Systematic and Optimal Cyclotomic Lattices and Diagonal Space-Time Block Code Designs*

Genyuan Wang, Huiyong Liao, Haiquan Wang, and Xiang-Gen Xia

Abstract

In this correspondence, a new and systematic design of cyclotomic lattices with full diversity is proposed by using some algebraic number theory. This design provides infinitely many full diversity cyclotomic lattices for a given lattice size. Based on the packing theory and the concrete form of the design, optimal cyclotomic lattices are presented by minimizing the mean transmission signal power for a given minimum (diversity) product (or equivalently maximizing the minimum product for a given mean transmission signal power). The newly proposed cyclotomic lattices can be applied to both space-time code designs for multi-antenna systems and linear precode design for signal space diversity in single antenna systems over fast Rayleigh fading channels. Although there are some cyclotomic lattices/space-time codes existed in the literature, most of them are not optimal.

Keywords: cyclotomic lattices, space-time block codes, algebraic number theory, cyclotomic fields, Galois theory

1 Introduction

Space-time block code designs have recently attracted considerable attentions, see for example [5]-[37]. There have been several kinds of space-time block code designs, for example, orthogonal space-time block code designs [12]-[23], unitary space-time code designs [24]-[29], algebraic space-time code designs [35]-[39], and lattice based diagonal space-time code designs using algebraic number theory [1]-[5]. Among these space-time code designs, some of them are linear, such as orthogonal space-time block codes [12]-[23] and lattice based diagonal space-time block codes using algebraic tools [1]-[5], where the linearity is in terms of the information symbols and provides certain fast decoding algorithms, such as the sphere decoding, see for example [30]-[34]. Orthogonal space-time block codes satisfy not only the linearity but also the orthogonality and therefore possesses an even faster maximum-likelihood (ML) decoding [12, 13]. However, their rates are limited [18]. This correspondence lies in the direction of systematic cyclotomic lattices and therefore linear lattice-based diagonal space-time block code designs using algebraic number theory studied in [1]-[5], which are not unitary and different from unitary diagonal space-time block codes proposed in [24]-[26], and also different from the diagonal codes proposed in [8].

*The authors are with the Department of Electrical and Computer Engineering, University of Delaware, Newark, DE 19716. Email: {gwang, liao, hwang, xxia}@ee.udel.edu. This work was supported in part by the Air Force Office of Scientific Research (AFOSR) under Grant No. F49620-02-1-0157, the National Science Foundation under Grants CCR-0097240 and CCR-0325180, and CTA-ARL DAAD-190120011. The material in this correspondence was presented in part at the IEEE Globecom, San Francisco, Dec. 2003 and the IEEE International Symposium on Information Theory, Chicago, June/July 2004.

Diagonal space-time block codes using algebraic number theory proposed in [5] were motivated from the designs of full diversity multi-dimensional signal constellations for resisting both Rayleigh fading and Gaussian additive noises proposed in [1, 2, 3]. These codes are built upon lattices $[\mathbf{y}_1, \cdots, \mathbf{y}_{L_t}]^T = G[\mathbf{x}_1, \cdots, \mathbf{x}_{L_t}]^T$, where L_t is the number of transmit antennas, ^{T} stands for the transpose, $\mathbf{x}_i$ represent complex-valued information symbols and G is a generating matrix and $\mathbf{y}_i$ are placed as diagonal elements in a diagonal space-time code. To resist both fading and additive noise, both good diversity product and good Euclidean distance of the codewords $[\mathbf{y}_1, \cdots, \mathbf{y}_{L_t}]^T$ are required, and G is a unitary matrix in [2, 4]. In [2], the construction of G over $\mathbb{Z}[\zeta_4]$ and $\mathbb{Z}[\zeta_3]$ was provided with unitary matrix G. In [4], a systematic unitary cyclotomic lattice code (G is unitary matrix) design scheme over a general number rings was proposed by using Fourier transform with Diophantine approximation theory. And the optimal unitary cyclotomic lattices are also provided in [4]. The unitariness of the generating matrix G in [2, 4] is used to maintain the Euclidean distance and the mean power of the transmission signals the same as that of the information symbols. To resist fading as commonly used in space-time coding, good diversity product is usually imposed, and some algebraic construction of G over $\mathbb{Z}[\zeta_4] = \mathbb{Z}[j]$ with $j = \sqrt{-1}$ (the entries of G are integrals over $\mathbb{Z}[\zeta_4]$) is proposed in [3] for information symbols $\mathbf{x}_i$ in $\mathbb{Z}[\zeta_4]$, i.e., QAM on the square lattice, such as QPSK and square 16-QAM. The case when generating matrix G is real and takes the forms of Hadamard transform is studied in [3, 5]. In [7], a different space-time code design of full diversity is proposed by also using cyclotomic field extensions without much analysis of the diversity product property and it is essentially equivalent to a kind of diagonal space-time code designs. In [9], a D-BLAST lattice code structure is proposed. In each layer of the D-BLAST lattice code, components of a more general high dimensional lattice is used, where, however, no new lattice designs is proposed while the unitary cyclotomic lattices in [2] are adopted in the D-BLAST lattice codes.

There are three issues that may affect the code performance in the above lattice based diagonal space-time code design, namely, (i) where the information symbols $\mathbf{x}_i$ belong to; (ii) where the elements of the generating matrix G belong to; and (iii) whether the generating matrix G is unitary. In this correspondence, we focus on the criterion of maximizing the diversity product and consider these three issues together in a general way: information symbols $\mathbf{x}_i$ may not necessarily be in $\mathbb{Z}[\zeta_4]$, elements of generating matrix G may not necessarily be integrals of $\mathbb{Z}[\zeta_4]$, and generating matrix G may not necessarily be unitary. Information symbols $\mathbf{x}_i$ and elements of generating matrix G are from general cyclotomic field extensions. We call such diagonal space-time block codes *cyclotomic space-time codes*. We propose a systematic construction of full diversity cyclotomic lattices and apply them to design space-time codes of full diversity for a general number of transmit antennas, and for a fixed number of transmit antennas, there are infinitely many cyclotomic space-time codes/lattices. Furthermore, we obtain and list the optimal ones among these cyclotomic space-time codes/lattices, where the optimality is in the sense that, for a fixed mean transmission signal power, its diversity product is maximized, or for a fixed diversity product, its mean transmission signal power is minimized. It turns out that most of the optimal cyclotomic space-time codes can not be obtained by using information symbols $\mathbf{x}_i$ in $\mathbb{Z}[\zeta_4]$, or by using generating matrix G with elements being integrals over $\mathbb{Z}[\zeta_4]$, or by using unitary generating matrices G. With our newly proposed optimal cyclotomic space-time codes, we present some new design examples of optimal cyclotomic space-time codes that have the best known diversity products of diagonal space-time codes. What we want to emphasize here is that the full diversity cyclotomic lattices we propose in this correspondence are mathematically *concrete* and systematic and therefore provide us the convenience to study the optimality. This is different from the existing lattice-based code designs in the literature where general algebraic numbers are used and it is hard to systematiclly formulate all general algebraic numbers and therefore difficult to study the optimality unless it is specified to a particular cyclotomic ring/field, such as $\mathbb{Z}[j]$, and unitary generating matrices. Another remark is that the cyclotomic lattices we propose in this correspondence can also be applied to linear precode designs for achieving signal space diversity for single antenna systems over fast Rayleigh fading channels as studied in [1, 2, 3].

This correspondence is organized as follows. In Section 2, we describe the problem in more details and introduce the necessary notations and concepts about lattices. In Section 3, we introduce a systematic design of full diversity cyclotomic lattices and diagonal space-time codes. Due to the non-unitariness of a generating matrix G, in Section 4, we first study the relationships between the generating matrix and its corresponding lattice, the signal mean power, and the diversity product, and then convert the criterion on maximizing diversity product to a criterion on generating matrices when the diversity product is fixed. And finally, in Section 4, we present the optimal cyclotomic lattices. In Section 5, some optimal cyclotomic space-time code designs are given based on the proposed optimal cyclotomic lattices studied in Section 4. In Section 6, we show some numerical simulation results.

The following notations are used throughout this correspondence: capital English letters, such as, K and G, represent matrices and bold small English letters, such as $\mathbf{x}$ and $\mathbf{y}$, represent complex symbols (or numbers or points) on two dimensional real lattices, small English letters, such as x, y and z, represent real symbols (or numbers or points) and

L_t: number of transmit antennas

$\mathbb{N}$: natural numbers

$\mathbb{Z}$: ring of integers

$\mathbb{Q}$: field of rational numbers

$\mathbb{R}$: field of real numbers

$\mathbb{C}$: field of complex numbers

$\phi(n)$: Euler totient function of positive integer n

$\zeta_m = \exp\left(j\frac{2\pi}{m}\right)$

$\mathbb{Z}[\zeta_m]$: ring generated by $\mathbb{Z}$ and ζ_m

K and G: real and complex generating matrices for real and complex lattices, respectively

$\Lambda_n(K)$: n dimensional real lattice of real generating matrix K

$\Gamma_n(G)$: n dimensional complex lattice of complex generating matrix G

$\mathbb{Q}(\zeta_m)$: number field generated by the rational field $\mathbb{Q}$ and ζ_m

$\Lambda_{\zeta_m} = \Lambda_2(K_{\zeta_m})$: two dimensional real lattice with generating matrix $K_{\zeta_m} = \begin{bmatrix} 1 & \cos(\frac{2\pi}{m}) \\ 0 & \sin(\frac{2\pi}{m}) \end{bmatrix}$

$[\mathbb{E} : \mathbb{F}]$: the extension degree of field $\mathbb{E}$ over field $\mathbb{F}$.

2 Complex Lattices and Problem Description

As mentioned in Introduction, we are interested in diagonal space-time block codes formed as follows. Let L_t be the number of transmit antennas. Let $\mathbf{x}_i$, $1 \le i \le L_t$, be information symbols taking from a certain constellation. Let G be an $L_t \times L_t$ matrix and

$$[\mathbf{y}_1, \cdots, \mathbf{y}_{L_t}]^T = G[\mathbf{x}_1, \cdots, \mathbf{x}_{L_t}]^T. \tag{1}$$

The diagonal space-time code Ω consists of $L_t \times L_t$ matrices of the form $\mathrm{diag}(\mathbf{y}_1, \cdots, \mathbf{y}_{L_t})$. We are interested in such a diagonal space-time code Ω that (i) it has the full rank property, i.e., any difference matrix of any two distinct matrices in Ω has full rank; and (ii) its following diversity product is as large as possible:

$$\xi = \min_{\mathrm{diag}(\mathbf{y}_1, \cdots, \mathbf{y}_{L_t}) \neq \mathrm{diag}(\mathbf{e}_1, \cdots, \mathbf{e}_{L_t}) \in \Omega} \prod_{i=1}^{L_t} |\mathbf{y}_i - \mathbf{e}_i|^2, \tag{2}$$

where the transmission signal mean power of $\mathbf{y}_i$ is fixed. The main goal of this correspondence is to properly determine an information signal constellation of $\mathbf{x}_i$ and a generating matrix G for a diagonal space-time code Ω with the above properties. To do so, we first introduce some concepts and properties on real and complex lattices.

2.1 Real and Complex Lattices

In this subsection, we first define real and complex lattices, and see some existing examples, and then formulate the problems we are interested, and finally present some properties of complex lattices that are used in the later sections for cyclotomic space-time code designs.

2.1.1 Definitions

We first define a real lattice.

Definition 1 *An n-dimensional real lattice $\Lambda_n(K)$ is a subset in $\mathbb{R}^n$:*

$$\Lambda_n(K) = \left\{ \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = K \begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix} \middle| \; z_i \in \mathbb{Z} \;\; for \; 1 \le i \le n \right\},$$

where $\mathbb{Z}$ is the ring of all integers and K is an $n \times n$ real matrix of full rank and called the generating matrix of the real lattice $\Lambda_n(K)$ and $\det(\Lambda_n(K)) \triangleq |\det(K)|$.

Clearly, $\Lambda_n(K)$ is a subgroup of $\mathbb{R}^n$ with component-wise addition. When $n = 2$, every point $[x_1, x_2]^T$ in a two dimensional real lattice $\Lambda_2(K)$ belongs to $\mathbb{R}^2$ and therefore can be thought of as a complex number $\mathbf{x} = x_1 + jx_2$ in the complex plane $\mathbb{C}$. In this correspondence, we do not distinguish a two dimensional real point $[x_1, x_2]^T \in \mathbb{R}^2$ and a complex number or point $\mathbf{x} = x_1 + jx_2 \in \mathbb{C}$ otherwise it is specified. To distinguish it from general two dimensional real lattices, for $\zeta_m = \exp(j\frac{2\pi}{m})$ we use Λ_{ζ_m} to denote the two dimensional real lattice with the generating matrix

$$K_{\zeta_m} = \begin{bmatrix} 1 & \cos(\frac{2\pi}{m}) \\ 0 & \sin(\frac{2\pi}{m}) \end{bmatrix} = \begin{bmatrix} 1 & \mathrm{Re}(\zeta_m) \\ 0 & \mathrm{Im}(\zeta_m) \end{bmatrix}, \tag{3}$$

where Re and Im stand for the real and imaginary parts of a complex number, respectively. Thus, $\Lambda_{\zeta_m} = \Lambda_2(K_{\zeta_m})$. This two dimensional real lattice is the base for signal constellations of cyclotomic space-time codes studied later. It is easy to check that

$$\Lambda_{\zeta_m} \subset \mathbb{Z}[\zeta_m], \ \Lambda_{\zeta_4} = \mathbb{Z}[\zeta_4] = \mathbb{Z}[j], \ \text{ and } \Lambda_{\zeta_3} = \Lambda_{\zeta_6} = \mathbb{Z}[\zeta_3] = \mathbb{Z}[\zeta_6], \tag{4}$$

and Λ_{ζ_4} is the square lattice.

A complex lattice defined below is a lattice based on a two dimensional real lattice.

Definition 2 *An n-dimensional complex lattice $\Gamma_n(G)$ over a two dimensional real lattice $\Lambda_2(K)$ is a subset of $\mathbb{C}^n$:*

$$\Gamma_n(G) = \left\{ \begin{bmatrix} \mathbf{y}_1 \\ \vdots \\ \mathbf{y}_n \end{bmatrix} = G \begin{bmatrix} \mathbf{x}_1 \\ \vdots \\ \mathbf{x}_n \end{bmatrix} \middle| \ \mathbf{x}_i \in \Lambda_2(K), \ \ \textit{for } 1 \le i \le n \right\}, \tag{5}$$

where G is an $n \times n$ complex matrix of full rank and called the generating matrix of the complex lattice $\Gamma_n(G)$. The above complex lattice is called a full diversity lattice if it satisfies

$$\prod_{i=1}^{n} |\mathbf{y}_i| > 0$$

for any non-zero vector $[\mathbf{x}_1, \cdots, \mathbf{x}_n]^T \neq [0, \cdots, 0]^T$ in $(\Lambda_2(K))^n$.

In Definition 2, points $\mathbf{x}_i$ from a two dimensional real lattice have been treated as complex numbers explained previously and therefore $\mathbf{y}_i$ are also complex numbers. On the other hand, if we treat all complex elements in matrix G and $\mathbf{x}_i$ and $\mathbf{y}_i$ as points in the two dimensional real space and two dimensional real lattices, respectively, the above n dimensional complex lattice can be also represented as a $2n$ dimensional real lattice as we shall see in more details later in Section 2.3.

2.1.2 Examples

With the above complex lattice definition, some recently proposed diagonal space-time codes in the literature can be formulated as complex lattices as listed in the following examples that motivate us to further generalize and improve these existing ones by considering general cyclotomic lattices as we shall see in Section 3.

Example 1. *Diagonal Algebraic Space-Time Block Codes – DAST Block Codes* [5, 3]

For $L_t = 2^q$, the DAST block code of size $|\Omega|^{L_t}$ is obtained from $[\mathbf{y}_1, \cdots, \mathbf{y}_{L_t}]^T = \mathbf{M}_{L_t}[\mathbf{x}_1, \cdots, \mathbf{x}_{L_t}]^T$, where $\mathbf{x}_l \in |\Omega|$-QAM, i.e., a QAM on the square lattice $\mathbb{Z}[\zeta_4]$, and $\mathbf{M}_{L_t}$ is an $L_t \times L_t$ real matrix and is generated in an iterative way as in the Hadamard matrix, [3],

$$\mathbf{M}_{L_t} = \left[\begin{array}{cc} \mathbf{M}^1_{L_t/2} & -\mathbf{M}^2_{L_t/2} \\ \mathbf{M}^2_{L_t/2} & \mathbf{M}^1_{L_t/2} \end{array} \right].$$

With this form of a *real* generating matrix $\mathbf{M}_{L_t}$ and an information signal constellation on the square lattice, it is found in [3] that the optimal generating matrices for $L_t = 2$ and $L_t = 4$ are, respectively,

$$\mathbf{M}_2 \triangleq \left[\begin{array}{cc} a & b \\ -b & a \end{array} \right], \text{ for } \ a = 0.5257, b = 0.8507,$$

and

$$\mathbf{M}_4 \triangleq \left[\begin{array}{cccc} a & b & c & d \\ -b & a & -d & c \\ -c & -d & a & b \\ d & -c & -b & a \end{array} \right], \text{ for } \ a = 0.2012, b = 0.3255, c = -0.4857, d = -0.7859.$$

When $L_t = 3$, the following form of matrices instead of the above Hadamard form was proposed in [3] for $\mathbf{x}_i$ in QAM on the square lattice:

$$\mathbf{M}_3 \triangleq \left[\begin{array}{ccc} a & b & c \\ b & c & a \\ -c & -a & -b \end{array} \right], \text{ for } \ a = \frac{1+\lambda}{1+\lambda+\lambda^2}, b = \lambda a, c = \frac{-\lambda}{1+\lambda} a,$$

where λ is a parameter. By using computer search, they found that the optimal λ for the space-time diagonal code is $\lambda = -2.24698$.

The above optimality is in the sense of maximizing the diversity product but restricted in either real Hadamard-form generating matrices for $L_t = 2$ and 4 or real generating matrices for $L_t = 3$ and moreover the information signal constellations are on the square lattice in $\mathbb{Z}[\zeta_4]$ (or Λ_{ζ_4}).

Example 2. *Good Codes for Fading Channels as well as Gaussian Channels* [2, 3]

In [2, 3], algebraic number theory is used to generate codes for both Gaussian channels and fading channels. These codes can also be thought of as a kind of complex lattice codes.

