On Optimal Multilayer Cyclotomic Space–Time Code Designs

Genyuan Wang and Xiang-Gen Xia, *Senior Member, IEEE*

***Abstract*—High rate and large diversity product (or coding advantage, or coding gain, or determinant distance, or minimum product distance) are two of the most important criteria often used for good space–time code designs. In recent (linear) lattice-based space–time code designs, more attention is paid to the high rate criterion but less to the large diversity product criterion. In this paper, we consider these two criteria together for multilayer cyclotomic space–time code designs. In a previous paper, we recently proposed a systematic cyclotomic diagonal space–time code design over a general cyclotomic number ring that has infinitely many designs for a fixed number of transmit antennas, where diagonal codes correspond to single-layer codes in this paper. In this paper, we first propose a general multilayer cyclotomic space–time codes. We present a general optimality theorem for these infinitely many cyclotomic diagonal (or single-layer) space–time codes over general cyclotomic number rings for a general number of transmit antennas. We then present optimal multilayer (full-rate) cyclotomic space–time code designs for two and three transmit antennas. We also present an optimal two-layer cyclotomic space–time code design for three and four transmit antennas. The optimality here is in the sense that, for a fixed mean transmission signal power, its diversity product is maximized, or equivalently, for a fixed diversity product, its mean transmission signal power is minimized. It should be emphasized that all the optimal multilayer cyclotomic space–time codes presented in this paper have the nonvanishing determinant property.**

***Index Terms*—Algebraic number theory, cyclotomic number rings and lattices, diversity product, full rate, multilayer space–time block codes, nonvanishing determinant.**

I. Introduction

LINEAR lattice based space–time block code designs from algebraic number rings/fields have recently attracted much attention, see for example [1]–[14], mainly due to the possibility of systematic constructions of full diversity and high rate codes, and their fast sphere decoding/demodulation [29]–[36]. Lattice-based diagonal space–time codes [4] are constructed based on lattices $[\boldsymbol{y}_1,\ldots,\boldsymbol{y}_{L_t}]^T = G[\boldsymbol{x}_1,\ldots,\boldsymbol{x}_{L_t}]^T$, where L_t is the number of transmit antennas, ^{T} stands for the transpose, $\boldsymbol{x}_i$ represent complex-valued information symbols, and G is a generating matrix, and $\boldsymbol{y}_i$ are placed as diagonal elements. This was motivated from the designs of full diversity multidimensional signal constellations for resisting both Rayleigh fading and Gaussian additive noises proposed in [1]–[3]. By properly selecting the generating matrix G and the information signal alphabet of $\boldsymbol{x}_i$, the diversity product 1 is guaranteed by a result in algebraic number theory [37], [38]. However, the symbol rate for the above diagonal codes is only 1. Orthogonal space–time block codes [22]–[28] are also lattice-based codes but their symbol rates cannot be above 1 [23], [27], [28]. Higher rate space–time codes have been proposed earlier in Bell Labs layered space–time (BLAST) architecture [15], linear dispersion codes [17]–[19], and threaded/multilayer codes [16]. By employing some algebraic number theory, lattice-based full-rate and full diversity threaded/multilayer space–time codes were later proposed in [5], [7], [8], [10], [11], [13], [12]. In these studies, not much has been discussed on the diversity product (or the so-called coding advantage, coding gain, determinant distance, or minimum product distance in the literature) issue while diversity product plays an important role in determining the symbol error rates (SER), see, for example, [20], [21]. Although for diagonal lattice-based space–time codes, the diversity products are fixed to 1 in the existing designs, their mean transmission signal powers could be different and the codes with the minimum mean transmission signal power would be optimal and preferred. In what follows, the optimality is always in the sense that the diversity product is maximal when the mean transmission signal power is fixed or equivalently the mean transmission signal power is minimized when the diversity product is fixed. Different optimality criteria, such as the peak-to-average power ratio (PAPR) and receiver complexity, have been considered in [12].

To address the above optimality, we need to have a broad class of valid (such as full diversity) codes with the same parameters including rates and sizes. For the above lattice-based space–time codes, there are three issues that may affect the code performance as pointed in [14]: i) where the information symbols $\boldsymbol{x}_i$ belong to; ii) where the elements of the generating matrix G belong to; and iii) whether the generating matrix G is unitary. In [14], these three issues were considered together in a general way and a more general cyclotomic space–time code design was proposed, where information symbols $\boldsymbol{x}_i$ 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, and information symbols $\boldsymbol{x}_i$ and elements of generating matrix G are from general cyclotomic field extensions. A systematic construction of cyclotomic diagonal space–time codes of full diversity was given in [14] for a general number of transmit antennas, where for a fixed

Manuscript received November 17, 2003; revised June 24, 2004. This work was supported in part by the Air Force Office of Scientific Research under Grant F49620-02-1-0157 and by the National Science Foundation under Grants CCR-0097240 and CCR-0325180.

The authors are with the Department of Electrical and Computer Engineering, University of Delaware, Newark, DE 19716 USA (e-mail: gwang @ee.udel.edu; xxia @ee.udel.edu).

Communicated by Ø. Ytrehus, Associate Editor for Coding Techniques.
Digital Object Identifier 10.1109/TIT.2004.842630

number of transmit antennas, there are infinitely many cyclotomic space–time codes/lattices. In [14], the optimality was converted to a criterion on the lattice generating matrix G by using the lattice packing theory, see, for example, [42]. Based on the criterion on matrix G, some optimal cyclotomic diagonal space–time codes or lattices were found for some specific numbers of transmit antennas but a general optimality theorem for a general number of transmit antennas has remained open. In [14], we also found that most existing ones in the literature are not optimal and most of the optimal generating matrices are not unitary.

In this paper, we first propose a more general multilayer cyclotomic space–time code design than the existing ones in the sense that cyclotomic lattices on different layers can be different and are of different mean powers. We then present a general optimality theorem for single-layer (or diagonal) cyclotomic space–time codes for a general number of transmit antennas, which solves the open problem that remains in [14]. We then present optimal multilayer cyclotomic space–time codes of full rate and full diversity for two and three transmit antennas. We also present optimal two-layer cyclotomic space–time codes for three and four transmit antennas. Similar to [14] for single-layer codes, we find that most of the existing multilayer codes are not optimal and the optimal generating matrices are usually not unitary. Although the optimal generating matrices are not unitary, the optimal codes do not have significant "capacity" loss. In addition, we emphasize that all the optimal multilayer cyclotomic space–time codes presented in this paper have the nonvanishing determinant property.

This paper is organized as follows. In Section II, we describe the problem in more details and briefly introduce the general cyclotomic lattices and diagonal cyclotomic space–time codes obtained previously in [14] as it is necessary for this paper to be self-contained . In Section III, we first introduce a systematic design of multilayer cyclotomic space–time codes, study the relationships between a generating matrix and its corresponding lattice, transmission signal mean power, and diversity product. We then present the optimality results on single-layer and multilayer cyclotomic space–time codes. In Section IV, we present some numerical simulation results. All lengthy proofs of the optimality theorems are in the Appendix.

The following notations are used throughout this paper: capital English letters, such as, K and G, represent matrices and bold face lower case English letters, such as $\boldsymbol{x}$ and $\boldsymbol{y}$, represent complex symbols (or numbers or points) on two-dimensional real lattices, lower case 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 number of positive integer n.
ζ_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 $K_{\zeta_m} = \begin{bmatrix} 1 & \cos(\frac{2\pi}{m}) \\ 0 & \sin(\frac{2\pi}{m}) \end{bmatrix}$.
Ω:	a set of space–time codeword matrices.
X:	a linear lattice based space–time code structure, such as the threaded/multilayer structure.
$[\mathbb{E}:\mathbb{F}]$:	the extension degree of field $\mathbb{E}$ over field $\mathbb{F}$.
^{H}:	complex conjugate and transpose.
$\otimes$:	Kronecker (or tensor) product.
$A = B \boxtimes C$	means $\lvert\det(A)\rvert = \lvert\det(A \otimes B)\rvert$.
$A^{\boxtimes i}$	$= \underbrace{A \boxtimes \cdots \boxtimes A}_{i}$.

II. Some Notations, Complex Lattices, and Cyclotomic Lattices

In this section, we first briefly describe some commonly used criteria, i.e., rank, diversity product, and symbol rate, in space–time code design, and then briefly review some necessary concepts on complex lattices and cyclotomic lattices proposed in [14] that shall be used in this paper. We also generalize some of these concepts for the purpose of constructing multilayer space–time codes.

A. Rank, Diversity Product, and Symbol Rate Criteria

Let L_t and L_r be the numbers of transmit and receive antennas, respectively, and Ω be a space–time code. The channel is assumed quasi-static. Let $C, E \in \Omega$ be two different space–time codeword matrices. Then, the pairwise error probability $\Pr\{C \to E\}$ of the coherent maximum-likelihood (ML) detection is upper-bounded by ([20], [21])

$$\Pr\{C \to E\} \le \frac{1}{2}\left(\prod_{i=1}^{r}\lambda_i\right)^{-L_r}\left(\frac{\eta}{4}\right)^{-rL_r} \tag{1}$$

where r is the rank of the difference matrix $C - E$, η is the signal-to-noise ratio (SNR) at the receive antennas, and λ_i, $i = 1, \ldots, r$, are the r nonzero eigenvalues of $(C-E)(C-E)^H$ and ^{H} stands for the Hermitian operation, i.e., complex conjugate and transpose.

Rank Criterion: A space–time code Ω is called to achieve *full diversity* if the rank of difference matrix $C - E$ is L_t, i.e., $r = L_t$ in (1), for any two different codeword matrices C and E in Ω. From (1) one can see that this criterion governs the SER at high SNR.

Determinant Criterion: When full diversity is achieved, the SER depends on the *diversity product* (or called coding advantage, coding gain, or minimum product distance in other literatures), which is defined by

$$d_{\min}(\Omega) = \min_{C\neq E\in\Omega} \left|\det(C-E)(C-E)^H\right|^{1/2} = \min_{C\neq E\in\Omega} \prod_{i=1}^{L_t} \lambda_i^{1/2}. \quad (2)$$

From (1) one can see that the larger the diversity product, the smaller is the upper bound of the SER.

Symbol Rate Criterion: Another criterion is symbol rate criterion, which is determined by the number of the distinct codeword matrices in Ω. In a linear space–time block code, the symbol rate is defined as follows. An information sequence is first mapped to k information symbols $s_1, s_2, \ldots, s_k$, in a constellation, for example, quadrature amplitude modulation (QAM), then these k information symbols are linearly placed into a space–time code matrix design X of time block size B. The symbol rate is defined by $R = k/B$ symbols per channel use (pcu). A space–time code with L_t transmit antennas is called to achieve *full rate* if its symbol rate is $R = L_t$ symbols pcu.

There have been considerable studies recently on full rate and full diversity space–time code designs, see, for example, [5], [7], [8], [10], [11], [13], [12] but not much studies on space–time code designs of full rate full diversity and large diversity product. The main emphasis in this paper is on the designs of full rate full diversity space–time codes with large (optimal) diversity product. In what follows, we say that a space–time code X_1 is *better* than another space–time code X_2 if the mean transmission signal power of X_1 is smaller than that of X_2, when their diversity products are the same and their symbol rates are the same. To do so, we first recall and generalize some concepts on lattices proposed and used in [14].

B. Real and Complex Lattices

We first define a real lattice.

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

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

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 $\det(\Lambda_n(K)) \triangleq |\det(K)|$.

It is clear that $\Lambda_n(K)$ is a subgroup of $\mathbb{R}^n$ with componentwise 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 $\boldsymbol{x} = x_1 + jx_2$ in the complex plane $\mathbb{C}$. In this paper, we do not distinguish between a two-dimensional real point $[x_1, x_2]^T \in \mathbb{R}^2$ and a complex number or point $\boldsymbol{x} = x_1 + jx_2 \in \mathbb{C}$; 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

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

where Re and Im stand for the real and imaginary parts of a complex number, respectively. Thus, $\Lambda_{\zeta_m} = \Lambda_2(K_{\zeta_m})$. It is easy to check that

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

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 $\mathbb{C}^n$

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

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

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

for any nonzero vector

$$[\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n]^T \neq [0, \ldots, 0]^T$$

in $(\Lambda_2(K))^n$.

With complex lattice points $[\boldsymbol{y}_1, \ldots, \boldsymbol{y}_n]^T$, a diagonal lattice-based space–time code X can be designed by placing these n components into the diagonal elements as $X = \mathrm{diag}(\boldsymbol{y}_1, \ldots, \boldsymbol{y}_n)$ and thus, its diversity product is

$$d_{\min}(G) \triangleq \min_{[\boldsymbol{x}_1,\ldots,\boldsymbol{x}_n]^T \neq [0,\ldots,0]^T} \prod_{i=1}^{n} |\boldsymbol{y}_i|.$$

For this diagonal space–time code, one is interested in its signal mean power of $\boldsymbol{y}_i$ and its diversity product $d_{\min}(G)$ in the sense that either the signal mean power is minimized when the diversity product is fixed or the diversity product is maximized when the signal mean power is fixed. To study the signal mean power, it is important to study the compactness of the lattice. To do so, the above complex lattice needs to be converted to a real lattice.

In Definition 2, points $\boldsymbol{x}_i$ from a two-dimensional real lattice have been treated as complex numbers explained previously and therefore $\boldsymbol{y}_i$ are also complex numbers. On the other hand, if we treat all complex elements in matrix G and $\boldsymbol{x}_i$ and $\boldsymbol{y}_i$ 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 follows.

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 $\{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n\}$ be n points on a two-dimensional real lattice $\Lambda_2(K)$ with generating matrix K. Let

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

Then, $[\boldsymbol{y}_1, \ldots, \boldsymbol{y}_n]^T$ is a point on the n-dimensional complex lattice $\Gamma_n(G)$ over $\Lambda_2(K)$.

We now rewrite $\boldsymbol{y}_i$ with its real part y_{R_i} and imaginary part y_{I_i} as $\boldsymbol{y}_i = y_{R_i} + jy_{I_i}$ 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 $\mathcal{G}_K \triangleq \mathcal{G} \cdot \mathrm{diag}(K, \ldots, K)$. Following Definition 1, in order to show that $\mathcal{G}_K$ is a real generating matrix of a $2n$-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 a two-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 a $2n$-dimensional real lattice $\Lambda_{2n}(\mathcal{G}_K)$.

Proposition 1: [14] 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, $|\det(\mathcal{G})| = |\det(G)|^2$.

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:

$$\begin{aligned} |\det(\mathcal{G}_K)| &= |\det(G)|^2 \cdot |\det(K)|^n \\ &= |\det(G)|^2 \cdot |\det(\Lambda_2(K))|^n. \end{aligned} \tag{11}$$

C. Composed Complex Lattices

We now generalize the above complex lattices used in [14] for diagonal (single-layer) space–time codes to composed complex lattices to be used later for multilayer space–time codes.

Definition 3: An nL-dimensional composed complex lattice $\Gamma_{nL}(G_1, \ldots, G_L)$ over $\Lambda_2(K_1) \times \cdots \times \Lambda_2(K_L)$ consists of all points $[\boldsymbol{y}_1, \ldots, \boldsymbol{y}_n, \boldsymbol{y}_{n+1}, \ldots, \boldsymbol{y}_{nL}]^T$, where each segment $[\boldsymbol{y}_{(l-1)n+1}, \ldots, \boldsymbol{y}_{ln}]^T$ of length n belongs to complex lattice $\Gamma_n(G_l)$ over $\Lambda_2(K_l)$, i.e.,

$$\begin{bmatrix} \boldsymbol{y}_{(l-1)n+1} \\ \vdots \\ \boldsymbol{y}_{ln} \end{bmatrix} = G_l \begin{bmatrix} \boldsymbol{x}_{(l-1)n+1} \\ \vdots \\ \boldsymbol{x}_{ln} \end{bmatrix} \quad \text{for } \boldsymbol{x}_{(l-1)n+i} \in \Lambda_2(K_l), \quad \text{for } 1 \le i \le n, 1 \le l \le L.$$

In fact, the above composed complex lattice definition can be stated in a more general form by simply relaxing $\boldsymbol{x}_i$ from a single two-dimensional real lattice $\Lambda_2(K)$ to several two-dimensional real lattices $\Lambda_2(K_l)$ in Definition 2. In this paper, we are only interested in the one in Definition 3 due to the special structure of multilayer cyclotomic space–time code designs later.

Similarly to a complex lattice, an nL-dimensional composed complex lattice can also be represented by a $2nL$-dimensional real lattice of generating matrix $\mathcal{G}_{K_1,\ldots,K_L}$ and the following determinant relationship holds:

$$|\det(\mathcal{G}_{K_1,\ldots,K_L})| = \prod_{l=1}^{L} |\det(G_l)|^2 \cdot |\det(K_l)|^n \tag{12}$$

which determines the packing compactness of the composed complex lattice as we shall see in the following subsection. With an nL-dimensional composed complex lattice, a linear lattice-based space–time code X of size $n \times n$ can be formed by placing these nL complex numbers $\boldsymbol{y}_i$ in X where each component of X is either $\boldsymbol{y}_i$ or 0 and each $\boldsymbol{y}_i$ appears once and only once (assume $L \le n$). In this way, the mean transmission signal power is the same as the composed complex lattice points or its equivalent real lattice points. When the placing rule in X in terms of $\boldsymbol{y}_i$ is fixed, such as the multilayer or threaded structure later, a space–time code design becomes a composed complex lattice design.

