well-defined, for it converges uniformly over any* $[\delta, \infty) \subset (0, \infty)$. *Since* e^{-y} *is a decreasing function, uniform convergence follows from convergence of* $\sum_{\lambda\in\Lambda} e^{-\pi\delta\|\lambda\|^2}$. *This latter convergence may be shown using the estimate*

$$|\mathbb{Z}^n \cap \mathcal{B}_n(0, r)| \leq \frac{1}{\sqrt{n\pi}} \left(\frac{\sqrt{2\pi e}r}{\sqrt{n}} + \sqrt{\frac{\pi e}{2}} \right)^n$$

obtained from lemmas 4.1.3 and 4.1.4. Indeed, if $\Lambda = \{Bx \,;\, x \in \mathbb{Z}^n\}$, *and if* σ_n *is a smallest singular value of* B, *then, for any* $x \in \mathbb{Z}^n$ *and* $u > 0$, *the inequality* $\|Gx\| < r$ *necessarily implies that* $\|x\| < r/\sigma_n$. *Hence,*

$$|\Lambda \cap \mathcal{B}_n(0, r)| \leq |\mathbb{Z}^n \cap \mathcal{B}_n(0, r/\sigma_n)| \leq \frac{1}{\sqrt{n\pi}} \left(\frac{r\sqrt{2\pi e}}{\sigma_n\sqrt{n}} + \sqrt{\frac{\pi e}{2}} \right)^n =: f(r).$$

Writing $d = d_{\min}(\Lambda)$, *we see that for any* $m \in \mathbb{N}$

$$\begin{aligned}\sum_{\lambda\in\Lambda\cap\mathcal{B}_n(0,d+m)} e^{-\pi\tau\|\lambda\|^2} &= 1 + \sum_{j=0}^{m-1} \sum_{\lambda\in\Lambda\,;\, j\leq\|\lambda\|-d<j+1} e^{-\pi\tau\|\lambda\|^2} \leq 1 + \sum_{j=0}^{m-1} \frac{|\Lambda \cap \mathcal{B}_n(0, d+j+1)|}{e^{\pi\delta(j+d)^2}} \\ &\leq 1 + \sum_{j=0}^{m-1} \frac{f(d+j+1)}{e^{\pi\delta(j+d)^2}} \leq 1 + \sum_{j=0}^{j_0-1} \frac{f(d+j+1)}{e^{\pi\delta(j+d)^2}} + \sum_{j=j_0}^{m-1} \frac{1}{j^2},\end{aligned}$$

where j_0 *is any natural such that* $j^2 f(d+j+1) \leq e^{\pi\delta(j+d)^2}$ *whenever* $j \geq j_0$, *and convergence follows.*

The following is a classical result.

Theorem 2.2.2 (Theta Series Functional Equation)**.** *For any lattice* $\Lambda \subset \mathbb{R}^n$ *and*

any $t > 0$,

$$\Theta_\Lambda(t) = t^{-n/2}\mu_L(\mathcal{V}(\Lambda))^{-1}\Theta_{\Lambda^*}(t^{-1}).$$

Since an integer lattice $\mathbb{Z}^n$ is self-dual and satisfies $\mu_L(\mathcal{V}(\mathbb{Z}^n)) = \mu_L([-1/2, 1/2]^n) = 1$, theorem 2.2.2 yields that, for any positive integer n and positive real t,

$$\Theta_{\mathbb{Z}^n}(t) = t^{-n/2}\Theta_{\mathbb{Z}^n}(t^{-1}) \tag{2.3}$$

2.2.2 Flatness Factor

If $\Lambda \subset \mathbb{R}^n$ is a lattice, $c \in \mathbb{R}^n$ and $\sigma > 0$, we define $f_{\sigma,c} : \Lambda \longrightarrow \mathbb{R}_{>0}$ by

$$f_{\sigma,c}(\lambda) = \frac{1}{(2\pi\sigma^2)^{n/2}} e^{-\|\lambda - c\|^2/(2\sigma^2)} \tag{2.4}$$

for every $\lambda \in \Lambda$. Further, if $S \subset \Lambda$, then we set $f_{\sigma,\mathbf{c}}(S) = \sum_{\lambda \in S} f_{\sigma,\mathbf{c}}(\lambda)$. Note that $f_{\sigma,0}(\Lambda) = \Theta_\Lambda\left(\frac{1}{2\pi\sigma^2}\right)$ and that $f_{\sigma,c+\lambda}(\Lambda) = f_{\sigma,c}(\Lambda)$ for any $\lambda \in \Lambda$.

Definition 2.2.3 (Flatness Factor)**.** Let $\Lambda \subset \mathbb{R}^n$ be a lattice. The flatness factor of Λ is defined to be the function $\epsilon_\Lambda : \mathbb{R}_{>0} \longrightarrow \mathbb{R}_{\geq 0}$ given, for each $\sigma > 0$, by

$$\epsilon_\Lambda(\sigma) = \max_{c \in \mathcal{V}(\Lambda)} \left|\mu_L(\mathcal{V}(\Lambda)) f_{\sigma,c}(\Lambda) - 1\right|.$$

Remark 6. *One may show using the extreme value theorem that the flatness factor as given in this definition is well-defined, but one may show more, namely, that the maximum is attained at* $c = 0$ *(see [3]), so*

$$\epsilon_\Lambda(\sigma) = \frac{\mu_L(\mathcal{V}(\Lambda))}{(2\pi\sigma^2)^{n/2}} \Theta_\Lambda\left(\frac{1}{2\pi\sigma^2}\right) - 1.$$

2.3 Construction-A Lattices

In this work, we are only concerned with construction−A lattices, which are carved from linear codes.

Definition 2.3.1 (Linear Code)**.** Let q be a prime power, and $n \in \mathbb{N}$. A subspace $C \subset \mathbb{F}_q^n$ is called a linear code. The dimension of C as a vector space is called the dimension of the code, and n the block-length.

If p is prime and $C \subset \mathbb{F}_p^n$ is a linear code, then using the canonical embedding $\mathbb{F}_p^n \hookrightarrow \mathbb{Z}^n$ one sees that the subgroup $C + p\mathbb{Z}^n \subset \mathbb{R}^n$ is a lattice; indeed, it is of rank at least n since it contains the ($\mathbb{R}-$independent, hence $\mathbb{Z}-$independent) $p-$scaled standard basis vectors $pe_1, \cdots, pe_n$, and, on the other hand, it is of rank at most n since it is discrete, for, with $\{r_j := jp + 1\}_{j\in\mathbb{N}}$

$$(C + p\mathbb{Z}^n) \cap \mathcal{B}_n(0, r_j) \subset \{c + pz \; ; \; c \in C, \; z \in \{0, \pm 1, \cdots, \pm j\}^n\}$$

so

$$|\, (C + p\mathbb{Z}^n) \cap \mathcal{B}_n(0, r_j)| \leq (p(2j + 1))^n < \infty$$

Definition 2.3.2 (Construction-A)**.** Let $n \geq 1$ be an integer, and $\Lambda \subset \mathbb{R}^n$ be a lattice. We call Λ a construction−A lattice if there is a prime p and a linear code $C \subset \mathbb{F}_p^n$ such that $\Lambda = C + p\mathbb{Z}^n$.

For any prime power q, integers $1 \leq k \leq n$ and matrix $M \in \mathbb{F}_q^{n\times k}$, the image of the $\mathbb{F}_q-$linear map $\varphi_M : \mathbb{F}_q^k \longrightarrow \mathbb{F}_q^n$, defined by $\varphi_M(x) = Mx$, is a linear code. It is also true that all linear codes may be constructed via this procedure.

Definition 2.3.3. Let p be prime, $1 \leq k \leq n$ be integers and $M \in \mathbb{F}_p^{n\times k}$. We define the linear code and lattice generated by M, respectively, by $C(M) := \mathrm{im}(\varphi_M)$ and $\Lambda(M) := C(M) + p\mathbb{Z}^n$.

For any prime p, integers $1 \leq k \leq n$ and real $a > 0$, we set

$$V_{(n,k,p,a)} = a^n p^{n-k}.$$

For any $M \in \mathbb{F}_p^{n\times k}$, we have that $\mu_L\left(\mathcal{V}(a\Lambda(M))\right) = a^n p^{n-\mathrm{rank}(M)}$. Thus, when M is full-rank,

$$\mu_L\left(\mathcal{V}(a\Lambda(M))\right) = V_{(n,k,p,a)}.$$

2.4 Lattice Ensembles

A collection of lattices $\mathfrak{C} \subset \mathbb{R}^n$, equipped with a probability measure, is called a lattice ensemble. Loeliger ensembles, carved from construction-A lattices, have been a cornerstone for much of the theory of lattice coding for the AWGN channel. In a nutshell, some Loeliger ensembles behave in a collectively uniform manner, hence, by the Minkowski-Hlawka-Siegel (MHS) theorem, they behave collectively reliably for the AWGN channel. We refrain from using the MHS theorem due to its inability to keep explicitness of the parameters of the lattices involved. Instead, we introduce a new explicit averaging argument in the next chapter. In this section, we introduce generalized Loeliger ensembles.

Definition 2.4.1. For any prime p, integers $0 < k < n$ and real $a > 0$, we call (n, k, p, a) a quadruple of parameters, and we denote it usually by $\mathfrak{p}$.

In the sequel, we endow any finite set T with the $\sigma-$algebra $\mathcal{P}(T)$, and a random variable over T always refers to a $T-$valued measurable function.

Definition 2.4.2. Let $\mathfrak{p} = (n, k, p, a)$ be a quadruple of parameters. We let $M_{\mathfrak{p}} \subset \mathbb{F}_p^{n\times k}$ denote the subset of all full-rank matrices. Also, we define $U'_{\mathfrak{p}}$ and $U_{\mathfrak{p}}$ as random matrices uniformly distributed over $\mathbb{F}_p^{n\times k}$ and $M_{\mathfrak{p}}$, respectively, and $u_{\mathfrak{p}}$ as a random vector uniformly distributed over $\mathbb{F}_p^k$. Further, for any random variable G over $\mathbb{F}_p^{n\times k}$,

we set $\xi^{\max}(G) = \max_{y\in\mathbb{F}_p^n\setminus\{0\}} \Pr(Gu_{\mathfrak{p}} = y)$ and $\xi^{(0)}(G) = \Pr(Gu_{\mathfrak{p}} = 0)$. We also denote $\xi_{\mathfrak{p}} = \xi^{(0)}(U'_{\mathfrak{p}})$ for short.

Remark 7. *Note that* $\xi^{\max}(U'_{\mathfrak{p}}) = \frac{1-\xi_{\mathfrak{p}}}{p^n-1}$. *Also, for any* $M \in \mathbb{F}_p^{n\times k}$, *we have that* $M0 = 0$, *so* $1/p^k \leq \xi_{\mathfrak{p}}$.

Let $\mathfrak{p} = (n, k, p, a)$ be a quadruple of parameters. By finiteness of $\mathbb{F}_p^{n\times k}$, we may extend a random variable G over $\mathbb{F}_p^{n\times k}$ to a random variable $\Lambda(G)$. More generally, consider any sets T_1 and T_2, where T_1 is finite, any random variable R over T_1 and any function $g : T_1 \longrightarrow T_2$. Replacing T_2 by the range of g, which is necessarily a finite set, it is clear that g is measurable. Hence, $g(R)$ is a well-defined random variable. In the sequel, we will consider the composition of random variables over finite sets with various functions. When we do so, we are assuming that a similar construction to the one discussed here is made. Then, such composition is a random variable.

Definition 2.4.3. Let $\mathfrak{p} = (n, k, p, a)$ be a quadruple of parameters. We set $\Lambda'_{\mathfrak{p}} = a\Lambda(U'_{\mathfrak{p}})$ and $\Lambda_{\mathfrak{p}} = a\Lambda(U_{\mathfrak{p}})$.

Note that $\Lambda'_{\mathfrak{p}}$ is a Loeliger ensemble, so in virtue of this, $\Lambda(G)$ may be considered as a generalized Loeliger ensemble for a nonnecessarily uniform G.

2.5 AWGN Channel

A communication channel where the output Y is given by a sum of the input X and a white Gaussian noise N independent of the input is called an Additive White Gaussian Noise (AWGN) channel. The central limit theorem along with the physics of electromagnetic waves tell us that the AWGN channel is a good model for many communication scenarios.

2.5.1 Preliminaries

For performance analysis, it is natural to impose power constraints, e.g., to consider, for a fixed noise $N \sim \mathcal{N}(0, \sigma_N^2 I_n)$ and a fixed positive real number P, channels $Y = X + N$ where the distribution of X varies but is only required to satisfy the average-power constraint $\frac{1}{n}\mathbb{E}\left[\|X\|^2\right] \leq P$. One could also consider a maximum-power constraint. In such cases, the AWGN channel is said to be power-constrained. The quantity P/σ_N^2 is known as the Signal-to-Noise-Ratio, and denoted SNR.