First of all, the best complex lattices $\Gamma_2(D_4)$ over Λ_{ζ_4}, $\Gamma_3(E_6)$ over Λ_{ζ_6}, and $\Gamma_4(E_8)$ over Λ_{ζ_4}, of dimensions 2, 3, and 4, respectively, (see for example [45]), for Gaussian channels were used in [2], where

$$D_4 = \left[\begin{array}{cc} 1 & 0 \\ 1 & \phi_2 \end{array} \right], \ \text{ for } \ \phi_2 = 1 + j,$$

$$E_6 = \left[\begin{array}{ccc} 1 & 0 & 0 \\ 1 & \phi_3 & 0 \\ 1 & 0 & \phi_3 \end{array} \right], \ \text{ for } \ \phi_3 = j\sqrt{3},$$

$$E_8 = \left[\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 1 & \phi_4 & 0 & 0 \\ 1 & 0 & \phi_4 & 0 \\ 1 & \phi_4 & \phi_4 & \phi_4^2 \end{array} \right], \ \text{ for } \ \phi_4 = 1 + j.$$

To resist fading, the above complex lattices were rotated in [2] to have the good diversity product property, i.e., non-zero diversity product (or full diversity) corresponding to the concept of space-time coding, as follows:

$$G_{2f} \triangleq \begin{bmatrix} 1 & \theta_2 \\ 1 & -\theta_2 \end{bmatrix} D_4, \quad \text{for} \quad \theta_2 = \exp\left(j\frac{\pi}{4}\right),$$

$$G_{3f} \triangleq \begin{bmatrix} 1 & -\theta_3 & \theta_3^2 \\ 1 & -\gamma\theta_3 & -(1+\gamma)\theta_3^2 \\ 1 & -\gamma^2\theta_3 & -(1+\gamma^2)\theta_3^2 \end{bmatrix} E_6, \quad \text{for } \theta_3 = \exp\left(j\frac{2\pi}{9}\right), \; \gamma = \frac{\sqrt{3}j-1}{2},$$

and

$$G_{4f} \triangleq \begin{bmatrix} 1 & \theta_4 & \theta_4^2 & \theta_4^3 \\ 1 & -\theta_4 & \theta_4^2 & -\theta_4^3 \\ 1 & j\theta_4 & -\theta_4^2 & -j\theta_4^3 \\ 1 & -j\theta_4 & -\theta_4^2 & j\theta_4^3 \end{bmatrix} E_8, \quad \text{for} \quad \theta_4 = \exp\left(j\frac{\pi}{8}\right).$$

The codes proposed in [2] are the complex lattices $\Gamma_2(G_{2f})$ over Λ_{ζ_4}, $\Gamma_3(G_{3f})$ over Λ_{ζ_3}, and $\Gamma_4(G_{4f})$ over Λ_{ζ_4}.

Example 3. *Rotated Codes Based on QAM on the Square Lattice* [3, 2]

For considering only fading channels, the diversity product can be focused. In this case, by deleting matrices D_4 and E_8 from the ones G_{2f} and G_{4f} in Example 2, respectively, complex lattices $\Gamma_2(G_2)$ and $\Gamma_4(G_4)$ over Λ_{ζ_4}, i.e., QAM on the square lattice, for $L_t = 2$ and 4 can be obtained with the following generating matrices:

$$G_2 \triangleq \begin{bmatrix} 1 & \theta_2 \\ 1 & -\theta_2 \end{bmatrix}, \quad \text{for} \quad \theta_2 = \exp\left(j\frac{\pi}{4}\right),$$

and

$$G_4 \triangleq \begin{bmatrix} 1 & \theta_4 & \theta_4^2 & \theta_4^3 \\ 1 & -\theta_4 & \theta_4^2 & -\theta_4^3 \\ 1 & j\theta_4 & -\theta_4^2 & -j\theta_4^3 \\ 1 & -j\theta_4 & -\theta_4^2 & j\theta_4^3 \end{bmatrix}, \quad \text{for} \quad \theta_4 = \exp\left(j\frac{\pi}{8}\right).$$

Since all entries of matrices D_4 and E_8 are in $\mathbb{Z}[j]$, it is clear that the complex lattice points of $\Gamma_2(G_{2f})$ and $\Gamma_4(G_{4f})$ in Example 2 are subsets of the complex lattices $\Gamma_2(G_2)$ and $\Gamma_4(G_4)$ in Example 3, respectively, i.e., $\Gamma_l(G_{lf}) \subset \Gamma_l(G_l)$ for $l = 2$ and 4.

2.2 Problems of Interest

We can see that, to form a space-time code as stated in the beginning of this section, we select a set of points in a complex lattice. From the definition of complex lattices, a complex lattice $\Gamma_n(G)$ over $\Lambda_2(K)$ is determined by a generating matrix G and a base 2 dimensional real lattice $\Lambda_2(K)$.

The question we are interested here is how can we generally choose the generating matrices G and K to achieve: (i) full diversity complex lattices and space-time codes; (ii) the optimal diversity products in the family, in a systematic way. In the later sections, we propose to form space-time codes from complex lattices with generating matrices G and K over general cyclotomic field extensions. To do so, let us study some properties on the relationship between n dimensional complex lattices and $2n$ dimensional real lattices. The reason for studying the relationship is because we need to estimate the mean power of complex lattice points $[\mathbf{y}_1, \cdots, \mathbf{y}_n]^T$ used as space-time codewords, which can be done if we convert it to an $2n$ dimensional real lattice and use some existing results on real lattices, such as the packing densities [45] as we shall see later.

2.3 Some Useful Properties of Real and Complex Lattices

Let us first see a relationship between an n dimensional complex lattice and a $2n$ dimensional real lattice. Let G be an $n \times n$ complex matrix,

$$G = \begin{bmatrix} g_{1,1} & g_{1,2} & \cdots & g_{1,n} \\ g_{2,1} & g_{2,2} & \cdots & g_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ g_{n,1} & g_{n,2} & \cdots & g_{n,n} \end{bmatrix}, \tag{6}$$

with $|\det(G)| > 0$, and $\{\mathbf{x}_1, \mathbf{x}_2, ..., \mathbf{x}_n\}$ be n points on a two dimensional real lattice $\Lambda_2(K)$ with generating matrix K. Let

$$\begin{bmatrix} \mathbf{y}_1 \\ \vdots \\ \mathbf{y}_n \end{bmatrix} = G \begin{bmatrix} \mathbf{x}_1 \\ \vdots \\ \mathbf{x}_n \end{bmatrix}. \tag{7}$$

Then, $[\mathbf{y_1}, ..., \mathbf{y_n}]^T$ is a point on the n dimensional complex lattice $\Gamma_n(G)$ over $\Lambda_2(K)$.

We now rewrite $\mathbf{y}_i$ with its real part y_{R_i} and imaginary part y_{I_i}, as $\mathbf{y}_i = y_{R_i} + jy_{I_i}$, and entries $g_{i,l}$ of G as $g_{i,l} = g_{R_{i,l}} + jg_{I_{i,l}}$. Then, (7) can be rewritten as

$$\begin{bmatrix} y_{R_1} \\ y_{I_1} \\ \vdots \\ y_{R_n} \\ y_{I_n} \end{bmatrix} = \mathcal{G} \begin{bmatrix} x_{R_1} \\ x_{I_1} \\ \vdots \\ x_{R_n} \\ x_{I_n} \end{bmatrix} = \mathcal{G} \begin{bmatrix} K & & & \\ & K & & \\ & & \ddots & \\ & & & K \end{bmatrix}_{2n \times 2n} \begin{bmatrix} z_{1,1} \\ z_{1,2} \\ \vdots \\ z_{n,1} \\ z_{n,2} \end{bmatrix}, \tag{8}$$

where $z_{i,1}, z_{i,2} \in \mathbb{Z}$ with

$$\begin{bmatrix} x_{i,1} \\ x_{i,2} \end{bmatrix} = K \begin{bmatrix} z_{i,1} \\ z_{i,2} \end{bmatrix}, \tag{9}$$

and $\mathcal{G}$ is a $2n \times 2n$ real matrix, which is from the real and imaginary parts of G as follows

$$\mathcal{G} \triangleq \begin{bmatrix} g_{R_{1,1}} & -g_{I_{1,1}} & \cdots & g_{R_{1,n}} & -g_{I_{1,n}} \\ g_{I_{1,1}} & g_{R_{1,1}} & \cdots & g_{I_{1,n}} & g_{R_{1,n}} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ g_{R_{n,1}} & -g_{I_{n,1}} & \cdots & a_{R_{n,n}} & -g_{I_{n,n}} \\ g_{I_{n,1}} & g_{R_{n,1}} & \cdots & a_{I_{n,n}} & g_{R_{n,n}} \end{bmatrix}. \tag{10}$$

Let $\mathcal{G}_K \triangleq \mathcal{G} \cdot \mathrm{diag}(K, \cdots, K)$. Following Definition 1, in order to show that $\mathcal{G}_K$ is a real generating matrix of an $2n$ dimensional real lattice, we only need to show it has full rank, i.e., $|\det(\mathcal{G}_K)| > 0$. Since K is the real generating matrix of 2 dimensional real lattice $\Lambda_2(K)$, $|\det(K)| > 0$. Thus, we only need to show that $|\det(\mathcal{G})| > 0$, which is given by the following proposition. Therefore, the n dimensional complex lattice $\Gamma_n(G)$ over $\Lambda_2(K)$ is represented as an $2n$ dimensional real lattice $\Lambda_{2n}(\mathcal{G}_K)$.

Proposition 1 *Let G be an $n \times n$ complex matrix defined in (6) and $\mathcal{G}$ be the $2n \times 2n$ real matrix defined in (10). Then, $|\det(\mathcal{G})| = |\det(G)|^2$.*

Proof. For $i = 1, ..., n$, by adding the product of the $2i$th row of $\mathcal{G}$ with $j = \sqrt{-1}$ to the $(2i-1)$th row of $\mathcal{G}$ in (10), matrix $\mathcal{G}$ becomes

$$\mathcal{G}_1 = \begin{bmatrix} g_{1,1} & jg_{1,1} & \cdots & g_{1,n} & jg_{1,n} \\ g_{I_{1,1}} & g_{R_{1,1}} & \cdots & g_{I_{1,n}} & g_{R_{1,n}} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ g_{n,1} & jg_{n,1} & \cdots & g_{n,n} & jg_{n,n} \\ g_{I_{n,1}} & g_{R_{n,1}} & \cdots & g_{I_{n,n}} & g_{R_{n,n}} \end{bmatrix}. \tag{11}$$

For $i = 1, ..., n$, by adding the product of the $(2i-1)$th column of $\mathcal{G}_1$ to the $2i$th column of $\mathcal{G}_1$ with $-j$, matrix $\mathcal{G}_1$ becomes

$$\mathcal{G}_2 = \begin{bmatrix} g_{1,1} & 0 & \cdots & g_{1,n} & 0 \\ g_{I_{1,1}} & g_{1,1}^* & \cdots & g_{I_{1,n}} & g_{1,n}^* \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ g_{n,1} & 0 & \cdots & g_{n,n} & 0 \\ g_{I_{n,1}} & g_{n,1}^* & \cdots & g_{I_{n,n}} & g_{n,n}^* \end{bmatrix}, \tag{12}$$

where $g_{i,l}^*$ are the complex conjugates of $g_{i,l}$. Next, by permuting the rows and the columns of $\mathcal{G}_2$, matrix $\mathcal{G}_2$ can be converted to

$$\mathcal{G}_3 = \begin{bmatrix} g_{1,1} & g_{1,2} & \cdots & 0 & 0 \\ g_{2,1} & g_{2,2} & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ g_{I_{n-1,1}} & g_{I_{n-1,2}} & \cdots & g_{n-1,n-1}^* & g_{n-1,n}^* \\ g_{I_{n,1}} & g_{I_{n,2}} & \cdots & g_{n,n-1}^* & g_{n,n}^* \end{bmatrix} = \begin{bmatrix} G & 0 \\ \mathrm{Im}(G) & G^* \end{bmatrix}, \tag{13}$$

where $\mathrm{Im}(G)$ is the imaginary part of matrix G and G^* is the complex conjugate of matrix G. Notice that, the elementary operations we implemented on $\mathcal{G}$ to get $\mathcal{G}_3$ have all determinants 1 and therefore, $|\det(\mathcal{G})| = |\det(\mathcal{G}_3)|$. Since $\det(\mathcal{G}_3) = |\det(G)|^2$, we have concluded the proof. **q.e.d.**

Proposition 1 tells us that an n dimensional complex lattice $\Gamma_n(G)$ over $\Lambda_2(K)$ can be equivalently represented as a $2n$ dimensional real lattice $\Lambda_{2n}(\mathcal{G}_K)$. Furthermore, the determinants of their generating matrices have the following relationship:

$$|\det(\mathcal{G}_K)| = |\det(G)|^2 \cdot |\det(K)|^n = |\det(G)|^2 \cdot |\det(\Lambda_2(K))|^n, \tag{14}$$

which is used later to determine the compactness of a complex lattice for a fixed minimum product (or diversity product).

3 Systematic Full Diversity Cyclotomic Lattices

For two positive integers n and m, let $N = mn$ and

$$L_t = \frac{\phi(N)}{\phi(m)}, \tag{15}$$

where $\phi(N)$ and $\phi(m)$ are the Euler totient functions[1] of N and m, respectively, there are total L_t distinct integers n_i, $1 \le i \le L_t$, with $0 = n_1 < n_2 < \cdots < n_{L_t} \le n-1$ such that $1 + n_i m$ and N are co-prime for any $1 \le i \le L_t$ (see for example pg. 75 of [43]). With these L_t integers, we define

$$G_{m,n} \triangleq \begin{bmatrix} \zeta_N & \zeta_N^2 & \cdots & \zeta_N^{L_t} \\ \zeta_N^{1+n_2 m} & \zeta_N^{2(1+n_2 m)} & \cdots & \zeta_N^{L_t(1+n_2 m)} \\ \vdots & \vdots & \ddots & \vdots \\ \zeta_N^{1+n_{L_t} m} & \zeta_N^{2(1+n_{L_t} m)} & \cdots & \zeta_N^{L_t(1+n_{L_t} m)} \end{bmatrix}_{L_t \times L_t}, \tag{16}$$

where $\zeta_N = \exp(j\frac{2\pi}{N})$. It is not hard to see that matrix $G_{m,n}$ has full rank since it is a Vandermonde matrix and $\zeta_N^{1+n_i m} - \zeta_N^{1+n_l m} \neq 0$ for $1 \le i \neq l \le L_t$. This means that matrix $G_{m,n}$ is eligible to be a generating matrix of a complex lattice as we defined in Section 2.1. We now define cyclotomic lattices.

Definition 3 *An L_t dimensional complex lattice $\Gamma_{L_t}(G_{m,n})$ over Λ_{ζ_m} is called a cyclotomic lattice, where $G_{m,n}$ is defined in (16) and Λ_{ζ_m} is the two dimensional real lattice with the generating matrix K_{ζ_m} defined in (3). Its minimum product[2] $d_{\min}(\Gamma_{L_t}(G_{m,n}))$ is defined by*

$$d_{min}(\Gamma_{L_t}(G_{m,n})) \triangleq \min_{[0,\cdots,\cdots,0]^T \neq [\mathbf{y}_1,\cdots,\mathbf{y}_{L_t}]^T \in \Gamma_{L_t}(G_{m,n})} \left| \prod_{i=1}^{L_t} \mathbf{y}_i \right|. \tag{17}$$

From this definition, a lattice point (or vector) $[\mathbf{y}_1, \cdots, \mathbf{y}_{L_t}]^T$ on a cyclotomic lattice can be generated by

$$[\mathbf{y}_1, \cdots, \mathbf{y}_{L_t}]^T = G_{m,n}[\mathbf{x}_1, \cdots, \mathbf{x}_{L_t}]^T \tag{18}$$

where $\mathbf{x}_i \in \Lambda_{\zeta_m} \subset \mathbb{Z}[\zeta_m]$. The generating matrix in (16) can be also written as

$$G_{m,n} = \mathrm{diag}(\zeta_N, \zeta_N^{1+n_2 m}, \cdots, \zeta_N^{1+n_{L_t} m})\hat{G}_{m,n}, \tag{19}$$

where

$$\hat{G}_{m,n} \triangleq \begin{bmatrix} 1 & \zeta_N & \cdots & \zeta_N^{L_t-1} \\ 1 & \zeta_N^{1+n_2 m} & \cdots & \zeta_N^{(L_t-1)(1+n_2 m)} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta_N^{1+n_{L_t} m} & \cdots & \zeta_N^{(L_t-1)(1+n_{L_t} m)} \end{bmatrix}_{L_t \times L_t}. \tag{20}$$

[1] The Euler totient function (or Euler function) $\phi(N)$ of N is the number of positive numbers that are less than N and co-prime with N. In fact, it can be expressed as $\phi(N) = \phi(p_1^{a_1})\phi(p_2^{a_2})\cdots\phi(p_r^{a_r})$ if $N = p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}$ for some distinct primes p_i. In particular, if p is a prime, $\phi(p^a) = p^a - p^{a-1}$, see for example [44]. It also implies that L_t is always an integer.

[2] In [5], it is called minimum product diversity. The reason why we use minimum product is because we want to distinguish it from the diversity product of the associated space-time code with this lattice as we shall see later. In [3], it is called product distance.

Thus, the complex lattice points $\mathbf{y}_i$ and $\hat{\mathbf{y}}_i$ of $\Gamma_{L_t}(G_{m,n})$ and $\Gamma_{L_t}(\hat{G}_{m,n})$, respectively, are related by

$$[\mathbf{y}_1, \mathbf{y}_2, \cdots, \mathbf{y}_{L_t}]^T = [\zeta_N \hat{\mathbf{y}}_1, \zeta_N^{1+n_1 m} \hat{\mathbf{y}}_2, \cdots, \zeta_N^{1+n_{L_t} m} \hat{\mathbf{y}}_{L_t}]^T. \tag{21}$$

Due to the fact that all elements ζ_N^i in (21) have unit norm, the complex lattice $\Gamma_{L_t}(G_{m,n})$ and the complex lattice $\Gamma_{L_t}(\hat{G}_{m,n})$ have the same minimum product, i.e., $d_{\min}(\Gamma_{L_t}(G_{m,n})) = d_{\min}(\hat{\Gamma}_{L_t}(G_{m,n}))$. Since the relationship (21) of the lattice points of the two complex lattices does not depend on the real lattice Λ_{ζ_m}, these two complex lattices are *equivalent* in terms of the properties, such as diversity product and mean signal energy, that we are interested in a space-time code as we shall study later. Therefore, for the notational convenience, we use $G_{m,n}$ throughout this correspondence otherwise it is specified.

Note that the entries of the generating matrix $G_{m,n}$ in (16) are all integrals over $\mathbb{Z}[\zeta_m]$, i.e., roots of monic polynomials[3] with coefficients in $\mathbb{Z}[\zeta_m]$.

Another representation for $G_{m,n}$ in (16) is

$$G_{m,n} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \zeta_n^{n_2} & \zeta_n^{2n_2} & \cdots & \zeta_n^{L_t n_2} \\ \vdots & \vdots & \ddots & \vdots \\ \zeta_n^{n_{L_t}} & \zeta_n^{2n_{L_t}} & \cdots & \zeta_n^{L_t n_{L_t}} \end{bmatrix}_{L_t \times L_t} \cdot \operatorname{diag}(\zeta_N, \zeta_N^2, \cdots, \zeta_N^{L_t}). \tag{22}$$

From the above representation and since $0 \le n_i < n$, one can clearly see that the generating matrix $G_{m,n}$ in (16) is unitary, i.e., the n-point DFT matrix, if and only if $L_t = n$.

We next define diagonal cyclotomic space-time codes.

