Design Criteria for Lattice Network Coding

Chen Feng  
Dept. of Electrical and Computer Eng.  
University of Toronto, Canada  
cfeng@eecg.utoronto.ca

Danilo Silva  
Dept. of Electrical Engineering  
Federal University of Santa Catarina, Brazil  
danilo@eel.ufsc.br

Frank R. Kschischang  
Dept. of Electrical and Computer Eng.  
University of Toronto, Canada  
frank@comm.utoronto.ca

Abstract—The compute-and-forward (C-F) relaying strategy proposed by Nazer and Gastpar is a powerful new approach to physical-layer network coding. Nazer-Gastpar’s construction of C-F codes relies on asymptotically-good lattice partitions that require the dimension of lattices to tend to infinity. Yet it remains unclear how such C-F codes can be constructed and analyzed under practical constraints. Motivated by this, an algebraic approach was taken to compute-and-forward, which provides a framework to study C-F codes constructed from finite-dimensional lattice partitions (also referred to as lattice network codes). It is shown that the receiver parameters \( \{a_\ell\} \) and \( \alpha \) should be chosen such that the quantity \( Q = |\alpha|^2 + 5MR \sum_{\ell=1}^L \|a_h - a_\ell\|^2 \) is minimized, and the lattice partition should be designed such that the minimum inter-cost distance is maximized. These design criteria imply that finding the optimal receiver parameters is equivalent to solving a shortest vector problem, and designing good lattice partitions can be reduced to the design of good linear codes for complex Construction A.

I. INTRODUCTION

The principle of network coding [1] is to allow intermediate nodes in a network to forward functions (typically linear combinations [2], [3]) of their incoming packets rather than individual packets. It is well understood that this principle generally increases the network throughput and in particular achieves the so-called multicast capacity [1]–[3]. Physical-layer network coding (PNC)—as the terminology suggests—moves this principle closer to the channel: rather than attempting to decode simultaneously received packets individually, intermediate nodes infer and forward linear combinations of these packets. With a sufficient number of such linear combinations, any destination node in the network is able to recover the original packets.

The basic idea of PNC appears to have been independently proposed by several research groups in 2006 (e.g., Zhang, Liew, and Lam [4], and Popovski and Yomo [5]). It is shown that—with a relay decoding and forwarding the modulo-two sum (XOR) of the transmitted packets—the throughput of a two-way relay channel can be significantly improved [4], [5]. Due to this remarkable potential, PNC has received considerable research attention in recent years, with a particular focus on two-way relay channels (e.g., [6], [7]).

In recent work, Nazer and Gastpar [8] propose the compute-and-forward approach, which moves beyond two-way relay channels. Their approach assumes a Gaussian multiple-access channel (MAC) model for each intermediate node, given by

\[
y = \sum_{\ell=1}^L h_\ell x_\ell + z,
\]

where \( h_\ell \) are (complex-valued) channel gains, and \( x_\ell \) are signal points in a (multidimensional) lattice. Intermediate nodes exploit the property that any integer combination of lattice points is again a lattice point. In the simplest version, an intermediate node selects integers \( \{a_\ell\} \) and a scalar \( \alpha \), and then attempts to decode the lattice point

\[
\alpha y = \sum_{\ell=1}^L a_\ell x_\ell + \sum_{\ell=1}^L (\alpha h_\ell - a_\ell) x_\ell + \alpha z.
\]

Here \( \{a_\ell\} \) and \( \alpha \) are carefully chosen so that the “effective noise,” \( \sum_{\ell=1}^L (\alpha h_\ell - a_\ell) x_\ell + \alpha z \), is made (in some sense) small. The intermediate node then maps the decoded lattice point into a linear combination (over some finite field) of the transmitted packets.

The construction of compute-and-forward codes in [8] relies on asymptotically-good lattice partitions described in [9]. Although such a code construction is essential to establish the so-called computation rate, it is unclear how to design and analyze compute-and-forward codes under practical constraints.

To address this question, we have taken an algebraic approach to compute-and-forward in our previous work [10], which generalizes real lattice partitions to \( R \)-lattice partitions, where \( R \) is a discrete subring of \( \mathbb{C} \) forming a principle ideal domain. This generalization provides an algebraic framework to study a large class of finite-dimensional lattice partitions. In particular, we provide a sufficient condition for lattice partitions to be PNC-compatible, and we also present some practical examples of the compute-and-forward codes suggested by our algebraic framework [10].