D. 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, [42] and for more de-

tails, we refer the reader to [42]. 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 [42, pp. 10 and 13]. It is mentioned in [42, p. 13] 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, on 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 lesser of the value $\det(\Lambda_n)$, 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 lower the value of $\det(\Lambda_n)$ or, equivalently, the lower the absolute value of the determinant of its generating matrix, the smaller is the mean signal power of the signal points in $\mathcal{S}$. This is the base for the following criterion of justifying that one composed complex lattice is better than the other composed complex lattice.

E. Criterion for Composed Complex Lattices for a Fixed Space–Time Code Structure

In this subsection, the space–time code matrix structure X, such as linear diagonal codes or linear threaded codes, is fixed and as mentioned previously, an nL-dimensional composed complex lattice $\Gamma_{nL}(G_1, \ldots, G_L)$ is used to place its components into the space–time code matrix X and designed one is denoted as $X(G_1, \ldots, G_L)$. The purpose of this subsection is to present a criterion on the design of a composed complex lattice such that the space–time code X with this lattice has a larger diversity product for a fixed mean signal power or smaller mean signal power for a fixed diversity product, where the diversity product is

$$d_{\min}(G_1, \ldots, G_L) \triangleq \min_{[\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{nL}]^T \neq [0, \ldots, 0]^T} \det(X(G_1, \ldots, G_L)). \tag{13}$$

From the discussions in the previous subsections, any nL-dimensional composed complex lattice can be converted to a $2nL$-dimensional real lattice and their corresponding signal powers are exactly the same. With the argument in the previous subsection and (12) we are ready to present a criterion to choose a composed complex lattice.

Definition 4: Let $\Gamma_{nL}(G_1, \ldots, G_L)$ and $\Gamma_{nL}(G'_1, \ldots, G'_L)$ be two nL-dimensional composed complex lattices over $\Lambda_2(K_1) \times \cdots \times \Lambda_2(K_L)$ and $\Lambda_2(K'_1) \times \cdots \times \Lambda_2(K'_L)$, respectively. We say composed complex lattice $\Gamma_{nL}(G_1, \ldots, G_L)$ is *better than* composed complex lattice $\Gamma_{nL}(G'_1, \ldots, G'_L)$, written as

$$\Gamma_{nL}(G_1, \ldots, G_L) \leq \Gamma_{nL}(G'_1, \ldots, G'_L)$$

if

$$\prod_{l=1}^{L} |\det(G_l)| \cdot |\det(K_l)|^{n/2} \leq \prod_{l=1}^{L} |\det(G'_l)| \cdot |\det(K'_l)|^{n/2}$$

when their diversity products are the same, i.e.,

$$d_{\min}(G_1, \ldots, G_L) = d_{\min}(G'_1, \ldots, G'_L)$$

where the diversity products are from (13).

When two diversity products are not the same, the two composed complex lattices can be normalized similar to what is done in [14] for diagonal codes and the following lemma is not hard to see.

Lemma 1: Let $\Gamma_{nL}(G_1, \ldots, G_L)$ and $\Gamma_{nL}(G'_1, \ldots, G'_L)$ be two nL-dimensional composed complex lattices over $\Lambda_2(K_1) \times \cdots \times \Lambda_2(K_L)$ and $\Lambda_2(K'_1) \times \cdots \times \Lambda_2(K'_L)$, respectively. The composed complex lattice $\Gamma_{nL}(G_1, \ldots, G_L)$ is better than the composed complex lattice $\Gamma_{nL}(G'_1, \ldots, G'_L)$, if

$$\frac{d_{\min}(G_1, \ldots, G_L)}{\prod_{l=1}^{L} |\det(G_l)| \cdot |\det(K_l)|^{n/2}} \geq \frac{d_{\min}(G'_1, \ldots, G'_L)}{\prod_{l=1}^{L} |\det(G'_l)| \cdot |\det(K'_l)|^{n/2}}. \tag{14}$$

These results coincide with the results presented in [14] for diagonal cyclotomic space–time codes and cyclotomic lattices when $L = 1$ and all n lattice components in $\Gamma_n(G)$ are placed in the diagonal elements of X, which is, in fact, a single-layer cyclotomic space–time code as we shall see later.

F. Cyclotomic Lattices and Diagonal/Single-Layer Cyclotomic Space–Time Codes

In this subsection, we recall cyclotomic lattices and diagonal cyclotomic space–time codes and some of their fundamental properties obtained in [14]. 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 numbers[1] of N and m, respectively, and L_t corresponds to the number of transmit antennas in a space–time code. Then, there is a total of L_t distinct integers l_i, $1 \leq i \leq L_t$, with $0 = l_1 < l_2 < \cdots < l_{L_t} \leq n-1$ such that $1 + l_i m$ and N are coprime for any $1 \leq i \leq L_t$ (see for example [39, p. 75]). With these L_t integers, we define

$$G_{m,n} \triangleq \begin{bmatrix} \zeta_N & \zeta_N^2 & \cdots & \zeta_N^{L_t} \\ \zeta_N^{1+l_2 m} & \zeta_N^{2(1+l_2 m)} & \cdots & \zeta_N^{L_t(1+l_2 m)} \\ \vdots & \vdots & \ddots & \vdots \\ \zeta_N^{1+l_{L_t} m} & \zeta_N^{2(1+l_{L_t} m)} & \cdots & \zeta_N^{L_t(1+l_{L_t} m)} \end{bmatrix}_{L_t \times L_t} \tag{16}$$

where $\zeta_N = \exp(j\frac{2\pi}{N})$. One can easily check that the above $G_{m,n}$ is unitary when $n = L_t$. It is not hard to see that matrix $G_{m,n}$ has full rank since it is a Vandermonde matrix and

[1]The Euler number (or Euler function) $\phi(N)$ of N is the number of positive integers that are less than N and coprime 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 [40]. It also implies that L_t is always an integer.

$\zeta_N^{1+l_{i_1}m} - \zeta_N^{1+l_{i_2}m} \neq 0$ for $1 \leq i_1 \neq i_2 \leq L_t$. This means that matrix $G_{m,n}$ is eligible to be a generating matrix of a complex lattice as we defined in Section II-A. We now define cyclotomic lattices.

Definition 5: 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

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

A cyclotomic lattice is a complex lattice. The above minimum product (17) for a complex lattice coincides with the diversity product defined in (13) when the space–time code structure X is diagonal. With a cyclotomic lattice, a diagonal (or single-layer) cyclotomic space–time code is defined as follows.

Definition 6: A diagonal cyclotomic space–time code Ω for L_t transmit antennas is defined by $\Omega = \{\mathrm{diag}(\boldsymbol{y}_1, \ldots, \boldsymbol{y}_{L_t})\}$ where $\boldsymbol{y}_i$ for $1 \leq i \leq L_t$ are defined as follows:

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

where $G_{m,n}$ is defined in (16),

$$[\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{L_t}]^T \in \mathcal{S} \subset (\mathbb{Z}[\zeta_m])^{L_t},$$

and $\mathcal{S}$ is a signal constellation for information symbols.

By employing some theory on cyclotomic number rings/fields, the following result was obtained in [14].

Theorem 1: [14] A cyclotomic lattice is a full diversity lattice and a diagonal cyclotomic space–time code has full diversity.

The novelty of the above general cyclotomic space–time lattices and codes presented in [14] is that the generating matrix $G_{m,n}$ is *concretely* found and given for any cyclotomic ring $\mathbb{Z}[\zeta_m]$ of any ζ_m for the full diversity, which has not yet appeared in the literature in the area where a discrete Fourier transform matrix that corresponds to the case when $L_t = n$ in the above $G_{m,n}$ or a Hadamard transform is commonly used.

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 was proved in [37], [38] that the minimum products of Gaussian cyclotomic lattices and Eisenstein cyclotomic lattices are 1.

From the above cyclotomic lattices, one can see that, for a fixed L_t in (15), there are infinite options of integer m and thus, infinite options of cyclotomic number ring $\mathbb{Z}[\zeta_m]$ or lattices 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? Several small numbers L_t of transmit antennas have been considered in [14]. In the next section, we present a general optimality theorem for a general L_t, which is cast in the single-layer cyclotomic space–time code context as a special case of the multilayer one.

[2]In [4], it is called minimum product diversity. The reason why we use the 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.

III. Multilayer Cyclotomic Space–Time Code Designs

In this section, we first propose a general structure of multilayer cyclotomic space–time codes. We then present optimal single-layer cyclotomic space–time codes for a general number of transmit antennas. We then present optimal multilayer cyclotomic space–time codes of full rates for two and three transmit antennas. We also present optimal two-layer cyclotomic space–time codes for three and four transmit antennas. After presenting the optimality results, we then propose three methods of selecting lattice points for a set of codeword matrices of a space–time code. Since the optimal multilayer cyclotomic space–time codes we find are not unitary as we shall see later, in this section we finally discuss the capacity issue.

A. A General Structure of Multilayer Cyclotomic Space–Time Codes

Following the general structure of threaded space–time codes in [16], we propose the following general multilayer cyclotomic space–time codes (i.e., code structure X as mentioned previously) that will be optimized later in terms of the mean transmission signal power and the diversity product.

Definition 7: Let L_t be the number of transmit antennas and $\Gamma_{L_t}(G_{m_l,n_l})$ be an L_t-dimensional cyclotomic lattice as defined in Section II-F, where G_{m_l,n_l} is defined in (16), for $l = 1, 2, \ldots, L_t$. Let $\rho_1, \ldots, \rho_{L_t}$ be L_t fixed complex numbers. Then, a multilayer cyclotomic space–time code structure is defined by (19) at the bottom of the page, where $[\boldsymbol{y}_l(1), \ldots, \boldsymbol{y}_l(L_t)]^T$ is a point in cyclotomic lattice $\Gamma_{L_t}(G_{m_l,n_l})$ for $l = 1, \ldots, L_t$. This multilayer cyclotomic space–time code is denoted by

$$X(\rho_1 G_{m_1,n_1}, \ldots, \rho_{L_t} G_{m_{L_t},n_{L_t}}).$$

An L-layer cyclotomic space–time code with $1 \leq L \leq L_t$ is defined as a multilayer cyclotomic space–time code

$$\begin{bmatrix} \rho_1\boldsymbol{y}_1(1) & \rho_2\boldsymbol{y}_2(1) & \cdots & \rho_{L_t-1}\boldsymbol{y}_{L_t-1}(1) & \rho_{L_t}\boldsymbol{y}_{L_t}(1) \\ \rho_{L_t}\boldsymbol{y}_{L_t}(2) & \rho_1\boldsymbol{y}_1(2) & \cdots & \rho_{L_t-2}\boldsymbol{y}_{L_t-2}(2) & \rho_{L_t-1}\boldsymbol{y}_{L_t-1}(2) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \rho_2\boldsymbol{y}_2(L_t) & \rho_3\boldsymbol{y}_3(L_t) & \cdots & \rho_{L_t}\boldsymbol{y}_{L_t}(L_t) & \rho_1\boldsymbol{y}_1(L_t) \end{bmatrix} \tag{19}$$

$X(\rho_1 G_{m_1,n_1},\ldots,\rho_{L_t} G_{m_{L_t},n_{L_t}})$ when $\rho_l = 0$ for $l > L$ and denoted by $X(\rho_1 G_{m_1,n_1},\ldots,\rho_L G_{m_L,n_L})$.

We now have the following result on the full diversity property for the above multilayer codes.

Theorem 2: For any integer L, with $1 \le L \le L_t$, an L-layer cyclotomic space time code

$$X(\rho_1 G_{m_1,n_1},\ldots,\rho_L G_{m_L,n_L})$$

in (19) has full diversity if $\rho_l = \rho_0^{l-1}$, $l = 1,\ldots,L$, satisfy one of the following conditions:

i) $\rho_0 = \zeta_{N_0}$ with $N_0 = n_0 \mathrm{lcm}(N_1,\ldots,N_L)$ and
$$n_0 = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}, \qquad n_0 \ge L_t(L-1)+1$$
where $p_1,\ldots,p_k$ are some prime factors of $\mathrm{lcm}(N_1,\ldots,N_L)$;

ii) $\rho_0 = e^{j\lambda}$ for an algebraic $\lambda \ne 0$, i.e., ρ_0 is transcendental;

iii) $\rho_0 = \sqrt{\beta}^{1/L_t}\zeta_{N_0'}$ with a proper integer β and $N_0' \le N_0$ with the same N_0 as in i);
where $N_l = m_l n_l$, with
$$L_t = \frac{\phi(m_l n_l)}{\phi(m_l)}, \qquad \text{for } l = 1,\ldots,L$$
and lcm stands for the least common multiple.

Proof: It is not hard to see that the determinant of any nonzero codeword is a nonzero polynomial of ρ_0 of order less than or equal to $L_t(L-1)$ with coefficients in $\mathbb{Q}(\zeta_{\mathrm{lcm}(N_1,\ldots,N_L)})$. Thus, the full diversity property is equivalent to stating that ρ_0 is not a root of such a polynomial.

Let us first consider condition i). By the definitions of N_0 and ζ_{N_0}, we know that $\mathbb{Q}(\zeta_{\mathrm{lcm}(N_1,\ldots,N_L)}) \subset \mathbb{Q}(\zeta_{N_0})$, and the dimension of the vector space $\mathbb{Q}(\zeta_{N_0})$ over field $\mathbb{Q}(\zeta_{\mathrm{lcm}(N_1,\ldots,N_L)})$ is

$$[\mathbb{Q}(\zeta_{N_0}) : \mathbb{Q}(\zeta_{\mathrm{lcm}(N_1,\ldots,N_L)})] = \frac{\phi(N_0)}{\phi(\mathrm{lcm}(N_1,\ldots,N_L))} = n_0 \ge L_t(L-1)+1.$$

From [39, p. 75], we know that $\{1,\zeta_{N_0},\zeta_{N_0}^2,\ldots,\zeta_{N_0}^{n_0-1}\}$ is a basis of vector space $\mathbb{Q}(\zeta_{N_0})$ over field $\mathbb{Q}(\zeta_{\mathrm{lcm}(N_1,\ldots,N_L)})$. Thus, the determinant of any nonzero codeword of L-layer space–time code for L_t transmit antennas can be considered as a nonzero linear combination of $1, \zeta_{N_0}, \zeta_{N_0}^2,\ldots,\zeta_{N_0}^{n_0-1}$ with coefficients in $\mathbb{Q}(\zeta_{\mathrm{lcm}(N_1,\ldots,N_L)})$, which cannot be zero from the linear independence of the basis.

For condition ii), its proof is similar to the proofs in [8], [13].

Condition iii) is broad enough that it contains the optimal multilayer cyclotomic space–time codes that will be found later. QED

Although the general form (19) of a multilayer cyclotomic space–time code and the first two conditions in the above theorem look similar to those that appeared in [8], [13], there are several differences as listed in the following.

- Similar to the one mentioned in Section II-F on diagonal cyclotomic space–time codes, we have presented *concrete* forms of generating lattices $G_{m,n}$, which will help us to find the optimal one later.
- The cyclotomic lattices G_{m_l,n_l} on different layers may be different, which differs from the existing ones in the literature where all these lattices are the same.
- The parameters ρ_l may not be necessarily on the unit circle as often required in the current literature for maintaining the capacity lossless property. As we shall see later, by relaxing this requirement, cyclotomic space–time codes with significantly better diversity products can be achieved while the capacity loss is not significant.

From Theorem 2, we can see that for a given $L \le L_t$, there are infinitely many L-layer cyclotomic space–time codes with full diversity. The question then becomes which one is optimal in the sense that the diversity product is optimal if the mean transmission signal power and the rate are fixed, or equivalently, the mean transmission power is minimized if the diversity product and the rate are fixed as mentioned before.

From Sections II-C–II-E, an L-layer cyclotomic space–time code is equivalent to an LL_t-dimensional composed complex lattice as

$$[\rho_1 \boldsymbol{y}_1(1),\ldots,\rho_1 \boldsymbol{y}_1(L_t),\ldots,\rho_L \boldsymbol{y}_L(1),\ldots,\rho_L \boldsymbol{y}_L(L_t)].$$

Therefore, from Lemma 1, the following lemma is obvious.

Lemma 2: An L-layer cyclotomic space-time code $X(\rho_1 G_{m_1,n_1},\ldots,\rho_L G_{m_L,n_L})$ is better than another L-layer cyclotomic space-time code $X(\rho_1' G_{m_1',n_1'},\ldots,\rho_L' G_{m_L',n_L'})$, if

$$\frac{d_{\min}(\rho_1 G_{m_1,n_1},\ldots,\rho_L G_{m_L,n_L})}{\prod_{l=1}^{L} |\det(\rho_l G_{m_l,n_l})| \cdot |\det(\Lambda_{\zeta_{m_l}})|^{L_t/2}} \ge \frac{d_{\min}(\rho_1' G_{m_1',n_1'},\ldots,\rho_L' G_{m_L',n_L'})}{\prod_{l=1}^{L} |\det(\rho_l' G_{m_l',n_l'})| \cdot |\det(\Lambda_{\zeta_{m_l'}})|^{L_t/2}}. \quad (20)$$

From this lemma, one can see that the problem of finding the optimal multilayer cyclotomic space–time code becomes a problem of finding the optimal generating matrices G_{m_l,n_l} and parameters ρ_l, $l = 1,\ldots,L$, such that the ratio

$$\frac{d_{\min}(\rho_1 G_{m_1,n_1},\ldots,\rho_L G_{m_L,n_L})}{\prod_{l=1}^{L} |\det(\rho_l G_{m_l,n_l})| \cdot |\det(\Lambda_{\zeta_{m_l}})|^{L_t/2}}$$

is maximized.