Definition 4 *A diagonal cyclotomic space-time code Ω for L_t transmit antennas is defined by $\Omega = \{diag(\mathbf{y}_1, \cdots, \mathbf{y}_{L_t})\}$ where $\mathbf{y}_i$ for $1 \le i \le L_t$ are defined as follows:*

$$[\mathbf{y}_1, \cdots, \mathbf{y}_{L_t}]^T = G_{m,n}[\mathbf{x}_1, \cdots, \mathbf{x}_{L_t}]^T \tag{23}$$

where $G_{m,n}$ is defined in (16), $[\mathbf{x}_1, \cdots, \mathbf{x}_{L_t}]^T \in \mathcal{S} \subset (\mathbb{Z}[\zeta_m])^{L_t}$, and $\mathcal{S}$ is a signal constellation for information symbols.

To fully understand the structure of cyclotomic lattice (16), we need some results on algebraic number theory, see for example [40]-[44], which also provides the motivation for us to define the above cyclotomic lattices and codes. From the algebraic number theory, it is known that field $\mathbb{Q}(\zeta_N)$ is an extension of field $\mathbb{Q}(\zeta_m)$ and field $\mathbb{Q}(\zeta_m)$ is also an extension of field $\mathbb{Q}$ of all rational numbers: $\mathbb{Q} \subset \mathbb{Q}(\zeta_m) \subset \mathbb{Q}(\zeta_N)$. An *automorphism* σ of field $\mathbb{Q}(\zeta_N)$ that fixes subfield $\mathbb{Q}(\zeta_m)$ is a one-to-one and onto mapping from $\mathbb{Q}(\zeta_N)$ to itself such that $\sigma(a+b) = \sigma(a) + \sigma(b)$ and $\sigma(ab) = \sigma(a)\sigma(b)$ for any $a, b \in \mathbb{Q}(\zeta_N)$ and $\sigma(a) = a$ for any $a \in \mathbb{Q}(\zeta_m)$.

[3] Monic means the coefficient of the highest order term in a polynomial is 1.

Theorem 1 *All the L_t automorphisms of field $\mathbb{Q}(\zeta_N)$, σ_i, $1 \le i \le L_t$, that fix subfield $\mathbb{Q}(\zeta_m)$ can be represented by*

$$\sigma_i(\zeta_N) = \zeta_N^{1+n_i m}, \quad \textit{for} \quad 1 \le i \le L_t, \tag{24}$$

where L_t is given in (15), and n_i, $1 \le i \le L_t$, are the integers that satisfy $0 = n_1 < n_2 < \cdots < n_{L_t} \le n-1$ and $1 + n_i m$ and N are co-prime for $1 \le i \le L_t$.

A proof of this theorem is in Appendix A. One can see that the integers appeared in the representations of the automorphisms in Theorem 1 are precisely the ones used in the construction of the above cyclotomic lattices. From the representations of the automorphisms σ_i in (24), the element at the ith row and the lth column in the generating matrix $G_{m,n}$ in (16) of the cyclotomic lattices can be represented as $\sigma_i(\zeta_N^l)$. Thus, the generating matrix $G_{m,n}$ in (16) can be rewritten as

$$G_{m,n} = \begin{bmatrix} \sigma_1(\zeta_N) & \sigma_1(\zeta_N^2) & \cdots & \sigma_1(\zeta_N^{L_t}) \\ \sigma_2(\zeta_N) & \sigma_2(\zeta_N^2) & \cdots & \sigma_2(\zeta_N^{L_t}) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_{L_t}(\zeta_N) & \sigma_{L_t}(\zeta_N^2) & \cdots & \sigma_{L_t}(\zeta_N^{L_t}) \end{bmatrix}, \tag{25}$$

where σ_i, $1 \le i \le L_t$, are all of the distinct automorphisms of $\mathbb{Q}(\zeta_N)$ that fix $\mathbb{Q}(\zeta_m)$.

As we can see from Appendix that, in fact, these automorphisms $\{\sigma_i : \ 1 \le i \le L_t\}$ form the quotient group (called Galois group) $\mathbb{Q}(\zeta_N)/\mathbb{Q}(\zeta_m)$ and L_t is the dimension of $\mathbb{Q}(\zeta_N)$ viewed as a vector space over its subfield $\mathbb{Q}(\zeta_m)$. L_t is also called the extension degree of $\mathbb{Q}(\zeta_N)$ over $\mathbb{Q}(\zeta_m)$ that is denoted by $[\mathbb{Q}(\zeta_N) : \mathbb{Q}(\zeta_m)]$, i.e., $[\mathbb{Q}(\zeta_N) : \mathbb{Q}(\zeta_m)] = L_t$. Because $\mathbb{Q}(\zeta_N)$ can be generated by ζ_N over $\mathbb{Q}(\zeta_m)$ and the order of the minimum polynomial of ζ_N over $\mathbb{Q}(\zeta_m)$ is L_t (see pg. 22 in [44]), we have

$$\sum_{i=1}^{L_t} \mathbf{x}_i \zeta_N^i = \zeta_N \sum_{i=0}^{L_t-1} \mathbf{x}_{i+1} \zeta_N^i \ne 0 \ \text{ if } \ [0, \cdots, 0]^T \ne [\mathbf{x}_1, \cdots, \mathbf{x}_{L_t}]^T \in (\mathbb{Q}(\zeta_m))^{L_t}, \tag{26}$$

which is also used in the proof of the following theorem. Property (26) can also be seen by viewing $\mathbb{Q}(\zeta_N)$ as a vector space over $\mathbb{Q}(\zeta_m)$ with ζ_N^i, $1 \le i \le L_t$, as basis elements. This part has the analogy with the finite field theory over the binary field used in the error correction coding theory, for example, the Galois field $\mathbb{G}(2^m)$ over the binary Galois field $\mathbb{G}(2)$. The above arguments imply why the matrix dimension L_t and the elements of the generating matrix $G_{m,n}$ are used in (16), which will become even clearer after the proof of the following full diversity property of a cyclotomic space-time code.

As we can see from the definition of the generating matrix $G_{m,n}$ in (16), it is unique when m and n are fixed. However, if only L_t is fixed, there are infinitely many possible integers m and m and n can both vary.

Theorem 2 *A cyclotomic lattice $\Gamma_{L_t}(G_{m,n})$ over Λ_{ζ_m} has full diversity and a diagonal cyclotomic space-time code has full diversity.*

Proof: We only need to prove that a diagonal cyclotomic space-time code has full diversity. Let $C_1 = \text{diag}(\mathbf{y}_1, \cdots, \mathbf{y}_{L_t}) \neq C_2 = \text{diag}(\mathbf{e}_1, \cdots, \mathbf{e}_{L_t}) \in \Omega$ be two different codewords. Thus, we need to show $\prod_{i=1}^{L_t} |\mathbf{y}_i - \mathbf{e}_i| > 0$. Let $[\mathbf{x}_1, \cdots, \mathbf{x}_{L_t}]^T, [\mathbf{u}_1, \cdots, \mathbf{u}_{L_t}]^T \in (\mathbb{Z}[\zeta_m])^{L_t}$ such that

$$[\mathbf{y}_1, \cdots, \mathbf{y}_{L_t}]^T = G_{m,n}[\mathbf{x}_1, \cdots, \mathbf{x}_{L_t}]^T \text{ and } [\mathbf{e}_1, \cdots, \mathbf{e}_{L_t}]^T = G_{m,n}[\mathbf{u}_1, \cdots, \mathbf{u}_{L_t}]^T.$$

Since $G_{m,n}$ has full rank, $[\mathbf{x}_1, \cdots, \mathbf{x}_{L_t}]^T \neq [\mathbf{u}_1, \cdots, \mathbf{u}_{L_t}]^T$. Let $[\mathbf{v}_1, \cdots, \mathbf{v}_{L_t}] = [\mathbf{x}_1, \cdots, \mathbf{x}_{L_t}]^T - [\mathbf{u}_1, \cdots, \mathbf{u}_{L_t}]^T$ and $[\mathbf{w}_1, \cdots, \mathbf{w}_{L_t}] = G_{m,n}[\mathbf{v}_1, \cdots, \mathbf{v}_{L_t}]$. Then, $\mathbf{w}_i = \mathbf{y}_i - \mathbf{e}_i$ and $[\mathbf{v}_1, \cdots, \mathbf{v}_{L_t}]^T \neq [0, \cdots, 0]^T$. So, we need to show $\prod_{i=1}^{L_t} |\mathbf{w}_i| > 0$.

From the generation of a cyclotomic space-time codeword in (23) and the properties and representations of the automorphisms σ_i in Theorem 1, we have $\mathbf{w}_i = \sigma_i(\zeta)$, $1 \leq i \leq L_t$, where

$$\zeta = \sum_{l=1}^{L_t} \mathbf{v}_l \zeta_N^l \neq 0,$$

since $[\mathbf{v}_1, \cdots, \mathbf{v}_{L_t}]^T \neq [0, \cdots, 0]^T$ and (26). Thus, $\prod_{i=1}^{L_t} |\mathbf{w}_i| = \prod_{i=1}^{L_t} |\sigma_i(\zeta)|$. Since all σ_i are automorphisms, $\sigma_i(\zeta) \neq 0$ when $\zeta \neq 0$, we have proved the result. **q.e.d.**

When $m = 4$, a cyclotomic lattice $\Gamma_{L_t}(G_{4,n})$ over Λ_{ζ_4} is called a *Gaussian cyclotomic lattice*, after the name of *Gaussian integers* $\mathbb{Z}[j] = \mathbb{Z}[\zeta_4]$. When $m = 3$ or $m = 6$, a cyclotomic lattice $\Gamma_{L_t}(G_{m,n})$ over Λ_{ζ_m} is called an *Eisenstein cyclotomic lattice*, after the name of *Eisenstein integers* $\mathbb{Z}[\zeta_3] = \mathbb{Z}[\zeta_6]$. For Gaussian cyclotomic lattices and Eisenstein cyclotomic lattices, it is stated in [2] that the minimum products (related to algebraic norms) are 1 and it was proved in [41, 40]. Since this result plays an important role in the optimal cyclotomic lattice/code designs as we shall see in Subsections 4.1 and 4.2, for the completeness, we list it as a proposition.

Proposition 2 *The minimum products of Gaussian cyclotomic lattices and Eisenstein cyclotomic lattices are* 1.

This result is used in the proof of Theorem 3 in Subsection 4.1. Although in a cyclotomic space-time code the information signal constellation $\mathcal{S}$ can be any subset of the product space $(\mathbb{Z}[\zeta_m])^{L_t}$ of the cyclotomic ring $\mathbb{Z}[\zeta_m]$, $\mathcal{S}$ is chosen from the product space $(\Lambda_{\zeta_m})^{L_t}$ of the lattice $\Lambda_{\zeta_m} \subset \mathbb{Z}[\zeta_m]$ as we discuss the optimality of the diagonal cyclotomic space-time codes in the next sections. When $\mathcal{S}$ is chosen from $(\Lambda_{\zeta_m})^{L_t}$, all the codeword vectors $[\mathbf{y}_1, \cdots, \mathbf{y}_{L_t}]^T$ are on the cyclotomic lattice $\Gamma_{L_t}(G_{m,n})$ over Λ_{ζ_m} as defined in Definition 3. Notice that $\Lambda_{\zeta_m} = \mathbb{Z}[\zeta_m]$ for $m = 3, 4, 6$ as indicated in (4).

From Definition 4 of a cyclotomic space-time code, one can see that, for a fixed L_t in (15), there are infinitely many options of integer m and thus infinitely many options of cyclotomic number ring $\mathbb{Z}[\zeta_m]$ or lattice Λ_{ζ_m} and also infinitely many options of the generating matrix $G_{m,n}$ in (16). Then, a natural question arises: *which one is optimal*Γ The optimality here is in the sense that, for a fixed signal mean power of $\mathbf{y}_i$, the diversity product of a cyclotomic space-time code is maximized among all different integers m, or equivalently, for a fixed diversity product, the signal mean power of $\mathbf{y}_i$ is minimized among all different integers m. To investigate the above optimality, in Subsection 4.1 we study the optimality of the minimum products of cyclotomic lattices by considering how this optimality relates to the complex lattice generating matrices $G_{m,n}$ and the real lattice generating matrices K_{ζ_m} in (3). Based on the theory developed in Subsection 4.1, we present optimal cyclotomic lattices in Subsection 4.2.

From the above definitions, it is not hard to see that the two generating matrices in Example 3 in Section 2.1.2 are two special cases of $L_t = 2$ and 4 with $m = 4$ here:

$$G_2 = \hat{G}_{4,2} \quad \text{and} \quad G_4 = \hat{G}_{4,4},$$

and the cyclotomic lattices or codes $\Gamma_2(G_2)$ and $\Gamma_4(G_4)$ over $\mathbb{Z}[\zeta_4] = \Lambda_{\zeta_4}$ are $\Gamma_2(\hat{G}_{4,2})$ (equivalent to $\Gamma_2(G_{4,2})$) and $\Gamma_4(\hat{G}_{4,4})$ (equivalent to $\Gamma_4(G_{4,4})$) over $\mathbb{Z}[\zeta_4] = \Lambda_{\zeta_4}$, respectively, which are not the optimal ones for 2 and 4 transmit antennas as we shall see in Section 5. In fact, in Section 5, we find that the cyclotomic lattices or codes $\Gamma_2(G_{6,2})$ and $\Gamma_4(G_{6,5})$ over $\mathbb{Z}[\zeta_6] = \Lambda_{\zeta_6}$ for 2 and 4 transmit antennas are optimal and strictly better than $\Gamma_2(G_2)$ and $\Gamma_4(G_4)$, respectively. Although the entries of $G_{6,2}$ and $G_{6,5}$ are integrals over $\mathbb{Z}[\zeta_6]$, they are not integrals over $\mathbb{Z}[j] = \mathbb{Z}[\zeta_4]$ while the entries of G_2 and G_4 are integrals over $\mathbb{Z}[j] = \mathbb{Z}[\zeta_4]$. In fact, as we shall see in Section 5 that the complex lattices $\Gamma_{L_t}(G_{4,n})$ over Λ_{ζ_4} are not optimal in most cases.

Since the codes proposed in Examples 1 and 2 are not only for fading channels but also for Gaussian channels, their product diversities are not as good as others. Some detailed calculations are shown later.

4 Optimal Cyclotomic Lattices

In this section, we study the optimality of cyclotomic lattices proposed in the preceding section. We first investugate the optimality criterion.

4.1 Criterion for Cyclotomic Lattice Designs

As described in Section 3, for a fixed L_t there are infinitely many cyclotomic lattices $\Gamma_{L_t}(G_{m,n})$ over Λ_{ζ_m} of full diversity for various m and n. In order to study which of them is better, we want to compare their mean signal powers when their diversity products or minimum products are the same. Before studying cyclotomic space-time codes, we study cyclotomic lattices by connecting their corresponding real lattice packing density and their signal mean power with their generating matrices.

4.1.1 Packing Density, Mean Signal Power, and Generating Matrix

For the compactness of a real lattice, the *packing density* concept has been introduced in for example [45] and for more details, we refer the reader to [45]. Let Λ_n be an n-dimensional real lattice. Its *sphere packing density* is defined by

$$\Delta = \frac{V_n \rho^n}{\det(\Lambda_n)^{1/2}},$$

where V_n is the volume of the n-dimensional ball with radius 1 and ρ is the half minimal distance between the lattice points called the *packing radius*. Its *center density* δ is defined by

$$\delta = \frac{\Delta}{V_n} = \rho^n (\det(\Lambda_n))^{-1/2},$$

see pg. 10 and pg. 13 of [45]. It is mentioned on pg. 13 in [45] that the center density δ of a real lattice Λ_n is the number of points of the lattice Λ_n in every ρ^n number of unit volumes, i.e., in average every ρ^n number of unit volumes (V_n) of $\mathbb{R}^n$ include $\rho^n(\det(\Lambda_n))^{-1/2}$ lattice points on lattice Λ_n. Therefore, in average there are $\det(\Lambda_n)^{-1/2}$ lattice points of lattice Λ_n in every unit volume of $\mathbb{R}^n$. This implies that, the less of the value $\det(\Lambda_n)$ is, the more points of Λ_n are included in the unit ball of $\mathbb{R}^n$. In other words, if we want to select a set $\mathcal{S} \subset \Lambda_n$ of lattice points of a fixed size, i.e., $|\mathcal{S}|$ is fixed, such that the mean signal power of the signal points in $\mathcal{S}$ is minimized, then, the less of the value $\det(\Lambda_n)$ is or equivalently the less of the absolute value of the determinant of its generating matrix is, the smaller the mean signal power of the signal points in $\mathcal{S}$ is. This is the base for the following criterion of justifying that one cyclotomic lattice is better than the other cyclotomic lattice when their minimum products are the same.

4.1.2 Cyclotomic Lattice Design Criterion

In this subsection, we first present the design criterion for a cyclotomic lattice and then present some properties on the criterion. From the discussions in Section 2.3, any n dimensional complex lattice can be converted to a $2n$ dimensional real lattice and their corresponding signal powers are exactly the same. For a cyclotomic lattice $\Gamma_{L_t}(G_{m,n})$ over Λ_{ζ_m}, the determinant of its corresponding $2L_t$ dimensional real lattice generating matrix $\mathcal{G}_K$ is

$$|\det(G_{m,n})|^2 \cdot |\det(K_{\zeta_m})|^{L_t}. \tag{27}$$

With the argument of Subsection 4.1.1 and (27) we are ready to present a criterion to choose a cyclotomic lattice.

Definition 5 *Let $\Gamma_{L_t}(G_{m_1,n_1})$ and $\Gamma_{L_t}(G_{m_2,n_2})$ be two L_t dimensional cyclotomic lattices over $\Lambda_{\zeta_{m_1}}$ and $\Lambda_{\zeta_{m_2}}$, respectively. We say cyclotomic lattice $\Gamma_{L_t}(G_{m_1,n_1})$ is* better than *cyclotomic lattice $\Gamma_{L_t}(G_{m_2,n_2})$, written as $\Gamma_{L_t}(G_{m_1,n_1}) \leq \Gamma_{L_t}(G_{m_2,n_2})$, if*

$$|\det(G_{m_1,n_1})| \cdot |\det(\Lambda_{\zeta_{m_1}})|^{L_t/2} \leq |\det(G_{m_2,n_2})| \cdot |\det(\Lambda_{\zeta_{m_2}})|^{L_t/2},$$

when their minimum products are the same, i.e., $d_{\min}(\Gamma_{L_t}(G_{m_1,n_1})) = d_{\min}(\Gamma_{L_t}(G_{m_2,n_2}))$.

One can clearly see that the above definition not only applies to cyclotomic lattices but also applies to general complex lattices defined in Section 2. With the above definition, we immediately have the following lemma by normalizing cyclotomic lattices.