The input X is drawn from a set $\mathcal{C}$ called the codebook, whose elements are called the codewords. In case $\mathcal{C}$ has finitely many elements, the rate of communication is defined as $\frac{1}{n}\log|\mathcal{C}|$, and is usually denoted by R. One way to extend these settings for an infinite codebook $\mathcal{C}$ is to consider a variable-rate coding scheme. In such a case, the rate becomes an averaged rate, for which it is known that the maximum achievable rate $R_{\max}$ satisfies

$$R_{\max} \geq \frac{1}{n}\mathbb{H}(X), \tag{2.5}$$

where $\mathbb{H}(X)$ is the entropy of X.

A rate R is said to be achievable if there is a sequence $\{\mathcal{C}_n\}_{n\in\mathbb{N}}$ of codebooks $\mathcal{C}_n \subset \mathbb{R}^n$ each of rate R such that the maximal probability of error for decoding the codebooks $\mathcal{C}_n$ under the Maximum A Posteriori (MAP) decoder approaches 0 as $n \longrightarrow \infty$. It is well-known that a rate $R > 0$ is achievable if and only if

$$R < \frac{1}{2}\log\left(1 + \mathrm{SNR}\right),$$

where $\frac{1}{2}\log\left(1 + \mathrm{SNR}\right)$ is called the capacity of the channel.

2.5.2 Lattice Decoding and AWGN-Goodness

Let $n \in \mathbb{N}$, and $\Lambda \subset \mathbb{R}^n$ be a lattice. We define $Q_\Lambda^{\mathrm{NN}} : \mathbb{R}^n \longrightarrow \Lambda$ by its restrictions to the Voronoi regions of Λ as $Q_\Lambda^{\mathrm{NN}}\big|_{\mathcal{V}_\lambda(\Lambda)} = \lambda$. Note that, for any $q \in \mathbb{R}^n$ and $\lambda \in \Lambda$, we have that $Q_\Lambda^{\mathrm{NN}}(\lambda + q) \neq \lambda$ if and only if $q \notin \mathcal{V}(\Lambda)$. Then, for any two random variables X and W,

$$\begin{aligned}
\Pr\left(Q_\Lambda^{\mathrm{NN}}(X+W) \neq X\right) &= \sum_{\lambda\in\Lambda} \Pr\left(Q_\Lambda^{\mathrm{NN}}(X+W) \neq X \mid X = \lambda\right) \cdot \Pr(X = \lambda) \\
&= \sum_{\lambda\in\Lambda} \Pr\left(Q_\Lambda^{\mathrm{NN}}(\lambda+W) \neq \lambda \mid X = \lambda\right) \cdot \Pr(X = \lambda) \\
&= \sum_{\lambda\in\Lambda} \Pr\left(W \notin \mathcal{V}(\Lambda) \mid X = \lambda\right) \cdot \Pr(X = \lambda) \\
&= \Pr\left(W \notin \mathcal{V}(\Lambda)\right) \qquad (2.6)
\end{aligned}$$

is independent of the distribution of X.

Definition 2.5.1. Let $n \in \mathbb{N}$, $\Lambda \subset \mathbb{R}^n$ be a lattice and W be an $\mathbb{R}^n-$valued random variable. We call $\Pr\left(W \notin \mathcal{V}(\Lambda)\right)$ the probability of error of nearest neighbor (or, lattice) decoding for the infinite constellation Λ over the AWGN channel with noise W.

The importance of AWGN-good lattices is great in coding theory. Recall that the Volume-to-Noise Ratio (VNR) of a lattice $\Lambda \subset \mathbb{R}^n$ is defined by $\gamma_\Lambda(\sigma) := \mu_L(\mathcal{V}(\Lambda))^{2/n}/\sigma^2$.

Definition 2.5.2. A sequence of lattices $\{\Lambda^{(n)}\}_{n\in\mathbb{N}}$ is said to be AWGN-good if $\liminf_{n\to\infty} \gamma_{\Lambda^{(n)}}(\sigma_{w,n}) > 2\pi e$ implies $\Pr\left(W^{(n)} \notin \mathcal{V}(\Lambda^{(n)})\right) \longrightarrow 0$ as $n \longrightarrow \infty$.

2.6 A Counting Function N_S

For ease of presentation, we use the following shorthand. For any $n \in \mathbb{Z}_{>0}$ and $S \subset \mathbb{R}^n$, define $N_S : \mathcal{P}(\mathbb{R}^n) \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$ by $N_S(\Lambda) = |\Lambda \cap (S \setminus \{0\})|$. The following lemma is easy to show.

Lemma 2.6.1. *For any $n \in \mathbb{N}$, set I, and sets $S \subset \mathbb{R}^n$ and $\bigcup_{i\in I} \Lambda_i = \Lambda \subset \mathbb{R}^n$, we have that*

$$N_S(\Lambda) = \sum_{i\in I} N_S(\Lambda_i)$$

if and only if $N_S(\Lambda) = \infty$ or $\bigcup_{i\neq j} I_i \cap I_j \subset \{0\} \cup S^c$. Also, for any $a > 0$,

$$N_S(a\Lambda) = N_{\frac{1}{a}S}(\Lambda).$$

2.7 The $q-$Pochhammer Symbol

Definition 2.7.1 ($q-$Pochhammer Symbol)**.** For any $(a, q, n) \in \mathbb{C} \times \mathbb{C} \times (\mathbb{Z} \cup \{\infty\})$, the $q-$Pochhammer symbol $(a; q)_n$ is defined by

$$(a;q)_n = \begin{cases} \prod_{\ell=0}^{n-1}(1 - aq^\ell), & \text{if } n \geq 0 \\ \prod_{\ell=n}^{-1}(1 - aq^\ell), & \text{otherwise} \end{cases}$$

whenever the product converges, and where the empty product is taken to be 1. When $a = q$ and $n = \infty$, one obtains the Euler function $\phi(q) = (q; q)_\infty$.

Remark 8. *The Euler function well be of interest to us when $1/q \in \mathscr{P}$. One can show that, if $|q| < 1$, the Euler function is well-defined and nonzero. This is clear for $q = 0$, so assume $|q| < 1$ and $q \neq 0$. The product $\phi(q)$ is well-defined and nonzero if and only if the series $S := \sum_{\ell=1}^{\infty} \ln(1 - q^\ell)$ converges. But, we have the Taylor*

expansions $\ln(1-q^\ell) = \sum_{m=1}^{\infty} \frac{q^{\ell m}}{m}$ *for each* $\ell \in \mathbb{N}$, *and Tonelli's theorem yields that*

$$\sum_{\ell=1}^{\infty} \left| \sum_{m=1}^{\infty} \frac{q^{\ell m}}{m} \right| \leq \sum_{m=1}^{\infty} \frac{1}{m} \sum_{\ell=1}^{\infty} |q|^{\ell m} = \sum_{m=1}^{\infty} \frac{1}{m(|q|^{-m}-1)} \leq \sum_{m=1}^{\infty} \frac{|q|^m}{1-|q|} = \frac{|q|}{(1-|q|)^2} < \infty,$$

so S *is absolutely convergent. Thus, in particular,* $\min_{p\in\mathscr{P},n\geq 0}(1/p;1/p)_n = \phi(1/2) > e^{-2}$. *In fact, one may show that* $\phi(1/2) = 0.288788\ldots$.

Chapter 3

Averaging Argument

A lattice sum is any well-defined sum $\sum_{\lambda\in\Lambda} s(\lambda)$, where Λ is a lattice and $s : \Lambda \longrightarrow \mathbb{R}$ is a function. Lattice sums occur naturally when dealing with lattice coding. We introduce here a new averaging argument that is capable of transforming the hard problem of finding a lattice sum for a general lattice into the easier one of finding a corresponding sum over integer lattices $\mathbb{Z}^n$.

3.1 Motivation: The Probability of Error and Lattice Sums

We describe in this section how an upper bound on a particular averaged lattice sum might yield a useful upper bound on the probability of error for lattice decoding for the AWGN channel.

Using a subset of a lattice $\Lambda \subset \mathbb{R}^n$ as a codebook for an AWGN channel in the presence of noise $W^{(n)}$, lattice decoding incurs a probability of error of exactly $\Pr\left(W^{(n)} \notin \mathcal{V}(\Lambda)\right)$. A lattice sum may be incorporated into this quantity, as follows. For any $q \in \mathbb{R}^n$, we have that $\emptyset = \Lambda \cap (\mathcal{B}_n(q, \|q\|) \setminus \{0\})$ if and only if $\|q\| = \min_{\lambda\in\Lambda} \|q - \lambda\|$. Thus, as $\Pr(W^{(n)} \in S) = 0$ whenever $S \subset \mathbb{R}^n$ is of measure 0,

and as the boundary of a Voronoi region is of measure 0, we get that

$$\begin{aligned}\Pr\left(W^{(n)} \notin \mathcal{V}(\Lambda)\right) &= \Pr\left(\left|\Lambda \cap \left(\mathcal{B}_n(W^{(n)}, \|W^{(n)}\|) \setminus \{0\}\right)\right| \geq 1\right) \\ &= \Pr\left(\sum_{\lambda \in \Lambda} \left|\{\lambda\} \cap \left(\mathcal{B}_n(W^{(n)}, \|W^{(n)}\|) \setminus \{0\}\right)\right| \geq 1\right) \end{aligned} \tag{3.1}$$

Recall the shorthand $N_S(\Lambda) = |\Lambda \cap (S \setminus \{0\})|$, and note that, by rewriting $N_S(\Lambda) = \sum_{\lambda \in \Lambda} |\{\lambda\} \cap (S \setminus \{0\})|$ we may regard this quantity as a lattice sum. Then, equation 3.1 is just

$$\Pr\left(W^{(n)} \notin \mathcal{V}(\Lambda)\right) = \Pr\left(N_{\mathcal{B}_n(W^{(n)}, \|W^{(n)}\|)}(\Lambda) \geq 1\right) \tag{3.2}$$

Furthermore, Markov's inequality yields that

$$\Pr\left(N_{\mathcal{B}_n(W^{(n)}, \|W^{(n)}\|)}(\Lambda) \geq 1\right) \leq \mathbb{E}\left[N_{\mathcal{B}_n(W^{(n)}, \|W^{(n)}\|)}(\Lambda)\right].$$

Now, suppose that Λ, instead of being a predetermined lattice, is chosen probabilistically from a lattice ensemble $\mathfrak{C}$, and suppose that one could upper bound the averaged lattice sum $\mathbb{E}_\Lambda\left[N_{\mathcal{B}_n(W^{(n)}, \|W^{(n)}\|)}(\Lambda)\right]$ by a constant $\delta > 0$ not depending on $W^{(n)}$. Then,

$$\mathbb{E}_\Lambda\left[\Pr_{W^{(n)}}\left(W^{(n)} \notin \mathcal{V}(\Lambda)\right)\right] \leq \mathbb{E}_{W^{(n)}}\left[\mathbb{E}_\Lambda\left[N_{\mathcal{B}_n(W^{(n)}, \|W^{(n)}\|)}(\Lambda)\right]\right] \leq \delta \tag{3.3}$$

where switching the order of expectations is justified by Tonelli's theorem as the random variable $N_{\mathcal{B}_n(W^{(n)}, \|W^{(n)}\|)}(\Lambda)$ is nonnegative and $\mathbb{E}_\Lambda$ is just a finite positive linear combination. Hence, for at least one $\Lambda_0 \in \mathfrak{C}$, we have that

$$\Pr\left(W^{(n)} \notin \mathcal{V}(\Lambda_0)\right) \leq \delta.$$

In short, an upper bound on an averaged lattice sum is also an upper bound on at least one lattice. Further, applying Markov's inequality on inequality 3.3 might allow

extending such a result to more than one lattice.

3.2 Proposed Averaging Argument

The following inequality is used to derive our averaging argument.