B. Optimal Single-Layer Cyclotomic Space–Time Codes

When $L = 1$, an L-layer cyclotomic space–time code becomes a single layer (or diagonal) cyclotomic space-time code. For single layer codes, optimal cyclotomic lattices or space-time codes for some small individual transmit numbers have been studied case by case in [14]. In this subsection, we present a general optimality for a general transmit antenna number L_t. Before presenting this result, let us first state a result obtained in [14].

Theorem 3: [14] Let $m_1 = 3$ or 6. Let $\Gamma_{L_t}(G_{m_1,n_1})$ be an $L_t \ge 2$-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

$$|\det(G_{m_1,n_1})| \le |\det(G_{m_2,n_2})|$$

then, lattice $\Gamma_{L_t}(G_{m_1,n_1})$ is better than lattice $\Gamma_{L_t}(G_{m_2,n_2})$.

This theorem holds mainly because the minimum product of an Eisenstein lattice is 1. 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. Similar to [14], we need the following lemma on Euler numbers.

Lemma 3: 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 $p_1,\ldots,p_l,q_1,\ldots,q_k,v_1,\ldots,v_h$ are distinct primes, $n_0 = q_1^{i_1}\cdots q_k^{i_k}$, and $\phi(n_0) = 1$ if $n_0 = 1$. Thus, $\gcd(m,n)$ is a factor of $\frac{\phi(mn)}{\phi(m)}$, where $\gcd(m,n)$ is the greatest common divisor of m and n.

This lemma is a direct consequence of the definition and the property of Euler numbers in Footnote 1. The following lemma on composed cyclotomic lattices plays the key rule in proving the general optimality result in the Appendix.

Lemma 4: Let m, n_1 and n_2 be positive integers and

$$L_1 = \frac{\phi(mn_1)}{\phi(m)} \quad \text{and} \quad L_2 = \frac{\phi(mn_1n_2)}{\phi(mn_1)}.$$

Then

$$|\det(G_{m,n_1n_2})| = |\det(G_{m,n_1})|^{L_2}\,|\det(G_{mn_1,n_2})|^{L_1}$$

where G_{m,n_1}, G_{mn_1,n_2}, and G_{m,n_1n_2} are the generating matrices of L_1-, L_2-, and L_1L_2-dimensional cyclotomic lattices $\Gamma_{L_1}(G_{m,n_1})$, $\Gamma_{L_2}(G_{mn_1,n_2})$, and $\Gamma_{L_1L_2}(G_{m,n_1n_2})$ over Λ_{ζ_m}, $\Lambda_{\zeta_{mn_1}}$, and Λ_{ζ_m}, respectively.

Lemma 4 gives us a relationship between the determinants $\det(G_{m,n_1})$, $\det(G_{mn_1,n_2})$, and $\det(G_{m,n_1n_2})$, of cyclotomic lattice generating matrices G_{m,n_1}, G_{mn_1,n_2}, and G_{m,n_1n_2} from different field extensions

$$\mathbb{Q}(\zeta_m) \subset \mathbb{Q}(\zeta_{mn_1}) \subset \mathbb{Q}(\zeta_{mn_1n_2}).$$

According to the notations in the Introduction, the result of Lemma 4 can be rewritten as

$$\begin{aligned}|\det(G_{m,n_1n_2})| &= |\det(G_{m,n_1}\otimes G_{mn_1,n_2})| \ \text{ or}\\ G_{m,n_1n_2} &= G_{m,n_1}\boxtimes G_{mn_1,n_2}\end{aligned} \tag{21}$$

where $G_{m,n_1}\otimes G_{mn_1,n_2}$ is the Kronecker (or tensor) product of matrices G_{m,n_1} and G_{mn_1,n_2}.

The proof of Lemma 4 is given in the Appendix. From the proof of Lemma 4, we know that Lemma 4 can be easily extended to more than two field extension cases, i.e., for any positive integers $m,n_1,n_2,n_3,\ldots,n_k$ and $N = n_1n_2\cdots n_k$, we have the following result:

$$\begin{aligned}&|\det(G_{m,N})|\\ &= \left|\det\left(G_{m,n_1}\otimes G_{mn_1,n_2}\otimes\cdots\otimes G_{mn_1\cdots n_{k-1},n_k}\right)\right|\end{aligned} \tag{22}$$

or, by the notation in the Introduction,

$$G_{m,N} = G_{m,n_1}\boxtimes G_{mn_1,n_2}\boxtimes\cdots\boxtimes G_{mn_1\cdots n_{k-1},n_k}.$$

Corollary 1: For any two positive integers m and n, let

$$n = p_1^{r_1}\cdots p_l^{r_l}q_1^{i_1}\cdots q_k^{i_k} \text{ and } m = p_1^{e_1}\cdots p_l^{e_l}v_1^{t_1}\cdots v_h^{t_h}$$

be their prime decompositions, where all p_i, q_i, v_i are distinct primes, and $L_t = \frac{\phi(mn)}{\phi(m)}$. Then, the determinant $\det(G_{m,n})$ of the generating matrix $G_{m,n}$ of the cyclotomic lattice $\Gamma_{L_t}(G_{m,n})$ satisfies

$$\begin{aligned}&|\det(G_{m,n})|\\ &= \left|\det\left(\left[\otimes_{s=1}^{l}(A_{p_s}^{\otimes r_s})\right]\otimes\left[\otimes_{w=1}^{k}\left(A_{q_w}^{\otimes(i_w-1)}\otimes B_{q_w}\right)\right]\right)\right|\end{aligned} \tag{23}$$

where A_{p_s} stands for the $p_s\times p_s$ discrete Fourier transform matrix

$$A_{p_s} = \begin{bmatrix} 1 & 1 & \cdots & 1\\ \zeta_{p_s} & \zeta_{p_s}^2 & \cdots & \zeta_{p_s}^{p_s}\\ \vdots & \vdots & \ddots & \vdots\\ \zeta_{p_s}^{p_s-1} & \zeta_{p_s}^{2(p_s-1)} & \cdots & \zeta_{p_s}^{p_s(p_s-1)}\end{bmatrix} \tag{24}$$

B_{q_w} is the $(q_w-1)\times(q_w-1)$ submatrix of matrix A_{q_w} with the q_wth row and the q_wth column absent, $A^{\otimes r}$ stands for the Kronecker product of r copies of A, i.e.,

$$A^{\otimes r} = \underbrace{A\otimes\cdots\otimes A}_{r}$$

and $\otimes_{s=1}^{l}A_{p_s} = A_{p_1}\otimes A_{p_2}\otimes\cdots A_{p_l}$. Also, $(\det(A_p))^2 = p^p$ for any positive integer p and $|\det(B_p)| = p^{(p-2)/2}$ for a prime p.

Proof: From (16) it is not hard to see that, for any prime p and any integer m

$$|\det(G_{m,p})| = \begin{cases}|\det(A_p)|, & \text{if } p \text{ is a factor of } m\\ |\det(B_p)|, & \text{otherwise.}\end{cases} \tag{25}$$

Let us consider the field extensions

$$\begin{aligned}\mathbb{Q}(\zeta_m)\subset\mathbb{Q}(\zeta_{mp_1})\subset\cdots\subset\mathbb{Q}(\zeta_{mN_1})\\ \subset\mathbb{Q}(\zeta_{mN_1q_1})\subset\cdots\subset\mathbb{Q}(\zeta_{mn})\end{aligned} \tag{26}$$

where $N_1 = \prod_{s=1}^{l}p_s^{r_s}$. Then this corollary can be easily proved by using Lemma 4 or (22), (26), and (25). The last determinant equalities of $\det(A_p)$ and $\det(B_p)$ can be obtained directly from the proof of Lemma 4. QED

By using the notation in the Introduction, (23) can be rewritten as

$$G_{m,n} = \left[\boxtimes_{s=1}^{l}(A_{p_s}^{\boxtimes r_s})\right]\boxtimes\left[\boxtimes_{w=1}^{k}\left(A_{q_w}^{\boxtimes(i_w-1)}\boxtimes B_{q_w}\right)\right]. \tag{27}$$

We now present a general optimality result for single-layer cyclotomic space–time codes.

Theorem 4: If the number of transmit antennas has the form

$$L_t = \frac{\phi(3n)}{\phi(3)} \quad \text{or} \quad \frac{\phi(6n)}{\phi(6)}, \qquad \text{for some integer } n \tag{28}$$

then the optimal single layer L_t-dimensional cyclotomic space–time code (or lattice) can be achieved by an Eisenstein cyclotomic lattice, i.e., $m = 3$ or $m = 6$, and the minimum product (or diversity product) of the optimal single-layer cyclotomic space–time code (or lattice) is 1.

Theorem 4 can be described in another way: the optimal single-layer cyclotomic space–time code can be achieved by

an Eisenstein cyclotomic lattice if L_t-dimensional Eisenstein cyclotomic lattices exist.

A proof of Theorem 4 for numbers of transmit antennas less than 3080 is given in the Appendix. With more tedious calculations, the result for more general numbers of transmit antennas can be similarly proved and we omit the details here. From this theorem, Lemma 1, and the footnote about Euler numbers, the following corollary can be obtained.

Corollary 2: If

$$L_t = 3^{r_1} p_2^{r_2-1}(p_2-1)\cdots p_k^{r_k-1}(p_k-1) \tag{29}$$

where $k \geq 1$, $p_2, \ldots, p_k$ are distinct primes and different from 3, and $r_1 \geq 0$, $r_2 \geq 1, \ldots, r_k \geq 1$ are integers, then the optimal single-layer L_t-dimensional cyclotomic space–time code (or lattice) can be achieved by an Eisenstein cyclotomic lattice, i.e., $m = 3$ or $m = 6$, and the minimum product of the optimal single-layer cyclotomic space–time code (or lattice) is 1.

Proof: This corollary can be easily proved by letting $n = 3^{r_1} p_2^{r_2} \cdots p_k^{r_k}$, and using Theorem 4, Lemma 1, and the footnote about Euler numbers. QED

As a remark, $k = 1$ in the above corollary means that the other terms $p_2, \ldots, p_k$ in (29) do not appear. Also, from this corollary, it is not hard to see that, if $L_t = \phi(3n)/\phi(3)$ for some integer n then $L_t = \phi(6n)/\phi(6)$ for some integer n and *vice versa*. Thus, in what follows we only consider L_t of the form $L_t = \phi(3n)/\phi(3)$ for some integer n. Although the numbers L_t of transmit antennas in (29) do not cover all positive integers, such as primes $5, 7$, etc., they cover a broad class of positive integers, such as $2, 3, 4, 6, 8, 9, 10, 12, 16, 18, 20, 22, 24, 27, 28, 30, 32, 36, 40, 42$, etc. Clearly, $L_t = p - 1$ for any prime p is covered by (29).

Theorem 4 tells us that, for L_t transmit antennas, if L_t-dimensional Eisenstein cyclotomic lattice exists, to find the optimal single-layer cyclotomic space–time code (or lattice) we only need to find the optimal lattice among pairs $(m, n) = (3, n), (6, n)$ instead of all possible candidate pairs (m, n). For a fixed $L_t = \phi(3n)/\phi(3)$, there are only a few cases of possible n that are not hard to compare individually. Because all the minimum products of Eisenstein cyclotomic lattices are 1 and

$$|\det(\Lambda_{\zeta_3})| = |\det(\Lambda_{\zeta_6})| = \sqrt{3}/2$$

from Lemma 1, we know that to find the optimal single-layer cyclotomic space–time code becomes to choose the integer n with the smallest determinant $|\det(G_{3,n})|$ or $|\det(G_{6,n})|$. For example, the generating matrices of two-, three-, and four-dimensional optimal cyclotomic lattices are $G_{3,4}$ or $G_{6,2}$, $G_{3,3}$ or $G_{6,3}$, and $G_{3,5}$ or $G_{6,5}$, respectively.

C. Optimal Full Rate (Two-Layer) Cyclotomic Space–Time Code for Two Transmit Antennas

In this subsection, we consider and find the optimal full rate full diversity cyclotomic space–time codes for two transmit antennas.

Theorem 5: For two transmit antennas, i.e., $L_t = 2$, the optimal full rate (two-layer) cyclotomic space–time code $X(\rho_1 G_{m_1,n_1}, \rho_2 G_{m_2,n_2})$ in (19) is reached by $\rho_1 = 1$ and $\rho_2 = \sqrt{1 \pm j}$, and $m_1 = m_2 = 4$ and $n_1 = n_2 = 3$. The diversity product is

$$d_{\min}(G_{4,3}, \sqrt{1 \pm j} G_{4,3}) = 1. \tag{30}$$

The proof of this theorem is given in the Appendix. The products of the two layers in the above code are shown in Fig. 1. It is easy to see that a set of codeword matrices of the optimal full rate cyclotomic space–time code for two transmit antennas contains the codeword matrices of the optimal single-layer cyclotomic space–time code as its subset by letting the second layer lattice points be zero. However, the diversity product of the two-layer code is not reduced compared to that of the single-layer code, i.e., 1. This tells us that adding another layer into the optimal single-layer code does not decrease the diversity product, i.e., has *nonvanishing determinant*.

The main idea for choosing the above parameter ρ_2 in the above optimal full rate full diversity cyclotomic space–time code is as follows. The determinant of a code in (19) is $\boldsymbol{y}_1(1)\boldsymbol{y}_1(2) - \rho_2^2 \boldsymbol{y}_2(1)\boldsymbol{y}_2(2)$, where

$$[\boldsymbol{y}_i(1), \boldsymbol{y}_i(2)]^T \in \Gamma_2(G_{m_i,n_i}), \qquad \text{for } i = 1, 2$$

and $\rho_1 = 1$ can be always chosen without loss of generality. When $\Gamma_2(G_{m_i,n_i})$ are Gaussian (Eisenstein) lattices, i.e., $m = 4$ ($m_i = 3$ or 6), from [37], [38], it is known that the products of the components $\boldsymbol{y}_i(1)\boldsymbol{y}_i(2)$ belong to lattice Λ_{ζ_4} ($\Lambda_{\zeta_3} = \Lambda_{\zeta_6}$) and therefore their norms are either 0 or at least 1. From Fig. 1, one can see that the set $\mathcal{S}_1$ of the products of all possible $\boldsymbol{y}_1(1)\boldsymbol{y}_1(2)$ for $[\boldsymbol{y}_1(1), \boldsymbol{y}_1(2)]^T \in \Gamma_2(G_{m_i,n_i})$ do not fill lattice Λ_{ζ_4} completely. Our idea to choose ρ_2 is in such a way that the set $\mathcal{S}_2$ of all products $\rho_2^2 \boldsymbol{y}_2(1)\boldsymbol{y}_2(2)$ not only belongs to lattice Λ_{ζ_4} but also does not intersect with $\mathcal{S}_1$. Therefore, the determinant $\boldsymbol{y}_1(1)\boldsymbol{y}_1(2) - \rho_2^2 \boldsymbol{y}_2(1)\boldsymbol{y}_2(2)$ is also on the lattice Λ_{ζ_4} and not 0, i.e., its norm is at least 1 and this means that the diversity product of the code is at least 1. This idea also applies to the other optimal multilayer cyclotomic space–time codes in the following subsections.

From the above idea, another remark we want to make here is that the two elements $\rho_2 \boldsymbol{y}_2(1)$ and $\rho_2 \boldsymbol{y}_2(2)$ in the second layer of the optimal code in Theorem 5 can be replaced by

$$\rho_2 \boldsymbol{y}_2(1) = \sqrt{1 \pm j}\exp(j\phi)\boldsymbol{z}_1$$

and

$$\rho_2 \boldsymbol{y}_2(2) = \sqrt{1 \pm j}\exp(j(k\pi/2 - \phi))\boldsymbol{z}_2$$

where ϕ is any real number, k is any integer, and $[\boldsymbol{z}_1, \boldsymbol{z}_2]^T$ belongs to $\Gamma_2(G_{4,3})$ according to $[\boldsymbol{y}_1(1), \boldsymbol{y}_1(2)]^T$ and the performance is the same as the optimal one.

Similar to the optimal code in Theorem 5, the following result can be obtained for Eisenstein lattices.