Lemma 1 *Let $\Gamma_{L_t}(G_{m_1,n_1})$ and $\Gamma_{L_t}(G_{m_2,n_2})$ be two L_t dimensional cyclotomic lattices over $\Lambda_{\zeta_{m_1}}$ and $\Lambda_{\zeta_{m_2}}$ with minimum products $d_{\min}(\Gamma_{L_t}(G_{m_1,n_1}))$ and $d_{\min}(\Gamma_{L_t}(G_{m_2,n_2}))$, respectively. Then, $\Gamma_{L_t}(G_{m_1,n_1})$ is better than $\Gamma_{L_t}(G_{m_2,n_2})$ if*

$$\frac{d_{\min}(\Gamma_{L_t}(G_{m_1,n_1}))}{|\det(\Lambda_{m_1})|^{L_t/2}|\det(G_{m_1,n_1})|} \geq \frac{d_{\min}(\Gamma_{L_t}(G_{m_2,n_2}))}{|\det(\Lambda_{m_2})|^{L_t/2}|\det(G_{m_2,n_2})|}.$$

Proof: The main idea to prove this lemma is to first normalize these two cyclotomic lattices such that their minimum products are the same and then compare the compactness (or average power) of the two normalized lattices.

The two $2L_t$ dimensional real lattice generating matrices can be written as

$$\mathcal{G}_{K_{\zeta_{m_i}}} = \mathcal{G}_i diag\left(K_{\zeta_{m_i}}, \cdots, K_{\zeta_{m_i}}\right),$$

where $2L_t$ dimensional real matrix $\mathcal{G}_i$ corresponds to the L_t dimensional complex matrix G_{m_i,n_i} for $i=1$ and 2. Their determinants satisfy

$$\left|\det\left(\mathcal{G}_{K_{\zeta_{m_i}}}\right)\right| = |\det(G_{m_i,n_i})|^2 |\det(\Lambda_{m_i})|^{L_t}, \quad \text{for } i=1,2.$$

We now normalize the complex lattices $\Gamma_{L_t}(G_{m_i,n_i})$ by normalizing their generating matrices G_{m_i,n_i} as follows:

$$\bar{G}_{m_i,n_i} = (d_{\min}(\Gamma_{L_t}(G_{m_i,n_i})))^{-1/L_t} G_{m_i,n_i}, \quad \text{for } i=1,2.$$

Then, the minimum products of the normalized cyclotomic lattices $\Gamma_{L_t}(\bar{G}_{m_i,n_i})$ are both 1. On the other hand, for $i=1$ and 2, the new determinants satisfy

$$\left|\det\left(\bar{\mathcal{G}}_{K_{\zeta_{m_i}}}\right)\right| = \left|\det\left(\bar{G}_{m_i,n_i}\right)\right|^2 \left|\det\left(\Lambda_{\zeta_{m_i}}\right)\right|^{L_t} = \frac{1}{d_{\min}(\Gamma_{L_t}(G_{m_i,n_i}))^2} |\det(G_{m_i,n_i})|^2 \left|\det\left(\Lambda_{\zeta_{m_i}}\right)\right|^{L_t}.$$

Thus, if

$$\frac{d_{\min}(\Gamma_{L_t}(G_{m_1,n_1}))}{\left|\det\left(\Lambda_{\zeta_{m_1}}\right)\right|^{L_t/2} |\det(G_{m_1,n_1})|} \geq \frac{d_{\min}(\Gamma_{L_t}(G_{m_2,n_2}))}{\left|\det\left(\Lambda_{\zeta_{m_2}}\right)\right|^{L_t/2} |\det(G_{m_2,n_2})|},$$

then we have

$$\left|\det\left(\bar{\mathcal{G}}_{K_{\zeta_{m_1}}}\right)\right| \leq \left|\det\left(\bar{\mathcal{G}}_{K_{\zeta_{m_2}}}\right)\right|. \tag{28}$$

This proves that the normalized cyclotomic lattice $\Gamma_{L_t}(\bar{G}_{m_1,n_1})$ is better than $\Gamma_{L_t}(\bar{G}_{m_2,n_2})$ in terms of the compactness. Since the normalized lattice $\Gamma_{L_t}(\bar{G}_{m_i,n_i})$ and its original lattice $\Gamma_{L_t}(G_{m_i,n_i})$ only differ by a scalar, their performances are the same. Thus, $\Gamma_{L_t}(G_{m_1,n_1})$ is better than $\Gamma_{L_t}(G_{m_2,n_2})$. Therefore, Lemma 1 is proved. **q.e.d.**

We next present an important property between Eisenstein lattices and other lattices, which is used in Subsection 4.2 for finding optimal cyclotomic lattices.

Theorem 3 *Let $m_1 = 3$ or 6. Let $\Gamma_{L_t}(G_{m_1,n_1})$ be an $L_t \geq 2$ dimensional Eisenstein cyclotomic lattice and $\Gamma_{L_t}(G_{m_2,n_2})$ be another L_t dimensional cyclotomic lattice over $\Lambda_{\zeta_{m_2}}$. If $|\det(G_{m_1,n_1})| \leq |\det(G_{m_2,n_2})|$, then lattice $\Gamma_{L_t}(G_{m_1,n_1})$ is better than lattice $\Gamma_{L_t}(G_{m_2,n_2})$.*

Proof: Since $\Lambda_{\zeta_3} = \Lambda_{\zeta_6}$, we only need to prove the case of $m_1 = 6$.

When $m_2 = 1$ or $m_2 = 2$, matrix G_{m_2,n_2} can not be used to generate an L_t dimensional complex lattice. Therefore, we only need to consider $m_2 \geq 3$.

For $m_2 = 3$ or $m_2 = 6$, $\left|\det\left(\Lambda_{\zeta_{m_2}}\right)\right| = |\det(\Lambda_{\zeta_3})|$, and Λ_{ζ_3} and Λ_{ζ_6} are the Eisenstein lattice. By using Lemma 1, this theorem is proved.

For $m_2 = 4$, both minimum products of the Gaussian cyclotomic lattice and the Eisenstein lattice are $d_{min}(\Gamma_{L_t}(G_{6,n_1})) = d_{min}(\Gamma_{L_t}(G_{4,n_2})) = 1$, and $|\det(\Lambda_{\zeta_6})| < |\det(\Lambda_{\zeta_4})|$. From Lemma 1, cyclotomic lattice $\Gamma_{L_t}(G_{6,n_1})$ is better than cyclotomic lattice $\Gamma_{L_t}(G_{4,n_2})$ when $|\det(G_{6,n_1})| \leq |\det(G_{4,n_2})|$. This proves the theorem.

For $m_2 = 5$, because $1 \in \Lambda_{\zeta_{m_2}}$, we let $[\mathbf{y}_1, \cdots, \mathbf{y}_{L_t}]^T = G_{m_2,n_2}[1, 0, \cdots, 0]^T$, it is easy to check that

$$\left|\prod_{i=1}^{L_t} \mathbf{y}_i\right| = 1.$$

Thus, the minimum product $d_{min}(\Gamma_{L_t}(G_{5,n_2})) \leq 1$. On the other hand,

$$|\det(\Lambda_{\zeta_5})| = \sin\left(\frac{2\pi}{5}\right) > \sin\left(\frac{2\pi}{6}\right) = |\det(\Lambda_{\zeta_6})|.$$

From Lemma 1, this theorem is proved.

We now consider the case when $m_2 > 6$. It is clear that $1 - \zeta_{m_2} \in \Lambda_{\zeta_{m_2}}$. Let

$$[\mathbf{y}_1, \cdots, \mathbf{y}_{L_t}]^T = G_{m_2,n_2}[1 - \zeta_{m_2}, 0, \cdots, 0]^T.$$

Then, the minimum product has to satisfy

$$d_{min}(\Gamma_{L_t}(G_{m_2,n_2})) \leq |\mathbf{y}_1 \cdots \mathbf{y}_{L_t}| = \left|\zeta_N \zeta_N^2 \cdots \zeta_N^{L_t}\right| |1 - \zeta_{m_2}|^{L_t} = |1 - \zeta_{m_2}|^{L_t} = 2^{L_t} \sin^{L_t}(\frac{\pi}{m_2}).$$

Since $\left|\det\left(\Lambda_{\zeta_{m_2}}\right)\right| = \sin(2\pi/m_2)$, the ratio of $d_{min}(\Gamma_{L_t}(G_{m_2,n_2}))$ and $\left|\det\left(\Lambda_{\zeta_{m_2}}\right)\right|^{L_t/2}$ can be represented as

$$\frac{d_{min}(\Gamma_{L_t}(G_{m_2,n_2}))}{\left|\det\left(\Lambda_{\zeta_{m_2}}\right)\right|^{L_t/2}} \leq \frac{2^{L_t/2} \sin^{L_t}(\pi/m_2)}{\sin^{L_t/2}(\pi/m_2) \cos^{L_t/2}(\pi/m_2)} = (2\tan(\pi/m_2))^{L_t/2} < 1 \quad \text{when } m_2 \geq 7. \tag{29}$$

$$\frac{d_{min}(\Gamma_{L_t}(G_{6,n_1}))}{|\det(\Lambda_{\zeta_6})|^{L_t/2}} = \frac{1}{\left(\frac{\sqrt{3}}{2}\right)^{L_t/2}} > 1 > \frac{d_{min}(\Gamma_{L_t}(G_{m_2,n_2}))}{\left|\det\left(\Lambda_{\zeta_{m_2}}\right)\right|^{L_t/2}} \quad \text{when } m_2 \geq 7.$$

This proves the theorem by using Lemma 1. **q.e.d.**

From Theorem 3, one can see that, to compare a cyclotomic lattice over Λ_{ζ_m} with $\Gamma_{L_t}(G_{6,n})$ over Λ_{ζ_6}, or with $\Gamma_{L_t}(G_{3,n})$ over Λ_{ζ_3}, it is sufficient to compare the absolute values of their generating matrix determinants and the two dimensional real lattices Λ_{ζ_m} can be ignored.

4.2 Optimal Cyclotomic Lattices

For a fixed $L_t = \phi(mn)/\phi(m)$, from Theorem 1 we know that there exist infinitely many cyclotomic lattices for infinitely many integers m and n that have full diversity. In this subsection, we present optimal cyclotomic lattices for various numbers L_t of transmit antennas among these infinitely many cyclotomic lattices.

Lemma 2 *For any two integers $n = p_1^{r_1} \cdots p_l^{r_l} q_1^{i_1} \cdots q_k^{i_k}$, $m = p_1^{e_1} \cdots p_l^{e_l} v_1^{t_1} \cdots v_h^{t_h}$, then*

$$\frac{\phi(mn)}{\phi(m)} = p_1^{r_1} \cdots p_l^{r_l} \phi(n_0),$$

where $p_1, \cdots, p_l, q_1, \cdots, q_k, v_1, \cdots, v_h$ are distinct primes and $n_0 = q_1^{i_1} \cdots q_k^{i_k}$. Thus, $gcd(m,n)$ is a factor of $\frac{\phi(mn)}{\phi(m)}$.

This lemma is a direct consequence of the definition and property of Euler totient function in Footnote 2 and will be used in the proof of the following theorm in Appendix B. We now present optimal cyclotomic lattice designs for different numbers of transmit antennas.

Theorem 4 *For $L_t \leq 32$, the optimal L_t dimensional cyclotomic lattices $\Gamma_{L_t}(G_{m,n})$ over Λ_{ζ_m} with generating matrices $G_{m,n}$ defined in (16) are listed in Table 1.*

Table 1 *Optimal Cyclotomic Lattices for L_t Transmit Antennas*

L_t	(m,n) *in* $G_{m,n}$	$\frac{d_{\min}(\Gamma_{L_t}(G_{m,n}))}{\lvert\det(\Lambda_{\zeta_m})\rvert^{L_t/2}\lvert\det(G_{m,n})\rvert}$
2	$(3,4),(4,3),(6,2)$	$\frac{1}{\sqrt{3}}$
3	$(3,3),(3,6),(6,3)$	$\frac{1}{4.1878}$
4	$(3,5),(3,10),(6,5)$	$\frac{1}{8.3852}$
6	$(3,7),(3,14),(6,7)$	$\frac{1}{84.2037}$
8	$(3,20),(4,15),(6,10)$	$\frac{1}{1.125\times 10^3}$
9	$(3,9),(3,18),(6,9)$	$\frac{1}{1.0303\times 10^4}$
10	$(3,11),(3,22),(6,11)$	$\frac{1}{2.3655\times 10^4}$
12	$(3,15),(3,30),(6,15)$	$\frac{1}{4.2981\times 10^5}$
16	$(3,40),(4,30),(6,20)$	$\frac{1}{3.24\times 10^8}$
18	$(3,21),(3,42),(6,21)$	$\frac{1}{1.1752\times 10^{10}}$
20	$(3,25),(3,50),(6,25)$	$\frac{1}{4.0484\times 10^{11}}$
22	$(3,23),(3,46),(6,23)$	$\frac{1}{4.083\times 10^{13}}$
24	$(3,35),(3,70),(6,35)$	$\frac{1}{9.8192\times 10^{13}}$
27	$(3,27),(3,54),(6,27)$	$\frac{1}{3.0205\times 10^{18}}$
28	$(3,29),(3,58),(6,29)$	$\frac{1}{7.3757\times 10^{18}}$
30	$(3,33),(3,66),(6,33)$	$\frac{1}{1.8992\times 10^{20}}$
32	$(3,80),(4,60),(6,40)$	$\frac{1}{6.8797\times 10^{21}}$

The proof of Theorem 4 is in Appendix B. From Theorem 4 we can see that:

(i) All the optimal cyclotomic lattices can be achieved by *Eisenstein* cyclotomic latices;

(ii) The optimal cyclotomic lattice can not be achieved by *Gaussian* lattice except $L_t = 2, 8, 16, 32$;

(iii) The $L_t = 4$ dimensional optimal cyclotomic lattice can not be achieved by *Gaussian* lattice;

(iv) Since as we explained in Section 3, the generating matrix $G_{m,n}$ is unitary if and only if $L_t = n$, most of the optimal generating matrices $G_{m,n}$ are not unitary.

We want to make another remark here. When the number of transmit antennas is a prime, i.e., $L_t = p$, if we let $m = pm_0$ and $n = p$ with $\gcd(p, m_0) = 1$, or $n = 2p$ with $\gcd(2p, m_0) = 1$, then it is not hard to show that

$$L_t = \frac{\phi(mn)}{\phi(m)} = \frac{p^2 - p}{p - 1} = p.$$

Thus, the corresponding $G_{m,n}$ in (16) can be used as a generating matrix to generate full diversity cyclotomic lattices (or space-time codes). However, which one is optimal remains open.

4.3 Comparison with Existing Lattices

Now let us compare our proposed optimal cyclotomic lattices with some existing ones based on our result in Lemma 1.

For the complex lattices $\Gamma_2(\mathbf{M}_2)$ and $\Gamma_4(\mathbf{M}_4)$ over Λ_{ζ_4} in Example 1 in in [3, 5], $|\det(\mathbf{M}_2)| = 1$, the minimum product $d_{min}(\Gamma_2(\mathbf{M}_2)) = \frac{\sqrt{5}}{5}$, and $|\det(\mathbf{M}_4)| = 1$ and the minimum product $d_{min}(\Gamma_4(\mathbf{M}_4)) = \frac{1}{40}$. Thus,

$$\frac{d_{min}(\Gamma_2(\mathbf{M}_2))}{|\det(\Lambda_{\zeta_4})\det(\mathbf{M}_2)|} = \frac{\sqrt{5}}{5} \quad \text{and} \quad \frac{d_{min}(\Gamma_4(\mathbf{M}_4))}{|\det(\Lambda_{\zeta_4})|^2\,|\det(\mathbf{M}_4)|} = \frac{1}{40}.$$

For the complex lattices $\Gamma_2(G_{2f})$ and $\Gamma_4(G_{4f})$ over Λ_{ζ_4} in Example 2 in [2, 3], $|\det(G_{2f})| = 2\sqrt{3}$, the minimum product $d_{min}(\Gamma_2(G_{2f})) = 1$, and $|\det(G_{4f})| = 64$ and the minimum product $d_{min}(\Gamma_4(G_{4f})) = 1$. Thus,

$$\frac{d_{min}(\Gamma_2(G_{2f}))}{|\det(\Lambda_{\zeta_4})\det(G_{2f})|} = \frac{1}{2\sqrt{3}} \quad \text{and} \quad \frac{d_{min}(\Gamma_4(G_{4f}))}{|\det(\Lambda_{\zeta_4})|^2\,|\det(G_{4f})|} = \frac{1}{64}.$$

For the complex lattices $\Gamma_2(G_2)$ and $\Gamma_4(G_4)$ over Λ_{ζ_4} in Example 3 in [2, 3], $|\det(G_2)| = 2$, the minimum product $d_{min}(\Gamma_2(G_2)) = 1$, and $|\det(G_4)| = 16$ and the minimum product $d_{min}(\Gamma_4(G_4)) = 1$. Thus,

$$\frac{d_{min}(\Gamma_2(G_2))}{|\det(\Lambda_{\zeta_4})\det(G_2)|} = \frac{1}{2} \quad \text{and} \quad \frac{d_{min}(\Gamma_4(G_4))}{|\det(\Lambda_{\zeta_4})|^2\,|\det(G_4)|} = \frac{1}{16}.$$

Notice that $G_2 = \hat{G}_{4,2}$ and $G_4 = \hat{G}_{4,4}$ and they are equivalent to $G_{4,2}$ and $G_{4,4}$, respectively, which are not optimal.

From Theorem 4 we know that cyclotomic lattice $\Gamma_2(G_{6,2})$ over $\Lambda_{\zeta_6} = \mathbb{Z}[\zeta_6]$ and cyclotomic lattice $\Gamma_2(G_{4,3})$ over $\Lambda_{\zeta_4} = \mathbb{Z}[j]$ are two optimal cyclotomic lattices for 2 transmit antennas, and cyclotomic lattices $\Gamma_4(G_{3,5})$ and $\Gamma_4(G_{6,5})$ over $\Lambda_{\zeta_3} = \Lambda_{\zeta_6} = \mathbb{Z}[\zeta_3] = \mathbb{Z}[\zeta_6]$ are two optimal cyclotomic lattices for 4 transmit antennas. Furthermore, $|\det(\Lambda_{\zeta_6})| = |\det(\Lambda_{\zeta_3})| = \frac{\sqrt{3}}{2}$, $|\det(G_{6,2})| = 2$,

$|\det(G_{4,3})| = \sqrt{3}$, $|\det(G_{3,5})| = |\det(G_{6,5})| = 11.1803$, and $d_{min}(\Gamma_2(G_{6,2})) = d_{min}(\Gamma_2(G_{4,3})) = d_{min}(\Gamma_4(G_{3,5})) = d_{min}(\Gamma_4(G_{6,5})) = 1$. Thus,

$$\frac{d_{min}(\Gamma_2(G_{6,2}))}{|\det(\Lambda_{\zeta_6})\det(G_{6,2})|} = \frac{d_{min}(\Gamma_2(G_{4,3}))}{|\det(\Lambda_{\zeta_4})\det(G_{4,3})|} = \frac{1}{\sqrt{3}} > \frac{1}{2},$$

and

$$\frac{d_{min}(\Gamma_4(G_{3,5}))}{|\det(\Lambda_{\zeta_3})|^2|\det(G_{3,5})|} = \frac{d_{min}(\Gamma_4(G_{6,5}))}{|\det(\Lambda_{\zeta_6})|^2|\det(G_{6,5})|} = \frac{4}{3\times 11.1803} > \frac{1}{16}.$$

This shows that the optimal cyclotomic lattices we present here are better than the existing examples in the literature.