Building upon our previous work, in this paper we aim to derive the design criteria for the compute-and-forward codes constructed from finite-dimensional lattice partitions (referred to as lattice network codes). More precisely, we seek explicit guidelines to choose the parameters \( \{a_\ell\} \) and \( \alpha \) and guidelines to design lattice partitions. To achieve this objective, we approximate the probability of decoding error for the lattice point \( \sum_{\ell=1}^L a_\ell x_\ell \). The major difficulty here is that the effective noise, \( \sum_{\ell=1}^L (\alpha h_\ell - a_\ell) x_\ell + \alpha z \), is not necessarily Gaussian.

To alleviate this difficulty, we focus on a special case in which the lattice partition admits hypercube shaping so that the signal point \( x_\ell \) is uniformly distributed over some hypercube. This assumption enables us not only to simplify the theoretical analysis, but also to reduce shaping complexity.
at the transmitters. Under this assumption, we show that—in order to reduce the error probability—the parameters \( \{a_\ell\} \) and \( \alpha \) should be chosen such that the quantity \( Q = |\alpha|^2 + \text{SNR} \sum_{\ell=1}^L \|a_\ell h_\ell - a_\ell \|^2 \) is minimized; moreover, the lattice partition should be chosen such that the minimum inter-coset distance is maximized under a given power constraint.

Applying these design criteria, we show that finding the optimal parameters \( \{a_\ell\} \) and \( \alpha \) is equivalent to solving a shortest vector problem (SVP) in a randomly generated lattice. Although solving the SVP is known to be NP hard, many efficient suboptimal algorithms exist, which are adequate if the corresponding quantity \( Q \) is small enough. With respect to the design of lattice partitions, we show that for the case of self-similar construction, designing a good lattice partition amounts to constructing a lattice with large minimum distance and small kissing number, which is a conventional lattice design problem; we show that for the case of complex Construction A, designing a good lattice partition amounts to constructing a linear code with large minimum Euclidean weight, which is related to conventional code construction problem.

II. LATTICE NETWORK CODING

A. Physical-Layer Network Coding

We start by reviewing the basic structure of a generic PNC system. As observed in [8], the cornerstone of a PNC scheme is the problem of computing linear functions over a Gaussian multiple-access channel (MAC), as illustrated in Fig. 1.

![Fig. 1. Computation over a Gaussian MAC.](image)

Each transmitter (indexed by \( \ell = 1, \ldots, L \)) is equipped with an identical encoder \( E : \mathbb{F}_q^k \to \mathbb{C}^n \) that maps a message vector \( w_\ell \in \mathbb{F}_q^k \) to a signal vector \( x_\ell = E(w_\ell) \in \mathbb{C}^n \) satisfying the average power constraint \( \frac{1}{L} E \| x_\ell \|^2 \leq P \). The rate of the encoder, in bits per complex dimension, is defined as \( (k \log_2 q)/n \). For simplicity, we assume that each \( w_\ell \) is uniformly distributed in \( \mathbb{F}_q^k \) and independent of each other.

The receiver observes a noisy linear combination of the transmitted signal vectors through a Gaussian MAC channel:

\[
y = \sum_{\ell=1}^L h_\ell x_\ell + z,
\]

where \( h_1, \ldots, h_L \in \mathbb{C} \) are the channel fading coefficients, \( z \sim \mathcal{CN}(0, \sigma^2 I_n) \) is a circularly-symmetric jointly-Gaussian complex random vector, and \( I_n \) is the \( n \times n \) identity matrix.

Let \( h \triangleq (h_1, \ldots, h_L) \in \mathbb{C}^L \) denote the channel coefficient vector. We assume that \( h \) is known at the receiver, but not at the transmitters.

The goal of the receiver is to reliably compute one or more linear combinations of transmitted message vectors. Specifically, the receiver first selects some (finite-field) coefficient vector \( \tilde{a} \triangleq (\tilde{a}_1, \ldots, \tilde{a}_L) \in \mathbb{F}_q^L \) based on \( h \). Then, it attempts to decode the linear combination \( u = \sum_{\ell=1}^L \tilde{a}_\ell w_\ell \) from the channel output \( y \) according to a decoder \( \tilde{D}(y | h, \tilde{a}) : \mathbb{C}^n \to \mathbb{F}_q^L \). Let \( \hat{u} = \tilde{D}(y | h, \tilde{a}) \) be the decoded linear combination. If \( \hat{u} \neq u \), we say a decoding error occurs. The probability of error of the decoder (as a function of \( h \) and \( \tilde{a} \)) is given by \( \Pr[\hat{u} \neq u] \).

An \((n, k, L, q)\) PNC scheme is defined by an encoder \( E(\cdot) \) and a decoder \( \tilde{D}(\cdot | h, \tilde{a}) \) for all \( h, \tilde{a} \). Ideally, a PNC scheme should have a high encoder rate and a low error probability, as well as efficient encoding and decoding methods.