Proposition 2: For two transmit antennas, i.e., $L_t = 2$, the diversity product of full rate (two-layer) cyclotomic space–time code $X(\rho_1 G_{m_1,n_1}, \rho_2 G_{m_2,n_2})$ in (19) with $\rho_1 = 1$ and $\rho_2 = 3^{1/4}\zeta_{24} = 3^{1/4}\exp(j\pi/12)$, and $m_1 = m_2 = 3$ and $n_1 = n_2 = 4$ (or $m_1 = m_2 = 6$ and $n_1 = n_2 = 2$) is 1, i.e.,

$$d_{\min}(G_{3,4}, 3^{1/4}\zeta_{24} G_{3,4}) = d_{\min}(G_{6,2}, 3^{1/4}\zeta_{24} G_{6,2}) = 1.$$

Its proof is similar to the proof of Lemma 5 in the proof of Theorem 5 in the Appendix. Similar to the optimal code in

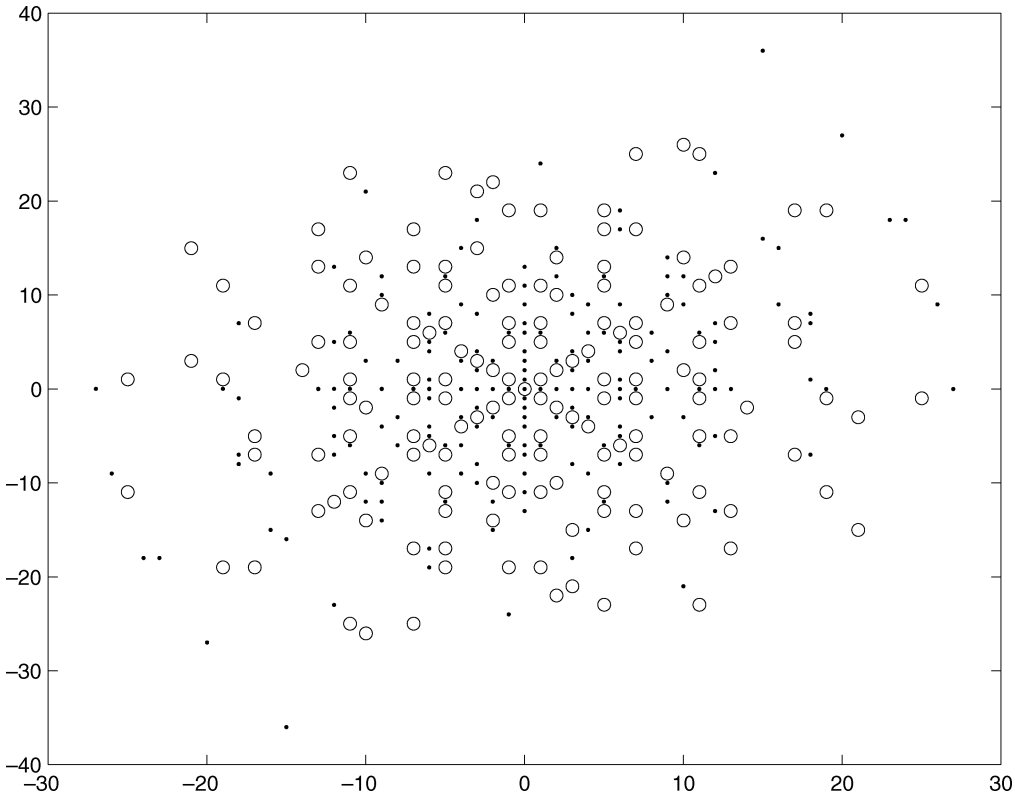

Fig. 1. Product distributions of lattice components on different layers in the optimal two-layer cyclotomic space–time code for two transmit antennas: "." stands for the first layer; "∘" stands for the second layer.

Theorem 5, the diversity product of code $X(G_{3,4}, 3^{1/4}\zeta_{24}G_{3,4})$ or$X(G_{6,2}, 3^{1/4}\zeta_{24}G_{6,2})$ does not decrease when the signal consetallation size increases, i.e., the codes have nonvanishing determinants. Also, the two elements $\rho_2\boldsymbol{y}_2(1)$ and $\rho_2\boldsymbol{y}_2(2)$ in the second layer can be replaced by

$$\rho_2\boldsymbol{y}_2(1) = 3^{1/4}\exp(j\phi)\boldsymbol{z}_1$$

and

$$\rho_2\boldsymbol{y}_2(2) = 3^{1/4}\exp(j(k\pi/3 + \pi/6 - \phi))\boldsymbol{z}_2$$

where ϕ is any real number, k is any integer, and $[\boldsymbol{z}_1, \boldsymbol{z}_2]^T$ belongs to $\Gamma_2(G_{6,2})$ or $\Gamma_2(G_{3,4})$ according to $[\boldsymbol{y}_1(1), \boldsymbol{y}_1(2)]^T$ and the performance does not change. Comparing the codes in Theorem 5 and Proposition 2 in terms of the normalized diversity products in Lemma 2, their normalized diversity products are

$$\frac{d_{\min}(G_{4,3}, \sqrt{1 \pm j}G_{3,4})}{|\det(G_{4,3})\det(\sqrt{1 \pm j}G_{4,3})| \cdot |\det(\Lambda_{\zeta_4})|^2} = \frac{1}{3\sqrt{2}}$$

and

$$\frac{d_{\min}(G_{3,4}, 3^{1/4}\zeta_{24}G_{3,4})}{|\det(G_{3,4})\det(3^{1/4}\zeta_{24}G_{3,4})| \cdot |\det(\Lambda_{\zeta_3})|^2} = \frac{d_{\min}(G_{6,2}, 3^{1/4}\zeta_{24}G_{6,2})}{|\det(G_{6,2})\det(3^{1/4}\zeta_{24}G_{6,2})| \cdot |\det(\Lambda_{\zeta_6})|^2} = \frac{1}{3\sqrt{3}}.$$

As a remark, from the previous section and [14] one can see that, in the single-layer or diagonal code case, cyclotomic codes $\Gamma(G_{4,3})$ over Λ_{ζ_4} and $\Gamma(G_{3,4})$ over Λ_{ζ_3} (or $\Gamma(G_{6,2})$ over Λ_{ζ_6}) reach the same optimal normalized diversity product but it is different in the two-layer code case as shown above.

To quantitatively compare these codes with the existing ones, let us normalize them as $X((1 \pm j)^{-1/2}G_{4,3}, G_{4,3})$ and $X(3^{-1/4}\zeta_{24}^{-1}G_{3,4}, G_{3,4})$ (or $X(3^{-1/4}\zeta_{24}^{-1}G_{6,2}, G_{6,2})$). These normalized codes have a lower mean transmission signal power than those in [8], [13] but its diversity products are $1/\sqrt{2}$ and $1/\sqrt{3}$, respectively, and larger than those in [8], [13].

D. Optimal Multilayer Cyclotomic Space–Time Codes for Three and Four Transmit Antennas

We first consider two-layer cyclotomic space–time codes for three and four transmit antennas.

Theorem 6: For three transmit antennas, i.e., $L_t = 3$, the optimal two-layer cyclotomic space–time code $X(\rho_1 G_{m_1,n_1}, \rho_2 G_{m_2,n_2})$ in (19) is reached by $\rho_1 = 1$ and $\rho_2 = 2^{1/3}$, and $m_1 = m_2 = 3$ and $n_1 = n_2 = 3$ (or $m_1 = m_2 = 6$ and $n_1 = n_2 = 3$). The diversity product is

$$d_{\min}(G_{3,3}, 2^{1/3}G_{3,3}) = d_{\min}(G_{6,3}, 2^{1/3}G_{6,3}) = 1. \quad (31)$$

A proof of this theorem is given in the Appendix. Similar to the two-antenna case, the three elements $\rho_2\boldsymbol{y}_2(i)$, $i = 1, 2, 3$, in the second layer of the optimal code in Theorem 6 can be replaced by

$$\rho_2\boldsymbol{y}_2(1) = 2^{1/3}\exp(j(\phi_1 + k_1\pi/3))\boldsymbol{z}_1$$
$$\rho_2\boldsymbol{y}_2(2) = 2^{1/3}\exp(j(\phi_2 + k_2\pi/3))\boldsymbol{z}_2$$

and

$$\rho_2\boldsymbol{y}_2(3) = 2^{1/3}\exp(-j(\phi_1 + \phi_2 + k_3\pi/3))\boldsymbol{z}_3$$

where ϕ_1 and ϕ_2 are any two real numbers, k_1, k_2, and k_3 are any integers, and $[\boldsymbol{z}_1, \boldsymbol{z}_2, \boldsymbol{z}_3]^T$ belongs to $\Gamma_3(G_{3,3})$ or $\Gamma_3(G_{6,3})$ according to $[\boldsymbol{y}_1(1), \boldsymbol{y}_1(2), \boldsymbol{y}_1(3)]^T$ and the performance is the same as the optimal one.

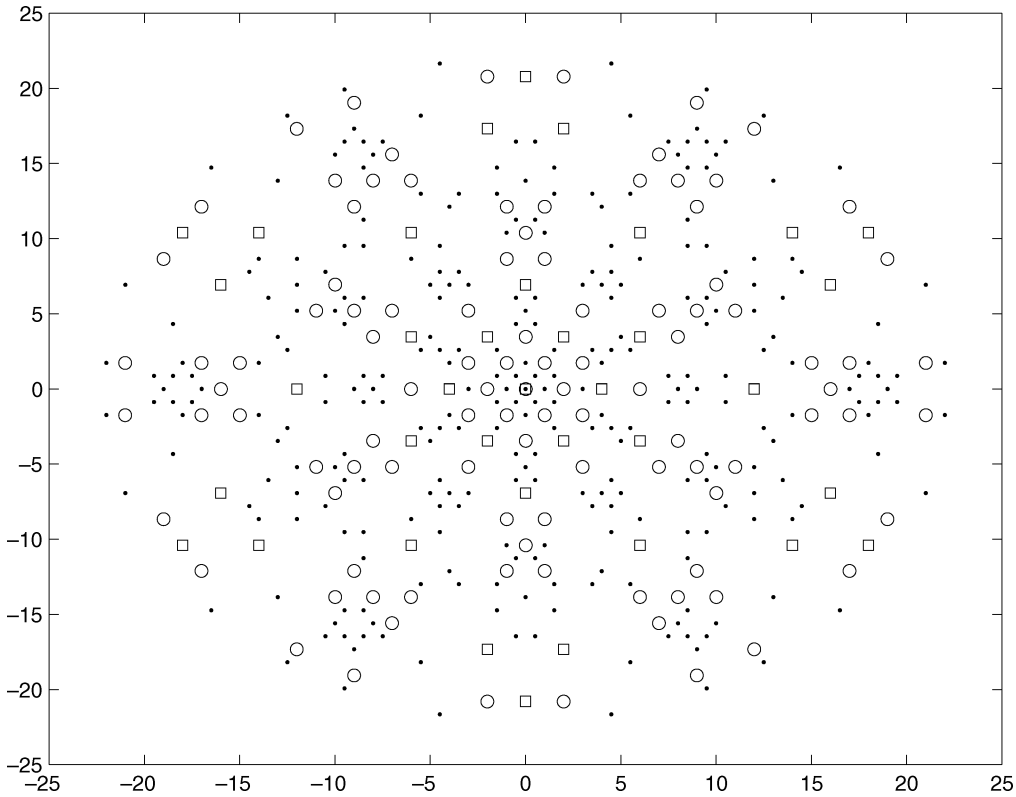

Fig. 2. Product distributions of lattice components on different layers in the optimal three-layer cyclotomic space–time code for three transmit antennas: "·" stands for the first layer; "∘" stands for the second layer; "□" stands for the third layer.

Theorem 7: For four transmit antennas, i.e., $L_t = 4$, the optimal two-layer cyclotomic space–time code $X(\rho_1 G_{m_1,n_1}, \rho_2 G_{m_2,n_2})$ in (19) is reached by $\rho_1 = 1$ and $\rho_2 = 3^{1/8}\zeta_{48} = 3^{1/8}\exp(j\pi/24)$, and $m_1 = m_2 = 3$ and $n_1 = n_2 = 5$ (or $m_1 = m_2 = 6$ and $n_1 = n_2 = 5$). The diversity product is

$$d_{\min}(G_{3,5}, 3^{1/8}\zeta_{48}G_{3,5}) = d_{\min}(G_{6,5}, 3^{1/8}\zeta_{48}G_{6,5}) = 1. \tag{32}$$

Its proof is similar to the proofs of the preceding theorems. We omit the details. Similarly, the four elements $\rho_2 \boldsymbol{y}_2(i)$, $i = 1, 2, 3, 4$, in the second layer of the optimal code in Theorem 7 can be replaced by

$$\rho_2 \boldsymbol{y}_2(1) = 3^{1/8}\exp(j\phi_1)\boldsymbol{z}_1$$
$$\rho_2 \boldsymbol{y}_2(2) = 3^{1/8}\exp(j\phi_2)\boldsymbol{z}_2$$
$$\rho_2 \boldsymbol{y}_2(3) = 3^{1/8}\exp(j\phi_3)\boldsymbol{z}_3$$

and

$$\rho_2 \boldsymbol{y}_2(4) = 3^{1/8}\exp(j(\pi/6 - \phi_1 - \phi_2 - \phi_3 + k\pi/3))\boldsymbol{z}_4$$

where ϕ_1, ϕ_2, and ϕ_3 are any real numbers, k is any integer, and $[\boldsymbol{z}_1, \boldsymbol{z}_2, \boldsymbol{z}_3, \boldsymbol{z}_4]^T$ belongs to $\Gamma_4(G_{3,5})$ or $\Gamma_4(G_{6,5})$ according to $[\boldsymbol{y}_1(1), \boldsymbol{y}_1(2), \boldsymbol{y}_1(3), \boldsymbol{y}_1(4)]^T$ and the performance is the same as the optimal one.

As a remark, the same idea as presented in [8] can be applied here to reduce the PAPR for our optimal two-layer cyclotomic space–time code for four transmit antennas by using the 4×4 Hadamard transform. Then, the new code has the form

$$X = \frac{1}{\sqrt{2}}\begin{bmatrix} \rho_1\boldsymbol{y}_1(1) & -\rho_2\boldsymbol{y}_2(4) & \rho_1\boldsymbol{y}_1(1) & \rho_2\boldsymbol{y}_2(4) \\ \rho_2\boldsymbol{y}_2(1) & \rho_1\boldsymbol{y}_1(2) & \rho_2\boldsymbol{y}_2(1) & \rho_1\boldsymbol{y}_1(2) \\ -\rho_1\boldsymbol{y}_1(3) & \rho_2\boldsymbol{y}_2(2) & \rho_1\boldsymbol{y}_1(3) & \rho_2\boldsymbol{y}_2(2) \\ -\rho_2\boldsymbol{y}_2(3) & -\rho_1\boldsymbol{y}_1(4) & \rho_2\boldsymbol{y}_2(3) & \rho_1\boldsymbol{y}_1(4) \end{bmatrix}. \tag{33}$$

We next consider three-layer cyclotomic space–time codes for three transmit antennas.

Theorem 8: For a three-layer cyclotomic space–time code

$$X = X(G_{3,3}, 2^{1/3}G_{3,3}, 4^{1/3}G_{3,3})$$

or

$$X = X(G_{6,3}, 2^{1/3}G_{6,3}, 4^{1/3}G_{6,3})$$

for three transmit antennas, its determinant is an Eisentein integer, i.e.,

$$\det(X) \in \mathbb{Z}[\zeta_6]. \tag{34}$$

Furthermore, its diversity product is 1, i.e.,

$$d_{\min}(G_{3,3}, 2^{1/3}G_{3,3}, 4^{1/3}G_{3,3}) = d_{\min}(G_{6,3}, 2^{1/3}G_{6,3}, 4^{1/3}G_{6,3}) = 1. \tag{35}$$

The proof of this theorem is given in the Appendix. The products of the three layers in the above code are shown in Fig. 2. Now we present optimal full rate cyclotomic space–time code for three transmit antennas.

Theorem 9: For three transmit antennas, i.e., $L_t = 3$, the optimal full rate (three-layer) cyclotomic space–time code $X(\rho_1 G_{m_1,n_1}, \rho_2 G_{m_2,n_2}, \rho_3 G_{m_3,n_3})$ in (19) is reached by $\rho_1 = 1$, $\rho_2 = 2^{1/3}$, and $\rho_3 = 4^{1/3}$, and $m_1 = m_2 = m_3 = 3$ and $n_1 = n_2 = n_3 = 3$ (or $m_1 = m_2 = m_3 = 6$ and $n_1 = n_2 = n_3 = 3$), i.e, $X(G_{3,3}, 2^{1/3}G_{3,3}, 4^{1/3}G_{3,3})$ (or $X(G_{6,3}, 2^{1/3}G_{6,3}, 4^{1/3}G_{6,3})$).

Proof: From Theorem 8, we know that

$$X(G_{6,3}, 2^{1/3}G_{6,3}, 4^{1/3}G_{6,3}) \text{ and } X(G_{3,3}, 2^{1/3}G_{3,3}, 4^{1/3}G_{3,3})$$

are full rate full diversity cyclotomic space–time codes with diversity product 1. The proof of the optimality can be obtained similar to Theorem 6 and the detailed proof is omitted. QED

Similar to the two transmit antenna case, the codeword matrices in the optimal two-layer space–time codes for both three and four transmit antennas and the optimal three-layer space–time codes for three transmit antennas contain those of the optimal single-layer codes as their subsets but their diversity products are the same as those of the optimal single-layer codes. In other words, adding other layers to the optimal single-layer code does not decrease the diversity product in the above cases, i.e., has the nonvanishing determinant.

E. Codeword Matrix (or Lattice Point) Selections

After an optimal L-layer cyclotomic space–time code structure X for L_t antennas is determined as in the previous subsections, to design a space–time code Ω for a practical system with a fixed throughput (bits pcu), one needs to select lattice points on the corresponding composed complex lattice as $\underline{\boldsymbol{y}} = G\underline{\boldsymbol{x}}$, where $\underline{\boldsymbol{x}}$ and $\underline{\boldsymbol{y}}$ are LL_t-dimensional complex vectors. From the results presented in the previous subsections, the diversity product is 1 for the optimal multilayer cyclotomic space–time codes no matter what the code size $|\Omega|$ is. Then, the codeword matrix or lattice point selection problem becomes a problem to select the points such that their mean power is minimized, which does not apply to the existing full rate and full diversity cyclotomic space–time codes in, for example, [8], [13], where there is no lower bound for the diversity product and the diversity product depends on the size of Ω. Let R be the throughput (bits pcu). Then, $|\Omega| = 2^{RL_t}$. Similar to what is done for diagonal code designs in [14], we now present three methods as follows.