Lemma 3.2.1. *For any quadruple of parameters* $\mathfrak{p} = (n, k, p, a)$, $M \in \mathbb{F}_p^{n\times k}$ *and* $s : \mathbb{R}^n \longrightarrow [0, \infty]$, *we have that*

$$\sum_{\lambda\in\Lambda(M)} s(\lambda) \leq p^k \sum_{y\in\mathbb{F}_p^n} \sum_{z\in\mathbb{Z}^n} \Pr(Mu_{\mathfrak{p}} = y) \cdot s(y + pz).$$

Proof. This follows from

$$\sum_{\lambda\in\Lambda(M)} s(\lambda) = \sum_{z\in\mathbb{Z}^n} \sum_{y\in\mathbb{F}_p^n} s(y + pz) \cdot 1_{C(M)}(y)$$

and $1_{C(M)}(y) \leq |\{x \in \mathbb{F}_p^k; Mx = y\}| = p^k \Pr(Mu_{\mathfrak{p}} = y)$. □

Proposition 3.2.2. *For any quadruple of parameters* $\mathfrak{p} = (n, k, p, a)$, *random variable* G *over* $\mathbb{F}_p^{n\times k}$ *and* $s : \mathbb{R}^n \longrightarrow [0, \infty]$, *we have that*

$$\mathbb{E}_G \left[\sum_{\lambda\in\Lambda(G)} s(\lambda) \right] \leq p^k \mathbb{E}_{Gu_{\mathfrak{p}}} \left[\sum_{z\in\mathbb{Z}^n} s(Gu_{\mathfrak{p}} + pz) \right].$$

Proof. By lemma 3.2.1, we have that

$$\begin{aligned} \mathbb{E}_G \left[\sum_{\lambda\in\Lambda(G)} s(\lambda) \right] &= \sum_{M\in\mathbb{F}_p^{n\times k}} \Pr(G = M) \sum_{\lambda\in\Lambda(M)} s(\lambda) \\ &\leq p^k \sum_{y\in\mathbb{F}_p^n} \Pr(Gu_{\mathfrak{p}} = y) \sum_{z\in\mathbb{Z}^n} s(y + pz) = p^k \mathbb{E}_{Gu_{\mathfrak{p}}} \left[\sum_{z\in\mathbb{Z}^n} s(Gu_{\mathfrak{p}} + pz) \right], \end{aligned}$$

as desired. □

Finally, our averaging argument is the following weaker, but more suggestive, form of proposition 3.2.2.

Proposition 3.2.3. *For any quadruple of parameters* $\mathfrak{p} = (n, k, p, a)$, *random variable* G *over* $\mathbb{F}_p^{n\times k}$ *and* $s : \mathbb{R}^n \longrightarrow [0, \infty]$, *we have that*

$$\mathbb{E}_G\left[\sum_{\lambda\in\Lambda(G)} s(\lambda)\right] \leq p^k\left(\sum_{z\in\mathbb{Z}^n} \xi^{\max}(G)s(z) + (\xi^{(0)}(G) - \xi^{\max}(G))s(pz)\right).$$

Further, if $s|_{p\mathbb{Z}^n} = 0$, *then*

$$\mathbb{E}_G\left[\sum_{\lambda\in\Lambda(G)} s(\lambda)\right] \leq p^k\xi^{\max}(G)\sum_{z\in\mathbb{Z}^n} s(z).$$

3.3 Applications

This averaging argument will be used in the following chapters to derive upper bounds for the two fundamental quantities we are seeking to control the size of: the probability of error for lattice decoding in an AWGN channel, and the flatness factor.

First, for a suitable choice (see proposition 4.1.2) of an indicator function in place of s in proposition 3.2.3, one obtains (along the lines of the discussion in section 3.1) an upper bound for the probability of error of lattice decoding in an AWGN channel.

The second application of the averaging argument is in proposition 5.1.1, where a Gaussian function is used in place of s in proposition 3.2.3 to obtain an upper bound on the average size of the lattice theta series, thereby giving an upper bound on the average size of the flatness factor.

3.4 Averaging Arguments in the Literature

We present here the two main averaging arguments used in the literature, which may be referred to collectively as the Minkowski-Hlawka-Siegel theorem.

Theorem 3.4.1 (MHS). *Fix $n \in \mathbb{N}$ and $V > 0$, and let*

$$\mathfrak{C} = \{\Lambda \subset \mathbb{R}^n \ ; \ \Lambda \text{ is a lattice and } \mu_L(\mathcal{V}(\Lambda)) = V\}.$$

Then, there is a probability measure ν on $\mathfrak{C}$ such that for any Riemann-integrable function $f : \mathbb{R}^n \longrightarrow \mathbb{R}$ of bounded support

$$\int_{\mathfrak{C}} \sum_{\lambda \in \Lambda} f(\lambda) \, d\nu(\Lambda) = V^{-1} \int_{\mathbb{R}^n} f(x) \, d\mu_L(x).$$

For any quadruple of parameters $\mathfrak{p} = (n, k, p, a)$, we call a subset $\mathcal{S} \subset M_{\mathfrak{p}}$ balanced if the function $g : \mathbb{F}_p^n \setminus \{0\} \longrightarrow \mathbb{N}$ defined by $g(y) := |\{S \in \mathcal{S} \ ; \ y \in S\mathbb{F}_p^k\}|$ is constant.

Theorem 3.4.2. *Fix $n \in \mathbb{N}$, $V > 0$, integers $0 < k < n$ and a Riemann-integrable function $f : \mathbb{R}^n \longrightarrow \mathbb{R}$ of bounded support. For each prime p, let $a_p > 0$ be such that the quadruple of parameters $\mathfrak{p}_p := (n, k, p, a_p)$ satisfies $V_{\mathfrak{p}_p} = V$, and let $\mathcal{S}_p \subset M_{\mathfrak{p}_p}$ be balanced. Then*

$$\lim_{p \to \infty} \frac{1}{|\mathcal{S}_p|} \sum_{S \in \mathcal{S}_p} \sum_{u \in a_p \Lambda(S) \setminus \{0\}} f(u) = V^{-1} \int_{\mathbb{R}^n} f(x) \, d\mu_L(x).$$

We note two weaknesses of the MHS theorem. First, it can only be applied to functions of bounded support. Hence, it cannot be applied to the lattice theta series, nor to the flatness factor. In [3], lattice theta series are averaged without appeal to the MHS theorem. Yet, the averaging in [3] approximates a Riemann sum as an integral, which is the second weakness that the MHS theorem suffers from. If the approximation is to be used to bound the probability of error, for example, then

one must compensate for the approximation error term. This error term is either unknown in general for the Lebesgue integral, or it is known to be polynomial in the mesh size at best for the Riemann integral. However, a polynomial in the mesh size is an exponentially decaying function only if the size of the prime number used for construction−A is exponential. Thus, to obtain practical parameters for the construction−A lattices, the MHS theorems must be dispensed with.

Chapter 4

AWGN-Good Lattices

In the literature, capacity-achieving lattice codes, for which the probability of error decays exponentially according to some form of Poltyrev's error exponent, are carved from AWGN-good lattices via either Voronoi (physical) shaping [2] or Gaussian (probabilistic) shaping [3]. We base our construction on that in [3]. However, in [3], no parameters are provided for which AWGN-good lattices exist. Parameters yielding AWGN-good lattices are provided in [2], but we prove here that less restrictive conditions can give rise to AWGN-good lattices. In particular, we show that primes of size sub-linear in the block-length yield AWGN-good lattices via construction$-$A.

4.1 Upper Bound on Probability of Error

An upper bound on the probability of error is first derived, then it is shown that some conditions on the quadruples of parameters make this upper bound decay exponentially with a Poltyrev exponent.

We introduce first the terms in the upper bound. For any quadruple of parameters $\mathfrak{p} = (n, k, p, a)$, any random variable G over $\mathbb{F}_p^{n\times k}$, and any $\rho > 0$, define (see Appendix A for an argument that this is a well-defined expression)

$$h(\mathfrak{p}, G, \rho) := \mathbb{E}_{W^{(n)}}\left[\mathbb{E}_G\left[N_{\mathcal{B}_n(W^{(n)},\rho)}(a\Lambda(G) \setminus ap\mathbb{Z}^n)\right] \;\middle|\; \|W^{(n)}\| = \rho\right] \tag{4.1}$$

Since $\mathbb{E}_G$ is a finite linear combination, and since the counting function N_S is always nonnegative, one may exchange the order of expectations in the definition of $h(\mathfrak{p}, G, \rho)$, i.e., we may rewrite $h(\mathfrak{p}, G, \rho) = \mathbb{E}_G \left[\mathbb{E}_{W^{(n)}} \left[N_{\mathcal{B}(W^{(n)},\rho)}(a\Lambda(G) \setminus ap\mathbb{Z}^n) \;\middle|\; \|W^{(n)}\| = \rho \right] \right]$. Define also

$$I_{\mathfrak{p}}\left(G, W^{(n)}\right) := \int_0^\infty f_{\|W^{(n)}\|}(\rho) \cdot \min\left(h(\mathfrak{p}, G, \rho), 1\right) \, d\rho \tag{4.2}$$

and

$$A_{\mathfrak{p}}^{\mathrm{NN}}(G, W^{(n)}) := \Pr(\|W^{(n)}\| > ap/2) + I_{\mathfrak{p}}\left(G, W^{(n)}\right) \tag{4.3}$$

We have the following upper bound on the averaged probability of error for lattice decoding.

Proposition 4.1.1. *For any quadruple of parameters $\mathfrak{p} = (n, k, p, a)$ and any random variable G over $\mathbb{F}_p^{n\times k}$, we have that*

$$\mathbb{E}_G\left[\Pr\left(W^{(n)} \notin \mathcal{V}(a\Lambda(G))\right)\right] \leq A_{\mathfrak{p}}^{\mathrm{NN}}(G, W^{(n)}).$$

Proof. First, note that, by equation 3.2,

$$\Pr\left(W^{(n)} \notin \mathcal{V}(a\Lambda(G))\right) = \Pr\left(N_{\mathcal{B}_n(W^{(n)}, \|W^{(n)}\|)}(a\Lambda(G)) \geq 1\right).$$

Conditioning on $\|W^{(n)}\|$, we get that

$$\Pr\left(W^{(n)} \notin \mathcal{V}(a\Lambda(G))\right) = \int_0^\infty f_{\|W^{(n)}\|}(r) \cdot \Pr(N_{\mathcal{B}_n(W^{(n)}, r)}(a\Lambda(G)) \geq 1 \mid \|W^{(n)}\| = r)\, dr.$$

For any subset $S \subset \mathbb{R}^n$ and any $r > 0$, denote

$$g(S, r) = \Pr(N_{\mathcal{B}_n(W^{(n)}, r)}(S) \geq 1 \mid \|W^{(n)}\| = r).$$

Since $g(S \cup T, r) \leq g(S, r) + g(T, r)$ whenever $S, T \subset \mathbb{R}^n$, we have that

$$\Pr\left(W^{(n)} \notin \mathcal{V}(a\Lambda(G))\right) \leq \int_0^\infty f_{\|W^{(n)}\|}(r) \cdot g(ap\mathbb{Z}^n, r)\, dr + \int_0^\infty f_{\|W^{(n)}\|}(r) \cdot g(a\Lambda(G) \setminus ap\mathbb{Z}^n, r)\, dr \tag{4.4}$$

We will upper bound the first integral in the right hand side of inequality 4.4 by $\Pr\left(\|W^{(n)}\| > ap/2\right)$, and the expectation, with respect to G, of the second integral by $I_{\mathfrak{p}}(G, W^{(n)})$.

Note that, for any $r > 0$, if $apx \in \mathcal{B}_n(q, r)$ for some $q \in \mathbb{R}^n$ and nonzero $x \in \mathbb{Z}^n$, then

$$ap - \|q\| \leq \|apx\| - \|q\| \leq \|apx - q\| \leq r,$$

so $ap - r \leq \|q\|$. Hence, for any $r > 0$,

$$\left\{q \in \mathbb{R}^n \,;\, N_{\mathcal{B}_n(q,r)}(ap\mathbb{Z}^n) \geq 1\right\} \subset \left\{q \in \mathbb{R}^n \,;\, \|q\| \geq ap - r\right\},$$

which yields

$$g(ap\mathbb{Z}^n, r) \leq \Pr\left((\|W^{(n)}\| \geq ap - r \,|\, \|W^{(n)}\| = r\right) = 1_{[ap/2,\infty)}(r).$$

Thus,

$$\int_0^\infty f_{\|W^{(n)}\|}(r) \cdot g(ap\mathbb{Z}^n, r)\, dr \leq \Pr\left(\|W^{(n)}\| \geq ap/2\right).$$

In addition, for any $r > 0$, Markov's inequality yields that

$$g(a\Lambda(G) \setminus ap\mathbb{Z}^n, r) \leq \mathbb{E}_{W^{(n)}}\left[N_{\mathcal{B}(W^{(n)},r)}(a\Lambda(G) \setminus ap\mathbb{Z}^n) \;\middle|\; \|W^{(n)}\| = r\right],$$

so $\mathbb{E}_G\left[g(a\Lambda(G) \setminus ap\mathbb{Z}^n, r)\right] \leq h(\mathfrak{p}, G, r)$. Further, being a probability, we always have

$g(a\Lambda(G) \setminus ap\mathbb{Z}^n, r) \leq 1$. Thus,

$$\begin{aligned}
&\mathbb{E}_G\left[\int_0^\infty f_{\|W^{(n)}\|}(r) \cdot g(a\Lambda(G) \setminus ap\mathbb{Z}^n, r)\, dr\right] \\
&= \int_0^\infty f_{\|W^{(n)}\|}(r) \cdot \mathbb{E}_G\left[g(a\Lambda(G) \setminus ap\mathbb{Z}^n, r)\right]\, dr \\
&\leq \int_0^\infty f_{\|W^{(n)}\|}(r) \cdot \min\left(h(\mathfrak{p}, G, r), 1\right)\, dr = I_{\mathfrak{p}}(G, W^{(n)}),
\end{aligned}$$

as desired. □

Now, we proceed to upper bounding the terms in $A_{\mathfrak{p}}^{\mathrm{NN}}(G, W^{(n)})$. The first application of our averaging argument (proposition 3.2.3) is via considering a lattice sum of an indicator function, as follows.