B. Lattice Network Coding

A lattice network coding (LNC) scheme is a lattice-partition-based approach to physical-layer network coding proposed in [10], which generalizes Nazer-Gastpar’s compute-and-forward approach [8].

Let \( R \) be a discrete subring of \( \mathbb{C} \). In addition, assume that \( R \) is a principal ideal domain (PID). Typical examples include the integer numbers \( \mathbb{Z} \), the Gaussian integers \( \mathbb{Z}[i] \), and the Eisenstein integers \( \mathbb{Z}[(-1 + i\sqrt{3})/2] \).

Let \( N \leq n \). An \( R\)-lattice of dimension \( N \) in \( \mathbb{C}^n \) is defined as the set of all \( R \)-linear combinations of \( N \) linearly independent vectors in \( \mathbb{C}^n \), i.e.,

\[
\Lambda = \{ rG_\Lambda : r \in R^N \}
\]

where \( G_\Lambda \in \mathbb{C}^{N \times N} \) is full-rank over \( \mathbb{C} \) and is called a generator matrix for \( \Lambda \).

An \( \Lambda \)-sublattice \( \Lambda' \) of \( \Lambda \) is a subset of \( \Lambda \) which is itself an \( \Lambda \)-lattice. The set of all the cosets of \( \Lambda' \) in \( \Lambda \), denoted by \( \Lambda / \Lambda' \), forms a partition of \( \Lambda \), and is hereafter called an \( \Lambda \)-lattice partition. Throughout this paper, we only consider the case of finite lattice partitions, i.e., the cardinality \( |\Lambda / \Lambda'| \) is finite, which is equivalent to saying that \( \Lambda' \) and \( \Lambda \) have the same dimension.

We say that a lattice partition \( \Lambda / \Lambda' \) is PNC-compatible if \( \Lambda / \Lambda' \) is isomorphic to \( \mathbb{F}_q^k \) for some \( q \) and \( k \). The conditions under which a lattice partition \( \Lambda / \Lambda' \) is PNC-compatible have been characterized in [10]. One condition is as follows: let \( \pi \) be a prime in \( R \) and let \( R_\pi \) denote the field \( R/(\pi) \); if \( \pi \Lambda \subseteq \Lambda' \), then \( \Lambda / \Lambda' \) is PNC-compatible. In this case, \( \Lambda / \Lambda' \) is isomorphic to \( R_\pi^k \) for some \( k \) and there exists a surjective \( R \)-module homomorphism \( \varphi : \Lambda \to R_\pi^k \) such that \( \Lambda' \) is the kernel of \( \varphi \).

1Let \( \sigma : R \to R_\pi \) be the natural homomorphism. We can make \( R_\pi^k \) into an \( R \)-module by defining the action of \( R \) on \( R_\pi \) as \( \sigma(a)w \).
Now we are ready to describe the basic structure of a generic LNC scheme. To this end, we introduce the definitions of lattice quantizers and lattice decoders.

A lattice quantizer is any function \( Q_\Lambda : \mathbb{C}^n \to \Lambda \) satisfying
\[
Q_\Lambda (\lambda + x) = \lambda + Q_\Lambda (x), \quad \forall \lambda \in \Lambda, \forall x \in \mathbb{C}^n.
\]

A particular example is the quantizer that maps \( x \in \mathbb{C}^n \) to the nearest lattice point in the Euclidean distance, i.e.,
\[
Q_\Lambda (x) = \arg \min_{\lambda \in \Lambda} \| x - \lambda \|,
\]
which is usually referred to as a lattice decoder \( D_\Lambda \) for \( \Lambda \).

For any lattice quantizer \( Q_\Lambda \), the set \( \mathcal{R}_f (\Lambda) \triangleq \{ x : Q_\Lambda (x) = 0 \} \) is called a fundamental region of the lattice \( \Lambda \). Clearly, any lattice quantizer is completely specified by a fundamental region \( \mathcal{R}_f (\Lambda) \).

A generic LNC scheme works as follows.

**Transmitter** \( \ell \) sends:
\[
x_\ell = \mathcal{E}(w_\ell) = \mathcal{F}(w_\ell) + d_\ell - Q_{\Lambda'}(\mathcal{F}(w_\ell) + d_\ell) \tag{1}
\]
where \( Q_{\Lambda'} : \mathbb{C}^n \to \Lambda' \) is a lattice quantizer for the sublattice \( \Lambda' \) and \( d_\ell \) is a dither uniformly distributed over the fundamental region \( \mathcal{R}_f (\Lambda') \). We assume that the dither \( d_\ell \) is known to transmitter \( \ell \) as well as to the receiver.