Method I: Component-Wise Independent Selection: In this case, all information symbol components of $\underline{\boldsymbol{x}}$ are independently selected. A signal constellation $\mathcal{S}$ of size $2^{R/L}$ needs to be selected on the two-dimensional real lattice Λ_{ζ_m} such that its total energy is minimized

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

Method II: Layer-Wise Independent Selection: In this case, L different layers are independently selected and $2^{RL_t/L}$ points on the cyclotomic lattice $\Gamma_{L_t}(G_{m,n})$ need to be selected such that the total energy is minimized

$$\mathcal{S} = \left\{ \underline{\boldsymbol{x}}_i = [\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{L_t}]^T, 1 \leq i \leq 2^{RL_t/L} : \underline{\boldsymbol{x}}_i \neq \underline{\boldsymbol{x}}_l \in (\Lambda(\zeta_m))^{L_t} \right\} \text{and } \min \sum_{\underline{\boldsymbol{x}} \in \mathcal{S}} \|G_{m,n}\underline{\boldsymbol{x}}\|^2.$$

Method III: Joint Layer Selection: In this case, L different layers are selected jointly and 2^{RL_t} lattice points on the composed complex lattice $\Gamma(\rho_1 G_{m,n}, \ldots, \rho_L G_{m,n})$ need to be selected such that the total energy is minimized

$$\mathcal{S} = \left\{ \underline{\boldsymbol{x}} = [\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{LL_t}]^T : \ \underline{\boldsymbol{x}}_i \neq \underline{\boldsymbol{x}}_l \in (\Lambda(\zeta_m))^{LL_t} \right\} \text{ and } \min \sum_{\underline{\boldsymbol{x}} \in \mathcal{S}} \|\text{diag}(\rho_l G_{m,n}, \ldots, \rho_L G_{m,n})\underline{\boldsymbol{x}}\|^2.$$

After the minimization is done, all composed complex lattice points (or codeword matrices) $\underline{\boldsymbol{y}}_i$ are shifted such that the mean is at the center 0, i.e.,

$$\underline{\boldsymbol{y}}_i - \frac{1}{|\Omega|} \sum_{l=1}^{|\Omega|} \underline{\boldsymbol{y}}_l.$$

F. Multilayer Space–Time Coded Channel "Capacity"

A space–time coded multiple-input multiple-output (MIMO) relationship is

$$Y_{L_r \times B} = A_{L_r \times L_t} X_{L_t \times B} + W_{L_r \times B} \tag{36}$$

where $X_{L_t \times B}, Y_{L_r \times B}, A_{L_r \times B}$, and $W_{L_r \times B}$ are the space–time coded signal matrix, the received signal matrix, the channel matrix, and the additive noise matrix, respectively. By stacking these matrices into column vectors column-wise, we have

$$\mathcal{Y}_{L_r B \times 1} = \mathcal{A}_{L_r B \times L_t B} \mathcal{X}_{L_t B \times 1} + \mathcal{W}_{L_r B \times 1} \tag{37}$$

where

$$\mathcal{A}_{L_r B \times L_t B} = A \otimes I_{B \times B} = \text{diag}(A, \ldots, A). \tag{38}$$

If the transmitted signal X is generated by a full rate (L_t-layer) cyclotomic space–time code $X(\rho_1 G_{m_1,n_2}, \ldots, \rho_{L_t} G_{m_{L_t},n_{L_t}})$ in (19), we have $B = L_t$ and $\mathcal{X}_{L_t L_t \times 1}$ can be written as in (39) at the bottom of the page, where $\boldsymbol{x}_{i,l}$ are the information symbols. Let

$$\bar{\mathcal{A}} = \mathcal{A}_{L_r B \times L_t B} \cdot \text{diag}(\rho_1 G_{m_1,n_1}, \ldots, \rho_{L_t} G_{m_{L_t},n_{L_t}}).$$

After the transmission power is normalized, the capacity of the space–time coded channel $\bar{\mathcal{A}}$ can be written as

$$\begin{aligned} & C_{\text{cyclotomic}} \\ &= \frac{1}{L_t} \log_2 \left(\det(I_{L_t L_t \times L_t L_t} + \gamma \bar{\mathcal{A}} \bar{\mathcal{A}}^H) \right) \\ &= \frac{1}{L_t} \sum_{l=1}^{L_t} \log_2 \left(\det(I_{L_t \times L_t} + |\rho_l|^2 \gamma A G_{m_l,n_l} G_{m_l,n_l}^H A^H) \right) \end{aligned} \tag{40}$$

where γ is the SNR.

$$\mathcal{X}_{L_t L_t \times 1} = \text{diag}(\rho_1 G_{m_1,n_1}, \ldots, \rho_{L_t} G_{m_{L_t},n_{L_t}})[\boldsymbol{x}_{1,1}, \ldots, \boldsymbol{x}_{1,L_t}, \ldots, \boldsymbol{x}_{L_t,1}, \ldots, \boldsymbol{x}_{L_t,L_t}]^T \tag{39}$$

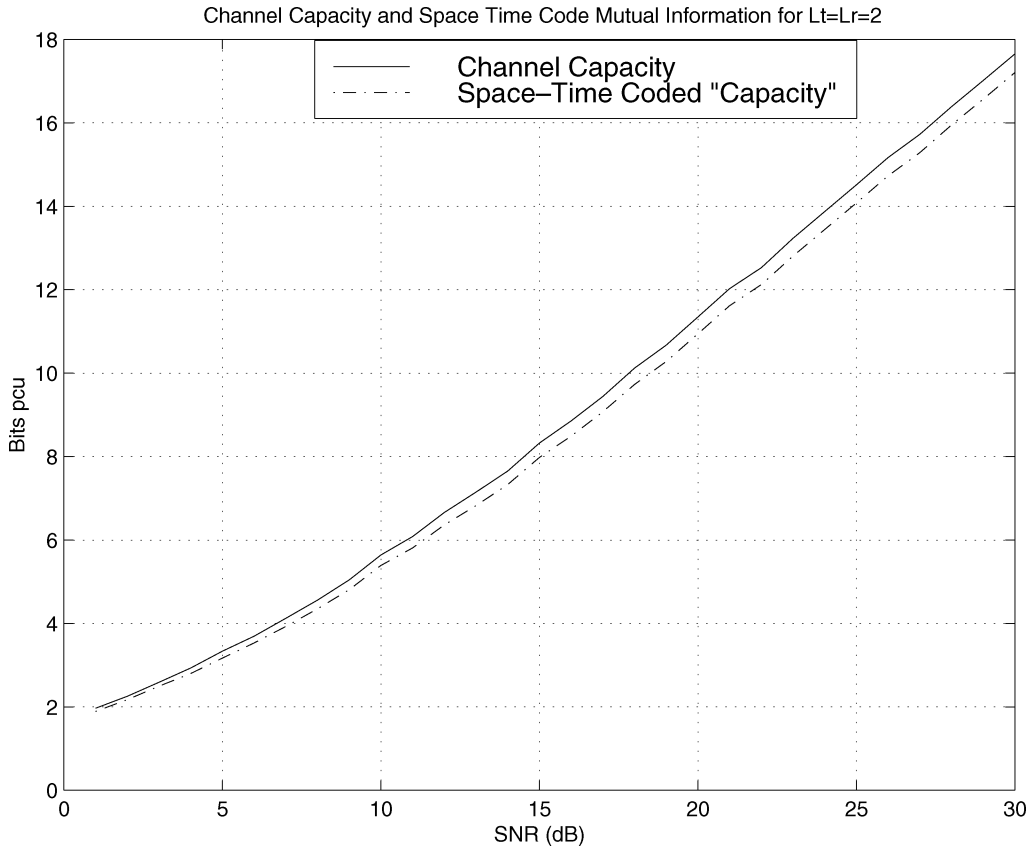

Fig. 3. Original and space–time coded channel capacities with the optimal full rate cyclotomic space–time code for two transmit and two receive antennas.

When all the generating matrices G_{m_l,n_l} are unitary matrices, the above capacity (40) becomes

$$C_{\text{cyclotomic}} = \frac{1}{L_t}\sum_{l=1}^{L_t}\log_2\left(\det(I_{L_t\times L_t} + |\rho_l|^2\gamma AA^H)\right) \tag{41}$$

which equals the original channel capacity $C(A)$ of channel A when all ρ_l satisfy $|\rho_l| = 1$. In this case, the cyclotomic space–time code is called *capacity lossless* [18], [17], [5], [8], [13].

Although in our optimal multilayer space–time codes presented in the previous subsections, $G_{4,3}$ for two antennas and $G_{3,3}$ and $G_{6,3}$ for three antennas are unitary, these codes are not capacity lossless because $|\rho_l| \neq 1$ for some l. However, the "capacities" of our optimal full rate cyclotomic space–time coded systems for two transmit two receive antennas and three transmit three receive antennas are calculated and only about 0.1- to 0.6-dB capacity loss as shown in Figs. 3 and 4, respectively, where "capacities" are the capacities of channels $\bar{\mathcal{A}}$ but not of the original channel $\mathcal{A}$.

IV. Simulation Results

In this section, we present some simulation results for two transmit and two receive antennas. The channel is assumed quasi-static fading. The entries of the channel matrix are independently identically complex Gaussian distributed with mean zero and variance 1.

Two multilayer cyclotomic space–time codes are compared. One is the full rate full diversity code $\boldsymbol{B}_{2,\phi}$ in [5] with

$$\boldsymbol{B}_{2,\phi} = \frac{1}{\sqrt{2}}\begin{bmatrix} s_1+\phi s_2 & \theta(s_3+\phi s_4) \\ \theta(s_3-\phi s_4) & s_1-\phi s_2 \end{bmatrix}$$

where s_1, s_2, s_3, s_4 are independently chosen from an M-QAM, and $\theta^2 = \phi = e^{j/2}$. The other is the optimal full rate (two-layer) full diversity cyclotomic space–time code $X(G_{4,3}, \sqrt{1+j}G_{4,3})$ where the lattice points are selected based on the layer joint selection method, i.e., Method III, in Section III-E. The reason why the four information symbols s_i in code $\boldsymbol{B}_{2,\phi}$ are independently rather than jointly selected is because this code does not have a fixed diversity product lower bound that code $X(G_{4,3}, \sqrt{1+j}G_{4,3})$ has and the diversity product depends on selected lattice points and therefore it is not easy to do the joint selection. Two different throughputs, $R = 4$ and 6 bits pcu, are simulated and the simulation results of symbol error rates versus SNR are shown in Figs. 5 and 6, respectively, where SNR is the SNR at each receive antenna. One can clearly see the performance improvement of the optimal cyclotomic codes over the nonoptimal ones in the literature.

V. Conclusion

In this paper, a systematic and general multilayer cyclotomic space–time code design has been proposed and several optimal

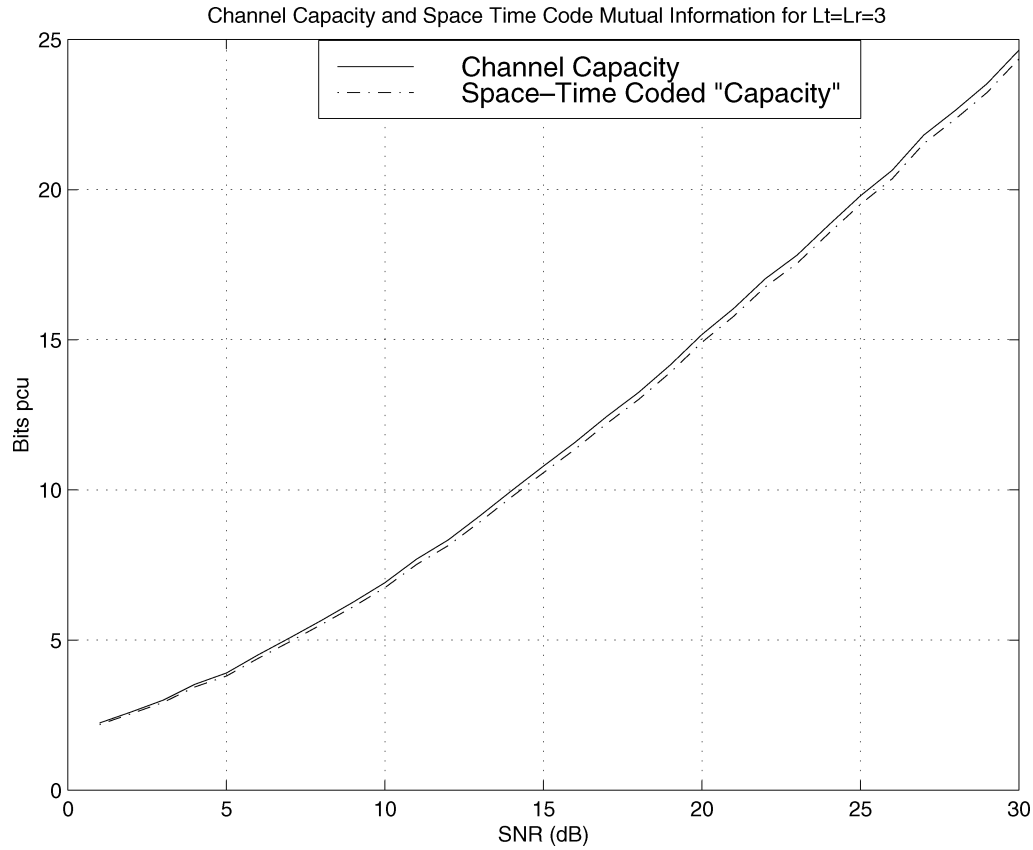

Fig. 4. Original and space–time coded channel capacities with the optimal full rate cyclotomic space–time code for three transmit and three receive antennas.

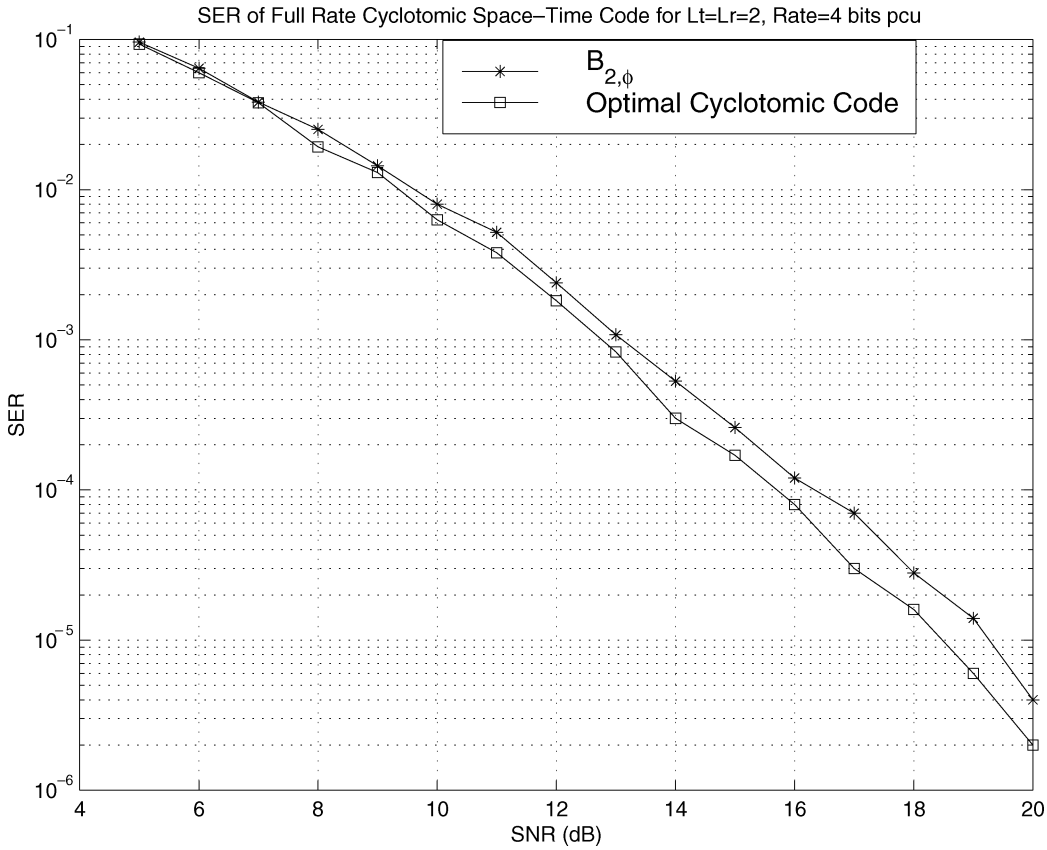

Fig. 5. Symbol error rates of full rate cyclotomic space–time codes with 4 bits pcu for two transmit and two receive antennas.