Proposition 4.1.2. *For any quadruple of parameters $\mathfrak{p} = (n, k, p, a)$, random variable G over $\mathbb{F}_p^{n\times k}$ and $S \subset \mathbb{R}^n$, we have that*

$$\mathbb{E}_G\left[N_S(a\Lambda(G) \setminus ap\mathbb{Z}^n)\right] \leq p^k \cdot \xi^{\max}(G) \cdot N_{\frac{1}{a}S}(\mathbb{Z}^n) \tag{4.5}$$

Proof. Using $s : \mathbb{R}^n \longrightarrow [0, \infty]$ defined by $s(\lambda) = N_S(\{a\lambda\} \setminus ap\mathbb{Z}^n)$ in proposition 3.2.3, one obtains, since $s|_{p\mathbb{Z}^n} = 0$,

$$\mathbb{E}_G\left[N_S(a\Lambda(G) \setminus ap\mathbb{Z}^n)\right] \leq p^k \cdot \xi^{\max}(G) \cdot N_S(a\mathbb{Z}^n \setminus ap\mathbb{Z}^n).$$

Now, inequality 4.5 follows from

$$N_S(a\mathbb{Z}^n \setminus ap\mathbb{Z}^n) \leq N_S(a\mathbb{Z}^n) = N_{\frac{1}{a}S}(\mathbb{Z}^n).$$

□

In view of equation 4.1 and inequality 4.5, it is useful to have an upper bound on the number of integer lattice points lying inside a hypersphere. One such bound is

given in the following lemma.

Lemma 4.1.3 ([4]). *For any $q \in \mathbb{R}^n$ and $r > 0$, we have that*

$$N_{\mathcal{B}_n(q,r)}\left(\mathbb{Z}^n\right) \leq \mu_L(\mathcal{B}_n(0,1)) \left(r + \frac{\sqrt{n}}{2}\right)^n.$$

Further, we have the following well-known estimate on the volume of $n-$balls.

Theorem 4.1.4. *For each $n \in \mathbb{N}$, we have that*

$$\mu_L(\mathcal{B}_n(0,1)) \leq \frac{1}{\sqrt{n\pi}} \left(\frac{2\pi e}{n}\right)^{n/2}.$$

Furthermore, as $n \longrightarrow \infty$, $\mu_L(\mathcal{B}_n(0,1)) \sim \frac{1}{\sqrt{n\pi}} \left(\frac{2\pi e}{n}\right)^{n/2}$.

Combining inequality 4.5, lemma 4.1.3 and theorem 4.1.4, one obtains the following inequality.

Corollary 4.1.4.1. *For any quadruple of parameters $\mathfrak{p} = (n, k, p, a)$, random variable G over $\mathbb{F}_p^{n\times k}$, $q \in \mathbb{R}^n$ and $r > 0$, we have that*

$$\mathbb{E}_G\left[N_{\mathcal{B}_n(q,r)}(a\Lambda(G) \setminus ap\mathbb{Z}^n)\right] \leq \frac{p^n \cdot \xi^{\max}(G)}{\sqrt{\pi n}} \left(\frac{r\sqrt{2\pi e}}{V_{\mathfrak{p}}^{1/n}\sqrt{n}} + \frac{\sqrt{\pi e/2}}{p^{1-k/n}}\right)^n \tag{4.6}$$

Employing inequality 4.6 into the definition of $h(\mathfrak{p}, G, r)$ in equation 4.1 one obtains the following inequality.

Corollary 4.1.4.2. *For any quadruple of parameters $\mathfrak{p} = (n, k, p, a)$, random variable G over $\mathbb{F}_p^{n\times k}$, and $r > 0$, we have that*

$$h(\mathfrak{p}, G, r) \leq \frac{p^n \cdot \xi^{\max}(G)}{\sqrt{\pi n}} \left(\frac{r\sqrt{2\pi e}}{V_{\mathfrak{p}}^{1/n}\sqrt{n}} + \frac{\sqrt{\pi e/2}}{p^{1-k/n}}\right)^n \tag{4.7}$$

With inequality 4.7 at hand, we derive an upper bound on $I_{\mathfrak{p}}(G, W^{(n)})$. Given a quadruple of parameters $\mathfrak{p} = (n, k, p, a)$ and two positive reals u and b, we introduce

the following shorthands:

$$\begin{aligned}
\varepsilon_{\mathfrak{p}} &:= V_{\mathfrak{p}}^{2/n}/(2\pi e\sigma_{w,n}^2) - 1 \\
L_{\mathfrak{p}} &:= \Pr\left(\|W^{(n)}\| > \sqrt{n\sigma_{w,n}^2(1+\varepsilon_{\mathfrak{p}})}\right) \\
C_{\mathfrak{p}} &:= \left[\sqrt{n\sigma_{w,n}^2}, \sqrt{n\sigma_{w,n}^2(1+\varepsilon_{\mathfrak{p}})}\right] \\
E_{\mathrm{sp}}(u) &:= 1_{[1,\infty)}(u) \cdot \frac{u - 1 - \log u}{2} \\
v_{\mathfrak{p}}^{\mathrm{NN}}(u,b) &:= E_{\mathrm{sp}}\left(\frac{u^2}{n\sigma_{w,n}^2}\right) - \frac{n-1}{n}\log\left(\frac{u}{\sqrt{n\sigma_{w,n}^2(1+b)}} + \frac{\sqrt{\pi e/2}}{p^{1-k/n}}\right) \\
K_{\mathfrak{p}} &:= \left(\frac{\sqrt{\pi e/2}}{p^{1-k/n}}\right)^n + n\left(\left(\frac{1}{\sqrt{1+\varepsilon_{\mathfrak{p}}}} + \frac{\sqrt{\pi e/2}}{p^{1-k/n}}\right)^n + e^{-n\cdot\inf_{u\in C_{\mathfrak{p}}} v_{\mathfrak{p}}^{\mathrm{NN}}(u,\varepsilon_{\mathfrak{p}})}\right)
\end{aligned}$$

Lemma 4.1.5. *Let $\mathfrak{p} = (n,k,p,a)$ be a quadruple of parameters such that $\varepsilon_{\mathfrak{p}} > 0$, and G be any random variable over $\mathbb{F}_p^{n\times k}$. Then,*

$$I_{\mathfrak{p}}\left(G, W^{(n)}\right) < \frac{\ell p^n \cdot \xi^{\max}(G)}{\sqrt{\pi n}} K_{\mathfrak{p}} + \left(1 - \frac{\ell p^n \cdot \xi^{\max}(G)}{\sqrt{\pi n}}\left(1 + \frac{\sqrt{\pi e/2}}{p^{1-k/n}}\right)^n\right) L_{\mathfrak{p}}$$

Proof. See Appendix B. □

4.2 Loeliger-Good Sequences

In view of lemma 4.1.5, we make the following definition.

Definition 4.2.1. For any sequence $\mathfrak{S} = \{\mathfrak{p}_n = (n, k_n, p_n, a_n)\}_{n\in\mathbb{Z}_{>1}}$, an $\mathfrak{S}$-*Lolieger-good sequence* is a sequence $\{G_n\}_{n\in\mathbb{Z}_{>1}}$ where, for each n, G_n is a random variable over $\mathbb{F}_{p_n}^{n\times k_n}$ and such that there is a sequence $\{\ell_n\}_{n\in\mathbb{Z}_{>1}} \subset [1,\infty)$ making

$$\liminf_{n\to\infty} \frac{\ell_n p_n^n \cdot \xi^{\max}(G_n)}{\sqrt{\pi n}}\left(1 + \frac{\sqrt{\pi e/2}}{p_n^{1-k_n/n}}\right)^n > 1 \tag{4.8}$$

and

$$\lim_{n\to\infty}\frac{1}{n}\log\left(\ell_n p_n^n\cdot\xi^{\max}(G_n)\right)\leq 0 \tag{4.9}$$

Remark 9. *If $\{G_n\}_{n\in\mathbb{Z}_{>1}}$ is $\mathfrak{S}$-Lolieger-good, and if $K_{\mathfrak{p}_n}\leq e^{-n(\alpha+o(1))}$ as $n\longrightarrow\infty$ for some constant $\alpha>0$, then we also have that $I_{\mathfrak{p}_n}(G_n,W^{(n)})\leq e^{-n(\alpha+o(1))}$ as $n\longrightarrow\infty$.*

4.3 Error Exponent

Powerful in deriving error exponents is the following version of the Chernoff bound.

Lemma 4.3.1 (Chernoff Bound, proposition 13.1.3 in [5])**.** *For any $r>0$,*

$$\Pr\left(\|W^{(n)}\|>r\right)\leq\exp\left(-nE_{\mathrm{sp}}\left(\frac{r^2}{n\sigma_{w,n}^2}\right)\right).$$

Recall that the unexpurgated Poltyrev exponent is given by

$$E_P^{\mathrm{un}}(b)=\begin{cases}E_{\mathrm{sp}}(b) & ,\ \text{if } 1\leq b<2\\ \frac{1}{2}\log\frac{eb}{4} & ,\ \text{if } 2\leq b.\end{cases},$$

and the Volume-to-Noise Ratio (VNR) of a lattice $\Lambda\subset\mathbb{R}^n$ is defined by $\gamma_\Lambda(\sigma):=\mu_L(\mathcal{V}(\Lambda))^{2/n}/\sigma^2$.

One might be able to make

$$A_{\mathfrak{p}}^{\mathrm{NN}}(G_n,W^{(n)})\leq\exp\left(-n\left(E_P^{\mathrm{un}}\left(\frac{\gamma_{a\Lambda(G_n)}(\sigma_{w,n})}{2\pi e}\right)+o(1)\right)\right),$$

as $n\longrightarrow\infty$, via bounding $\Pr(\|W^{(n)}\|>a_np_n/2)$ using the Chernoff bound, and $I_{\mathfrak{p}_n}\left(G_n,W^{(n)}\right)$ as in lemma 4.1.5. Theorems 4.4.1 and 7.1.1 discuss this.

A relation between $\inf_{u\in C_{\mathfrak{p}}}v_{\mathfrak{p}}^{\mathrm{NN}}(u,\varepsilon_{\mathfrak{p}})$ and Poltyrev's unexpurgated error exponent is given in the following lemma.

Lemma 4.3.2. *Let* $\{\mathfrak{p}_n = (n, k_n, p_n, a_n)\}_{n\in\mathbb{Z}_{>1}}$ *be a sequence of quadruples of parameters, and* $b > 0$. *For each integer* $n > 1$, *set* $C_n := \left[\sqrt{n\sigma^2_{w,n}}, \sqrt{n\sigma^2_{w,n}(1+b)}\right]$. *If* $\lim_{n\to\infty} p_n^{1-k_n/n} = \infty$, *then*

$$\lim_{n\to\infty} \inf_{u\in C_n} v^{\mathrm{NN}}_{\mathfrak{p}_n}(u, b) = E_P^{\mathrm{un}}(1+b).$$

Proof. See Appendix C. □

4.4 AWGN-Goodness

The following theorem shows that primes of size at least comparable to the square root of the block length make lattice decoding reliable.