Observe that \( x_\ell \in \mathcal{R}_f (\Lambda') \) by the definition of \( Q_{\Lambda'} \). Further, as shown in [9], if \( d_\ell \) is uniformly distributed over \( \mathcal{R}_f (\Lambda') \), so is \( x_\ell \). In other words, the average power of the transmitted signal \( x_\ell \) is determined by the second moment of the fundamental region \( \mathcal{R}_f (\Lambda') \).

**Receiver computes:**
\[
\hat{u} = D(y|h, \tilde{a}) = \varphi \left( D_\Lambda \left( \alpha y - \sum_{\ell=1}^L a_\ell d_\ell \right) \right)
\]
where \( \alpha \in \mathbb{C} \) and \( a = (a_1, \ldots, a_L) \in \mathbb{R}^L \) are receiver parameters. Note that
\[
\hat{u} = \varphi \left( D_\Lambda \left( \sum_{\ell=1}^L a_\ell (x_\ell - d_\ell) + \sum_{\ell=1}^L (\alpha h_\ell - a_\ell) x_\ell + \alpha z \right) \right) = \varphi \left( \sum_{\ell=1}^L a_\ell \mathcal{F}(w_\ell) \right) + \varphi \left( D_\Lambda (n) \right)
\]
\[
= \sum_{\ell=1}^L \sigma(a_\ell) w_\ell + \varphi \left( D_\Lambda (n) \right)
\]
where
\[
n = \sum_{\ell=1}^L (\alpha h_\ell - a_\ell) x_\ell + \alpha z \tag{2}
\]
is called the effective noise. Hence, the linear combination \( u = \sum_{\ell=1}^L \sigma(a_\ell) w_\ell \) is computed correctly if and only if the effective noise \( n \) satisfies \( D_\Lambda (n) \in \Lambda' \). In other words, we have the following equality for the error probability
\[
Pr[\hat{u} \neq u] = Pr[D_\Lambda (n) \notin \Lambda'].
\]

**Remark:** For any receiver parameter \( a \), the corresponding (finite-field) coefficient vector \( \tilde{a} \) is given by \( \tilde{a} = \sigma(a) \). This connects the decoder \( D(\cdot|h, \hat{a}) \) for LNC to the decoder \( D(\cdot|h, \tilde{a}) \) for PNC.

III. **Probability of Error for Hypercube Shaping**

From a receiver’s perspective, the probability of decoding error should be made as small as possible. This suggests the study of the error probability \( Pr[D_\Lambda (n) \notin \Lambda'] \). Note that the effective noise \( n \) is not necessarily Gaussian, making the analysis nontrivial. In this paper, we focus on a special case in which the fundamental region \( \mathcal{R}_f (\Lambda') \) is a hypercube in \( \mathbb{C}^n \), i.e., \( \mathcal{R}_f (\Lambda') = [-b, b]^{2n} \) for some \( b > 0 \). This corresponds to the so-called hypercube shaping in [11]. It is easy to see that, under hypercube shaping, the average power consumption is given by \( P = \frac{1}{4} E[\| x_\ell \|^2] = \frac{3}{2} b^2 \).

Let \( \Lambda/\Lambda' \) be an \( R \)-lattice partition, and assume that hypercube shaping is used. We will show that the error probability \( Pr[D_\Lambda (n) \notin \Lambda'] \) is closely related to the minimum inter-coset distance, defined as follows.

The inter-coset distance, \( d(\lambda_1 + \Lambda', \lambda_2 + \Lambda') \), between two cosets \( \lambda_1 + \Lambda', \lambda_2 + \Lambda' \) of \( \Lambda/\Lambda' \) is defined as
\[
d(\lambda_1 + \Lambda', \lambda_2 + \Lambda') \triangleq \min_{\alpha \in \Lambda} \| x_1 - x_2 \|, \quad x_1 \in \lambda_1 + \Lambda', \quad x_2 \in \lambda_2 + \Lambda'.
\]
Note that \( d(\lambda_1 + \Lambda', \lambda_2 + \Lambda') = 0 \) if and only if \( \lambda_1 + \Lambda' = \lambda_2 + \Lambda' \).

We then define the minimum inter-coset distance between elements of \( \Lambda/\Lambda' \) as
\[
d(\Lambda/\Lambda') \triangleq \min_{\lambda_1, \lambda_2} d(\lambda_1 + \Lambda', \lambda_2 + \Lambda'), \quad \lambda_1 + \Lambda' \neq \lambda_2 + \Lambda'.
\]
Clearly, \( d(\Lambda/\Lambda') \) corresponds to the length of the shortest vectors in the set difference \( \Lambda \setminus \Lambda' \).

Let \( N(\Lambda \setminus \Lambda') \) denote the number of the shortest vectors in \( \Lambda \setminus \Lambda' \). We have the following union bound estimate (UBE) of the error probability \( Pr[D_\Lambda (n) \notin \Lambda'] \).