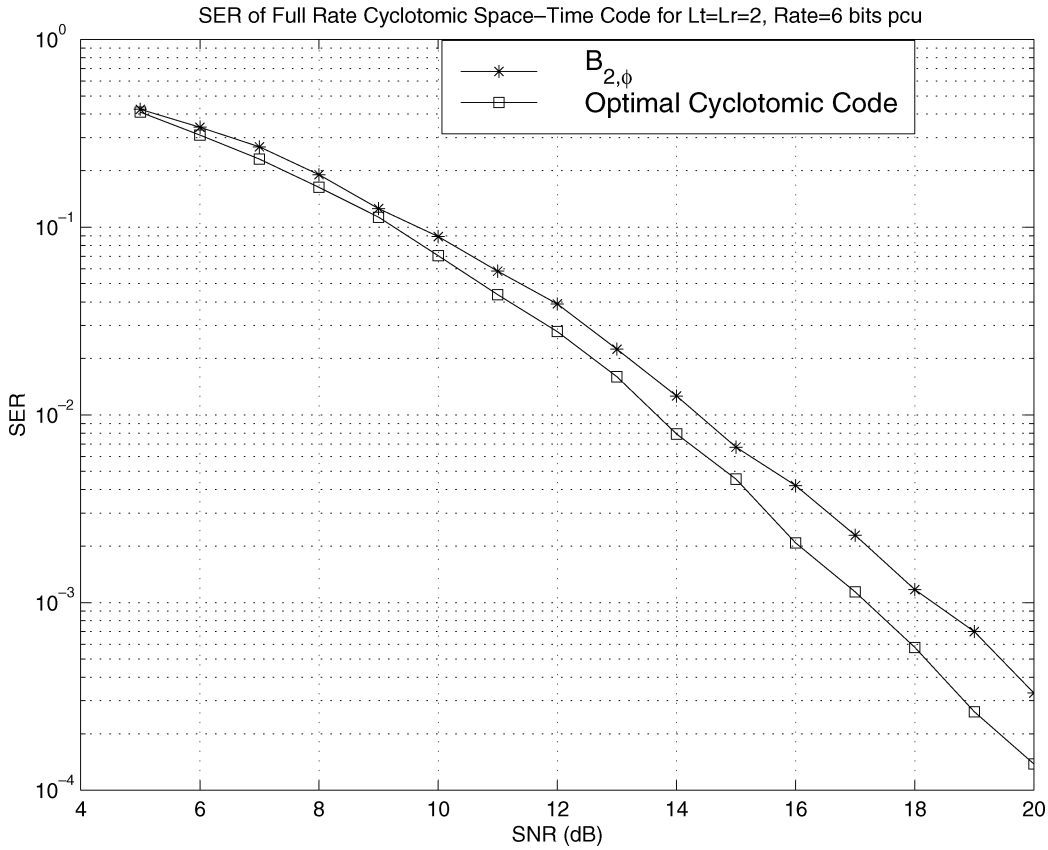

Fig. 6. Symbol error rates of full rate cyclotomic space-time codes with 6 bits *pcu* for two transmit and two receive antennas.

multilayer cyclotomic space–time codes and code families have been obtained, where the optimality is in the sense that the mean transmission signal power is minimized when the diversity product is fixed. In particular, optimal single-layer (diagonal) cyclotomic space–time codes have been found for a general number L_t of transmit antennas as long as L_t can be represented as $L_t = \phi(3n)/\phi(3)$ for some n that covers a broad family of L_t, where $\phi(n)$ is the Euler number of n. The optimal full rate cyclotomic space–time codes for two and three transmit antennas have been obtained. Optimal two-layer cyclotomic space–time codes have been obtained for three and four transmit antennas. We want to emphasize here that all the optimal multilayer cyclotomic space–time codes obtained in this paper have the nonvanishing determinant property.

As a remark, after we submitted this paper in November of 2003, we have come across recent works [43]–[48] on various constructions of nonvanishing determinant full rate space–time codes. It is not hard to check that the optimal full rate (two-layer) cyclotomic code for two transmit antennas presented in Theorem 5 in this paper has slightly better lattice (packing) compaction than the Golden code [45] does.

APPENDIX

A. Proof of Lemma 4

We first consider three special cases.

Case I: $n_2 = \prod_{i=1}^{s} p_i^{r_i}$ *and* p_i *Divides* mn_1 *for* $i = 1, 2, \ldots, s$*:* In this case, from Lemma 3, we have

$$L_2 = \frac{\phi(mn_1n_2)}{\phi(mn_1)} = n_2.$$

Let $N = mn_1n_2$. From (16), G_{mn_1,n_2} can be rewritten as (42) at the bottom of the page. Let

$$G = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & \zeta_{n_2} & \cdots & \zeta_{n_2}^{(n_2-1)} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta_{n_2}^{(n_2-1)} & \cdots & \zeta_{n_2}^{(n_2-1)^2} \end{bmatrix}_{n_2 \times n_2}. \tag{43}$$

$$G_{mn_1,n_2} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \zeta_{n_2} & \zeta_{n_2}^2 & \cdots & \zeta_{n_2}^{n_2} \\ \vdots & \vdots & \ddots & \vdots \\ \zeta_{n_2}^{(n_2-1)} & \zeta_{n_2}^{2(n_2-1)} & \cdots & \zeta_{n_2}^{n_2(n_2-1)} \end{bmatrix}_{n_2 \times n_2} \begin{bmatrix} \zeta_N & & & \\ & \zeta_N^2 & & \\ & & \ddots & \\ & & & \zeta_N^{n_2} \end{bmatrix}. \tag{42}$$

It is not hard to check that

$$GG = \begin{bmatrix} n_2 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & n_2 \\ 0 & 0 & \cdots & n_2 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & n_2 \cdots & 0 & 0 \\ 0 & n_2 & 0 \cdots & 0 & 0 \end{bmatrix}. \tag{44}$$

Thus, $(\det(G))^2 = \pm n_2^{n_2}$. Therefore,

$$\begin{aligned} \det(G_{mn_1,n_2}) &= (\pm 1)^{1/2} n_2^{n_2/2} \zeta_{n_2}^{\frac{n_2(n_2-1)}{2}} \zeta_N^{\frac{n_2(n_2+1)}{2}} \\ &= (\pm 1)^{1/2} n_2^{n_2/2} (-1)^{n_2-1} \zeta_{mn_1}^{(n_2+1)/2}. \end{aligned} \tag{45}$$

This implies

$$(\det(G_{mn_1,n_2}))^2 = \pm n_2^{n_2} \zeta_{mn_1}^{n_2+1} \in \mathbb{Q}(\zeta_{mn_1}). \tag{46}$$

For $k = 1, \ldots, L_1$, let τ_k be the $L_1 = \frac{\phi(mn_1)}{\phi(m)}$ embeddings of the field $\mathbb{Q}(\zeta_{mn_1})$ into $\mathbb{C}$ that fixes $\mathbb{Q}(\zeta_m)$ and $\tau_k(\zeta_{mn_1}) = \zeta_{mn_1}^{l_k}$ for some integer l_k, see [39, p. 75]. Then, we obtain

$$\tau_k((\det(G_{mn_1,n_2}))^2) = \tau_k(n_2^{n_2}) \tau_k(\zeta_{mn_1}^{(n_2+1)}) = n_2^{n_2} \zeta_{mn_1}^{l_k(n_2+1)}. \tag{47}$$

From (47), we know that the *relative norm*

$$\mathbb{N}_{\mathbb{Q}(\zeta_{mn_1})/\mathbb{Q}(\zeta_m)} \left((\det(G_{mn_1,n_2}))^2 \right)$$

of $(\det(G_{mn_1,n_2}))^2$ is [41]

$$\begin{aligned} \mathbb{N}_{\mathbb{Q}(\zeta_{mn_1})/\mathbb{Q}(\zeta_m)} \left((\det(G_{mn_1,n_2}))^2 \right) &= \prod_{k=1}^{L_1} \tau_k((\det(G_{mn_1,n_2}))^2) \\ &= n_2^{n_2 L_1} \zeta_{mn_1}^{(n_2+1)\sum_{k=1}^{L_1} l_k}. \end{aligned} \tag{48}$$

By the Theorem of Relative Discriminants in Tower [41], we have

$$\begin{aligned} &\Delta_{\mathbb{Q}(\zeta_{mn_1n_2})/\mathbb{Q}(\zeta_m)} \\ &= \Delta_{\mathbb{Q}(\zeta_{mn_1})/\mathbb{Q}(\zeta_m)}^{n_2} \mathbb{N}_{\mathbb{Q}(\zeta_{mn_1})/\mathbb{Q}(\zeta_m)} \left(\Delta_{\mathbb{Q}(\zeta_{mn_1n_2})/\mathbb{Q}(\zeta_{mn_1})} \right) \end{aligned} \tag{49}$$

where

$$\Delta_{\mathbb{Q}(\zeta_{mn_1n_2})/\mathbb{Q}(\zeta_m)} = (\det(G_{m,n_1n_2}))^2 \tag{50}$$

$$\Delta_{\mathbb{Q}(\zeta_{mn_1n_2})/\mathbb{Q}(\zeta_{mn_1})} = (\det(G_{mn_1,n_2}))^2 \tag{51}$$

and

$$\Delta_{\mathbb{Q}(\zeta_{mn_1})/\mathbb{Q}(\zeta_m)} = (\det(G_{m,n_1}))^2. \tag{52}$$

From (48)–(52), we have

$$\begin{aligned} &|\det(G_{m,n_1n_2})|^2 \\ &\quad = |\det(G_{m,n_1})|^{2n_2} \left| \mathbb{N}_{\mathbb{Q}(\zeta_{mn_1})/\mathbb{Q}(\zeta_m)} \left((\det(G_{mn_1,n_2}))^2 \right) \right| \\ &\quad = |\det(G_{m,n_1})|^{2n_2} \left| n_2^{n_2 L_1} \zeta_{ml_1}^{(l_2+1)\sum_{k=1}^{L_1} l_k} \right| \\ &\quad = |\det(G_{m,n_1})|^{2n_2} \, n_2^{n_2 L_1}. \end{aligned} \tag{53}$$

Using (46) again, we have

$$\begin{aligned} |\det(G_{m,n_1n_2})|^2 &= |\det(G_{m,n_1})|^{2n_2} \, |\det(G_{mn_1,n_2})|^{2L_1} \\ &= |\det(G_{m,n_1}) \otimes G_{mn_1,n_2})|^2 \end{aligned} \tag{54}$$

which proves the lemma.

Case II: n_2 is a Prime Number and Coprime With mn_1: In this case, from Lemma 3 we have

$$\frac{\phi(mn_1n_2)}{\phi(mn_1)} = n_2 - 1 = L_2.$$

From (16)

$$\begin{aligned} &G_{mn_1,n_2} \\ &= \begin{bmatrix} \zeta_{n_2}^{l_1} & \zeta_{n_2}^{2l_1} & \cdots & \zeta_{n_2}^{(n_2-1)l_1} \\ \zeta_{n_2}^{l_2} & \zeta_{n_2}^{2l_2} & \cdots & \zeta_{n_2}^{(n_2-1)l_2} \\ \vdots & \vdots & \ddots & \vdots \\ \zeta_{n_2}^{l_{n_2-1}} & \zeta_{n_2}^{2l_{n_2-1}} & \cdots & \zeta_{n_2}^{(n_2-1)l_{n_2-1}} \end{bmatrix}_{(n_2-1)\times(n_2-1)} \\ &\quad \times \begin{bmatrix} \zeta_N & & & \\ & \zeta_N^2 & & \\ & & \ddots & \\ & & & \zeta_N^{(n_2-1)} \end{bmatrix} \end{aligned} \tag{55}$$

where $N = mn_1n_2$, $l_k, k = 1, 2, \ldots, n_2 - 1$, are $n_2 - 1$ distinct integers in $\{0, 1, \ldots, n_2 - 1\}$ such that $1 + l_k mn_1$ and N are coprime. Let

$$G = \begin{bmatrix} \zeta_{n_2}^{l_1} & \zeta_{n_2}^{2l_1} & \cdots & \zeta_{n_2}^{(n_2-1)l_1} \\ \zeta_{n_2}^{l_2} & \zeta_{n_2}^{2l_2} & \cdots & \zeta_{n_2}^{(n_2-1)l_2} \\ \vdots & \vdots & \ddots & \vdots \\ \zeta_{n_2}^{l_{n_2-1}} & \zeta_{n_2}^{2l_{n_2-1}} & \cdots & \zeta_{n_2}^{(n_2-1)l_{n_2-1}} \end{bmatrix}_{(n_2-1)\times(n_2-1)}. \tag{56}$$

Let n_0 be the integer that is not taken by l_k in $\{0, 1, \ldots, n_2 - 1\}$, i.e., $0 \le n_0 \le n_2 - 1$ but $n_0 \ne l_k$ for $k = 1, 2, \ldots, n_2 - 1$. By multiplying the kth column of G by $\zeta_{n_2}^{-kn_0}$ for $k = 1, 2, \ldots, n_2 - 1$ and then reordering the matrix row-wisely, G can be changed into

$$G_{n_2} = \begin{bmatrix} \zeta_{n_2} & \zeta_{n_2}^2 & \cdots & \zeta_{n_2}^{(n_2-1)} \\ \zeta_{n_2}^2 & \zeta_{n_2}^4 & \cdots & \zeta_{n_2}^{2(n_2-1)} \\ \vdots & \vdots & \ddots & \vdots \\ \zeta_{n_2}^{n_2-1} & \zeta_{n_2}^{2(n_2-1)} & \cdots & \zeta_{n_2}^{(n_2-1)^2} \end{bmatrix} \tag{57}$$

and

$$\begin{aligned} \det(G) &= \pm \zeta_{n_2}^{-n_0 \sum_{i=1}^{n_2-1} i} \det(G_{n_2}) \\ &= \pm \zeta_{n_2}^{-n_0 \frac{(n_2-1)n_2}{2}} \det(G_{n_2}) \\ &= \pm \exp(-jn_0(n_2-1)\pi) \det(G_{n_2}) \\ &= \pm (-1)^{n_0(n_2-1)+1} \det(G_{n_2}). \end{aligned} \tag{58}$$

If $n_2 = 2$, then mn_1 is an odd number and $\phi(mn_1n_2) = \phi(mn_1)$, $G_{m,n_1n_2} = G_{m,n_1}$, and $G_{mn_1,n_2} = 1$. Thus, this is a trivial case. We next assume $n_2 > 2$.

By [41, Theorem 2.32 , p. 84] and since n_2 is a prime, we have

$$\det(G_{n_2}^2) = (-1)^{\frac{n_2-1}{2}} n_2^{n_2-2} \in \mathbb{Z} \subset \mathbb{Q}. \tag{59}$$

Thus,

$$(\det(G))^2 = (-1)^{\frac{n_2-1}{2}} n_2^{n_2-2} \in \mathbb{Z} \subset \mathbb{Q} \tag{60}$$

and

$$\begin{aligned}(\det(G_{mn_1,n_2}))^2 &= \det(G)^2 \zeta_N^{n_2(n_2+1)} \\ &= (-1)^{\frac{n_2-1}{2}} n_2^{n_2-2} \zeta_N^{n_2(n_2+1)} \\ &= (-1)^{\frac{n_2-1}{2}} n_2^{n_2-2} \zeta_{mn_1}^{n_2+1} \in \mathbb{Z}(\zeta_{mn_1}) \subset \mathbb{Q}(\zeta_{mn_1})\end{aligned} \tag{61}$$

which is similar to (46) in Case I. Then, this case can be similarly proved by using the same arguments as in (47)–(54) in Case I.

Case III: $n_2 = p^k$, p, and mn_1 are Coprime: In this case, we consider the tower of field extensions

$$\mathbb{Q}(\zeta_m) \subset \mathbb{Q}(\zeta_{mn_1}) \subset \mathbb{Q}(\zeta_{mn_1 p}) \subset \mathbb{Q}(\zeta_{mn_1 p^k}).$$

From Case II, we know that

$$|\det(G_{m,n_1 p})| = |\det(G_{m,n_1} \otimes G_{mn_1,p})| \tag{62}$$

and from Case I, we have

$$\begin{aligned}\left|\det(G_{m,n_1 p^k})\right| &= \left|\det(G_{m,n_1 p p^{k-1}})\right| \\ &= \left|\det(G_{m,n_1 p} \otimes G_{mn_1 p,p^{k-1}})\right|.\end{aligned} \tag{63}$$

By combining (62) and (63), we have

$$\begin{aligned}&|\det(G_{m,n_1 p^k})| \\ &= \left|\det(G_{m,n_1} \otimes G_{mn_1,p}) \otimes G_{mn_1 p,p^{k-1}})\right| \\ &= |\det(G_{m,n_1})|^{L_2} \left|\det(G_{mn_1,p}) \otimes G_{mn_1 p,p^{k-1}})\right|^{L_1}.\end{aligned} \tag{64}$$

From Case I again, we have

$$\begin{aligned}\left|\det(G_{mn_1,p^k})\right| &= \left|\det(G_{mn_1,pp^{k-1}})\right| \\ &= \left|\det(G_{mn_1,p}) \otimes G_{mn_1 p,p^{k-1}})\right|.\end{aligned} \tag{65}$$

By combining (64) and (65), we finally have

$$\begin{aligned}\left|\det(G_{m,n_1 p^k})\right| &= |\det(G_{m,n_1})|^{L_2} \left|\det(G_{mn_1,p^k})\right|^{L_1} \\ &= |\det(G_{m,n_1} \otimes G_{mn_1,n_2})|\end{aligned} \tag{66}$$

which proves the lemma.

General Case: In general, n_2 can be written as $n_2 = n_2' \prod_{i=1}^{s} p_i^{r_s}$ where p_i, $i = 1, \ldots, s$, are distinct primes and none of these primes p_i divides mn_1, and all the prime factors of n_2' divide mn_1. One can see that n_2' is similar to Case I while p_i are similar to Case III. Consider the field extensions

$$\begin{aligned}\mathbb{Q}(\zeta_m) \subset \mathbb{Q}(\zeta_{mn_1}) \subset \mathbb{Q}(\zeta_{mn_1 n_2'}) \\ \subset \mathbb{Q}(\zeta_{mn_1 n_2' p_1^{t_1}}) \subset \cdots \subset \mathbb{Q}(\zeta_{mn_1 n_2}).\end{aligned}$$

By using the results of Case I and Case III, repeatedly, the lemma can then be proved. QED

B. Proof of Theorem 4

Our basic idea to prove this theorem is: for any given L_t-dimensional cyclotomic lattice $\Gamma_{L_t}(G_{m,n})$ over Λ_{ζ_m} with generating matrix $G_{m,n}$, we find an Eisenstein cyclotomic lattice $\Gamma_{L_t}(G_{3,n_0})$ or $\Gamma_{L_t}(G_{6,n_0})$ over $\Lambda_{\zeta_3} = \Lambda_{\zeta_6}$ such that $\Gamma_{L_t}(G_{3,n_0})$ or $\Gamma_{L_t}(G_{6,n_0})$ over Λ_{ζ_3} is better than $\Gamma_{L_t}(G_{m,n})$.