Theorem 4.4.1. *Let* $\mathfrak{S} = \{\mathfrak{p}_n = (n, k_n, p_n, a_n)\}_{n\in\mathbb{Z}_{>1}}$ *be a sequence of quadruples of parameters such that the sequence* $\{\varepsilon_{\mathfrak{p}_n}\}_{n\in\mathbb{Z}_{>1}}$ *is constant and strictly positive, and denote this common value by* ε. *Let* $\{G_n\}_{n\in\mathbb{Z}_{>1}}$ *be an* $\mathfrak{S}$*-Loeliger-good sequence, and let* $\delta > 1$. *Assume that, for each* n,

$$p_n > \left(\frac{2\delta n}{\pi e(1+\varepsilon)}\right)^{n/(2k_n)},$$

and that $\lim_{n\to\infty} p_n^{1-k_n/n} = \infty$. *Then, as* $n \longrightarrow \infty$,

$$A^{\mathrm{NN}}_{\mathfrak{p}_n}(G_n, W^{(n)}) \leq e^{-n(\min(E_{\mathrm{sp}}(\delta), E_P^{\mathrm{un}}(1+\varepsilon))+o(1))} \tag{4.10}$$

Proof. Set $\beta := \min(E_{\mathrm{sp}}(\delta), E_P^{\mathrm{un}}(1+\varepsilon))$. Then, equation 4.3 and lemma 4.1.5 yield that, as $n \longrightarrow \infty$,

$$A^{\mathrm{NN}}_{\mathfrak{p}_n}(G_n, W^{(n)}) \leq \Pr(\|W^{(n)}\| > a_n p_n/2) + e^{-n\cdot o(1)} K_{\mathfrak{p}_n},$$

where

$$K_{\mathfrak{p}_n} = \left(\frac{\sqrt{\pi e/2}}{p_n^{1-k_n/n}}\right)^n + n\left(\left(\frac{1}{\sqrt{1+\varepsilon}} + \frac{\sqrt{\pi e/2}}{p_n^{1-k_n/n}}\right)^n + e^{-n\cdot\inf_{u\in C_{\mathfrak{p}_n}} v_{\mathfrak{p}_n}^{\mathrm{NN}}(u,\varepsilon)}\right).$$

Now, the limit $\lim_{n\to\infty} p_n^{1-k_n/n} = \infty$ implies that $\left(\frac{\sqrt{\pi e/2}}{p_n^{1-k_n/n}}\right)^n < e^{-\beta n}$ for n large enough, and, as $n \longrightarrow \infty$,

$$\log\left(\frac{1}{\sqrt{1+\varepsilon}} + \frac{\sqrt{\pi e/2}}{p_n^{1-k_n/n}}\right)^{-1} - \frac{\log n}{n} = \frac{1}{2}\log(1+\varepsilon) + o(1)$$

Further, since, for any $b > 0$, $\frac{1}{2}\log(1+b) > E_P^{\mathrm{un}}(1+b)$, we have that $\frac{1}{2}\log(1+\varepsilon) > \beta$. Also, lemma 4.3.2 implies that $\inf_{u\in C_{\mathfrak{p}_n}} v_{\mathfrak{p}_n}^{\mathrm{NN}}(u,\varepsilon) = E_P^{\mathrm{un}}(1+\varepsilon) + o(1)$ as $n \longrightarrow \infty$. Hence, $K_{\mathfrak{p}_n} \leq e^{-n(\beta+o(1))}$ as $n \longrightarrow \infty$.

Finally, for each n, we have that

$$a_n p_n = V_{\mathfrak{p}_n}^{1/n} p_n^{k_n/n} = p_n^{k_n/n}\sqrt{2\pi e\sigma_{w,n}^2(1+\varepsilon)} > 2\sqrt{\delta n\sigma_{w,n}^2},$$

so the Chernoff bound yields

$$\Pr(\|W^{(n)}\| > a_n p_n/2) < e^{-nE_{\mathrm{sp}}(\delta)} \leq e^{-n\beta},$$

and inequality 4.10 follows. □

Note that E_{sp} maps $[1,\infty)$ bijectively into $[0,\infty)$. Hence, we may define a function $E_T : [1,\infty) \longrightarrow [1,\infty)$ such that $E_T(b) = E_{\mathrm{sp}}^{-1}(E_P^{\mathrm{un}}(b))$. Note that $E_T(b) = b$ for $b \in [1,2]$, and $E_T(b) \leq b$ in general. Then, if δ in theorem 4.4.1 is chosen as $\delta = E_T(1+\varepsilon)$, we get that $B_{\mathfrak{p}_n}^{\mathrm{NN}}(W^{(n)}) \leq e^{-n(E_P^{\mathrm{un}}(1+\varepsilon)+o(1))}$.

Chapter 5

Flatness

Ling and Belfiore define the flatness factor $\epsilon_\Lambda : \mathbb{R}_{>0} \longrightarrow [0, \infty)$ of a lattice $\Lambda \subset \mathbb{R}^n$ in [3] and derive the expression

$$\epsilon_\Lambda(\sigma) = \frac{\mu_L(\mathcal{V}(\Lambda))}{(2\pi\sigma^2)^{n/2}} \Theta_\Lambda\left(\frac{1}{2\pi\sigma^2}\right) - 1 \tag{5.1}$$

It is desirable, for lattice Gaussian coding, to have this flatness factor be small. Proposition 5.1.1 will give an estimate on the average size of the flatness factor, and theorem 5.3.2 will give conditions under which this estimate is small.

5.1 Upper Bound on Flatness Factor

For any $\tau > 0$, quadruple of parameters $\mathfrak{p} = (n, k, p, a)$ and random variable G over $\mathbb{F}_p^{n\times k}$, define

$$A_{\mathfrak{p}}^{\mathrm{Fl}}(G,W^{(n)},\tau) := p^k \xi^{\max}(G) \cdot \Theta_{\mathbb{Z}^n}(a^2\tau) + p^k(\xi^{(0)}(G) - \xi^{\max}(G)) \cdot \Theta_{\mathbb{Z}^n}(a^2p^2\tau) \tag{5.2}$$

and

$$B_{\mathfrak{p}}^{\mathrm{Fl}}(G, W^{(n)}, \tau) := V_{\mathfrak{p}}\tau^{n/2} A_{\mathfrak{p}}^{\mathrm{Fl}}(U_{\mathfrak{p}}, W^{(n)}, \tau) - 1 \tag{5.3}$$

The second application of the averaging argument is via considering a Gaussian

function.

Proposition 5.1.1. *For any quadruple of parameters* $\mathfrak{p} = (n, k, p, a)$*, random variable* G *over* $\mathbb{F}_p^{n\times k}$*, and* $\tau > 0$*, we have that*

$$\mathbb{E}_G\left[\Theta_{a\Lambda(G)}(\tau)\right] \leq A_{\mathfrak{p}}^{\mathrm{Fl}}(G, W^{(n)}, \tau) \tag{5.4}$$

Furthermore, if $\Pr(G \in M_{\mathfrak{p}}) > 0$*, then*

$$\mathbb{E}_G\left[\epsilon_{a\Lambda(G)}\left(\frac{1}{\sqrt{2\pi\tau}}\right)\middle| G \in M_{\mathfrak{p}}\right] \leq \frac{B_{\mathfrak{p}}^{\mathrm{Fl}}(G, W^{(n)}, \tau)}{\Pr(G \in M_{\mathfrak{p}})} \tag{5.5}$$

Proof. Define $s : \mathbb{R}^n \longrightarrow [0, \infty]$ by $s(\lambda) = e^{-\pi\tau\|a\lambda\|^2}$. Then, $\sum_{\lambda\in\Lambda(G)} s(\lambda) = \Theta_{a\Lambda(G)}(\tau)$, and inequality 5.4 follows immediately from the averaging argument (proposition 3.2.3).

Inequality 5.5 follows from 5.4 in view of equations 5.1 and 5.3 since $\mu_L(\mathcal{V}(a\Lambda(G))) = V_{\mathfrak{p}}$ when $G \in M_{\mathfrak{p}}$. □

The theta series functional equation for the integer lattice (see equation 2.3) implies that we may rewrite

$$A_{\mathfrak{p}}^{\mathrm{Fl}}(G, W^{(n)}, \tau) = V_{\mathfrak{p}}^{-1} p^n \tau^{-n/2} \xi^{\max}(G) \cdot \Theta_{\mathbb{Z}^n}\left(\frac{1}{a^2\tau}\right) + p^k(\xi^{(0)}(G) - \xi^{\max}(G)) \cdot \Theta_{\mathbb{Z}^n}(a^2p^2\tau) \tag{5.6}$$

Then,

$$B_{\mathfrak{p}}^{\mathrm{Fl}}(G, W^{(n)}, \tau) = p^n \xi^{\max}(G) \cdot \Theta_{\mathbb{Z}^n}\left(\frac{1}{a^2\tau}\right) - 1 + V_{\mathfrak{p}}\tau^{n/2} p^k(\xi^{(0)}(G) - \xi^{\max}(G)) \cdot \Theta_{\mathbb{Z}^n}(a^2p^2\tau) \tag{5.7}$$

5.2 Flatness-Good Sequences

In view of equation 5.7, we introduce the following definition.

Definition 5.2.1. For any sequence $\mathfrak{S} = \{\mathfrak{p}_n = (n, k_n, p_n, a_n)\}_{n\in\mathbb{Z}_{>1}}$, an $\mathfrak{S}$-*flatness-good sequence* is a sequence $\{G_n\}_{n\in\mathbb{Z}_{>1}}$ where, for each n, G_n is a random variable over $\mathbb{F}_{p_n}^{n\times k_n}$ such that $\liminf_{n\to\infty} \Pr\left(G_n \in M_{\mathfrak{p}_n}\right) > 0$,

$$\limsup_{n\to\infty} p_n^n \xi^{\max}(G_n) \leq 1 \tag{5.8}$$

and, for any $\beta > 1$,

$$\lim_{n\to\infty} \frac{p_n^{k_n}(\xi^{(0)}(G_n) - \xi^{\max}(G_n))}{\beta^n} = 0 \tag{5.9}$$

Remark 10. *The flatness factor associated with a flatness-good sequence vanishes, as the blocklength grows without bound, provided that the theta series in equation 5.7 are asymptotically 1.*

5.3 Vanishing Flatness Factor

The following lemma gives a necessary and sufficient condition under which the integer lattice theta series achieves its minimum possible value asymptotically. First, for any positive integer n and $\tau > 0$, note that

$$\Theta_{\mathbb{Z}^n}(\tau) = \left(\theta(0, i\tau)\right)^n,$$

where $\theta(0, i\tau) := \sum_{z\in\mathbb{Z}} e^{-\pi\tau z^2}$ is the Jacobi theta function.

Lemma 5.3.1. *For any sequence $\{c_n\}_{n\in\mathbb{N}} \subset \mathbb{R}_{>0}$, we have that $\lim_{n\to\infty} \Theta_{\mathbb{Z}^n}(c_n) = 1$ if and only if $n = o(e^{\pi c_n})$ as $n \longrightarrow \infty$.*

Proof. First, note that, for every n,

$$1 + \frac{2}{e^{\pi c_n}} < \theta(0, ic_n) = 1 + 2\sum_{z=1}^{\infty} e^{-\pi c_n z^2} < 1 + 2\sum_{z=1}^{\infty} e^{-\pi c_n z} = 1 + \frac{2}{e^{\pi c_n} - 1}.$$

Now, assume that $n = o(e^{\pi c_n})$ as $n \longrightarrow \infty$. Then, $\lim_{n\to\infty} \frac{n}{e^{\pi c_n}-1} = 0$, and for all large n

$$1 < (\theta(0, ic_n))^n < \left(\left(1 + \frac{2}{e^{\pi c_n} - 1}\right)^{(e^{\pi c_n}-1)/2}\right)^{2n/(e^{\pi c_n}-1)} < e^{2n/(e^{\pi c_n}-1)}.$$

Hence, $\lim_{n\to\infty}(\theta(0, ic_n))^n = 1$.

For the converse, assume that $\lim_{n\to\infty}(\theta(0, ic_n))^n = 1$. Then,

$$\lim_{n\to\infty}\left(\left(1 + \frac{2}{e^{\pi c_n}}\right)^{e^{\pi c_n}/2}\right)^{2n/e^{\pi c_n}} = 1.$$

Thus, $\lim_{n\to\infty} c_n = \infty$. Hence, for all large n,

$$2^{2n/e^{\pi c_n}} < \left(\left(1 + \frac{2}{e^{\pi c_n}}\right)^{e^{\pi c_n}/2}\right)^{2n/e^{\pi c_n}},$$

implying that $n = o(e^{\pi c_n})$. □

The main theorem of this chapter gives sufficient conditions under which the flatness factor vanishes.

Theorem 5.3.2. *Let $\tau_1 > \cdots > \tau_\ell > 0$, let $\mathfrak{S} = \{\mathfrak{p}_n = (n, k_n, p_n, a_n)\}_{n\in\mathbb{Z}_{>1}}$ be a sequence of quadruples of parameters, and let $\{G_n\}_{n\in\mathbb{Z}_{>1}}$ be a $\mathfrak{S}$-flatness-good sequence. For each $j \in \{1, \cdots, \ell\}$, and $n \in \mathbb{Z}_{>1}$, let $f_j(n)$ and $g_j(n)$ be given by*

$$a_n = \sqrt{\frac{\pi}{\tau_j \log(n/f_j(n))}} \quad \textit{and} \quad p_n = \left(\frac{\log(n/g_j(n))}{\pi V_{\mathfrak{p}_n}^{2/n}\tau_j}\right)^{n/(2k_n)} \tag{5.10}$$

If $\limsup_{n\to\infty} \tau_1 V_{\mathfrak{p}_n}^{2/n} < 1$, and if

$$\lim_{n\to\infty} \max_j \left(\max\left(f_j(n), g_j(n)\right)\right) = 0,$$

then $\max_j \lim_{n\to\infty} B_{\mathfrak{p}_n}^{\mathrm{Fl}}(G_n, W^{(n)}, \tau_j) = 0$.