5 Diagonal Cyclotomic Space-Time Code Designs

By using the cyclotomic lattices proposed in the last section and the structures studied in [2] and [5], we can generate some new diagonal space-time codes and linear precodes for fast fading channels. To design a rate R cyclotomic space-time code for L_t transmitters is to find a subset Ω of some L_t dimensional cyclotomic lattice $\Gamma_{L_t}(G_{m,n})$ such that it can achieve good performance.

5.1 Design Schemes

To design a cyclotomic space-time code Ω of a certain size $|\Omega|$, we first select an optimal L_t dimensional cyclotomic lattice by using the criterion developed in Section 4. After a cyclotomic lattice $\Gamma_{L_t}(G_{m,n})$ is selected, we select $|\Omega|$ points on the lattice with the smallest total signal energy. The theory developed in Sections 3 have ensured that such a space-time code has full diversity and a good diversity product. Let us formulate it in details below. Assume cyclotomic lattice $\Gamma_{L_t}(G_{m,n})$ over Λ_{ζ_m} is selected. Let $\underline{\mathbf{y}} = [\mathbf{y}_1, \cdots, \mathbf{y}_{L_t}]^T$, diag($\underline{\mathbf{y}}$)=diag($\mathbf{y}_1, \cdots, \mathbf{y}_{L_t}$), $\underline{\mathbf{x}} = [\mathbf{x}_1, \cdots, \mathbf{x}_{L_t}]^T \in (\Lambda_{\zeta_m})^{L_t}$, and $\underline{\mathbf{y}} = G_{m,n}\underline{\mathbf{x}}$. The goal of designing a cyclotomic code Ω of size $|\Omega|$ here is to select

$$\Omega_1 = \{\mathrm{diag}(\underline{\mathbf{y}}_i) : \ \underline{\mathbf{y}}_i = G_{m,n}\underline{\mathbf{x}}_i, \underline{\mathbf{x}}_i \neq \underline{\mathbf{x}}_l \in (\Lambda_{\zeta_m})^{L_t}, 1 \leq i \neq l \leq |\Omega|\} \tag{30}$$

such that

$$\sum_{i=1}^{|\Omega|} \|\underline{\mathbf{y}}_i\|^2 \ \text{ is minimized.} \tag{31}$$

Since the vectors $\underline{\mathbf{y}}_i$ are on a lattice, the mean of all the codewords may not be zero, i.e.,

$$\underline{\mu} \triangleq \frac{1}{|\Omega|}\sum_{i=1}^{|\Omega|}\underline{\mathbf{y}}_i \neq 0,$$

which may waste the transmission signal power. Therefore, we need to shift the selected space-time code to the origin to form the final diagonal space-time code

$$\Omega = \{\mathrm{diag}(\underline{\mathbf{y}}_i - \underline{\mu}) : \ 1 \leq i \leq |\Omega|\}. \tag{32}$$

There are at least two approaches to solve this problem depending on how the information symbols $\underline{\mathbf{x}}$ are selected and binary information bits are mapped to space-time codewords. Notice that $\underline{\mathbf{x}} = [\mathbf{x}_1, \cdots, \mathbf{x}_{L_t}]^T$ and each component $\mathbf{x}_i$ can be thought of as either a two dimensional real lattice point on Λ_{ζ_m} or equivalently a complex number as explained in Section 2.

Method I: Component-wise Independent Selection – Λ_{ζ_m}**-QAM**

In this case, the space-time code size has to have the form of $|\Omega| = 2^{RL_t}$, where R is the throughput in bits per second per Hz (bits/s/Hz) and the components $\mathbf{x}_i$ in $\underline{\mathbf{x}}$ are independently selected from 2^R-QAM located on the two dimensional lattice Λ_{ζ_m}, such as the conventional QAM on the square lattice if $m = 4$ and QAM on the equilateral triangular lattice if $m = 3$ or 6. This method is described as follows.

Select 2^R-QAM signal constellation $\mathcal{S}$ on the lattice Λ_{ζ_m} such that its total energy is minimized:

$$\mathcal{S} = \{\mathbf{x}_i : \ \mathbf{x}_i \neq \mathbf{x}_l \in \Lambda(\zeta_m), \ 1 \leq i \neq l \leq 2^R\} \ \text{ and } \ \min \sum_{\mathbf{x} \in \mathcal{S} \subset \Lambda_{\zeta_m}} \|\mathbf{x}\|^2.$$

This method is called Λ_{ζ_m}-QAM for convenience and in case $\Lambda_{\zeta_m} = \mathbb{Z}[\zeta_m]$, it is called $\mathbb{Z}[\zeta_m]$-QAM.

With this method, binary information bits are first mapped to complex symbols $\mathbf{x}_i \in \mathcal{S}$, $1 \leq i \leq L_t$. Then, these symbols $\mathbf{x}_i$ are encoded into diagonal space-time codewords as described in (30)-(32) for Ω_1 and Ω.

Method II: Joint Component Selection – Λ_{ζ_m}**-Joint**

In this case, since the components $\mathbf{x}_i \in \Lambda_{\zeta_m}$ of $\underline{\mathbf{x}}$ are jointly considered, we should be able to minimize the codeword vector $\underline{\mathbf{y}}$ energy as described in (30)-(31) by selecting the optimal $|\Omega|$ distinct vectors $\underline{\mathbf{x}}_i^o \in (\Lambda_{\zeta_m})^{L_t}$ for $1 \leq i \leq |\Omega|$. Then, let $\mathcal{S} = \{\underline{\mathbf{x}}_i^o : \ 1 \leq i \leq |\Omega|\}$.

With this method, the encoding can be done as follows. Each $\log_2(|\Omega|)$ bits of binary information are mapped to a vector, say $\underline{\mathbf{x}}_{i_0}^o$, in $\mathcal{S}$. Then, this vector $\underline{\mathbf{x}}_{i_0}^o$ is used to generate a diagonal space-time code $\text{diag}(\underline{\mathbf{y}}_{i_0}^o - \underline{\mu})$, where

$$\underline{\mathbf{y}}_{i_0}^o = G_{m,n}\underline{\mathbf{x}}_{i_0}^o \ \text{ and } \ \underline{\mu} = \frac{1}{|\Omega|}\sum_{i=1}^{|\Omega|}\underline{\mathbf{y}}_i^o.$$

5.2 Some Design Examples of Optimal Cyclotomic Space-Time Codes

Based on the optimal cyclotomic lattices found in the previous section, we can design optimal cyclotomic space-time codes as described in Section 5.1. We now present a few examples based on the optimal cyclotomic lattices for $L_t = 2$ and $L_t = 4$ in Section 4 and the two methods, Method I, i.e., the "Λ_{ζ_m}-QAM" method, and Method II, i.e., the "Λ_{ζ_m}-Joint" method, introduced in Section 5.1. The energies of space-time codewords are normalized in the following way: for L_t transmit antennas and a space-time code of rate R bits/s/Hz, the total energy of $2^{L_t \times R}$ diagonal matrices (or codewords) is normalized into $2^{L_t \times R}$. We then compare these codes with the existing ones in

[2, 3]. For the cyclotomic lattices G_2 and G_4 in Example 3 [3, 2], which correspond to the non-optimal $G_{4,2}$ and $G_{4,4}$ in the family presented in this correspondence as we explained before, we also use Method I and Method II to design the optimal cyclotomic space-time codes. The diversity products for these codes are listed in Table 2 and Table 3. One can clearly see the improvement of the optimal cyclotomic space-time codes presented in this correspondence over the existing ones in the literature.

Table 2 *Diversity Products of Diagonal Codes for Two Transmit Antennas*

Bit Rates	Space-Time Codes				
(bits/s/Hz)	$\mathbf{M}_2$-$\mathbb{Z}[j]$-QAM	G_2-$\mathbb{Z}[j]$-QAM	G_2-$\mathbb{Z}[j]$-Joint	$G_{6,2}$-Λ_{ζ_6}-QAM	$G_{6,2}$-Λ_{ζ_6}-Joint
2	$\frac{1}{4.47}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$
3	$\frac{1}{5.5231}$	$\frac{1}{5}$	$\frac{1}{4.6562}$	$\frac{1}{4.3125}$	$\frac{1}{4.125}$
4	$\frac{1}{11.2}$	$\frac{1}{10}$	$\frac{1}{9.5703}$	$\frac{1}{8.75}$	$\frac{1}{8.2266}$

Table 3 *Diversity Products of Diagonal Codes for Four Transmit Antennas*

Bit Rates	Space-Time Codes				
ts/s/Hz)	$\mathbf{M}_4$-$\mathbb{Z}[j]$-QAM	G_4-$\mathbb{Z}[j]$-QAM	G_4-$\mathbb{Z}[j]$-Joint	$G_{6,5}$-Λ_{ζ_6}-QAM	$G_{6,5}$-Λ_{ζ_6}-Joint
2	$\frac{1}{640}$	$\frac{1}{256}$	$\frac{1}{256}$	$\frac{1}{128}$	$\frac{1}{104.98}$
3	$\frac{1}{1000}$	$\frac{1}{400}$	$\frac{1}{323.2265}$	$\frac{1}{297.5625}$	$\frac{1}{170.514}$
4	$\frac{1}{4000}$	$\frac{1}{1600}$	$\frac{1}{1305.9}$	$\frac{1}{1225}$	$\frac{1}{681.8418}$

6 Simulation Results

In this section, we present some simulation results for 4 transmit and 2 receive antennas. Similar to that in [5], the codeword is normalized such that the mean power of codewords at all transmit antennas is 1. The additive white Gaussian noise at each receive antenna has a variance $\sigma^2 = 1/\text{SNR}= L_r/(2\text{SNR})$ per real dimension, where L_r is the number of receive antennas and SNR is the signal to noise ratio at each receive antenna. The channel is assumed quasi-static Rayleigh fading. Two kinds of diagonal cyclotomic space-time codes are compared: the non-optimal one but the best in the existing literature, i.e., G_4 in [3, 5], and the optimal one, i.e., $G_{6,5}$ found in Section 4 and listed in Table 2. The simulation results of codeword error probability for three different bit rates R, $R = 2$, 3, and 4, are shown in Fig. 1, Fig. 2, and Fig. 3, respectively, where "-QAM" and "-Joint" correspond to the two different diagonal cyclotomic space-time code design methods, Method I and Method II, respectively, in Section 5. For rate $R = 2$ case in Fig. 1, the code G_4-QAM and G_4-Joint are the same and so only G_4-QAM is shown. The reason why the codeword error probability is provided is that the Gray mapping for Method II, i.e., "-Joint" is not available. In these figures, the DAST codes in [5, 3] are also compared. One can clearly see the performance improvement of the optimal cyclotomic codes over the non-optimal ones in the literature, which has illustrated the theoretical results obtained in Subsection 5.2.

7 Conclusions

In this correspondence, a systematic and full diversity cyclotomic lattice design has been proposed. The newly proposed full diversity cyclotomic lattices have a *concrete* form and infinitely many members for a fixed lattice dimention. Due to the concrete form of the cyclotomic lattice generating matrices, we have presented the optimal cyclotomic lattices based on the packing density theory, where the optimality is in the sense of minimizing the mean transmission signal power for a fixed minimum (diversity) product or equivalently maximizing the minimum product for a fixed mean transmission signal power. It is found that (i) the square lattice $\mathbb{Z}[j]$ based designs are not optimal in most cases and (ii) the optimal generating matrices are not unitary in most cases. The cyclotomic lattices have immediate applications in the designs of diagonal space-time block codes for multiple antennas and linear precodes for achieving signal space diversity for single antenna systems over fast Rayleigh fading channels.

Diagonal codes have applications not only as space-time codes themselves but also in quasi-orthogonal space-time code designs as recently observed in [20], where it is shown that, for a fixed quasi-orthogonal design, the diversity product of a quasi-orthogonal space-time code equivalently depends on the diversity product of a diagonal space-time code. Although the optimality on the cyclotomic lattices has been studied for various numbers of transmit antennas, it is still open for several numbers of transmit antennas, such as $L_t = 5$. As explained in Section 2, an L_t dimensional complex lattice can be converted to a $2L_t$ dimensional real lattice. In contrast, a $2L_t$ dimensional real vector on an $2L_t$ dimensional real lattice can be used to form an L_t dimensional complex vector by grouping each two consecutive real components into a complex number and the signal energy does not change in the conversion. In other words, any $2L_t$ dimensional real lattice can also be used to design a complex-valued diagonal space-time code. The difference is that these L_t dimensional complex vectors may not necessarily form a complex lattice and in case they form a complex lattice, then it is equivalent to a complex lattice studied in Section 2. Therefore, the complex lattice design is a special case of the above real lattice design. We believe that the ultimate goal of the lattice based diagonal space-time code design is to design optimal $2L_t \times 2L_t$ real generating matrix K such that the $2L_t$ dimensional real lattice has the maximal minimum product when the mean signal power is fixed. As a final remark, optimal cyclotomic lattices for more general number, L_t, transmit antennas have been recently obtained in [46, 47].

Appendix A: Proof of Theorem 1

Before we prove Theorem 1, we need some results on algebraic number fields.

Let $\mathbb{F}$ be a field and $\mathbb{F}[x]$ denote the polynomial ring over $\mathbb{F}$, i.e., all polynomials with coefficients in $\mathbb{F}$. Let $f(x) \in \mathbb{F}[x]$. A *splitting field* of $f(x)$ is a field extension $\mathbb{E}$ of $\mathbb{F}$ such that polynomial $f(x)$ splits in $\mathbb{E}$, i.e., $f(x)$ can be factorized into order 1 polynomials of coefficients in $\mathbb{E}$, but it does not split in any proper subfield of $\mathbb{E}$. For more details about a split field, see for example [42]. $\mathbb{E}$ is called the splitting field of $f(x)$ over $\mathbb{F}$.

Let $\mathbb{F} \subset \mathbb{E}$ be two fields and assume that $\mathbb{E}$ is a splitting field of a polynomial over $\mathbb{F}$. Galois group $Gal(\mathbb{E}/\mathbb{F})$ denotes the quotient group of $\mathbb{F}$ in $\mathbb{E}$, i.e., $\mathbb{E}/\mathbb{F}$, and consists of all the automorphisms of $\mathbb{E}$ that fix $\mathbb{F}$.

We now cite three results (Propositions) from algebraic number fields, which are used to prove Theorem 1.

Proposition 3 *(pg. 36, [42]) If $\mathbb{E}$ is the splitting field of a polynomial $f(x) \in \mathbb{F}[x]$ over $\mathbb{F}$, then $|Gal(\mathbb{E}/\mathbb{F})| = [\mathbb{E} : \mathbb{F}]$, i.e., the extension degree of $\mathbb{E}$ over $\mathbb{F}$.*

Proposition 4 *(pg. 75, [43]) If $\mathbb{K}$ is the splitting field of $x^n - 1$ over $\mathbb{Q}$, then $[\mathbb{K} : \mathbb{Q}] = \phi(n)$ and $Gal(\mathbb{K}/\mathbb{Q}) = \{n_i : 1 \leq n_i \leq n-1 \text{ and } gcd(n_i, n) = 1\}$. Moreover, if ω is a primitive n^{th} root of unity in $\mathbb{K}$, then $Gal(\mathbb{K}/\mathbb{Q}) = \{\sigma_i : gcd(i,n) = 1, 1 \leq i \leq n-1\}$, where σ_i is determined by $\sigma_i(\omega) = \omega^i$.*

An example of $\mathbb{K}$ in Proposition 4 is $\mathbb{K} = \mathbb{Q}(\zeta_n)$. In Proposition 4, gcd stands for the greatest common advisor and $gcd(a,b) = 1$ means a and b are co-prime.

Proposition 5 *(pg. 37, [42]) Let $\mathbb{F} \subset \mathbb{B} \subset \mathbb{E}$ be three fields and $\mathbb{B}$ be the splitting field of some polynomial $f(x) \in \mathbb{F}[x]$ over $\mathbb{F}$ and $\mathbb{E}$ be the splitting field of another polynomial $g(x) \in \mathbb{F}[x]$ over $\mathbb{F}$. Then, $Gal(\mathbb{E}/\mathbb{B})$ is a normal subgroup of $Gal(\mathbb{E}/\mathbb{F})$, and the quotient group $Gal(\mathbb{E}/\mathbb{F}) \big/ Gal(\mathbb{E}/\mathbb{B}) \cong Gal(\mathbb{B}/\mathbb{F})$.*

We are now ready to prove Theorem 1. To use Proposition 5, let $\mathbb{F} = \mathbb{Q}$, $\mathbb{B} = \mathbb{Q}(\zeta_m)$, $\mathbb{E} = \mathbb{Q}(\zeta_{mn})$, $f(x) = x^m - 1$, and $g(x) = x^{mn} - 1$. Then, it is easy to check that $\mathbb{Q}(\zeta_m)$ is the splitting field of $f(x) = x^m - 1$ over $\mathbb{Q}$ and $\mathbb{Q}(\zeta_{mn})$ is the splitting field of $g(x) = x^{mn} - 1$ over $\mathbb{Q}$. From Proposition 3, we have

$$|Gal(\mathbb{Q}(\zeta_{mn})/\mathbb{Q})| = [\mathbb{Q}(\zeta_{mn}) : \mathbb{Q}] = \phi(mn) \text{ and } |Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q})| = [\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \phi(m).$$

Using the results in Proposition 4 and Proposition 5, we have

$$Gal(\mathbb{Q}(\zeta_{mn})/\mathbb{Q}) = \{\sigma_i : gcd(i, mn) = 1, 1 \leq i \leq mn-1\},$$

$$Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q}) = \{\sigma_i : gcd(i, m) = 1, 1 \leq i \leq m-1\},$$

and $Gal(\mathbb{Q}(\zeta_{mn})/\mathbb{Q}(\zeta_m))$ is the coset of $Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ in $Gal(\mathbb{Q}(\zeta_{mn})/\mathbb{Q})$. Therefore,

$$Gal(\mathbb{Q}(\zeta_{mn})/\mathbb{Q}(\zeta_m)) = \{\sigma_{1+mn_i} : gcd(1+mn_i, mn) = 1, 0 \leq n_i \leq n-1\},$$

which can be seen from the fact that σ_{1+n_im} is in the coset of $\sigma_1 \in Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ in $Gal(\mathbb{Q}(\zeta_{mn})/\mathbb{Q})$. This means that there are $L_t = \frac{\phi(mn)}{\phi(m)}$ automorphisms σ_i of $\mathbb{Q}(\zeta_{mn})$ that fix $\mathbb{Q}(\zeta_m)$, and all of them have the property $\sigma_i(\zeta_N) = \zeta_N^{1+n_im}$, where $N = mn$. **q.e.d.**

Appendix B: Proof of Theorem 4

Case of $L_t = 2$

For two transmit antennas, we have the following Theorem.