**Theorem 1 (Probability of Decoding Error):** Let \( \Lambda/\Lambda' \) be an \( R \)-lattice partition. Assume that hypercube shaping is used for \( \Lambda/\Lambda' \). Then for any given receiver parameters \( \alpha \in \mathbb{C} \) and \( a \in \mathbb{R}^L \), the union bound estimate of the probability of decoding error is
\[
Pr[D_\Lambda (n) \notin \Lambda'] \approx N(\Lambda \setminus \Lambda') \exp \left(-\frac{d^2(\Lambda/\Lambda')}{4\sigma^2 Q} \right)
\]
for high signal-to-noise ratios, where the quantity \( Q \) is given by
\[
Q = |\alpha|^2 + \text{SNR} \| \alpha h - a \|^2
\]
and \( \text{SNR} = P/\sigma^2 \).

The proof is given in the Appendix.

**Remark:** It can be shown that the UBE for an AWGN channel using lattice partitions is given by
\[
Pr[\text{error}] \approx N(\Lambda \setminus \Lambda') \exp \left(-\frac{d^2(\Lambda/\Lambda')}{4\sigma^2} \right).
\]
Hence, there is a factor of \( 1/Q \) of loss in the SNR for lattice network coding, which can be interpreted as the “cost of lattice network coding.”
IV. Design Criteria for Lattice Network Coding

Theorem 1 suggests the following design criteria for lattice network coding under hypercube shaping, which provide explicit guidelines for finding receiver parameters and designing lattice partitions.

Design criteria: The receiver parameters $\alpha$ and $a$ should be chosen such that the quantity $Q = |\alpha|^2 + \text{SNR}||a\mathbf{h} - a||^2$ is minimized. The lattice partition $\Lambda/\Lambda'$ should be chosen such that the minimum inter-coset distance $d(\Lambda/\Lambda')$ is maximized under power constraint $P$ and the parameter $\mathcal{N}(\Lambda \setminus \Lambda')$ is minimized.

A. Finding Receiver Parameters

We first show that finding the optimal receiver parameters $\alpha$ and $a$ is essentially a shortest vector problem (SVP). Following the design criteria, the optimal $\alpha$ and $a$ are defined as

$$\alpha_{\text{opt}}, a_{\text{opt}} = \arg \min_{\alpha \in \mathbb{C}, a \neq 0} \left\{ |\alpha|^2 + \text{SNR}||a\mathbf{h} - a||^2 \right\}. \quad (3)$$

It is interesting to note that this criterion matches perfectly with the criterion derived in [8] for maximizing the computation rate. Hence, the methods and results in [8] can be carried over here, as shown in the following proposition.

Proposition 1: For any given $a \neq 0$, the optimal $\alpha$, denoted by $\alpha_{\text{opt}}(a)$, is given by

$$\alpha_{\text{opt}}(a) = \frac{ah^\dagger \text{SNR}}{\text{SNR}||\mathbf{h}||^2 + 1};$$

and the corresponding quantity $Q$, denoted by $Q(a)$, is given by

$$Q(a) = aM a^\dagger,$$

where the matrix $M$ is

$$M = \text{SNR}I_n - \frac{\text{SNR}^2}{\text{SNR}||\mathbf{h}||^2 + 1} h^\dagger \mathbf{h}.$$

We observe that the matrix $M$ is Hermitian and positive-definite. Hence, $M$ has a Cholesky decomposition $M = LL^\dagger$, where $L$ is a lower triangular matrix. It follows that

$$Q(a) = aM a^\dagger = ||aL||^2.$$

Therefore, the optimal $a$ is given by

$$a_{\text{opt}} = \arg \min_{a \neq 0} ||aL||,$$

which is a shortest vector problem.

In other words, the receiver should solve the SVP in order to find the optimal parameters $\alpha$ and $a$. Although solving the SVP is known to be NP hard, many efficient suboptimal algorithms exist, such as the celebrated LLL algorithm [12] and its complex version, which have a polynomial complexity. As implied in Proposition 1, suboptimal algorithms are adequate if the corresponding $Q(a)$ is small enough.

B. Designing Lattice Partitions

We next discuss the design of lattice partitions. We begin with the self-similar construction of lattice partitions in which the sublattice $\Lambda'$ is a scaled version of the lattice $\Lambda$. We then turn to another well-known construction of lattice partitions — complex Construction A [13].