Proof. For each j, the conditions given on f_j and g_j imply that $n = o(e^{\pi/(a_n^2\tau_j)})$ and $n = o(e^{\pi a_n^2 p_n^2 \tau_j})$, respectively, so, by lemma 5.3.1, $\lim_{n\to\infty} \Theta_{\mathbb{Z}^n}\left(\frac{1}{a^2\tau_j}\right) = 1 = \lim_{n\to\infty} \Theta_{\mathbb{Z}^n}\left(a^2p^2\tau_j\right)$. Thus, for each j, equations 5.7, 5.8 and 5.9 yield the limit $\lim_{n\to\infty} B^{\mathrm{Fl}}_{\mathfrak{p}_n}(G_n, W^{(n)}, \tau_j) = 0$, and the desired result follows. □

Chapter 6

Good Sequences of Random Variables

We show that, whenever $p_n k_n, p_n^{n-k_n} \longrightarrow \infty$, the sequence $\{\Lambda_{(n,k_n,p_n,a_n)}\}_{n\in\mathbb{Z}_{>1}}$ is both flatness-good and Loeliger-good.

6.1 Flatness-Good Implies Loeliger-Good

Proposition 6.1.1. *For any sequence of quadruples of parameters* $\mathfrak{S} = \{\mathfrak{p}_n = (n, k_n, p_n, a_n)\}_{n\in\mathbb{Z}_{>1}}$ *such that* $\lim_{n\to\infty} p_n k_n = \infty$, *an* $\mathfrak{S}$*-flatness-good sequence is also* $\mathfrak{S}$*-Lolieger-good.*

Proof. Let $\{G_n\}_{n\in\mathbb{Z}_{>1}}$ be an $\mathfrak{S}$-flatness-good sequence. Then, in particular,

$$\liminf_{n\to\infty} \Pr\left(G_n \in M_{\mathfrak{p}_n}\right) > 0 \tag{6.1}$$

and

$$\limsup_{n\to\infty} p_n^n \xi^{\max}(G_n) \leq 1 \tag{6.2}$$

If $d = \liminf_{n\to\infty} \Pr\left(G_n \in M_{\mathfrak{p}_n}\right)$, then, as $\xi^{\max}(G_n) \geq (1-\xi^{(0)}(G_n))/(p_n^n - 1)$ and $\xi^{(0)}(G_n) \leq 1/p_n^{k_n} + (1-d)$, we get that, for all large n (e.g., all $n \geq n_0$ where n_0 is

such that $1/p_{n_0}^{k_{n_0}} \leq d/2$)

$$p_n^n \xi^{\max}(G_n) \left(1 + \frac{\sqrt{\pi e/2}}{p_n^{1-k_n/n}}\right)^n > d/2$$

Also, inequality 6.2 implies that

$$\limsup_{n\to\infty} \frac{1}{n} \log\left((4/d)\sqrt{n\pi} p_n^n \cdot \xi^{\max}(G_n)\right) \leq 0.$$

Hence, with $\ell_n = (4/d)\sqrt{n\pi}$, we see that $\{G_n\}_{n\in\mathbb{Z}_{>1}}$ is $\mathfrak{S}$-Lolieger-good. □

6.2 The sequence $\Lambda_{\mathfrak{p}_n}$ is Flatness-Good

Note that, for any quadruple of parameters $\mathfrak{p} = (n, k, p, a)$,

$$\xi_{\mathfrak{p}} = \sum_{j=0}^{k} \Pr(U'_{\mathfrak{p}} u_{\mathfrak{p}} = 0 \,|\, \operatorname{rank}(U'_{\mathfrak{p}}) = j) \Pr(\operatorname{rank}(U'_{\mathfrak{p}}) = j) = \sum_{j=0}^{k} \frac{1}{p^j} \Pr(\operatorname{rank}(U'_{\mathfrak{p}}) = j) \tag{6.3}$$

We next analyze the term $\Pr(\operatorname{rank}(U'_{\mathfrak{p}}) = j)$. The following is a well-known fact.

Lemma 6.2.1. *Fix a quadruple of parameters $\mathfrak{p} = (n, k, p, a)$. Then, $\Pr(\operatorname{rank}(U'_{\mathfrak{p}}) = 0) = 1/p^{nk}$, and, for any integer $1 \leq j \leq k$,*

$$\begin{aligned}\Pr(\operatorname{rank}(U'_{\mathfrak{p}}) = j) &= \frac{1}{p^{nk}} \cdot \frac{(p^n - 1)\cdots(p^n - p^{j-1}) \cdot (p^k - 1)\cdots(p^{k-(j-1)} - 1)}{(p-1)\cdots(p^j - 1)} \\ &= \frac{1}{p^{(n-j)(k-j)}} \cdot \frac{\left(\frac{1}{p};\frac{1}{p}\right)_n \left(\frac{1}{p};\frac{1}{p}\right)_k}{\left(\frac{1}{p};\frac{1}{p}\right)_j \left(\frac{1}{p};\frac{1}{p}\right)_{n-j} \left(\frac{1}{p};\frac{1}{p}\right)_{k-j}}.\end{aligned}$$

Using lemma 6.2.1, one may prove the following bounds on $\Pr(\operatorname{rank}(U'_{\mathfrak{p}}) = j)$.

Lemma 6.2.2. *For any quadruple of parameters $\mathfrak{p} = (n, k, p, a)$, and any $1 \leq j \leq$*

$k-1$, *we have that*

$$\Pr(\operatorname{rank}(U'_{\mathfrak{p}}) = j) < \frac{1}{p^{(n-k+1)(k-j)}\phi(1/2)} \tag{6.4}$$

Also, $\Pr(\operatorname{rank}(U'_{\mathfrak{p}}) = k) > 1 - p^{k-n}$.

Proof. Note that, for any $m < \ell$, $\phi(1/2) \leq \left(\frac{1}{p};\frac{1}{p}\right)_{\ell} < \left(\frac{1}{p};\frac{1}{p}\right)_{m}$. Thus, for any $1 \leq j \leq k-1$,

$$\frac{\left(\frac{1}{p};\frac{1}{p}\right)_{n}\left(\frac{1}{p};\frac{1}{p}\right)_{k}}{\left(\frac{1}{p};\frac{1}{p}\right)_{j}\left(\frac{1}{p};\frac{1}{p}\right)_{n-j}\left(\frac{1}{p};\frac{1}{p}\right)_{k-j}} < \frac{1}{\phi(1/2)}.$$

Then, lemma 6.2.1 yields 6.4.

For each $1 \leq j \leq k$, let $\mathfrak{p}_j = (n, j, p, a)$, and note that $\mathfrak{p}_k = \mathfrak{p}$ and $\delta_j := \Pr(\operatorname{rank}(U'_{\mathfrak{p}_j}) = j) = \frac{\left(\frac{1}{p};\frac{1}{p}\right)_{n}}{\left(\frac{1}{p};\frac{1}{p}\right)_{n-j}}$. We will show that $\delta_k > 1 - p^{k-n}$. First, note that $2 \leq p$ implies that $\frac{2}{p} - \frac{1}{p^{n-j+1}} < 1$, so

$$1 - \frac{2}{p^{n-j}} + \frac{1}{p^{2(n-j)}} > 1 - \frac{1}{p^{n-j-1}},$$

or, $(1-p^{j-n})^2 > (1-p^{j+1-n})$ for any j. Thus, for any $1 \leq j \leq k-1$, if we have that $\delta_j > 1 - p^{j-n}$, we would also have

$$\delta_{j+1} = (1-p^{j-n})\delta_j > (1-p^{j-n})^2 > (1-p^{j+1-n}).$$

As $\delta_1 = 1 - p^{-n} > 1 - p^{1-n}$, we see that $\delta_k > (1-p^{k-n})$, as desired. □

Lemma 6.2.3. *Let* $\{\mathfrak{p}_n = (n, k_n, p_n, a_n)\}_{n\in\mathbb{Z}_{>1}}$ *be a sequence of quadruples of parameters. If* $\lim_{n\to\infty} p_n^{n-k_n} = \infty = \lim_{n\to\infty} p_n k_n$, *then*

$$\lim_{n\to\infty} \xi^{(0)}(U_{\mathfrak{p}_n}) p_n^{k_n} = \lim_{n\to\infty} \xi^{(0)}(U'_{\mathfrak{p}_n}) p_n^{k_n} = 1,$$

and

$$\lim_{n\to\infty} \xi^{\max}(U_{\mathfrak{p}_n}) p_n^n = \lim_{n\to\infty} \xi^{\max}(U'_{\mathfrak{p}_n}) p_n^n = 1.$$

Proof. For each n, we have that $\frac{1}{p_n^{k_n}} \leq \xi_{\mathfrak{p}_n}$ and, by equation 6.3 and inequality 6.4,

$$\begin{aligned}
\xi_{\mathfrak{p}_n} &< \frac{1}{p_n^{nk_n}} + \frac{1}{p_n^{k_n}} \left(1 + \frac{1}{\phi(1/2)} \sum_{j=1}^{k_n-1} \frac{1}{\left(p_n^{(n-k_n)}\right)^{k_n-j}} \right) \\
&< \frac{1}{p_n^{nk_n}} + \frac{1}{p_n^{k_n}} \left(1 + \frac{1}{\phi(1/2)} \sum_{j=1}^{\infty} \frac{1}{\left(p_n^{(n-k_n)}\right)^{j}} \right) \\
&= \frac{1}{p_n^{nk_n}} + \frac{1}{p_n^{k_n}} \left(1 + \frac{1}{\phi(1/2)(p_n^{n-k_n}-1)} \right),
\end{aligned}$$

so we get that $\lim_{n\to\infty} \xi^{(0)}(U'_{\mathfrak{p}_n}) p_n^{k_n} = 1$ (recall that $\xi^{(0)}(U'_{\mathfrak{p}_n}) = \xi_{\mathfrak{p}_n}$ by definition). From $\xi^{\max}_{\mathfrak{p}_n}(U'_{\mathfrak{p}_n}) = (1-\xi_{\mathfrak{p}_n})/(p_n^n - 1)$ we get $\lim_{n\to\infty} \xi^{\max}(U'_{\mathfrak{p}_n}) p_n^n = 1$. The other two equalities follow from these two since the second part of lemma 6.2.2 implies that

$$\frac{1}{p_n^{k_n}} \leq \xi^{(0)}(U_{\mathfrak{p}_n}) \leq \frac{\xi^{(0)}(U'_{\mathfrak{p}_n})}{1 - p_n^{k_n - n}}$$

and

$$\frac{1 - \xi^{(0)}(U_{\mathfrak{p}_n})}{p_n^n - 1} \leq \xi^{\max}(U_{\mathfrak{p}_n}) \leq \frac{\xi^{\max}(U'_{\mathfrak{p}_n})}{1 - p_n^{k_n - n}}.$$

□

The following result is an immediate consequence.

Corollary 6.2.3.1. *For any sequence of quadruples of parameters* $\mathfrak{S} = \{\mathfrak{p}_n = (n, k_n, p_n, a_n)\}_{n\in\mathbb{Z}_{>1}}$ *such that* $\lim_{n\to\infty} p_n^{n-k_n} = \infty$, *the sequence* $\{G_n := \Lambda_{\mathfrak{p}_n}\}_{n\in\mathbb{Z}_{>1}}$ *is* $\mathfrak{S}$*-flatness-good.*

Chapter 7

Lattice Gaussian Coding

In this chapter, a wide range of quadruples of parameters are shown to yield reliable and capacity achieving coding.

7.1 Compatibility of Flatness and AWGN-Goodness

The usefulness of the results of theorems 4.4.1 and 5.3.2 hinges on the compatibility of the their premises. In this section, we show that the premises are compatible, i.e., that there exists a wide range of quadruples of parameters satisfying the premises in these theorems simultaneously.

We assume, for the remaining of the discussion, that $\sigma_{w,n}$ is constant in n, and set $\sigma_w = \sigma_{w,n}$.

Theorem 7.1.1. *Let $\tau_1 > \cdots > \tau_\ell > 0$ be such that $2\pi e\sigma_w^2\tau_1 < 1$, and fix $b \in (2\pi e\sigma_w^2, 1/\tau_1)$. Then, for any sequence $\{\mathfrak{p}_n = (n, k_n, p_n, a_n)\}_{n\in\mathbb{Z}_{>1}}$ of quadruples of parameters with*

$$p_n > \max\left(\left(\frac{2}{\pi e}n\right)^{n/(2k_n)}, \left(\frac{1}{\pi}\log n\right)^{n/(2(n-k_n))}\right) \tag{7.1}$$

and $\{V_{\mathfrak{p}_n}^{2/n}\}_{n\in\mathbb{Z}_{>1}} \subset (2\pi e\sigma_w^2, b]$, *we have that, with* f_j *and* g_j *as in (5.10),*

$$\lim_{n\to\infty} \max_j (\max(f_j(n), g_j(n))) = 0.$$

Proof. Note that the double sequence (in n and in j) $\tau_j V_{\mathfrak{p}_n}^{2/n}$ is bounded away from 0; indeed, $\inf_{n,j} \tau_j V_{\mathfrak{p}_n}^{2/n} \geq 2\pi e\sigma_w^2\tau_\ell > 0$.