Let m and n be integers of prime decompositions $n = p_1^{r_1} \cdots p_l^{r_l} q_1^{i_1} \cdots q_k^{i_k}$, $m = p_1^{e_1} \cdots p_l^{e_l} v_1^{t_1} \cdots v_h^{t_h}$, and $L_t = \frac{\phi(mn)}{\phi(m)}$, where p_j, q_j, v_j are distinct primes and $r_j, i_j, e_j, t_j \geq 1$, and p_j may be 1. Let $n_0 = \bar{p}_1^{u_1} \cdots \bar{p}_g^{u_g}$ with distinct primes $\bar{p}_i$ and $u_i \geq 1$ such that $L_t = \phi(mn)/\phi(m) = \phi(3n_0)/\phi(3)$. We next want to prove this theorem in two different cases: one is when m and n have no common prime factors greater than 3 and the other, when m and n have some common prime factors greater than 3. In the first case, under most situations, we can show that the determinant $|\det(G_{3,n_0})|$ (or $|\det(G_{6,n_0})|$) is less than or equal to $|\det(G_{m,n})|$ and then by Theorem 3, we know that $\Gamma_{L_t}(G_{3,n_0})$ or $\Gamma_{L_t}(G_{6,n_0})$ is better than $\Gamma_{L_t}(G_{m,n})$, where we do not need to consider the minimum products (or diversity products) $d_{\min}(\Gamma_{L_t}(G_{m,n}))$ and $d_{\min}(\Gamma_{L_t}(G_{3,n_0}))$. In the second case and one situation of the first case, we need to consider the minimum products $d_{\min}(\Gamma_{L_t}(G_{m,n}))$ and $d_{\min}(\Gamma_{L_t}(G_{3,n_0}))$ in addition to the determinants $|\det(G_{3,n_0})|$ and $|\det(G_{m,n})|$, i.e., we need to compare the following ratios:

$$\frac{d_{\min}(\Gamma_{L_t}(G_{m,n}))}{|\det(G_{m,n})||\det(\Lambda_{\zeta_m})|^{L_t/2}} \text{ and } \frac{d_{\min}(\Gamma_{L_t}(G_{3,n_0}))}{|\det(G_{3,n_0})||\det(\Lambda_{\zeta_3})|^{L_t/2}}.$$

Case 1: $p_1, \ldots, p_l$ are $1, 2$, or 3, i.e., m and n Have No Other Common Factor Than $1, 2$, or 3: Let us consider the first subcase.

Subcase 1.1: 3 is not a factor of n.

When 2 is not a common factor of m and n, we choose $n_0 = n$. Then

$$\frac{\phi(3n_0)}{\phi(3)} = \frac{\phi(mn)}{\phi(m)} = q_1^{i_1-1}(q_1-1)\cdots q_k^{i_k-1}(q_k-1) = L_t,$$

and

$$G_{3,n_0} = \boxtimes_{w=1}^{k} \left[A_{q_w}^{\boxtimes(i_w-1)} \boxtimes B_{q_w}\right] = G_{m,n}.$$

When 2 is a common factor of m and n, $n = 2^{r_1} q_1^{i_1} \cdots q_k^{i_k}$. Choose $n_0 = 2n$. Then

$$\frac{\phi(3n_0)}{\phi(3)} = \frac{\phi(mn)}{\phi(m)} = 2^{r_1} q_1^{i_1-1}(q_1-1)\cdots q_k^{i_k-1}(q_k-1).$$

By using Lemma 4 and $|B_2| = 1$, we have

$$\begin{aligned}G_{3,n_0} &= A_2^{\boxtimes r_1} \boxtimes B_2 \boxtimes_{w=1}^{k} \left[A_{q_w}^{\boxtimes(i_w-1)} \boxtimes B_{q_w}\right] \\ &= A_2^{\boxtimes r_1} \boxtimes_{w=1}^{k} \left[A_{q_w}^{\boxtimes(i_w-1)} \boxtimes B_{q_w}\right] = G_{m,n}.\end{aligned}$$

In either situation, we have $|\det(G_{3,n_0})| = |\det(G_{m,n})|$. By Theorem 3, we have proved the theorem in this subcase.

Subcase 1.2: 3 is a factor of n.

The proof of the theorem in this subcase is given under two different situations: 3 is a factor of m, and 3 is not a factor of m.

Subcase 1.2.1: 3 is a common factor of n and m.

In this subcase, we first consider when 2 is not a common factor of m and n. In this case, $n = 3^{r_1} q_1^{i_1} \cdots q_k^{i_k}$ with $r_1 \geq 1$ and

$$L_t = \frac{\phi(mn)}{\phi(m)} = 3^{r_1} q_1^{i_1-1}(q_1-1)\cdots q_k^{i_k-1}(q_k-1).$$

Choose $n_0 = n$. Then, since $q_1, \ldots, q_k$ are distinct prime numbers and different from 3

$$\frac{\phi(3n_0)}{\phi(3)} = 3^{r_1} q_1^{i_1-1}(q_1-1)\cdots q_k^{i_k-1}(q_k-1) = L_t.$$

By using Lemma 4

$$G_{3,n_0} = A_3^{\boxtimes r_1} \boxtimes_{w=1}^{k} \left[A_{q_w}^{\boxtimes(i_w-1)} \boxtimes B_{q_w}\right] = G_{m,n}$$

i.e.,

$$\left|\det(G_{3,n_0})\right| = \left|\det(G_{m,n})\right|.$$

We then consider the case when 2 is a common factor of m and n. Similar to Subcase 1.1, we can also choose $n_0 = 2n$ and $|\det(G_{3,n_0})| = |\det(G_{m,n})|$ by using Lemma 4 and $|B_2| = 1$. Thus, the theorem is proved in this subcase.

Subcase 1.2.2: 3 is a factor of n but not a factor of m.

When 2 is not a common factor of m and n, $n = 3^{i_1} q_2^{i_2} \cdots q_k^{i_k}$, and

$$L_t = \frac{\phi(mn)}{\phi(m)} = 3^{i_1-1}(3-1)q_2^{i_2-1}(q_2-1)\cdots q_k^{i_k-1}(q_k-1)$$
$$G_{m,n} = A_3^{\boxtimes(i_1-1)} \boxtimes B_3 \boxtimes_{w=2}^{k} \left[A_{q_w}^{\boxtimes(i_w-1)} \boxtimes B_{q_w}\right] = G \boxtimes B_3 \tag{67}$$

i.e.,

$$\left|\det(G_{m,n})\right| = \left|\det(G)\right|^2 \left|\det(B_3)\right|^{L_t/2} \tag{68}$$

where

$$G = A_3^{\boxtimes(i_1-1)} \boxtimes_{w=2}^{k} \left[A_{q_w}^{\boxtimes(i_w-1)} \boxtimes B_{q_w}\right]. \tag{69}$$

Let $n_0 = 2^2 3^{i_1-1} q_2^{i_2} \cdots q_k^{i_k} = \frac{4n}{3}$, and we have

$$\frac{\phi(3n_0)}{\phi(3)} = 2 \times 3^{i_1-1} q_2^{i_2-1}(q_2-1)\cdots q_k^{i_k-1}(q_k-1) = L_t$$

and

$$G_{3,n_0} = A_2 \boxtimes B_2 \boxtimes A_3^{\boxtimes(i_1-1)} \boxtimes_{w=2}^{k} \left[A_{q_w}^{\boxtimes(i_w-1)} \boxtimes B_{q_w}\right] = G \boxtimes A_2 \tag{70}$$

i.e.,

$$\left|\det(G_{3,n_0})\right| = \left|\det(G)\right|^2 \left|\det(A_2)\right|^{L_t/2}. \tag{71}$$

When 2 is a common factor of m and n, $n = 2^{r_1} 3^{i_1} q_2^{i_2} \cdots q_k^{i_k}$, and

$$L_t = \frac{\phi(mn)}{\phi(m)} = 3^{i_1-1}(3-1)2^{r_1} q_2^{i_2-1}(q_2-1) \cdots q_k^{i_k-1}(q_k-1)$$
$$G_{m,n} = A_3^{\boxtimes(i_1-1)} \boxtimes B_3 \boxtimes A_2^{\boxtimes r_1} \boxtimes_{w=2}^{k} \left[A_{q_w}^{\boxtimes(i_w-1)} \boxtimes B_{q_w}\right] = G \boxtimes B_3, \tag{72}$$

i.e.,

$$\left|\det(G_{m,n})\right| = \left|\det(G)\right|^2 \left|\det(B_3)\right|^{L_t/2} \tag{73}$$

where

$$G = A_3^{\boxtimes i_1-1} \boxtimes A_2^{\boxtimes r_1} \boxtimes_{w=2}^{k} \left[A_{q_w}^{\boxtimes(i_w-1)} \boxtimes B_{q_w}\right]. \tag{74}$$

Let $n_0 = 2^{r_1+2} 3^{i_1-1} q_2^{i_2} \cdots q_k^{i_k} = \frac{4n}{3}$, and we have

$$\frac{\phi(3n_0)}{\phi(3)} = 3^{i_1-1} 2^{r_1+1} q_2^{i_2-1}(q_2-1)\cdots q_k^{i_k-1}(q_k-1) = L_t$$

and by noticing $|B_2| = 1$

$$G_{3,n_0} = A_2^{\boxtimes(r_1+1)} \boxtimes B_2 \boxtimes A_3^{\boxtimes(i_1-1)} \boxtimes_{w=2}^{k} \left[A_{q_w}^{\boxtimes(i_w-1)} \boxtimes B_{q_w}\right] = G \boxtimes A_2, \tag{75}$$

i.e.,

$$\left|\det(G_{3,n_0})\right| = \left|\det(G)\right|^2 \left|\det(A_2)\right|^{L_t/2}. \tag{76}$$

We next prove

$$\frac{d_{\min}(\Gamma_{L_t}(G_{m,n}))}{\left|\det(G_{m,n})\right| \left|\det(\Lambda_{\zeta_m})\right|^{L_t/2}} \leq \frac{d_{\min}(\Gamma_{L_t}(G_{3,n_0}))}{\left|\det(G_{3,n_0})\right| \left|\det(\Lambda_{\zeta_3})\right|^{L_t/2}}. \tag{77}$$

When $m = 3$, $\Gamma_{L_t}(G_{m,n})$ is an Eisenstein cyclotomic lattice itself. So, we may assume $m = 4$ or $m \geq 5$.

Subcase 1.2.2.1: 3 is a factor of n and $m = 4$.

In this subcase

$$d_{\min}(\Gamma_{L_t}(G_{4,n})) = d_{\min}(\Gamma_{L_t}(G_{3,n_0})) = 1$$

and

$$\left|\det(A_2)\det(\Lambda_{\zeta_3})\right| = \left|\det(B_3)\det(\Lambda_{\zeta_4})\right| = \sqrt{3}.$$

From (67) and (70), or (72) and (75), we have

$$\left|\det(G_{m,n})\right| \left|\det(\Lambda_{\zeta_4})\right|^{L_t/2} = \left|\det(G_{3,n_0})\right| \left|\det(\Lambda_{\zeta_3})\right|^{L_t/2}.$$

Thus, we have

$$\frac{d_{\min}(\Gamma_{L_t}(G_{m,n}))}{\left|\det(G_{m,n})\right| \left|\det(\Lambda_{\zeta_m})\right|^{L_t/2}} = \frac{d_{\min}(\Gamma_{L_t}(G_{3,n_0}))}{\left|\det(G_{3,n_0})\right| \left|\det(\Lambda_{\zeta_3})\right|^{L_t/2}} \tag{78}$$

which proves (77).

Subcase 1.2.2.2: 3 is a factor of n but not a factor of m, and $m \geq 5$.

We first estimate the minimum product $d_{\min}(\Gamma_{L_t}(G_{m,n}))$. To do so, we divide the problem into two situations: m is an even number or both m and n are odd number; and m is an odd number but n is an even number.

i) m is an even number or both m and n are odd numbers.

In this situation, n has the form of $n = 2^{r_1}3^{i_1}q_2^{i_2}\cdots q_k^{i_k}$ and

$$\begin{aligned} L_t &= \frac{\phi(mn)}{\phi(m)} \\ &= 2^{r_1}3^{i_1-1}(3-1)q_2^{i_2-1}(q_2-1)\cdots q_k^{i_k-1}(q_k-1) \end{aligned} \tag{79}$$

where $r_1 = 0$ when m and n are both odd numbers. Let

$$N_0' = 2^{r_1}3^{i_1-1}q_2^{i_2-1}\cdots q_k^{i_k-1}, \text{ and } N' = N_0'q_2\cdots q_k. \tag{80}$$

Then,

$$n = N_0'3q_2\cdots q_k = 3N' \tag{81}$$

and

$$L_t = N_0'(3-1)(q_2-1)\cdots(q_k-1). \tag{82}$$

From the definition of generating matrix $G_{m,n}$ of cyclotomic lattice $\Gamma_{L_t}(G_{m,n})$, we know that the element g_{j_1,j_2} of $G_{m,n}$ at the j_1th row and the j_2th column is $\sigma_{j_1}(\zeta_{mn}^{j_2})$, where σ_{j_1} is an embedding from $\mathbb{Q}(\zeta_{mn})$ to $\mathbb{C}$ that fixes $\mathbb{Q}(\zeta_m)$ and $\sigma_{j_1}(\zeta_{mn}) = \zeta_{mn}^{1+l_{j_1}m}$, such that $0 \leq 1+l_{j_1}m \leq mn$, and $1+l_{j_1}m$ is coprime with mn.

Since q_i in (79) are distinct primes greater than 3, it is not hard to show that when

$$\begin{aligned} L_t &< 2(5-1)(7-1)(11-1)(13-1)(17-1)(19-1)(23-1) \\ &= 36495360, \end{aligned} \tag{83}$$

the following inequality holds:

$$(3-1)(q_2-1)\cdots(q_k-1) \geq q_2\cdots q_k + \frac{1}{N_0'} \tag{84}$$

i.e.,

$$L_t \geq N' + 1 = n/3 + 1. \tag{85}$$

Now we can define an L_t-dimensional vector

$$\boldsymbol{x} = [\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{L_t}] \in \Lambda_{\zeta_m} \times \cdots \times \Lambda_{\zeta_m}$$

with $\boldsymbol{x}_l = 1 - \zeta_m$, when $l = 1$; $\boldsymbol{x}_l = -(1-\zeta_m)$, when $l = N' + 1$; otherwise, $\boldsymbol{x}_l = 0$. Thus,

$$\boldsymbol{y} = [\boldsymbol{y}_1, \ldots, \boldsymbol{y}_{L_t}]^T = G_{m,n}\boldsymbol{x}^T \in \Gamma_{L_t}(G_{m,n})$$

and

$$\begin{aligned} \boldsymbol{y}_i &= (1-\zeta_m)\left[\sigma_i(\zeta_{mn}) - \sigma_i(\zeta_{mn}^{N'+1})\right] \\ &= \sigma_i(\zeta_{mn})(1-\zeta_m)\sigma_i(1-\zeta_{mn}^{N'}) \\ &= \sigma_i(\zeta_{mn})(1-\zeta_m)\sigma_i(1-\zeta_{3m}). \end{aligned} \tag{86}$$

Since $|\sigma_i(\zeta_{mn})| = 1$, $|\boldsymbol{y}_i| = |1-\zeta_m||\sigma_i(1-\zeta_{3m})|$. Then we have

$$\begin{aligned} d_{\min}(\Gamma_{L_t}(G_{m,n})) &\leq |\boldsymbol{y}_1\cdots\boldsymbol{y}_{L_t}| \\ &= |1-\zeta_m|^{L_t}\left|N_{\mathbb{Q}(\zeta_{mn})/\mathbb{Q}(\zeta_m)}(1-\zeta_{3m})\right| \end{aligned} \tag{87}$$

by using the definition of *Relative Norm* [41].

ii) m is an odd number but n is an even number.