1) Self-Similar Construction: Let $\Lambda' = \pi \Lambda$ for some prime element $\pi$ in $R$. It is straightforward to check $\Lambda/\Lambda'$ is PNC-compatible. For this construction, it is easy to see that

$$d(\Lambda/\Lambda') = d_{\text{min}}(\Lambda)$$

where $d_{\text{min}}(\Lambda)$ is the minimum distance of $\Lambda$ and $K_{\text{min}}(\Lambda)$ is the kissing number, which is defined as the number of nearest neighbors to any lattice points in $\Lambda$. Hence, designing a good lattice partition amounts to designing a lattice $\Lambda$ with large $d_{\text{min}}(\Lambda)$ and small $K_{\text{min}}(\Lambda)$, which is a conventional lattice design problem.

2) Complex Construction A: Let $\pi$ be a nonzero non-unit element in $R$ and let $R_\pi$ denote the quotient ring $R/\langle \pi \rangle$. Let $\sigma : R \rightarrow R_\pi$ be the natural (ring) homomorphism and extend $\sigma$ to an $R$-module homomorphism $\sigma : R^n \rightarrow R_\pi^n$. Let $C$ be a linear code over $R_\pi$ of length $n$. Define an $R$-lattice $\Lambda_C$ as

$$\Lambda_C = \{ \lambda \in R^n : \sigma(\lambda) \in \mathbb{C}\}.$$

Let $\Lambda'_C = \{ \pi \cdot r : r \in R^n \}$. It is easy to see that $\Lambda'_C$ is a sublattice of $\Lambda_C$. Hence, we obtain a lattice partition $\Lambda_c/\Lambda'_C$ from the linear code $C$. Further, it is easy to check that $\pi \Lambda_C \subseteq \Lambda'_C$. Hence, $\Lambda_c/\Lambda'_C$ is PNC-compatible if $\pi$ is a prime element in $R$.

To enforce the existence of hypercube shaping, we choose $R$ as the set of Gaussian integers given by $\mathbb{Z}[i] \triangleq \{a + bi : a, b \in \mathbb{Z}\}$ and $\pi$ as a prime number in $\mathbb{Z}$ of the form $4n + 3$. It is easy to check that $\pi$ is a prime element in $\mathbb{Z}[i]$ and the sublattice $\Lambda'_C$ is given by $\pi \mathbb{Z}[i]^n$ whose Voronoi region is $\mathcal{V}(\Lambda'_C) = [-\pi/2, \pi/2]^{2n}$, which is a hypercube in $\mathbb{C}^n$. In other words, $\Lambda_c/\Lambda'_C$ is PNC-compatible that admits hypercube shaping. Optionally, $\Lambda_c/\Lambda'_C$ may be scaled if needed to satisfy the average power constraint.

We now relate $d(\Lambda_c/\Lambda'_C)$ and $\mathcal{N}(\Lambda_c \setminus \Lambda'_C)$ to parameters of the linear code $C$. For each codeword $e = (c_1 + \langle \pi \rangle, \ldots, c_n + \langle \pi \rangle)$ in $C$, let $\langle e \rangle$ denote one of the coset representatives for $e$ that have the minimum Euclidean norm. It is easy to check that $\langle e \rangle$ is uniquely given by

$$\langle e \rangle = (c_1 - \lfloor c_1/\pi \rfloor \times \pi, \ldots, c_n - \lfloor c_n/\pi \rfloor \times \pi),$$

where $\lfloor \cdot \rfloor : \mathbb{C} \rightarrow \mathbb{Z}[i]$ is the rounding operation that maps a complex number to its closest Gaussian integer in $\mathbb{Z}[i]$. The Euclidean weight $w_E(e)$ of $e$ can then be defined as the squared Euclidean norm of $\langle e \rangle$, that is, $w_E(e) = ||\langle e \rangle||^2$. Let $w_{E\text{min}}(C)$ be the minimum Euclidean weight of nonzero codewords in $C$ (i.e., $w_{E\text{min}}(C) = \min\{w_E(e) : e \neq 0, e \in C\}$) and let $A_{w_{E\text{min}}}$ be the number of codewords of weight $w_{E\text{min}}$. Then we have the following result:

Proposition 2: Let $C$ be a linear code over $\mathbb{Z}[i]$, and let $\Lambda_c/\Lambda'_C$ be a lattice partition constructed from $C$ using complex construction A. Suppose that $\Lambda_c/\Lambda'_C$ is scaled by $\gamma$ in order to satisfy the average power constraint. Then

$$d^2(\Lambda_c/\Lambda'_C) = \gamma^2 w_{E\text{min}}^2$$

and $\mathcal{N}(\Lambda_c \setminus \Lambda'_C) = A_{w_{E\text{min}}}$. 