Set $\delta' = 2/(\pi e)$. Since $p_n > (\delta' n)^{n/(2k_n)}$, $g_j(n) < ne^{-\tau_j V_{\mathfrak{p}_n}^{2/n}\delta' n}$ so $g_j(n) = o(1)$. Moreover, since $p_n > \left(\frac{1}{\pi}\log n\right)^{n/(2(n-k_n))}$ and $\tau_j V_{\mathfrak{p}_n}^{2/n} < \tau_1 b$, writing $a_n = V_{\mathfrak{p}_n}^{1/n}/p_n^{1-k_n/n}$ we see that

$$f_j(n) = ne^{-\pi p_n^{2(1-k_n/n)}/(\tau_j V_n^{2/n})} < n^{1-1/(\tau_1 b)}$$

so also $f_j(n) = o(1)$. □

Remark 11. *Note that, if* $p_n > \left(\frac{1}{\pi}\log n\right)^{n/(2(n-k_n))}$, *then* $\lim_{n\to\infty} p_n^{1-k_n/n} = \infty$.

7.2 Capacity-Achieving Lattice Gaussian Codes

In [3], Ling and Belfiore introduce lattice Gaussian coding, and elegantly use the flatness factor to prove that this coding scheme can achieve the capacity of the AWGN channel.

Let $\sigma_s > 0$, $c \in \mathbb{R}^n$ and Λ be a lattice in $\mathbb{R}^n$. Recall that we defined $f_{\sigma_s,c} : \mathbb{R}^n \longrightarrow (0,\infty)$ by $f_{\sigma_s,c}(y) = e^{-\|y-c\|^2/(2\sigma_s^2)}/(2\pi\sigma_s^2)^{n/2}$, and $f_{\sigma_s,c}(\Lambda) = \sum_{\lambda\in\Lambda} f_{\sigma_s,c}(\lambda)$ for short. A lattice Gaussian random variable (over Λ with a shift vector c and parameter σ_s) is defined via its probability mass function $D_{\Lambda,\sigma_s,c} : \Lambda \longrightarrow (0,1)$, given by $D_{\Lambda,\sigma_s,c}(\lambda) = f_{\sigma_s,c}(\lambda)/f_{\sigma_s,c}(\Lambda)$.

If a signal X is drawn according to $D_{\Lambda,\sigma_s,c}$, with $\epsilon_\Lambda(\sigma_s) < 1$, is used in an AWGN channel $Y = X + Z$, where the noise Z has variance σ_z^2, Ling and Belfiore show that the probability of error under MAP decoding $P_e^{\mathrm{LG}}(\Lambda, \sigma_s, c; \sigma_z)$ can be upper bounded

as

$$P_e^{\mathrm{LG}}(\Lambda, \sigma_s, c; \sigma_z) \leq \frac{1 + \epsilon_\Lambda\left(\widetilde{\sigma}\right)}{1 - \epsilon_\Lambda\left(\sigma_s\right)} \cdot \Pr((\widetilde{\sigma}/\sigma_s)Z \notin \mathcal{V}(\Lambda)),$$

where $\widetilde{\sigma} = \sigma_s^2/\sqrt{\sigma_s^2 + \sigma_z^2}$. In the remaining of the paper, we set $\sigma_w = (\widetilde{\sigma}/\sigma_s)\sigma_z$.

Further, with $P = \frac{1}{n}\mathbb{E}[\|X - c\|^2]$, the entropy $\mathbb{H}(X)$ satisfies

$$\begin{aligned}\mathbb{H}(X) &= \log\left((2\pi\sigma_s^2)^{n/2} f_{\sigma_s, c}(\Lambda)\right) + \frac{n}{2} \cdot \frac{P}{\sigma_s^2} \\ &\geq \log\left(\frac{\left(1 - \epsilon_\Lambda\left(\sigma_s\right)\right)\left(2\pi\sigma_s^2\right)^{n/2}}{\mu_L(\mathcal{V}(\Lambda))}\right) + \frac{n}{2} \cdot \frac{P}{\sigma_s^2}\end{aligned}$$

So, with $\mu(\mathcal{V}(\Lambda))^{2/n} = 2\pi e\sigma_w^2(1 + \varepsilon)$ and $\varepsilon > 0$, the maximum achievable rate $R_{\max}^{\mathrm{LG}}(\Lambda, \sigma_s, c; \sigma_z)$ satisfies

$$R_{\max}^{\mathrm{LG}}(\Lambda, \sigma_s, c; \sigma_z) \geq \frac{1}{n}\mathbb{H}(X) \geq \frac{1}{2}\log\left(\frac{\left(1 - \epsilon_\Lambda\left(\sigma_s\right)\right)^{2/n}}{(1 + \varepsilon)e^{1 - P/\sigma_s^2}}\right) + \frac{1}{2}\log\left(1 + \frac{\sigma_s^2}{\sigma_z^2}\right).$$

Fix a $t \in (0, \pi)$. Suppose that, for each $n \in \mathbb{Z}_{>1}$, $\Lambda^{(n)}$ is a lattice in $\mathbb{R}^n$ such that $\epsilon_{\Lambda^{(n)}}\left(\sigma_s/\sqrt{\frac{\pi}{\pi - t}}\right) < 1$, and $c_n \in \mathbb{R}^n$ is any shift vector. For each n, let $X^{(n)}$ be a random variable distributed according to $D_{\Lambda^{(n)}, \sigma_s, c_n}$, and set $P_n = \frac{1}{n}\mathbb{E}[\|X^{(n)} - c_n\|^2]$. Ling and Belfiore show that $\lim_{n\to\infty} \frac{P_n}{\sigma_s} = 1$. In such a case, with $\mathrm{SNR}_n = P_n/\sigma_z^2$, one has that for any $\varepsilon' > \frac{1}{2}\log(1 + \varepsilon)$,

$$R_{\max}^{\mathrm{LG}}(\Lambda^{(n)}, \sigma_s, c; \sigma_z) \geq \frac{1}{2}\log(1 + \mathrm{SNR}_n) - \varepsilon'$$

if n is large enough.

The following theorem quantifies the primes needed for Ling and Belfiore's construction.

Theorem 7.2.1. *Assume that $\sigma_s^2/\sigma_z^2 > e$. Let $\{c_n\}_{n\in\mathbb{Z}_{>1}}$ be any sequence of shift vectors $c_n \in \mathbb{R}^n$, $\eta \in (0, \frac{1}{2}\log\sigma_s^2/(e\sigma_z^2))$ and $\gamma \in (2\pi e, 2\pi e^{1+2\eta}]$. Then, there exists a*

sequence $\{\ell_n\}_{n\in\mathbb{Z}_{>1}} \subset \mathbb{R}_{>0}$ *satisfying* $\lim_{n\to\infty} \ell_n = 0$ *such that any sequence* $\{p_n\}_{n\in\mathbb{Z}_{>1}}$ *of primes satisfying*

$$p_n > \left(\frac{2}{\pi e} n\right)^{\frac{1}{2}(1+\ell_n)}$$

can be extended into a sequence of quadruples of parameters $\{\mathfrak{p}_n = (n, k_n, p_n, a_n)\}_{n\in\mathbb{Z}_{>1}}$ *satisfying both* $\gamma_{\Lambda_{\mathfrak{p}_n}}(\sigma_w) = \gamma$ *for every* n *and*

$$\Pr\Big\{ P_e^{\mathrm{LG}}(\Lambda_{\mathfrak{p}_n}, \sigma_s, c_n; \sigma_z) \le e^{-n(E_P^{\mathrm{un}}(\gamma/(2\pi e))+h(n))}, \\ R_{\max}^{\mathrm{LG}}(\Lambda_{\mathfrak{p}_n}, \sigma_s, c_n; \sigma_z) > \frac{1}{2}\log\left(1+\mathrm{SNR}_n\right) - \eta \Big\} \longrightarrow 1$$

as $n \longrightarrow \infty$, *where* $h(n) = o(1)$.

Proof. Set $\delta' = 2/(\pi e)$. First, equating the two terms in the right hand side of 7.1 yields $k_n^* := n\log\left(\frac{2n}{\pi e}\right) / \log\left(\frac{2n}{\pi^2 e}\log n\right)$ and that both terms are equal to

$$(\delta' n)^{\frac{1}{2}\left(1+\frac{\log\left(\frac{1}{\pi}\log n\right)}{\log \delta' n}\right)}.$$

Thus, setting $\ell_n := n/\lfloor k_n^* \rfloor - 1$, we see that $\ell_n \longrightarrow 0$ and any prime satisfying $p_n > (\delta' n)^{\frac{1}{2}(1+\ell_n)}$ will also satisfy inequality 7.1 with $k_n := \lfloor k_n^* \rfloor$.

Now, set $\tau_1 = 1/(2\pi\widetilde{\sigma}^2)$, $\tau_2 = 1/(2(\pi - t)\sigma_s^2)$ and $\tau_3 = 1/(2\pi\sigma_s^2)$, where t is small enough so that $\tau_1 > \tau_2 > \tau_3 > 0$. Note that $2\pi e\sigma_w^2\tau_1 < 1$ is equivalent to $\sigma_s^2/\sigma_z^2 > e$. For each n, choose a_n so that $\gamma_{\Lambda_{\mathfrak{p}_n}}(\sigma_w) = \gamma$. Then, $\limsup_{n\to\infty} \tau_1 V_{\mathfrak{p}_n}^{2/n} \le e^{1+2\eta}\sigma_z^2/\sigma_s^2 < 1$. Then, theorem 7.1.1 yields that theorems 4.4.1 and 5.3.2 apply, and, in view of propositions 4.1.1 and 5.1.1, Markov's inequality yields the desired result. □

Chapter 8

Conclusion

We give a new averaging argument that transforms lattice sums into simpler ones rather than into integrals, thereby saving the explicitness of the construction parameters. This averaging argument enables the proof that capacity-achieving lattice Gaussian codes exist for which the size of the primes is comparable with the squared root of the block-length. Future work includes investigation on whether the condition SNR $> e$ can be removed via this approach, whether expurgation affects the size of the parameters, and the optimal complexity trade-off between p_n and k_n.

Bibliography

[1] H. Loeliger, "Averaging bounds for lattices and linear codes", *IEEE Transaction on Information Theory*, vol. 43, no. 6, pp. 1767-11773, 1997.

[2] U. Erez and R. Zamir, "Achieving $\frac{1}{2}\log(1+SNR)$ on the AWGN channel with lattice encoding and decoding," *IEEE Transaction on Information Theory*, vol. 50, no. 10, pp. 2293–2314, 2004.

[3] C. Ling and J. Belfiore, "Achieving AWGN channel capacity with lattice gaussian coding," *IEEE Transaction on Information Theory*, vol. 60, no. 10, pp. 5918–5929, 2014.

[4] O. Ordentlich and U. Erez, "A simple proof for the existence of "good" pairs of nested lattices," *IEEE 27th Convention of Electrical & Electronics Engineers in Israel (IEEEI)*, 2012.

[5] R. Zamir, *Lattice Coding for Signals and Networks*, Cambridge University Press, 2014.

APPENDICES

A Measure Theory Considerations

Tonelli's theorem assures that the various interchanges of integrals made in this work are justified.