Theorem 5 *For two transmit antennas,* $\Gamma_2(G_{3,4})$ *over* Λ_{ζ_3}*,* $\Gamma_2(G_{6,2})$ *over* Λ_{ζ_6}*, and* $\Gamma_2(G_{4,3})$ *over* Λ_{ζ_4} *are the optimal cyclotomic lattices with*

$$\frac{d_{min}(\Gamma_2(G_{3,4}))}{|\det(\Lambda_{\zeta_3})\det(G_{3,4})|} = \frac{d_{min}(\Gamma_2(G_{6,2}))}{|\det(\Lambda_{\zeta_6})\det(G_{6,2})|} = \frac{d_{min}(\Gamma_2(G_{4,3}))}{|\det(\Lambda_{\zeta_4})\det(G_{4,3})|} = \frac{\sqrt{3}}{3},$$

where

$$G_{3,4} = G_{6,2} = \begin{bmatrix} \zeta_{12} & \zeta_{12}^2 \\ -\zeta_{12} & \zeta_{12}^2 \end{bmatrix}, \qquad G_{4,3} = \begin{bmatrix} \zeta_{12} & \zeta_{12}^2 \\ \zeta_{12}\zeta_3 & \zeta_{12}^2\zeta_3^2 \end{bmatrix}.$$

Proof: From (3),

$$\Lambda_{\zeta_3} = \begin{bmatrix} 1 & \cos(2\pi/3) \\ 0 & \sin(2\pi/3) \end{bmatrix}, \ \Lambda_{\zeta_6} = \begin{bmatrix} 1 & \cos(\pi/3) \\ 0 & \sin(\pi/3) \end{bmatrix}, \ \text{ and } \ \Lambda_{\zeta_4} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

It is easy to check

$$|\det(G_{3,4})|\,|\det(\Lambda_{\zeta_3})| = |\det(G_{6,2})|\,|\det(\Lambda_{\zeta_6})| = |\det(G_{4,3})|\,|\det(\Lambda_{\zeta_4})| = \sqrt{3}.$$

From Proposition 2, we know

$$d_{min}(\Gamma_2(G_{3,4})) = d_{min}(\Gamma_2(G_{6,2})) = d_{min}(\Gamma_2(G_{4,3})) = 1.$$

Thus,

$$\frac{d_{min}(\Gamma_2(G_{3,4}))}{|\det(\Lambda_{\zeta_3})\det(G_{3,4})|} = \frac{d_{min}(\Gamma_2(G_{6,2}))}{|\det(\Lambda_{\zeta_6})\det(G_{6,2})|} = \frac{d_{min}(\Gamma_2(G_{4,3}))}{|\det(\Lambda_{\zeta_4})\det(G_{4,3})|} = \frac{\sqrt{3}}{3}.$$

This implies that $\Gamma_2(G_{3,4})$ over Λ_{ζ_3}, $\Gamma_2(G_{6,2})$ over Λ_{ζ_6}, and $\Gamma_2(G_{4,3})$ over Λ_{ζ_4} are the same according to the criterion in Section 4.2.

We next prove that they are optimal among cyclotomic lattices $\Gamma_2(G_{m,n})$ for any integers m and n with $\frac{\phi(mn)}{\phi(n)} = 2$. Since $L_t = 2$, there are two integers n_1 and n_2 in the generating matrix $G_{m,n}$ in (16). Since $n_1 = 0$, to determine $G_{m,n}$, we only need to determine the integer n_2 with $0 < n_2 < n$ such that $1 + n_2 m$ and mn are co-prime.

Let m and n be integers and $N = mn$ such that $\frac{\phi(N)}{\phi(m)} = 2$. There are two different cases: $\gcd(m, n) = 1$ and $\gcd(m, n) > 1$.

Case 1. $\gcd(m, n) = 1$

In this case, m and n are co-prime and $\phi(N) = \phi(mn) = \phi(m)\phi(n)$. Thus, we have $\frac{\phi(N)}{\phi(m)} = \phi(n) = 2$. Therefore, there are only three subcases for values n: $n = 3$, $n = 4$, or $n = 6$.

Subcase 1.1. $\gcd(m, n) = 1$, $n = 4$ In this subcase, m is an odd number. In order to find the form of the generating matrix $G_{m,n}$ in (16), we need to find the integer n_2 in the range from 1 to

$n-1=3$ such that $1+n_2m$ and $4m$ are co-prime. Since m is odd, n_2 has to be even and therefore, n_2 has to be 2, i.e., $n_2=2$. This implies that the generating matrix $G_{m,4}$ in (16) is

$$G_{m,4}=\left[\begin{array}{cc}\zeta_N & \zeta_N^2\\ \zeta_N^{1+2m} & \zeta_N^{2(1+2m)}\end{array}\right]=\left[\begin{array}{cc}1 & 1\\ \zeta_4^2 & \zeta_4^4\end{array}\right]\left[\begin{array}{cc}\zeta_N & 0\\ 0 & \zeta_N^2\end{array}\right].$$

It is not hard to see that $|\det(G_{m,4})|=2$. By using the result in Theorem 3, we know that $\Gamma_2(G_{3,4})$ over Λ_{ζ_3} is the optimal cyclotomic lattice in this class.

Subcase 1.2. $\gcd(m,n)=1$, $n=3$

In this subcase, m can not be divided by 3 and the integer n_2 in $G_{m,n}$ has only two possibilities of $n_2=1$ or $n_2=2$. Since m can not be divided by 3, m has only two different forms, $m=3m_0+1$ and $m=3m_0+2$ for integers m_0.

(i) Consider the case when $m=3m_0+1$. If $n_2=2$, then $1+n_2m=1+2m=3+3m_0$ that is not co-prime with $mn=3m$. This proves that $n_2=1$ when $m=3m_0+1$.

(ii) Consider the case when $m=3m_0+2$. If $n_2=1$, $1+n_2m=1+m=3m_0+3$ that is not co-prime with $mn=3m$. This proves that $n_2=2$ when $m=3m_0+2$. Go back to the generating matrix $G_{m,3}$:

$$G_{m,3}=\left[\begin{array}{cc}\zeta_N & \zeta_N^2\\ \zeta_N^{1+n_2m} & \zeta_N^{2(1+n_2m)}\end{array}\right]=\left[\begin{array}{cc}1 & 1\\ \zeta_3^{n_2} & \zeta_3^{2n_2}\end{array}\right]\left[\begin{array}{cc}\zeta_N & 0\\ 0 & \zeta_N^2\end{array}\right].$$

Since $m\geq 3$ and $\gcd(m,3)=1$, we have $m\geq 4$. we next prove that $\Gamma_2(G_{4,3})$ over Λ_{ζ_4} is the optimal among the cyclotomic lattices in class $\Gamma_2(G_{m,3})$ over Λ_{ζ_m} for $m\geq 4$. Since 1 and ζ_m belong to $\Lambda_{\zeta_m}\subset\mathbb{Z}[\zeta_m]$, points $\mathbf{x}=1-\zeta_m$ and $-\mathbf{x}$ are on lattice $\Lambda_{\zeta_m}\subset\mathbb{Z}[\zeta_m]$. Thus,

$$\left[\begin{array}{c}\mathbf{y}_1\\ \mathbf{y}_2\end{array}\right]=\left[\begin{array}{cc}\zeta_N & \zeta_N^2\\ \zeta_N^{1+n_2m} & \zeta_N^{2(1+n_2m)}\end{array}\right]\left[\begin{array}{c}\mathbf{x}\\ -\mathbf{x}\end{array}\right]$$

is a point on the cyclotomic lattice $\Gamma_2(G_{m,3})$ over Λ_{ζ_m}. Therefore, the minimum product $d_{min}(\Gamma_2(G_{m,3}))$ satisfies

$$d_{min}(\Gamma_2(G_{m,3}))\leq|\mathbf{x}|^2\left|(1-\zeta_{3m})\left(1-\zeta_3^{n_2}\zeta_{3m}\right)\right|.$$

Let

$$f(m)=\frac{|\mathbf{x}|^2\left|(1-\zeta_{3m})\left(1-\zeta_3^{n_2}\zeta_{3m}\right)\right|}{|\det(\Lambda_{\zeta_m})|},$$

Since $|\mathbf{x}|=2\sin(\pi/m)$ and $|\det(\Lambda_m)|=\sin(2\pi/m)$, we have

$$f(m)=2\tan(\pi/m)\left|(1-\zeta_{3m})\left(1-\zeta_3^{n_2}\zeta_{3m}\right)\right|.$$

By the discussions in (i) and (ii), we have

$$f(m)=\begin{cases}2\tan(\pi/m)\left|(1-\zeta_{3m})\left(1-\zeta_3\zeta_{3m}\right)\right| & \text{if } m=3m_0+1,\quad m_0\geq 1,\\ 2\tan(\pi/m)\left|(1-\zeta_{3m})\left(1-\zeta_3^2\zeta_{3m}\right)\right| & \text{if } m=3m_0+2,\quad m_0\geq 1.\end{cases}$$

It is easy to check that

$$\frac{d_{min}(\Gamma_2(G_{m,3}))}{|\det(\Lambda_{\zeta_m})|}\leq f(m)\leq f(5)<0.9<1=\frac{d_{min}(\Gamma_2(G_{4,3}))}{|\det(\Lambda_{\zeta_4})|}\quad\text{for } m\geq 5.$$

From Theorem 3, the optimality of cyclotomic lattice $\Gamma_2(G_{4,3})$ over Λ_{ζ_4} also holds in this case.

Subcase 1.3. $\gcd(m,n)=1$, $n=6$

This subcase is similar to Subcase 1.1 when $n=4$.

Case 2. $\gcd(m,n)>1$

From Lemma 2 we know

$$2=\frac{\phi(N)}{\phi(m)}=\frac{\phi(mn)}{\phi(m)}\geq \gcd(m,n)>1.$$

Thus, we have $\gcd(m,n)=2$. We next want to show $n=2$. In fact, if $n=2n_0$ for $n_0>1$ and n_0 is even, then $n=2^r n_0'$ with $r\geq 2$ and $n_0'\geq 1$. From Lemma 2, it is not hard to see

$$\frac{\phi(mn)}{\phi(m)}\geq 4.$$

If $n=2n_0$ for $n_0>1$ and n_0 is odd, then $n_0\geq 3$ and $\gcd(m,n_0)=1$ due to $\gcd(m,n)=2$.

From Lemma 2, it is not hard to see

$$\frac{\phi(mn)}{\phi(m)}=2\phi(n_0)>2,$$

which is because $\phi(n_0)>1$ when $n_0>2$. This contradicts with the assumption of $L_t=2$ and therefore proves $n=2$.

Since $\gcd(m,2)=2$, m has to be even. Since $n=2$, the two integers n_1 and n_2 in $G_{m,2}$ in (16) have to be $n_1=0$ and $n_2=1$. Thus,

$$G_{m,2}=\begin{bmatrix}\zeta_N & \zeta_N^2\\ \zeta_N^{1+m} & \zeta_N^{2(1+m)}\end{bmatrix}=\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}\zeta_N & 0\\ 0 & \zeta_N^2\end{bmatrix}.$$

In this case, $|\det(G_{m,2})|=2$ for any even m. By Theorem 3, we know that the best cyclotomic lattice in this class is $\Gamma_2(G_{6,2})$ over $\Lambda_{\zeta_6}=\mathbb{Z}[\zeta_6]$. Furthermore, since $|\det(\Lambda_{\zeta_4})|>|\det(\Lambda_{\zeta_6})|$, lattice $\Gamma_2(G_{6,2})$ over Λ_{ζ_6} is strictly better than $\Gamma_2(G_{4,2})$ over Λ_{ζ_4} that is the same as G_2 in Example 3. **q.e.d.**

Case of $L_t=3$

In this subsection, we present the optimal cyclotomic lattices for three transmit antennas, i.e., $L_t=3$.

Theorem 6 *For three transmit antennas, $\Gamma_3(G_{3,6})$ over Λ_{ζ_3}, $\Gamma_3(G_{6,3})$ over Λ_{ζ_6}, and $\Gamma_3(G_{3,3})$ over Λ_{ζ_3} are the optimal cyclotomic lattices with*

$$\frac{d_{min}(\Gamma_3(G_{3,6}))}{|\det(\Lambda_{\zeta_3})|^{3/2}|\det(G_{3,6})|}=\frac{d_{min}(\Gamma_3(G_{6,3}))}{|\det(\Lambda_{\zeta_6})|^{3/2}|\det(G_{6,3})|}=\frac{d_{min}(\Gamma_3(G_{3,3}))}{|\det(\Lambda_{\zeta_3})|^{3/2}|\det(G_{3,3})|}=\frac{1}{\left(\frac{\sqrt{3}}{2}\right)^{3/2}\times 5.1963},$$

where

$$G_{3,6}=G_{6,3}=\begin{bmatrix}1 & 1 & 1\\ \zeta_3 & \zeta_3^2 & \zeta_3^3\\ \zeta_3^2 & \zeta_3^4 & \zeta_3^6\end{bmatrix}\begin{bmatrix}\zeta_{18} & 0 & 0\\ 0 & \zeta_{18}^2 & 0\\ 0 & 0 & \zeta_{18}^3\end{bmatrix},\qquad G_{3,3}=\begin{bmatrix}1 & 1 & 1\\ \zeta_3 & \zeta_3^2 & \zeta_3^3\\ \zeta_3^2 & \zeta_3^4 & \zeta_3^6\end{bmatrix}\begin{bmatrix}\zeta_9 & 0 & 0\\ 0 & \zeta_9^2 & 0\\ 0 & 0 & \zeta_9^3\end{bmatrix}.$$

Proof. It is easy to check that $\Gamma_3(G_{3,6})$ over $\Lambda_{\zeta_3} = \mathbb{Z}[\zeta_3]$, $\Gamma_3(G_{6,3})$ over $\Lambda_{\zeta_6} = \mathbb{Z}[\zeta_6]$, and $\Gamma_3(G_{3,3})$ over Λ_{ζ_3} are cyclotomic lattices with $|\det(G_{3,6})| = |\det(G_{6,3})| = |\det(G_{3,3})| = 5.1963$. Thus, they are the same according to the criterion in Section 4.2. We next prove that they are the optimal cyclotomic lattices for $L_t = 3$.

Since $L_t = 3$, there are three integers n_1, n_2 and n_3 in the generating matrix $G_{m,n}$ in (16). We next determine these integers for different possible m and n.

We first consider integer n. Let m and n be two positive integers with $N = mn$ such that $\frac{\phi(N)}{\phi(m)} = L_t = 3$. We claim $\gcd(m,n) > 1$. In fact, if $\gcd(m,n) = 1$, then

$$3 = \frac{\phi(N)}{\phi(m)} = \phi(n).$$

But there does not exist any positive integer n such that $\phi(n) = 3$. Since, from Lemma 2, $\gcd(m,n)$ is a factor of $L_t = 3$, we have proved that $\gcd(m,n) = 3$. Thus, $n = 3n_0$ and $m = 3m_0$ and m_0 and n_0 are co-prime. We next show $n = 3$ or $n = 6$.

We now claim that n_0 can not be divided by 3. In fact, if n_0 can be divided by 3, then we let $n_0 = 3^r k_0$ and $r \geq 1$ and $\gcd(k_0, 3) = 1$. Since $\gcd(m_0, n_0) = 1$, we have $\gcd(m_0, 3) = 1$. Thus, from Lemma 2, we have

$$\frac{\phi(mn)}{\phi(n)} = \frac{\phi(3^{1+r} m_0 k_0)}{\phi(3m_0)} = 3^{1+r}\phi(k_0) = 3,$$

which implies $r = 0$ and contradicts with the assumption. The above property also implies that $n_0 = k_0$ and $\phi(n_0) = \phi(k_0) = 1$, Therefore, we have proved that there are only two possibilities for integer n: either $n_0 = 1$, i.e., $n = 3$, or $n_0 = 2$, i.e., $n = 6$.

Case 1. $n = 3$

In this case, $n_1 = 0$, $n_2 = 1$, and $n_2 = 2$ in (16) and the generating matrix $G_{m,3}$ is Λ_{ζ_m} is:

$$G_{m,3} = \begin{bmatrix} \zeta_N & \zeta_N^2 & \zeta_N^3 \\ \zeta_N^{1+m} & \zeta_N^{2(1+m)} & \zeta_N^{3(1+m)} \\ \zeta_N^{1+2m} & \zeta_N^{2(1+2m)} & \zeta_N^{3(1+2m)} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ \zeta_3 & \zeta_3^2 & \zeta_3^3 \\ \zeta_3^2 & \zeta_3^4 & \zeta_3^6 \end{bmatrix} \begin{bmatrix} \zeta_N & 0 & 0 \\ 0 & \zeta_N^2 & 0 \\ 0 & 0 & \zeta_N^3 \end{bmatrix}.$$

Thus, all the determinants $|\det(G_{m,3})| = 5.1962$ are the same for different integers $m = 3m_0$. From Theorem 3, we know that the best cyclotomic lattice in this class is $\Gamma_3(G_{6,3})$ over Λ_{ζ_6}, or $\Gamma_3(G_{3,3})$ over Λ_{ζ_3}. This proves the theorem.

Case 2. $n = 6$

In this case, $n_0 = 2$. Since $\gcd(m_0, n_0) = 1$, m_0 has to be odd. We next determine integers n_i for $i = 1, 2, 3$ and $0 = n_1 < n_2 < n_3 \leq 5$ such that $1 + n_i m$ and mn are co-prime for $i = 1, 2, 3$. Since m is an odd number, $1 + m$, $1 + 3m$ and $1 + 5m$ are even numbers and therefore have a common factor 2 with $mn = 6m$. Thus, n_i can not be $1, 3$, or 5. This proves that $n_1 = 0$, $n_2 = 2$, and $n_3 = 4$ and the generating matrix $G_{m,3}$ is

$$\begin{aligned} G_{m,6} &= \begin{bmatrix} \zeta_N & \zeta_N^2 & \zeta_N^3 \\ \zeta_N^{1+2m} & \zeta_N^{2(1+2m)} & \zeta_N^{3(1+2m)} \\ \zeta_N^{1+4m} & \zeta_N^{2(1+4m)} & \zeta_N^{3(1+4m)} \end{bmatrix} \\ &= \begin{bmatrix} 1 & 1 & 1 \\ \zeta_6^2 & \zeta_6^4 & \zeta_6^6 \\ \zeta_6^4 & \zeta_6^8 & \zeta_6^{12} \end{bmatrix} \begin{bmatrix} \zeta_N & 0 & 0 \\ 0 & \zeta_N^2 & 0 \\ 0 & 0 & \zeta_N^3 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ \zeta_3 & \zeta_3^2 & \zeta_3^3 \\ \zeta_3^2 & \zeta_3^4 & \zeta_3^6 \end{bmatrix} \begin{bmatrix} \zeta_N & 0 & 0 \\ 0 & \zeta_N^2 & 0 \\ 0 & 0 & \zeta_N^3 \end{bmatrix}. \end{aligned}$$

From Theorem 3, the best cyclotomic lattice in class $\Gamma_3(G_{m,6})$ over Λ_{ζ_m} is $\Gamma_3(G_{3,6})$ over Λ_{ζ_6}.

q.e.d.

It is not hard to see that $G_{3,6}$, $G_{6,3}$ and $G_{3,3}$ are all unitary.

Case of $L_t = 4$

For four transmit antennas, we have the following Theorem.