Further, the shortest vector in \( \mathcal{C} \) is unique due to the uniqueness of \( \langle c \rangle \). Hence, we have

\[
\mathcal{N}(\mathcal{C} \setminus \mathcal{C}') = \sum_{\mathcal{L} \in \mathcal{C}} I[\|\mathcal{L} + \mathcal{C}'\| = l(\mathcal{L} \setminus \mathcal{C}')] = \sum_{c \in \mathcal{C}} I[|w_E(c)| = w_E^\text{min}]
\]

where \( I[\cdot] \) is the indicator function, completing the proof. 

Proposition 2 suggests that the problem of designing good lattice partitions using complex Construction A amounts to the construction of linear code \( \mathcal{C} \) with large \( w_E^\text{min} \) and small \( w_H^\text{min} \). Consider a coset given by \( \mathcal{L} + \mathcal{C}' \). Suppose that \( \sigma(\mathcal{L}) = c \) for some \( c \in \mathcal{C} \). Then the length of the shortest vectors in \( \mathcal{L} + \mathcal{C}' \), denoted by \( l(\mathcal{L} + \mathcal{C}') \), is given by

\[
l(\mathcal{L} + \mathcal{C}') = \gamma \|\langle c \rangle\|.
\]

Further, the shortest vector in \( \mathcal{L} + \mathcal{C}' \) is unique due to the uniqueness of \( \langle c \rangle \). Hence, we have

\[
\mathcal{N}(\mathcal{L} + \mathcal{C}') = \sum_{\mathcal{L} \in \mathcal{C}} I[l(\mathcal{L} + \mathcal{C}') = l(\mathcal{L} \setminus \mathcal{C}')] = \sum_{c \in \mathcal{C}} I[|w_E(c)| = w_E^\text{min}].
\]

Proposition 3: Let \( \pi = 1 + i \) be a prime in \( \mathbb{Z}[i] \) and let \( \mathcal{C} \) be a linear code over \( \mathbb{Z}[i] \). Then the minimum Euclidean weight \( w_E^\text{min}(\mathcal{C}) \) of \( \mathcal{C} \) can be lower bounded by

\[
w_E^\text{min}(\mathcal{C}) \geq w_M^\text{min}(\mathcal{C}),
\]

where \( w_M^\text{min}(\mathcal{C}) \) is the minimum Mannonheim weight of nonzero codewords in \( \mathcal{C} \). Then we have the following lower bound for the minimum Euclidean weight \( w_E^\text{min}(\mathcal{C}) \).

Proposition 3: Let \( \pi = 1 + i \) be a prime in \( \mathbb{Z}[i] \) and let \( \mathcal{C} \) be a linear code over \( \mathbb{Z}[i] \). Then the minimum Euclidean weight \( w_E^\text{min}(\mathcal{C}) \) of \( \mathcal{C} \) can be lower bounded by

\[
w_E^\text{min}(\mathcal{C}) \geq w_M^\text{min}(\mathcal{C}),
\]

where \( w_M^\text{min}(\mathcal{C}) \) is the minimum Mannonheim weight of nonzero codewords in \( \mathcal{C} \). Then we have the following lower bound for the minimum Euclidean weight \( w_E^\text{min}(\mathcal{C}) \).

Proposition 3: Let \( \pi = 1 + i \) be a prime in \( \mathbb{Z}[i] \) and let \( \mathcal{C} \) be a linear code over \( \mathbb{Z}[i] \). Then the minimum Euclidean weight \( w_E^\text{min}(\mathcal{C}) \) of \( \mathcal{C} \) can be lower bounded by

\[
w_E^\text{min}(\mathcal{C}) \geq w_M^\text{min}(\mathcal{C}),
\]

where \( w_M^\text{min}(\mathcal{C}) \) is the minimum Mannonheim weight of nonzero codewords in \( \mathcal{C} \). Then we have the following lower bound for the minimum Euclidean weight \( w_E^\text{min}(\mathcal{C}) \).

Proof: For each \( c \in \mathcal{C} \), we have

\[
|c^*|^2 \geq w_M(\{c\}) = w_M(c).
\]

Suppose that \( c^* \) is a codeword of the minimum Euclidean weight. Then we have

\[
|c^*|^2 \geq w_M(\{c^*\}) \geq w_M^\text{min}(\mathcal{C}),
\]

completing the proof.