Theorem A.0.2 (Tonelli)**.** *Let (X, Σ_1, μ) and (Y, Σ_2, ν) be $\sigma-$finite measure spaces, and $f : X \times Y \longrightarrow [0, \infty]$ be measurable. Then,*

$$\int_X \int_Y f(x, y)\, d\nu\, d\mu = \int_Y \int_X f(x, y)\, d\mu\, d\nu = \int_{X\times Y} f(x, y)\, d\mu \times \nu.$$

Remark 12. *When ν is the counting measure, the theorem yields that $\int_X \sum_{y\in Y} f(x, y)\, d\mu = \sum_{y\in Y} \int_X f(x, y)\, d\mu$. If μ is also the counting measure, then the theorem yields that $\sum_{x\in X} \sum_{y\in Y} f(x, y) = \sum_{y\in Y} \sum_{x\in X} f(x, y)$. Also, an extension yields that, when $X = \prod_{i=1}^{n} X_i$ is countable and $f : X \longrightarrow [0, \infty]$ is any function, $\sum_{i=\pi(1)}^{\pi(n)} \sum_{x_i\in X_i} f(x_1, \cdots, x_n) = \sum_{x\in X} f(x)$ for any permutation π in the symmetric group S_n.*

Denote the $n-$sphere by $\mathbb{S}^{n-1}$. For a fixed $M \in \mathbb{F}_p^{n\times k}$, discreteness of $a\Lambda(M)$ implies that $|\mathcal{B}(0, 2r) \cap a\Lambda(M)| < \infty$. Thus, in particular, $\max_{w\in\mathbb{S}^{n-1}}\{N_{\mathcal{B}(w,r)}(a\Lambda(M) \setminus ap\mathbb{Z}^n)\}$ exists and is finite. Denote this maximum by ℓ. Let $f_M : r\mathbb{S}^{n-1} \longrightarrow \{0, \cdots, \ell\}$ be

defined by $f_M(w) = N_{\mathcal{B}(w,r)}(a\Lambda(M) \setminus ap\mathbb{Z}^n)$. By discreteness of $a\Lambda(M)$, $f_M^{-1}(\{j\})$, for any $0 \leq j \leq \ell$, is a countable union of closed subsets of $r\mathbb{S}^{n-1}$. In particular, each $f_M^{-1}(\{j\})$ is measurable. Thus, for any Borel-measurable set $B \subset \mathbb{R}_{>0}$, the set $f_M^{-1}(B) = f^{-1}(B \cap \{0, \cdots, \ell\}) = \bigcup_{j \in B_\ell} f_M^{-1}(\{j\})$, where $B_\ell = B \cap \{0, \cdots, \ell\}$, is measurable. Hence, f_M is a well-defined random variable, and $\mathbb{E}_{W^{(n)}}[f_M(W^{(n)})]$ is well-defined. Further, as, for any random variable G over $\mathbb{F}_p^{n \times k}$, $\mathbb{E}_G[f_G(W^{(n)})] = \sum_{M \in \mathbb{F}_p^{n \times k}} \Pr(G = M) f_M(W^{(n)})$ is a finite sum, $\mathbb{E}_{W^{(n)}}[\mathbb{E}_G[f_G(W^{(n)})]]$ is also well-defined, and, by non-negativity of each $f_M(W^{(n)})$, we may interchange the order of expectations.

B Proof of Lemma 4.1.5: Upper Bound on $I_{\mathfrak{p}}(G, W^{(n)})$

Proof (of Lemma 4.1.5). First, for any $\rho > 0$, inequality 4.7 reads

$$h(\mathfrak{p}, G, \rho) \leq \frac{p^n \cdot \xi^{\max}(G)}{\sqrt{\pi n}} \left(\frac{\rho}{\sqrt{n\sigma_{w,n}^2(1+\varepsilon_{\mathfrak{p}})}} + \frac{\sqrt{\pi e/2}}{p^{1-k/n}} \right)^n \tag{B.1}$$

For readability, we will drop the subscript on $\varepsilon_{\mathfrak{p}}$. Then, for any $\ell \geq 1$,

$$I_{\mathfrak{p}}\left(G, W^{(n)}\right) < \frac{\ell p^n \cdot \xi^{\max}(G)}{\sqrt{\pi n}} \int_0^{\sqrt{n\sigma_{w,n}^2(1+\varepsilon)}} f_{\|W^{(n)}\|}(r) \cdot \left(\frac{r}{\sqrt{n\sigma_{w,n}^2(1+\varepsilon)}} + \frac{\sqrt{\pi e/2}}{p^{1-k/n}} \right)^n dr$$
$$+ \Pr\left(\|W^{(n)}\| > \sqrt{n\sigma_{w,n}^2(1+\varepsilon)} \right).$$

Now, integration by parts yields that, since $\frac{\partial}{\partial r}\left(-\Pr(\|W^{(n)}\| > r)\right) = f_{\|W^{(n)}\|}(r, n)$,

$$\int_0^{\sqrt{n\sigma_{w,n}^2(1+\varepsilon)}} f_{\|W^{(n)}\|}(r) \left(\frac{r}{\sqrt{n\sigma_{w,n}^2(1+\varepsilon)}} + \frac{\sqrt{\pi e/2}}{p^{1-k/n}} \right)^n dr$$
$$= -\Pr\left(\|W^{(n)}\| > \sqrt{n\sigma_{w,n}^2(1+\varepsilon)} \right) \left(1 + \frac{\sqrt{\pi e/2}}{p^{1-k/n}} \right)^n + \left(\frac{\sqrt{\pi e/2}}{p^{1-k/n}} \right)^n$$
$$+ \sqrt{\frac{n}{\sigma_{w,n}^2(1+\varepsilon)}} J_{0, \sqrt{n\sigma_{w,n}^2(1+\varepsilon)}},$$

where

$$J_{\alpha,\alpha'} := \int_{\alpha}^{\alpha'} \Pr(\|W^{(n)}\| > r) \cdot \left(\frac{r}{\sqrt{n\sigma_{w,n}^2(1+\varepsilon)}} + \frac{\sqrt{\pi e/2}}{p^{1-k/n}} \right)^{n-1} dr$$

Now, note that

$$J_{0,\sqrt{n\sigma_{w,n}^2}} \leq \sqrt{n\sigma_{w,n}^2} \left(\frac{1}{\sqrt{1+\varepsilon}} + \frac{\sqrt{\pi e/2}}{p^{1-k/n}} \right)^{n-1},$$

and, by lemma 4.3.1,

$$\begin{aligned} J_{\sqrt{n\sigma_{w,n}^2},\sqrt{n\sigma_{w,n}^2(1+\varepsilon)}} &\leq \int_{\sqrt{n\sigma_{w,n}^2}}^{\sqrt{n\sigma_{w,n}^2(1+\varepsilon)}} e^{-nE_{\mathrm{sp}}\left(\frac{r^2}{n\sigma_{w,n}^2}\right)} \cdot \left(\frac{r}{\sqrt{n\sigma_{w,n}^2(1+\varepsilon)}} + \frac{\sqrt{\pi e/2}}{p^{1-k/n}} \right)^{n-1} dr \\ &= \int_{\sqrt{n\sigma_{w,n}^2}}^{\sqrt{n\sigma_{w,n}^2(1+\varepsilon)}} e^{-n\cdot v_{\mathfrak{p}}^{\mathrm{NN}}(r,\varepsilon)}\, dr \\ &\leq \sqrt{n\sigma_{w,n}^2(1+\varepsilon)} e^{-n\cdot \inf_{u\in C_{\mathfrak{p}}} v_{\mathfrak{p}}^{\mathrm{NN}}(u,\varepsilon)}. \end{aligned}$$

Hence, we get that

$$I_{\mathfrak{p}}\left(G, W^{(n)}\right) < \frac{\ell p^n \cdot \xi^{\max}(G)}{\sqrt{\pi n}} K_{\mathfrak{p}} + \left(1 - \frac{\ell p^n \cdot \xi^{\max}(G)}{\sqrt{\pi n}} \left(1 + \frac{\sqrt{\pi e/2}}{p^{1-k/n}} \right)^n \right) L_{\mathfrak{p}}.$$

□

C Proof of Lemma 4.3.2: Poltyrev Error Exponent

Before proving lemma 4.3.2, note that, for any $b > 0$, the function $v_{\mathfrak{p}}^{\mathrm{NN}}(\cdot, b)$ is strictly convex over $[0, \infty)$. Indeed, for any $u \in \mathbb{R}_{\geq 0}$,

$$\frac{\partial^2}{\partial u^2} v_{\mathfrak{p}}^{\mathrm{NN}}(u, b) = \frac{1}{n\sigma_{w,n}^2} + \frac{1}{u^2} + \frac{(n-1)/n}{\left(u + \frac{\sqrt{n\sigma_{w,n}^2 \pi e/2}}{p^{1-k/n}}\right)^2} > 0.$$

In particular, $v_{\mathfrak{p}}^{\mathrm{NN}}(\cdot, b)$ has a unique minimum over any bounded closed subinterval of $[0, \infty)$.

Proof (of Lemma 4.3.2). For each n, define $f_{n,b} : \mathbb{R}_{\geq 0} \longrightarrow \mathbb{R}$ by

$$f_{n,b}(y) = \frac{\partial}{\partial u} v_{\mathfrak{p}_n}^{\mathrm{NN}}(u, b)\Big|_{u=y} = \frac{y}{n\sigma_{w,n}^2} - \frac{1}{y} - \frac{(n-1)/n}{y + \frac{\sqrt{\pi e n \sigma_{w,n}^2 (1+b)/2}}{p_n^{1-k_n/n}}}$$

and denote $u_n := \operatorname{argmin}_{u \in C_n} v_{\mathfrak{p}_n}^{\mathrm{NN}}(u, b)$. Note that, for each n,

$$f_{n,b}\left(\sqrt{n\sigma_{w,n}^2(1+b)}\right) = \frac{1}{\sqrt{n\sigma_{w,n}^2(1+b)}} \left(b - \frac{(n-1)/n}{1 + \frac{\sqrt{\pi e/2}}{p_n^{1-k_n/n}}}\right) \tag{C.1}$$

$$f_{n,b}\left(\sqrt{2n\sigma_{w,n}^2}\right) = \frac{1}{\sqrt{2n\sigma_{w,n}^2}} \left(1 - \frac{(n-1)/n}{1 + \frac{\sqrt{\pi e(1+b)}}{2p_n^{1-k_n/n}}}\right) > 0 \tag{C.2}$$

If $b < 1$, then equation $C.1$ implies that $u_n = \sqrt{n\sigma_{w,n}^2(1+b)}$ for all large n. As

$$v_{\mathfrak{p}_n}^{\mathrm{NN}}\left(\sqrt{n\sigma_{w,n}^2(1+b)}, b\right) = E_{\mathrm{sp}}(1+b) - \frac{n-1}{n}\log\left(1 + \frac{\sqrt{\pi e/2}}{p_n^{1-k_n/n}}\right)$$

we see that $\inf_{u\in C_n} v_{\mathfrak{p}_n}^{\mathrm{NN}}(u,b) = E_P^{\mathrm{un}}(1+b) + o(1)$ in this case.

Now, assume that $b \geq 1$. Then, for each n, $\sqrt{2n\sigma_{w,n}^2} \in C_n$, so inequality C.2 implies that $\delta_n := \frac{u_n}{\sqrt{2n\sigma_{w,n}^2}} < 1$. On the other hand, the sequence $\{\alpha_n := 1 - 1/\min(n, 1 + p_n^{1-k_n/n}/\sqrt{\pi e(1+b)})\}_{n\in\mathbb{Z}_{>1}} \subset (0,1)$ satisfies $\lim_{n\to\infty}\alpha_n = 1$ and $\alpha_n < \delta_n$ for all large n; indeed, for all large n, we have that $2\alpha_n > 1$, so

$$\begin{aligned}\alpha_n\sqrt{2n\sigma_{w,n}^2}f_{n,b}\left(\alpha_n\sqrt{2n\sigma_{w,n}^2}\right) &= 2\alpha_n^2 - 1 - \frac{(n-1)/n}{1 + \frac{\sqrt{\pi e(1+b)}}{2\alpha_n p_n^{1-k_n/n}}} < 2\alpha_n^2 - 1 - \frac{(n-1)/n}{1 + \frac{\sqrt{\pi e(1+b)}}{p_n^{1-k_n/n}}} \\ &= 2\alpha_n^2 - 1 - \left(1 - \frac{1}{n}\right)\left(1 - \frac{1}{\frac{p_n^{1-k_n/n}}{\sqrt{\pi e(1+b)}} + 1}\right) \leq \alpha_n^2 - 1 < 0.\end{aligned}$$

Thus, we have that $\lim_{n\to\infty}\delta_n = 1$, and

$$\lim_{n\to\infty} v_{\mathfrak{p}_n}^{\mathrm{NN}}(\delta_n\sqrt{2n\sigma_{w,n}^2}) = \lim_{n\to\infty} E_{\mathrm{sp}}(2\delta_n^2) - \frac{n-1}{n}\log\left(\frac{\delta_n\sqrt{2}}{\sqrt{1+b}} + \frac{\sqrt{\pi e/2}}{p_n^{1-k_n/n}}\right) = \frac{1}{2}\log\frac{e(1+b)}{4},$$

so $\inf_{u\in C_n} v_{\mathfrak{p}_n}^{\mathrm{NN}}(u,b) = E_P^{\mathrm{un}}(1+b) + o(1)$ in this case too. □

D Papers

• W. Alghamdi, W. Abediseid and M.S. Alouini "On the Construction of Capacity Achieving Lattice Codes ", *Accepted in IEEE International Symposium on Information Theory (ISIT)*, Barcelona, Spain, July 2016.

• W. Alghamdi, W. Abediseid and M.S. Alouini "On the Construction of Capacity Achieving Lattice Codes ", *In preparation for the IEEE Transactions on Information Theory.*