Theorem 7 *For four transmit antennas, $\Gamma_4(G_{3,5})$ over Λ_{ζ_3}, $\Gamma_4(G_{3,10})$ over Λ_{ζ_3}, and $\Gamma_4(G_{6,5})$ over Λ_{ζ_6} are the optimal cyclotomic lattices with*

$$\frac{d_{min}(\Gamma_4(G_{3,5}))}{|\det(\Lambda_{\zeta_3})|^2 |\det(G_{3,5})|} = \frac{d_{min}(\Gamma_4(G_{3,10}))}{|\det(\Lambda_{\zeta_3})|^2 |\det(G_{3,10})|} = \frac{d_{min}(\Gamma_4(G_{6,5}))}{|\det(\Lambda_{\zeta_6})|^2 |\det(G_{6,5})|} = \frac{4}{3 \times 11.1803},$$

where

$$G_{3,5} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ \zeta_5 & \zeta_5^2 & \zeta_5^3 & \zeta_5^4 \\ \zeta_5^2 & \zeta_5^4 & \zeta_5^6 & \zeta_5^8 \\ \zeta_5^4 & \zeta_5^8 & \zeta_5^{12} & \zeta_5^{16} \end{bmatrix} \begin{bmatrix} \zeta_{15} & 0 & 0 & 0 \\ 0 & \zeta_{15}^2 & 0 & 0 \\ 0 & 0 & \zeta_{15}^3 & 0 \\ 0 & 0 & 0 & \zeta_{15}^4 \end{bmatrix}, \quad G_{3,10} = G_{6,5} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ \zeta_5 & \zeta_5^2 & \zeta_5^3 & \zeta_5^4 \\ \zeta_5^2 & \zeta_5^4 & \zeta_5^6 & \zeta_5^8 \\ \zeta_5^3 & \zeta_5^6 & \zeta_5^9 & \zeta_5^{12} \end{bmatrix} \begin{bmatrix} \zeta_{30} & 0 & 0 & 0 \\ 0 & \zeta_{30}^2 & 0 & 0 \\ 0 & 0 & \zeta_{30}^3 & 0 \\ 0 & 0 & 0 & \zeta_{30}^4 \end{bmatrix}.$$

Proof. It is easy to check that $\Gamma_4(G_{3,5})$ over Λ_{ζ_3}, $\Gamma_4(G_{3,10})$ over Λ_{ζ_3}, and $\Gamma_4(G_{6,5})$ over Λ_{ζ_6} are three 4 dimensional cyclotomic lattices and have the same packing densities and the same minimum products. In the following, we compare them with other 4 dimensional cyclotomic lattices.

To determine a $G_{m,n}$ in (16), we need to determine the 4 integers n_i and integers m and n. Let m and n be integers with $N = mn$ and $\frac{\phi(N)}{\phi(m)} = L_t = 4$. There are two different cases: $\gcd(m,n) = 1$ and $\gcd(m,n) > 1$.

Case 1. $gcd(m,n) = 1$

In this case,

$$\frac{\phi(N)}{\phi(m)} = \phi(n) = 4,$$

and therefore, there are only four cases for integer n: $n = 5$, $n = 8$, $n = 10$, and $n = 12$.

Subcase 1.1. $\gcd(m,n) = 1$ **and** $n = 5$

In this case,

$$G_{m,5} = \begin{bmatrix} \zeta_5^{n_1} & \zeta_5^{2n_1} & \zeta_5^{3n_1} & \zeta_5^{4n_1} \\ \zeta_5^{n_2} & \zeta_5^{2n_2} & \zeta_5^{3n_2} & \zeta_5^{4n_2} \\ \zeta_5^{n_3} & \zeta_5^{2n_3} & \zeta_5^{3n_3} & \zeta_5^{4n_3} \\ \zeta_5^{n_4} & \zeta_5^{2n_4} & \zeta_5^{3n_4} & \zeta_5^{4n_4} \end{bmatrix} \begin{bmatrix} \zeta_N & 0 & 0 & 0 \\ 0 & \zeta_N^2 & 0 & 0 \\ 0 & 0 & \zeta_N^3 & 0 \\ 0 & 0 & 0 & \zeta_N^4 \end{bmatrix},$$

and $0 = n_1 < n_2 < n_3 < n_4 \leq 4$. Since matrix

$$\begin{bmatrix} \zeta_5^{n_1} & \zeta_5^{2n_1} & \zeta_5^{3n_1} & \zeta_5^{4n_1} \\ \zeta_5^{n_2} & \zeta_5^{2n_2} & \zeta_5^{3n_2} & \zeta_5^{4n_2} \\ \zeta_5^{n_3} & \zeta_5^{2n_3} & \zeta_5^{3n_3} & \zeta_5^{4n_3} \\ \zeta_5^{n_4} & \zeta_5^{2n_4} & \zeta_5^{3n_4} & \zeta_5^{4n_4} \end{bmatrix}$$

is a Vandermonde matrix of entry variables $\zeta_5^{n_i}, i = 1, ..., 4$ that take four different values from 5 equally spaced points $\exp\left(\frac{j2k\pi}{5}\right), k = 0, ..., 4$ on the unit circle. The different choices of (n_1, n_2, n_3, n_4) does not change the absolute value of the determinant $|\det(G_{m,5})| = 11.1803$. Therefore, from Theorem 3, the optimal cyclotomic lattices in the class $G_{m,5}$ are $\Gamma_4(G_{3,5})$ and $\Gamma_4(G_{6,5})$ over Λ_{ζ_6}.

Subcase 1.2. $\gcd(m, n) = 1$ **and** $n = 8$

In this subcase, m has to be an odd number. Thus, the four integers n_i in (16) have to be $n_1 = 0, n_2 = 2, n_3 = 4, n_4 = 6$ so that $1 + n_i m$ and $8m$ are co-prime. Thus,

$$G_{m,8} = \begin{bmatrix} \zeta_N & \zeta_N^2 & \zeta_N^3 & \zeta_N^4 \\ \zeta_N^{1+2m} & \zeta_N^{2(1+2m)} & \zeta_N^{3(1+2m)} & \zeta_N^{4(1+2m)} \\ \zeta_N^{1+4m} & \zeta_N^{2(1+4m)} & \zeta_N^{3(1+4m)} & \zeta_N^{4(1+4m)} \\ \zeta_N^{1+6m} & \zeta_N^{2(1+6m)} & \zeta_N^{3(1+6m)} & \zeta_N^{4(1+6m)} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ \zeta_8^2 & \zeta_8^4 & \zeta_8^6 & \zeta_8^8 \\ \zeta_8^4 & \zeta_8^8 & \zeta_8^{12} & \zeta_8^{16} \\ \zeta_8^6 & \zeta_8^{12} & \zeta_8^{18} & \zeta_8^{24} \end{bmatrix} \begin{bmatrix} \zeta_N & 0 & 0 & 0 \\ 0 & \zeta_N^2 & 0 & 0 \\ 0 & 0 & \zeta_N^3 & 0 \\ 0 & 0 & 0 & \zeta_N^4 \end{bmatrix},$$

and their determinant absolute values are the same: $|\det(G_{m,8})| = 16 > 11.1803 = |\det(G_{6,5})|$. From Theorem 3, the optimal cyclotomic lattice can not be in this class.

Subcase 1.3. $\gcd(m, n) = 1$ **and** $n = 10$

In this case, m has to be odd and similar to the previous case, n_i have to be even. Thus, $0 = n_1 < n_2 < n_3 < n_4 \leq 8$ have to take four of the 5 integers $\{0, 2, 4, 6, 8\}$, or $0 = n_1' = \frac{n_1}{2} < n_2' = \frac{n_2}{2} < n_3' = \frac{n_3}{2} < n_4' = \frac{n_4}{2} \leq 4$ have to take four of the 5 integers $\{0, 1, 2, 3, 4\}$ Also, the generating matrix

$$G_{m,10} = \begin{bmatrix} \zeta_{10}^{n_1} & \zeta_{10}^{2n_1} & \zeta_{10}^{3n_1} & \zeta_{10}^{4n_1} \\ \zeta_{10}^{n_2} & \zeta_{10}^{2n_2} & \zeta_{10}^{3n_2} & \zeta_{10}^{4n_2} \\ \zeta_{10}^{n_3} & \zeta_{10}^{2n_3} & \zeta_{10}^{3n_3} & \zeta_{10}^{4n_3} \\ \zeta_{10}^{n_4} & \zeta_{10}^{2n_4} & \zeta_{10}^{3n_4} & \zeta_{10}^{4n_4} \end{bmatrix} \begin{bmatrix} \zeta_N & 0 & 0 & 0 \\ 0 & \zeta_N^2 & 0 & 0 \\ 0 & 0 & \zeta_N^3 & 0 \\ 0 & 0 & 0 & \zeta_N^4 \end{bmatrix} = \begin{bmatrix} \zeta_5^{n_1'} & \zeta_5^{2n_1'} & \zeta_5^{3n_1'} & \zeta_5^{4n_1'} \\ \zeta_5^{n_2'} & \zeta_5^{2n_2'} & \zeta_5^{3n_2'} & \zeta_5^{4n_2'} \\ \zeta_5^{n_3'} & \zeta_5^{2n_3'} & \zeta_5^{3n_3'} & \zeta_5^{4n_3'} \\ \zeta_5^{n_4'} & \zeta_5^{2n_4'} & \zeta_5^{3n_4'} & \zeta_5^{4n_4'} \end{bmatrix} \begin{bmatrix} \zeta_N & 0 & 0 & 0 \\ 0 & \zeta_N^2 & 0 & 0 \\ 0 & 0 & \zeta_N^3 & 0 \\ 0 & 0 & 0 & \zeta_N^4 \end{bmatrix}.$$

Then, it is back to Subcase 1.1.

Subcase 1.4. $\gcd(m, n) = 1$ **and** $n = 12$

In this subcase, m is an odd number, and m can not be divided by 3. The four integers $n_i, i = 1, ..., 4$, in (16) are even number, i.e., $n_i = 2n_i'$ for some integers n_i'. Then, $n_2' < n_3' < n_4' \in \{1, 2, 3, 4, 5\}$. Let $m = 3m_0 + m_1$ for $m_1 = 1$ or $m_1 = 2$. Thus, $1 + 2n_i'm = 6n_i'm_0 + 1 + 2n_i'm_1$. If $m_1 = 1$, then $1 + 2n_i'm$ can be divided by 3 when $n_i' = 1$ or $n_i' = 4$. If $m_1 = 2$, then $1 + 2n_i'm$ can be divided by 3 if $n_i' = 2$ or $n_i' = 5$. Since $1 + n_i m$ has to be co-prime with $n = 12$ and therefore can not be divided by 3, we have

$$(n_2', n_3', n_4') = (2, 3, 5), \quad \text{when} \quad m_1 = 1$$

and

$$(n_2', n_3', n_4') = (1, 3, 4), \quad \text{when} \quad m_1 = 2.$$

On the other hand,

$$G_{m,12}=\begin{bmatrix} \zeta_N & \zeta_N^2 & \zeta_N^3 & \zeta_N^4 \\ \zeta_N^{1+2n_2'm} & \zeta_N^{2(1+2n_2'm)} & \zeta_N^{3(1+2n_2'm)} & \zeta_N^{4(1+2n_2'm)} \\ \zeta_N^{1+2n_3'm} & \zeta_N^{2(1+2n_3'm)} & \zeta_N^{3(1+2n_3'm)} & \zeta_N^{4(1+2n_3'm)} \\ \zeta_N^{1+2n_4'm} & \zeta_N^{2(1+2n_4'm)} & \zeta_N^{3(1+2n_4'm)} & \zeta_N^{4(1+2n_4'm)} \end{bmatrix}=\begin{bmatrix} 1 & 1 & 1 & 1 \\ \zeta_6^{n_2'} & \zeta_6^{2n_2'} & \zeta_6^{3n_2'} & \zeta_6^{4n_2} \\ \zeta_6^{n_3'} & \zeta_6^{2n_3'} & \zeta_6^{3n_3'} & \zeta_6^{4n_3} \\ \zeta_6^{n_4'} & \zeta_6^{2n_4'} & \zeta_6^{3n_4'} & \zeta_6^{4n_4} \end{bmatrix}\begin{bmatrix} \zeta_N & 0 & 0 & 0 \\ 0 & \zeta_N^2 & 0 & 0 \\ 0 & 0 & \zeta_N^3 & 0 \\ 0 & 0 & 0 & \zeta_N^4 \end{bmatrix}.$$

From the above analysis, the two possibilities of integers n_i for $m_1 = 1$ and $m_1 = 2$ correspond to the four points $\{1, \zeta_6^{n_2'}, \zeta_6^{n_3'}, \zeta_6^{n_4'}\}$ and its rotated version on the unit circle and therefore don't change the absolute value of the Vandermonde matrix in the above $G_{m,12}$. Thus,

$$|\det(G_{m,12})| = 12 > 11.1803 = |\det(G_{6,5})|.$$

From Theorem 3, class $\Gamma_4(G_{m,12})$ over Λ_{ζ_m} does not include the optimal one.

Case 2. $\gcd(m,n) > 1$

In this subcase, because

$$4 = \frac{\phi(N)}{\phi(m)} \geq \gcd(m,n),$$

we have $\gcd(m,n) \leq 4$ and $\gcd(m,n)$ is a factor of 4 from Lemma 2. Thus, the common prime factor of m and n can only be 2. Let $n = 2^r n_0$, where n_0 is an odd number. From Lemma 2,

$$4 = \frac{\phi(N)}{\phi(m)} = 2^r \phi(n_0).$$

Therefore, we have two cases:

(i) $r = 1$ and $\phi(n_0) = 2$, i.e., $n_0 = 3, n = 6, m = 2m_0$,

(ii) $r = 2$ and $\phi(n_0) = 1$, i.e., $n_0 = 1, n = 4, m = 2m_0$.

Subcase 2.1. $n = 4$

In this case, the four integers n_i in $G_{m,4}$ in (16) are $0, 1, 2, 3$ and

$$G_{m,4}=\begin{bmatrix} \zeta_N & \zeta_N^2 & \zeta_N^3 & \zeta_N^4 \\ \zeta_N^{1+m} & \zeta_N^{2(1+m)} & \zeta_N^{3(1+m)} & \zeta_N^{4(1+m)} \\ \zeta_N^{1+2m} & \zeta_N^{2(1+2m)} & \zeta_N^{3(1+2m)} & \zeta_N^{4(1+2m)} \\ \zeta_N^{1+3m} & \zeta_N^{2(1+3m)} & \zeta_N^{3(1+3m)} & \zeta_N^{4(1+3m)} \end{bmatrix}=\begin{bmatrix} 1 & 1 & 1 & 1 \\ \zeta_4 & \zeta_4^2 & \zeta_4^3 & \zeta_4^4 \\ \zeta_4^2 & \zeta_4^4 & \zeta_4^6 & \zeta_4^8 \\ \zeta_4^3 & \zeta_4^6 & \zeta_4^9 & \zeta_4^{12} \end{bmatrix}\begin{bmatrix} \zeta_N & 0 & 0 & 0 \\ 0 & \zeta_N^2 & 0 & 0 \\ 0 & 0 & \zeta_N^3 & 0 \\ 0 & 0 & 0 & \zeta_N^4 \end{bmatrix}.$$

Therefore, for all m, the determinant absolute values are the same

$$|\det(G_{m,4})| = 16 > 11.1083 = |\det(G_{6,5})|.$$

From Theorem 3, class $\Gamma_4(G_{m,4})$ over Λ_m does not include the optimal one.

Subcase 2.2. $n = 6$

In this subcase, the four integers n_i satisfy that, $1 + n_i m$ and $N = mn$ are co-primes, and $n_1, n_2, n_3, n_4 \in \{0, 1, 2, 3, 4, 5\}$. Since the only prime common factor of m and 6 is 2, integer m can not be divided by 3. Let $m = 3m_0 + m_1$, $m_1 = 1$ or $m_1 = 2$. Similar to the proof in Subcase 1.4, if we take $n_1 = 0$, we know that,

$$(n_2, n_3, n_4) = (2, 3, 5), \quad \text{when } m_1 = 1$$

and

$$(n_2, n_3, n_4) = (1, 3, 4), \quad \text{when} \;\; m_1 = 2.$$

On the other hand, the generating matrix is

$$G_{m,6} = \begin{bmatrix} \zeta_N & \zeta_N^2 & \zeta_N^3 & \zeta_N^4 \\ \zeta_N^{1+n_2 m} & \zeta_N^{2(1+n_2 m)} & \zeta_N^{3(1+n_2 m)} & \zeta_N^{4(1+n_2 m)} \\ \zeta_N^{1+n_3 m} & \zeta_N^{2(1+n_3 m)} & \zeta_N^{3(1+n_3 m)} & \zeta_N^{4(1+n_3 m)} \\ \zeta_N^{1+n_4 m} & \zeta_N^{2(1+n_4 m)} & \zeta_N^{3(1+n_4 m)} & \zeta_N^{4(1+n_4 m)} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ \zeta_6^{n_1} & \zeta_6^{2n_1} & \zeta_6^{3n_1} & \zeta_6^{4n_1} \\ \zeta_6^{n_2} & \zeta_6^{2n_2} & \zeta_6^{3n_2} & \zeta_6^{4n_2} \\ \zeta_6^{n_3} & \zeta_6^{2n_3} & \zeta_6^{3n_3} & \zeta_6^{4n_2} \end{bmatrix} \begin{bmatrix} \zeta_N & 0 & 0 & 0 \\ 0 & \zeta_N^2 & 0 & 0 \\ 0 & 0 & \zeta_N^3 & 0 \\ 0 & 0 & 0 & \zeta_N^4 \end{bmatrix}.$$

Similar to the proof of Subcase 1.4, for all m, the absolute values of the determinants of $G_{m,6}$ are the same:

$$|\det(G_{m,6})| = 12 > 11.1803 = |\det(G_{6,5})|.$$

From Theorem 3, this class $\Gamma_4(G_{m,6})$ over Λ_{ζ_m} does not include the optimal one.

By summarizing all the above cases, we have proved that $\Gamma_4(G_{3,5})$ and $\Gamma_4(G_{6,5})$ over Λ_{ζ_6} are the optimal cyclotomic lattices for 4 transmit antennas.

q.e.d.

It is easy to check that matrices $G_{3,5}$, $G_{3,10}$, and $G_{6,5}$ are not unitary.

Cases of $L_t = 6, 8, 9$

In this subsection, we present the optimal cyclotomic lattices for six, eight and nine transmit antennas, i.e., $L_t = 6, 8, 9$ without proofs. Their proofs are similar to the ones in Sections 5.1-5.3 by using the same techniques. We also list optimal cyclotomic lattices for some other numbers of transmit antennas.