Hence, codes of large \( w_M^\text{min} \) have large \( w_E^\text{min} \).
\[ \leq \sum_{\lambda \in \mathcal{N}(\Lambda \setminus \Lambda')} e^{-\nu \|\lambda\|^2/2} E\left[e^{\nu \Re\{\lambda^T x\}}\right], \; \forall \nu > 0 \tag{6} \]

where (5) follows from the union bound and (6) follows from the Chernoff bound. From (2), we have

\[ E\left[e^{\nu \Re\{\lambda^T x\}}\right] = E\left[e^{\nu \Re\{\lambda^T \left(\sum_{i} (a_i - a_i') x_i + a \lambda\} \right)}\right] = E\left[e^{\nu \Re\{\lambda^T \alpha x\}}\right] = e^{\frac{1}{2} \nu^2 \|\alpha\|^2 \|x\|^2} \prod_{\ell} E\left[e^{\nu \Re\{\lambda^T (a_{\ell} - a_{\ell}') x_{\ell}\}}\right] \tag{7} \]

\[ = e^{\frac{1}{2} \nu^2 \|\alpha\|^2 \|x\|^2} \prod_{\ell} E\left[e^{\nu \Re\{\lambda^T (a_{\ell} - a_{\ell}') x_{\ell}\}}\right] \tag{8} \]

where (7) follows from the independence of \(x_1, \ldots, x_L, z\) and (8) follows from the moment-generating function of a circularly symmetric complex Gaussian random vector.

Lemma 2: Let \(x \in \mathbb{C}^n\) be a complex random vector uniformly distributed over the complex \(n\)-cube \([-b, b]^{2n}\), where \(b > 0\). Then

\[ E\left[\Re\{v^T x\}\right] \leq e^{\|v\|^2 b^2/6}. \]

Proof: We have

\[ E\left[\Re\{v^T x\}\right] = E\left[\Re\{v^T x\} + \Im\{v^T x\}\right] = \prod_{i=1}^n E\left[\Re\{v_i x_i\}\right] E\left[\Im\{v_i x_i\}\right] = \prod_{i=1}^n \sinh(\Re\{v_i x_i\}) \sinh(\Im\{v_i x_i\}) \leq \prod_{i=1}^n \exp\left(\frac{(\Re\{v_i x_i\})^2}{6}\right) \exp\left(\frac{(\Im\{v_i x_i\})^2}{6}\right) = \exp\left(\frac{b^2}{6} \|v\|^2\right) \tag{11} \]

where (9) follows from the independence among each real/imaginary component, (10) follows from the moment-generating function of a uniform random variable, and (11) follows from \(\sinh(x)/x \leq e^{x^2/6}\) (which can be obtained by simple Taylor expansion).

Note that \(P = \frac{1}{n} E[\|x\|^2] = \frac{2}{3} b^2\). Thus, we have

\[ E\left[e^{\nu \Re\{\lambda^T x\}}\right] \leq e^{\frac{1}{2} \nu^2 \|\alpha\|^2 \|x\|^2} \prod_{\ell} E\left[e^{\nu \Re\{\lambda^T (a_{\ell} - a_{\ell}') x_{\ell}\}}\right] \frac{P}{4} = e^{\frac{1}{2} \nu^2 \|\alpha\|^2 \|x\|^2} e^{\nu \Re\{\lambda^T (a_{\ell} - a_{\ell}') x_{\ell}\}} \frac{P}{4} = e^{\frac{1}{2} \nu^2 \|\alpha\|^2 \|x\|^2} Q, \]

where the quantity \(Q\) is given by

\[ Q = \|\alpha\|^2 + \text{SNR} \|\alpha h - a\|^2 \]

and \(\text{SNR} = P/\sigma^2\). It follows that

\[ \Pr[\|n\| \notin \mathcal{R}_V(0)] \leq \sum_{\lambda \in \mathcal{N}(\Lambda \setminus \Lambda')} e^{-\nu \|\lambda\|^2/2 + \frac{1}{2} \nu^2 \|\lambda\|^2 \|x\|^2 \sigma^2 Q}, \; \forall \nu > 0 \]

Choosing \(\nu = 1/(\sigma^2 Q)\), we have

\[ \Pr[\|n\| \notin \mathcal{R}_V(0)] \leq \sum_{\lambda \in \mathcal{N}(\Lambda \setminus \Lambda')} e^{-\frac{|\lambda|^2}{4\sigma^2 Q}}. \]

For high signal-to-noise ratios, we have

\[ \sum_{\lambda \in \mathcal{N}(\Lambda \setminus \Lambda')} e^{-\frac{|\lambda|^2}{4\sigma^2 Q}} \approx \mathcal{N}(\Lambda \setminus \Lambda') \exp\left(-\frac{d^2(\Lambda / \Lambda')}{4\sigma^2 Q}\right). \]

Therefore, we have

\[ \Pr[D_{\Lambda}(n) \notin \Lambda] \leq \Pr[\|n\| \notin \mathcal{R}_V(0)] \approx \mathcal{N}(\Lambda \setminus \Lambda') \exp\left(-\frac{d^2(\Lambda / \Lambda')}{4\sigma^2 Q}\right), \]

completing the proof of Theorem 1.

References