Theorem 8 *For six transmit antennas, $\Gamma_6(G_{3,7})$ over Λ_{ζ_3}, $\Gamma_6(G_{3,14})$ over Λ_{ζ_3}, and $\Gamma_6(G_{6,7})$ over Λ_{ζ_6} are the optimal cyclotomic lattices with*

$$\frac{d_{min}(\Gamma_6(G_{3,7}))}{|\det(\Lambda_{\zeta_3})|^3 \, |\det(G_{3,7})|} = \frac{d_{min}(\Gamma_6(G_{3,14}))}{|\det(\Lambda_{\zeta_3})|^3 \, |\det(G_{3,14})|} = \frac{d_{min}(\Gamma_6(G_{6,7}))}{|\det(\Lambda_{\zeta_6})|^3 \, |\det(G_{6,7})|} = \frac{8}{3\sqrt{3} \times 129.64},$$

where

$$G_{3,7} = (a_{i,l})_{6\times 6}, a_{i,l} = \zeta_7^{n_i(l-1)} \zeta_{21}^l, n_1 = 0, n_2 = 1, n_3 = 3, n_4 = 4, n_5 = 5, n_6 = 6,$$

$$G_{3,14} = G_{6,7} = (a_{i,l})_{6\times 6}, a_{i,l} = \zeta_7^{n_i(l-1)} \zeta_{42}^l, n_1 = 0, n_2 = 2, n_3 = 3, n_4 = 4, n_5 = 5, n_6 = 6.$$

Theorem 9 *For eight transmit antennas, $\Gamma_8(G_{3,20})$ over Λ_{ζ_3}, $\Gamma_8(G_{4,15})$ over Λ_{ζ_4}, and $\Gamma_8(G_{6,10})$ over Λ_{ζ_6} are the optimal cyclotomic lattices with*

$$\frac{d_{min}(\Gamma_8(G_{3,20}))}{|\det(\Lambda_{\zeta_3})|\,|^4 \det(G_{3,20})|} = \frac{d_{min}(\Gamma_8(G_{4,15}))}{|\det(\Lambda_{\zeta_4})|^4 \, |\det(G_{4,15})|} = \frac{d_{min}(\Gamma_8(G_{6,10}))}{|\det(\Lambda_{\zeta_6})|^4 \, |\det(G_{6,10})|} = \frac{1}{1125},$$

where

$$G_{3,20} = G_{6,10} = (a_{i,l})_{8\times 8},$$

with

$$a_{i,l} = \zeta_{20}^{n_i(l-1)} \zeta_{60}^{l}, \quad (n_1, n_2, n_3, n_4, n_5, n_6, n_7, n_8) = (0, 2, 4, 6, 10, 12, 14, 16);$$

and

$$G_{4,15} = (a_{i,l})_{8\times 8},$$

with

$$a_{i,l} = \zeta_{15}^{n_i(l-1)} \zeta_{60}^{l}, \quad (n_1, n_2, n_3, n_4, n_5, n_6, n_7, n_8) = (0, 3, 4, 7, 9, 10, 12, 13).$$

Theorem 10 *For nine transmit antennas, $\Gamma_9(G_{3,9})$ over Λ_{ζ_3}, $\Gamma_9(G_{3,18})$ over Λ_{ζ_3}, and $\Gamma_9(G_{6,9})$ over Λ_{ζ_6} are the optimal cyclotomic lattices with*

$$\frac{d_{min}(\Gamma_9(G_{3,9}))}{|\det(\Lambda_{\zeta_3})|^{9/2} |\det(G_{3,9})|} = \frac{d_{min}(\Gamma_9(G_{3,18}))}{|\det(\Lambda_{\zeta_3})|^{9/2} |\det(G_{3,18})|} = \frac{d_{min}(\Gamma_9(G_{6,9}))}{|\det(\Lambda_{\zeta_6})|^{9/2} |\det(G_{6,9})|} = \frac{16\times\sqrt{2}}{9\times\sqrt[4]{3}\times 19683},$$

where,

$$G_{3,9} = (a_{i,l})_{9\times 9}, \quad a_{i,l} = \zeta_9^{(i-1)(l-1)} \zeta_{27}^{l};$$

and

$$G_{3,18} = G_{6,9} = (a_{i,l})_{9\times 9}, \quad a_{i,l} = \zeta_9^{(i-1)(l-1)} \zeta_{54}^{l}.$$

Proofs are similar to before.

Other Cases in Theorem 4 can be similarly proved.

References

[1] K. Boulle and J.-C. Belfiore, "Modulation schemes designed for the Rayleigh fading channel," *Proc. CISS'92,* Princeton, NJ, Mar. 1992.

[2] X. Giraud, E. Boutillon, and J.-C. Belfiore, "Algebraic tools to build modulation schemes for fading channels," *IEEE Trans. Inform. Theory*, vol. 43, pp.938-952, May 1997.

[3] J. Boutros and E. Viterbo, "Signal space diversity: a power- and bandwidth-efficient diversity technique for the Rayleigh fading channel," *IEEE Trans. Inform. Theory*, vol. 44, pp. 1453-1467, July 1998.

[4] M. O. Damen, H. El Gamal, and N. C. Beaulieu "A systematic construction of full diversity algebraic constellations," *Proc. Canadian Workshop on Information Theory (CWIT 2003)*, Waterloo, Canada, May 2003.

[5] M. O. Damen, K. A. Meraim, and J.-C. Belfiore, "Diagonal algebraic space-time block codes," *IEEE Trans. Inform. Theory*, vol. 48, pp. 628-636, March 2002.

[6] M. O. Damen, A. Tewfik, and J.-C. Belfiore, "A construction of a space-time code based on number theory," *IEEE Trans. Inform. Theory,* vol.48, pp. 753-760, March 2002.

[7] B. A. Sethuraman and B. Sundar Rajan, "Full-rank space-time block codes from division algebras", Preprint May, 2002. Partially presented in ICC'2002 and ISIT'2002.

[8] V. M. DaSilva and E. S. Sousa, "Fading-resistant modulation using several transmitter antennas," *IEEE Trans. Commun.,* vol.45, pp. 1236-1244, Oct. 1997.

[9] N. Prasad and M. K. Varanasi, "D-BLAST lattice codes for MIMO block Rayleigh fading channels," *40th Annual Allerton Conf. on Comm. Control, and Comput.,* Monticello, IL, Oct., 2002.

[10] J.-C. Guey, M. P. Fitz, M. R. Bell, and W.-Y. Kuo, "Signal design for transmitter diversity wireless communication systems over Rayleigh fading channels," *Proc. IEEE VTC'96*, pp.136-140. Also in *IEEE Trans. Commun.*, vol. 47, pp. 527-537, Apr. 1999.

[11] V. Tarokh, N. Seshadri, and A. R. Calderbank, "Space-time codes for high data rate wireless communication: Performance criterion and code construction," *IEEE Trans. Inform. Theory*, vol. 44, no. 2, pp. 744-765, 1998.

[12] S. Alamouti, "A simple transmit diversity technique for wireless communications," *IEEE J. Select. Areas Commun.*, vol. 16, no. 8, pp. 1451-1458, 1998.

[13] V. Tarokh, H. Jafarkhani, and A. R. Calderbank, "Space-time block codes from orthogonal designs," *IEEE Trans. Inform. Theory*, vol. 45, no. 5, pp. 1456-1467, 1999.

[14] G. Ganesan and P. Stoica, "Space-time block codes: a maximum SNR," *IEEE Trans. Inform. Theory*, vol. 47, no. 4, pp. 1650-1656, 2001.

[15] H. Jafarkhani, "A quasi-orthogonal space-time block code," *IEEE Trans. Commun.,* vol. 49, no.1, pp.1-4,2001.

[16] O. Tirkkonen, A. Boariu, and A. Hottinen, "Minimal non-orthogonality rate 1 space-time block code for 3+ Tx antennas," *IEEE 6th Int. Symp. on Spread-Spectrum Tech. & Appl. (ISSSTA 2000),* pp. 429-432, Sept. 2000.

[17] B. Hassibi and B. M. Hochwald, "High-rate codes that are linear in space and time," *IEEE Trans. Inform. Theory*, vol.48, pp.1473-1484, June 2002.

[18] H. Wang and X.-G. Xia, "Upper bounds of rates of complex orthogonal designs," *IEEE Trans. Inform. Theory*, vol. 49, pp. 2788-2796, Oct. 2003.

[19] W. Su and X.-G. Xia, "Two generalized complex orthogonal space-time block codes of rates 7/11 and 3/5 for 5 and 6 transmit antennas," *IEEE Trans. Inform. Theory*, vol. 49, no. 1, pp. 313-316, 2003.

[20] W. Su and X.-G. Xia, "Signal constellations for quasi-orthogonal space-time block codes with full diversity," *IEEE Trans. Inform. Theory*, submitted, 2002. Also *Proc. Globecom*, Taipei, Dec. 2002.

[21] X.-B. Liang, "Orthogonal designs with maximal rates," *IEEE Trans. Inform. Theory*, vol.49, pp. 2468-2503, Oct. 2003.

[22] W. Su, X.-G. Xia, and K. J. R. Liu, "A systematic design of high-rate complex orthogonal space-time block codes," *IEEE Commun. Letters*, vol. 8, no. 6, pp.380-382, June 2004.

[23] K. Lu, S. Fu, and X.-G. Xia, "Closed form designs of complex orthogonal space-time block codes of rates (k+1)/(2k) for 2k or 2k+1 transmit antennas," submitted to *IEEE Trans. on Information Theory*, Aug. 2003. Also, *Proc. ISIT*, Chicago, June/July 2004.

[24] B. L. Hughes, "Differential space-time modulation," *IEEE Trans. Inform. Theory,* vol.46, no.7, pp. 2567-2578, 2000.

[25] B. L. Hughes, "Optimal space-time constellations from groups," *IEEE Trans. Inform. Theory,* vol.49, pp.401-410, Feb. 2003.

[26] B. M. Hochward and W. Sweldens, "Differential unitary space-time modulation," *IEEE Trans. Commun.,* vol.48, no.12, pp. 2041-2052, 2000.

[27] A. Shokrollahi, B. Hassibi, B. M. Hochward and W. Sweldens, "Representation theory for high-rate multiple-antenna code design," *IEEE Trans. Inform. Theory,* vol.47, pp. 2335-2367, Sept. 2001.

[28] B. Hassibi and B. M. Hochwald, "Cayley differential unitary space-time codes," *IEEE Trans. Inform. Theory*, vol.48, pp.1485-1503, June 2002.

[29] X.-B. Liang and X.-G. Xia, "Unitary signal constellations for space-time modulation with two transmit antennas: Parametric codes, optimal designs, and bounds," *IEEE Trans. Inform. Theory,* vol.48, pp. 2291-2322, Aug. 2002.

[30] W. H. Mow, "Maximum likelihood sequence estimation from the lattice viewpoint," *IEEE Trans, Inform. Theory*, vol.40, pp.1591-1600, Oct. 1994. Also M. Phil. Thesis. Dept. of Inform. Eng., the Chinese Univ. of Hong Kong, June 1991.

[31] W. H. Mow, "Universal lattice decoding: principle and recent advances," *Wireless Commun. Mobile Comput.*, vol.3, pp.553-569, Aug. 2003.

[32] M. O. Damen, K. Abed-Meraim, and J. C. Belfiore, "Generalized sphere decoder for asymmetrical space-time communication architecture," *IEE Electron. Lett.,* vol. 36, pp.166, Jan. 2000.

[33] M. O. Damen, A. Chkeif, and J. C. Belfiore, "Lattice code decoder for space-time codes," *IEEE Commun. Lett.*, vol.4, pp.161-163, May 2000.

[34] H. Vikalo and B. Hassibi, "Maximum-likelihood sequence detection of multiple antenna systems over dispersive channels via sphere decoding," *EURASIP J. Applied Signal Processing,* vol. 2002, no.5, pp.525-531, 2002.

[35] A. R. Hammons, Jr. and H. El Gamal, "On the theory of space time codes for PSK modulation," *IEEE Trans. Inform. Theory*, vol. 46, pp. 524-542, Mar. 2000.

[36] H. El Gamal and A. R. Hammons, Jr., "On the design of algebraic space-time codes for MIMO block-fading channels," *IEEE Trans. Inform. Theory,* vol.49, no. 1, pp. 151-163, Jan. 2003.

[37] Y. Liu, M. P. Fitz, and O. Y. Takeshita, "A rank criterion for QAM space-time codes," *IEEE Trans. Inform. Theory,* vol.48, no. 12, pp. 3062-3079, 2002.

[38] H.-f. Lu and P. V. Kumar, "A unified construction of space-time codes with optimal rate-diversity tradeoff," submitted to *IEEE Trans. Inform. Theory*, 2003.

[39] H.-f. Lu and P. V. Kumar, "Rate-diversity tradeoff of space-time codes with fixed alphabet and optimal constructions for PSK modulation," *IEEE Trans. Inform. Theory*, vol.49, pp. 2747-2751, Oct. 2003.

[40] S. Lang, *Algebraic Number Fields*, Springer-Verlag, New York, 1986.

[41] D. A. Marcus, *Number Fields*, Springer-Verlag, New York, 1977.

[42] J. Rotman, *Galois Theory*, Springer-Verlag, New York, 1990.

[43] P. Morandi, *Field and Galois Theory*, erlag, New York, 1996.

[44] I. Stewart, and D. Tall, *Algebraic Number Theory and Fermat's Last Theorem*, 3rd Ed., A K Peters, Natick, Massachusetts, 2002.

[45] J. H. Conway, and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, 3rd Ed., Springer-Verlag, New York, 1998.

[46] G. Wang and X.-G. Xia, "On optimal cyclotomic lattices and diagonal/single-layer space-time block codes," *Proc. ISIT 2004*, June 27-July 2, Chicago, USA, 2004.

[47] G. Wang and X.-G. Xia, "On optimal multi-layer cyclotomic space-time code designs," submitted to *IEEE Trans. Inform. Theory*, Nov. 2003.

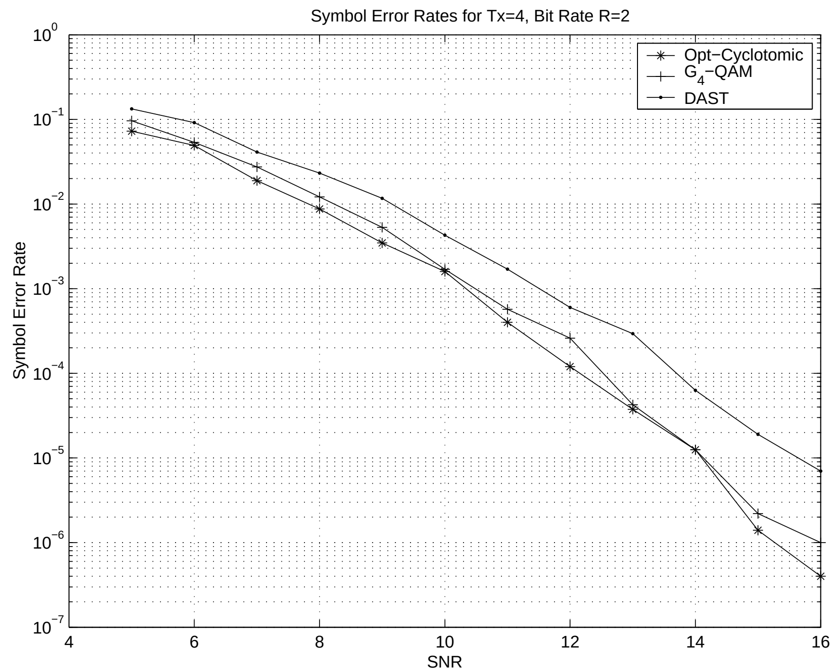

Figure 1: Codeword error rate comparisons: 4 transmit antennas, 2 receive antennas, and 2 bits/s/Hz.

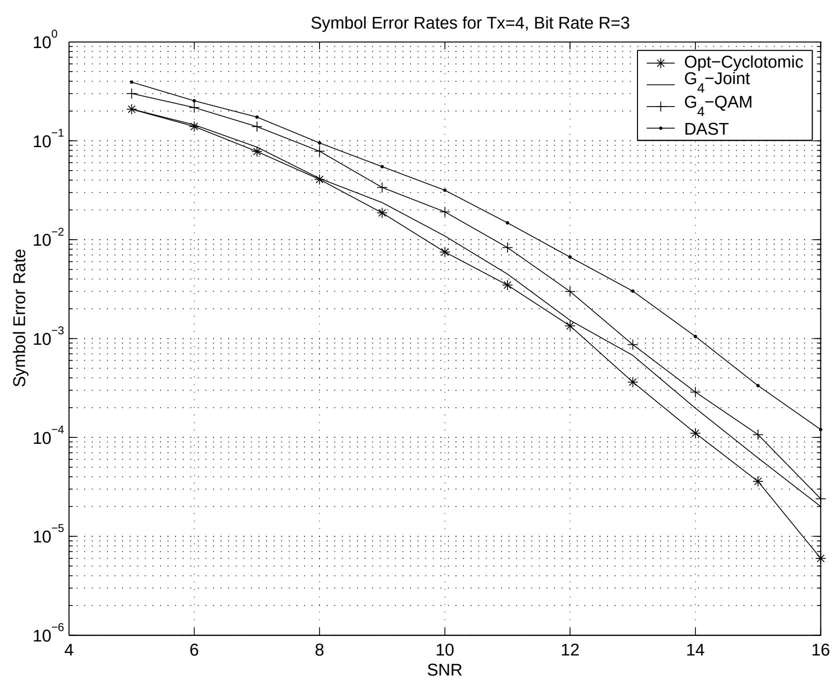

Figure 2: Codeword error rate comparisons: 4 transmit antennas, 2 receive antennas, and 3 bits/s/Hz.

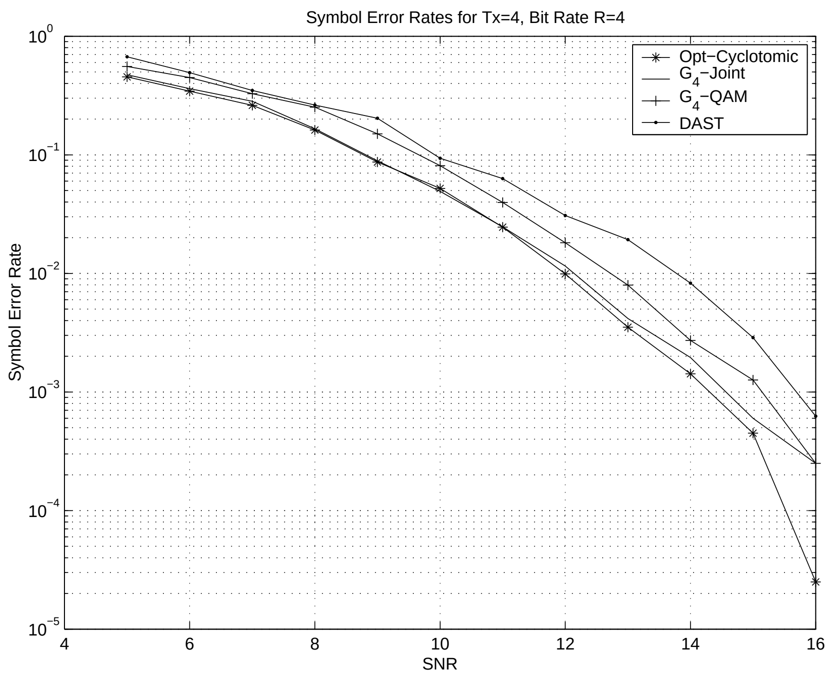

Figure 3: Codeword error rate comparisons: 4 transmit antennas, 2 receive antennas, and 4 bits/s/Hz.