In this situation, $n = 3^{i_1}2^{i_2}q_3^{i_3}\cdots q_k^{i_k}$. And

$$\begin{aligned} L_t &= \frac{\phi(mn)}{\phi(m)} \\ &= 3^{i_1-1}(3-1)2^{i_2-1}q_3^{i_3-1}(q_3-1)\cdots q_k^{i_k-1}(q_k-1). \end{aligned} \tag{88}$$

Let

$$N_0' = 3^{i_1-1}2^{i_2-1}q_3^{i_3-1}\cdots q_k^{i_k-1} \quad \text{and} \quad N' = N_0'q_2\cdots q_k. \tag{89}$$

Then

$$n = N_0'3\times 2q_2\cdots q_k = 6N' \tag{90}$$

and

$$L_t = N_0'(3-1)(q_2-1)\cdots(q_k-1). \tag{91}$$

Since the inequality (84) also holds here, we have

$$L_t \geq N' + 1 = n/6 + 1. \tag{92}$$

Similar to the previous situation, we define an L_t-dimensional vector

$$\boldsymbol{x} = [\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{L_t}] \in \Lambda_{\zeta_m} \times \cdots \times \Lambda_{\zeta_m}$$

with $\boldsymbol{x}_l = 1 - \zeta_m$, when $l = 1$; $\boldsymbol{x}_l = -(1-\zeta_m)$, when $l = N' + 1$; otherwise, $\boldsymbol{x}_l = 0$. We then have

$$\boldsymbol{y}_i = \sigma_i(\zeta_{mn})(1-\zeta_m)\sigma_i(1-\zeta_{6m}), \tag{93}$$

and

$$\begin{aligned} d_{\min}(\Gamma_{L_t}(G_{m,n})) &\leq |\boldsymbol{y}_1\cdots\boldsymbol{y}_{L_t}| \\ &= |1-\zeta_m|^{L_t}\left|\mathbb{N}_{\mathbb{Q}(\zeta_{mn})/\mathbb{Q}(\zeta_m)}(1-\zeta_{6m})\right|. \end{aligned} \tag{94}$$

In both situations, (87) and (94) can be rewritten as

$$\begin{aligned} d_{\min}(\Gamma_{L_t}(G_{m,n})) &\leq |\boldsymbol{y}_1\cdots\boldsymbol{y}_{L_t}| \\ &= |1-\zeta_m|^{L_t}\left|\mathbb{N}_{\mathbb{Q}(\zeta_{mn})/\mathbb{Q}(\zeta_m)}(1-\zeta_{3m'})\right| \end{aligned} \tag{95}$$

where $m' = m$ in (87) and $m' = 2m$ in (94). We next want to further estimate the right-hand side of (95).

Since

$$\begin{aligned} &1-\zeta_{3m'} \in \mathbb{Z}(\zeta_{3m'}) \subset \mathbb{Q}(\zeta_{3m'}) \\ &[\mathbb{Q}(\zeta_{mn}) : \mathbb{Q}(\zeta_{3m'})] = L_t/2,\ [\mathbb{Q}(\zeta_{3m'}) : \mathbb{Q}(\zeta_m)] = 2 \end{aligned}$$

from the Relative Norm Theorem [41], we have

$$\begin{aligned}&\left|\mathbb{N}_{\mathbb{Q}(\zeta_{mn})/\mathbb{Q}(\zeta_m)}(1-\zeta_{3m'})\right|\\&=\left|\mathbb{N}_{\mathbb{Q}(\zeta_{3m'})/\mathbb{Q}(\zeta_m)}\left(N_{\mathbb{Q}(\zeta_{mn})/\mathbb{Q}(\zeta_{3m'})}(1-\zeta_{3m'})\right)\right|\\&=\left|\mathbb{N}_{\mathbb{Q}(\zeta_{3m'})/\mathbb{Q}(\zeta_m)}\left((1-\zeta_{3m'})^{L_t/2}\right)\right|\\&=\left|\mathbb{N}_{\mathbb{Q}(\zeta_{3m'})/\mathbb{Q}(\zeta_m)}(1-\zeta_{3m'})\right|^{L_t/2}.\end{aligned}\tag{96}$$

We now consider the field extension $\mathbb{Q}(\zeta_m)\subset\mathbb{Q}(\zeta_{3m'})$. Since 3 is not a factor of m and $m'=2m$ may occur only when m is odd, $\frac{\phi(3m')}{\phi(m)}=2$, from [39, p. 75], there are two embeddings τ_1 and τ_2 from $\mathbb{Q}(\zeta_{3m'})$ to $\mathbb{C}$ that fix $\mathbb{Q}(\zeta_m)$, with $\tau_1(\zeta_{3m'})=\zeta_{3m'}$, $\tau_2(\zeta_{3m'})=\zeta_{3m'}^{l_2m'+1}$, where $l_2=1$, when $m'=3m_0+1$, for some integer m_0; $l_2=2$, when $m'=3m_0+2$, for some integer m_0. Therefore, (95) can be rewritten as

$$\begin{aligned}&d_{\min}(\Gamma_{L_t}(G_{m,n}))\\&\quad\le\left|1-\zeta_m\right|^{L_t}\left|\mathbb{N}_{\mathbb{Q}(\zeta_{mn})/\mathbb{Q}(\zeta_m)}(1-\zeta_{3m'})\right|=d_{m',3}^{L_t/2}\end{aligned}\tag{97}$$

where

$$d_{m',3}\triangleq\left|1-\zeta_m\right|^2 f_{3m'}\tag{98}$$

$$f_{3m'}\triangleq\begin{cases}\left|(1-\zeta_{3m'})(1-\zeta_3\zeta_{3m'})\right|, & \text{if } m'=3m_0+1,\ m_0\ge1\\ \left|(1-\zeta_{3m'})(1-\zeta_3^2\zeta_{3m'})\right|, & \text{if } m'=3m_0+2,\ m_0\ge1.\end{cases}\tag{99}$$

Thus, from (97) and (68) we have

$$\begin{aligned}&\frac{d_{\min}\left(\Gamma_{L_t}(G_{m,n})\right)}{\left|\det(G_{m,n})\right|\left|\det(\Lambda_{\zeta_m})\right|^{L_t/2}}\\&\le\frac{d_{m',3}^{L_t/2}}{\left|\det(G)\right|^2\left|\det(B_3)\right|^{L_t/2}\left|\det(\Lambda_{\zeta_m})\right|^{L_t/2}}\\&=\frac{1}{\left|\det(G)\right|^2}\left(\frac{d_{m',3}}{\left|\det(\Lambda_{\zeta_m})\det(B_3)\right|}\right)^{L_t/2}.\end{aligned}\tag{100}$$

We next consider the cyclotomic lattice $\Gamma_{L_t}(G_{3,n_0})$. Since the minimum product of lattice $\Gamma_{L_t}(G_{3,n_0})$ is

$$d_{\min}\left(\Gamma_{L_t}(G_{3,n_0})\right)=1$$

and the determinant of Λ_{ζ_3} is $\det(\Lambda_{\zeta_3})=\sqrt{3}/2$, from (70), we have

$$\begin{aligned}&\frac{d_{\min}\left(\Gamma_{L_t}(G_{3,n_0})\right)}{\left|\det(G_{3,n_0})\right|\left|\det(\Lambda_{\zeta_3})\right|^{L_t/2}}\\&=\frac{1}{\left|\det(G)\right|^2\left|\det(A_2)\det(\Lambda_{\zeta_3})\right|^{L_t/2}}\\&=\frac{1}{\left|\det(G)\right|^2}\frac{1}{\left|\det(B_3)\right|^{L_t/2}}\end{aligned}\tag{101}$$

where second equation is because

$$\left|\det(B_3)\right|=\left|\det(A_2)\det(\Lambda_{\zeta_3})\right|.$$

By comparing (101) with (100), to prove the theorem, we only need to prove

$$\frac{d_{m',3}}{\left|\det(\Lambda_{\zeta_m})\right|}\le1.$$

In fact, if we let

$$g_1(m)\triangleq\frac{d_{m',3}}{\left|\det(\Lambda_{\zeta_m})\right|}=\frac{d_{m',3}}{\sin(2\pi/m)}=2\tan(\pi/m)\,f_{3m'},\quad m\ge5\tag{102}$$

it is easy to check that $g_1(m)$ is a decreasing function of m, and $g_1(m)\le g_1(5)<0.9<1$ for $m\ge5$. As a remark, when L_t does not satisfy (83), the above estimation can be refined in a tedious manner with more cases and is omitted here, while in a practical system the number of transmit antennas L_t may always satisfy (83).

Case 2: There is Some $p_s\ge5$, i.e., m and n Have Common Prime Factors Greater Than 4: By the assumption of the theorem, there is an integer n_0 such that

$$L_t=\frac{\phi(3n_0)}{\phi(3)}=\frac{\phi(mn)}{\phi(m)}.$$

Let us assume $n_0=3^{u_0}\bar{p}_1^{u_1}\cdots\bar{p}_g^{u_g}$, with $u_0\ge0$ and 3, $\bar{p}_1,\ldots,\bar{p}_g$ are distinct primes. Hence, we have

$$\begin{aligned}L_t&=\frac{\phi(mn)}{\phi(m)}=p_1^{r_1}\cdots p_l^{r_l}q_1^{i_1-1}(q_1-1)\cdots q_k^{i_k-1}(q_k-1)\\&=\frac{\phi(3n_0)}{\phi(3)}=3^{u_0}\bar{p}_1^{u_1-1}(\bar{p}_1-1)\cdots\bar{p}_g^{u_g-1}(\bar{p}_g-1).\end{aligned}\tag{103}$$

We next estimate $\left|\det(G_{3,n_0})\right|$, $d_{\min}(\Gamma_{G_{m,n}})$, $\left|\det(G_{m,n})\right|$, and then show

$$\frac{d_{\min}\left(\Gamma_{L_t}(G_{m,n})\right)}{\left|\det(G_{m,n})\right|\left|\det(\Lambda_{\zeta_m})\right|^{L_t/2}}\le\frac{1}{\left|\det(G_{3,n_0})\right|\left|\det(\Lambda_{\zeta_3})\right|^{L_t/2}}.\tag{104}$$

i) Estimate $\left|\det(G_{3,n_0})\right|$

From Lemma 4, we have

$$G_{3,n_0}=A_3^{u_0}\boxtimes_{t=1}^{g}\left[A_{\bar{p}_t}^{u_t-1}\boxtimes B_{\bar{p}_t}\right].\tag{105}$$

Since $\left|\det(A_N)\right|=N^{N/2}$ for any integer $N>0$, and

$$\begin{aligned}\left|\det(A_{N_1}\boxtimes A_{N_2})\right|&=\left|\det(A_{N_1})\right|^{N_2}\left|\det(A_{N_2})\right|^{N_1}\\&=\left|\det(A_{N_1N_2})\right|\end{aligned}\tag{106}$$

Equation (106) can be rewritten as

$$A_{N_1N_2}=A_{N_1}\boxtimes A_{N_2}.\tag{107}$$

Thus, (105) can be rewritten as

$$G_{3,n_0}=A_{N_0}\boxtimes(\boxtimes_{t=1}^{g}B_{\bar{p}_t})\tag{108}$$

where

$$N_0=3^{u_0}\prod_{t=1}^{g}\bar{p}_t^{u_t-1}.$$

From Lemma 1, we have $\left|\det(B_p)\right|^2=p^{p-2}$ for any prime $p\ge2$. For notational convenience, we use B_N to denote an $(N-1)\times(N-1)$ matrix with determinant

$$\left|\det(B_N)\right|\triangleq N^{(N-2)/2}\tag{109}$$

for any integer N even if N is not a prime. One can check that, for any two integers p and q greater than 2

$$\begin{aligned}|\det(B_p \boxtimes B_q)|^2 &= |\det(B_p)|^{2(q-1)} |\det(B_q)|^{2(p-1)} \\ &= p^{(q-1)(p-2)} q^{(p-1)(q-2)} \\ &\le ((p-1)(q-1)+1))^{(p-1)(q-1)-1}.\end{aligned} \tag{110}$$

Then, (108) can be rewritten as

$$|\det(G_{3,n_0})| \le |\det(A_{N_0} \boxtimes B_{\bar{p}_0})| \tag{111}$$

where $\bar{p}_0 = (\prod_{t=1}^{g} (\bar{p}_t - 1)) + 1$.

For any two integers $N_1 \ge 1$ and $N_2 \ge 2$ except in the cases when $N_2 = 2$ and $N_1 = 2, 3, 4, 5$, one can check that

$$N_1^{N_1 N_2} (N_2+1)^{N_1(N_2-1)} \le (N_1 N_2 + 1)^{N_1 N_2 - 1} \tag{112}$$

which means

$$|\det(A_{N_1} \boxtimes B_{N_2+1})| \le |\det(B_{N_1 N_2+1})|. \tag{113}$$

By the assumption of Case 2, there is some prime number $p_s \ge 5$, and p_s is a factor of some $\bar{p}_t$ or some $\bar{p}_t - 1$ for some $t = 1, \ldots, g$. Thus, $N_0 \ge 5$ or $\bar{p}_0 \ge 2 \times 5 + 1 = 11$ in (111). Since $N_0(\bar{p}_0 - 1) = L_t$, by combining (111) and (113) and repeatedly using (110) we have

$$|\det(G_{3,n_0})| \le |\det(B_{L_t+1})|. \tag{114}$$

ii) Estimate $d_{\min}(\Gamma_{L_t}(G_{m,n}))$

Without loss of generality, we may assume $1 < q_1 < \cdots < q_k$. If $k = 1$ and $q_1 = 2$, then $n = p_1^{r_1} \cdots p_l^{r_l} 2^{i_1}$ and

$$G_{m,n} = A_{p_1^{r_1} \cdots p_l^{r_l}} \boxtimes B_2 \boxtimes A_2^{\boxtimes i_1 - 1} = A_{L_t}.$$

By using (114), we have

$$\begin{aligned}&|\det(G_{m,n})|^2 \\ &\quad = |\det(A_{L_t})|^2 = L_t^{L_t} \\ &\quad > (L_t+1)^{L_t-1} = |\det(B_{L_t+1})|^2 \ge |\det(G_{3,n_0})|^2.\end{aligned} \tag{115}$$

By using Theorem 3, Theorem 4 is proved.

In the case when $q_1 = 2$ and $q_2 \ge 3$, similar to Subcase 1.2.2.2, we may use $m' = q_1 m = 2m$. Thus, without loss of generality, we may assume $q_1 \ge 3$. Let

$$\mathcal{P} \triangleq p_1^{r_1} \cdots p_l^{r_l}, N_0' \triangleq \mathcal{P} q_1^{i_1 - 1} \cdots q_k^{i_k - 1}, N' \triangleq N_0' q_2 \cdots q_k. \tag{116}$$

Then

$$n = N_0' q_1 \cdots q_k = q_1 N' \tag{117}$$

and

$$\begin{aligned}L_t &= \frac{\phi(mn)}{\phi(m)} = \mathcal{P} q_1^{i_1 - 1} (q_1 - 1) \cdots q_k^{i_k - 1} (q_k - 1) \\ &= N_0' (q_1 - 1) \cdots (q_k - 1).\end{aligned} \tag{118}$$

From the assumption of Case 2, there is a $p_s \ge 5$, thus, we have $\mathcal{P} \ge 5$. Similar to (84), when $q_1 = 3$ we have

$$(q_1 - 1) \cdots (q_k - 1) \ge q_2 \cdots q_k + 1/N_0' \tag{119}$$

i.e.,

$$L_t \ge N' + 1 = n/3 + 1 \tag{120}$$

and when $7 \ge q_1 \ge 5$ we have

$$(q_1 - 1) \cdots (q_k - 1) \ge 2 q_2 \cdots q_k + 1/N_0' \tag{121}$$

i.e.,

$$L_t \ge 2N' + 1 = 2n/q_1 + 1 \tag{122}$$

and when $q_1 \ge 11$ we have

$$(q_1 - 1) \cdots (q_k - 1) \ge 3 q_2 \cdots q_k + 1/N_0' \tag{123}$$

i.e.,

$$L_t \ge 3N' + 1 = 3n/q_1 + 1. \tag{124}$$

Similar to Subcase 1.2.2.2, we define an L_t-dimensional vector $\boldsymbol{x} = [\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{L_t}]$ as $\boldsymbol{x}_v = (1 - \zeta_m)\alpha_v$, $v = 1, \ldots, L_t$, where α_v are constants defined in two cases: a) $\alpha_1 = 1$, $\alpha_{1+N'} = -1$, and $\alpha_v = 0$ for other v, when $q_1 = 3$; b) $\alpha_1 = 1$, $\alpha_{1+N'} = -2$, $\alpha_{1+2N'} = 1$, and $\alpha_v = 0$ for other v, when $q_1 \ge 5$.

Let $\boldsymbol{y} = [\boldsymbol{y}_1, \ldots, \boldsymbol{y}_{L_t}]^T = G_{m,n} \boldsymbol{x}^T \in \Gamma_{L_t}(G_{m,n})$. Similar to (86) and (93), we have

$$\begin{aligned}d_{\min}(\Gamma_{L_t}(G_{m,n})) &\le |\boldsymbol{y}_1 \cdots \boldsymbol{y}_{L_t}| \\ &= |1 - \zeta_m|^{L_t} \left| N_{\mathbb{Q}(\zeta_{mn})/\mathbb{Q}(\zeta_m)}(\theta_{q_1,m}) \right|\end{aligned} \tag{125}$$

where

$$\theta_{q_1,m} = \sum_{v=1}^{L_t} \alpha_v \zeta_{q_1 m}^{v-1} \in \mathbb{Z}[\zeta_{q_1 m}] \subset \mathbb{Q}(\zeta_{q_1 m}) \subset \mathbb{Q}(\zeta_{mn}).$$

From the Relative Norm Theorem [41], we have

$$\begin{aligned}&|\mathbb{N}_{\mathbb{Q}(\zeta_{mn})/\mathbb{Q}(\zeta_m)}(\theta_{q_1,m})| \\ &= \left| \mathbb{N}_{\mathbb{Q}(\zeta_{q_1 m})/\mathbb{Q}(\zeta_m)} \left(N_{\mathbb{Q}(\zeta_{mn})/\mathbb{Q}(\zeta_{q_1 m})}(\theta_{q_1,m}) \right) \right| \\ &= \left| \mathbb{N}_{\mathbb{Q}(\zeta_{q_1 m})/\mathbb{Q}(\zeta_m)} \left((\theta_{q_1,m})^{L_t/(q_1-1)} \right) \right| \\ &= \left| \mathbb{N}_{\mathbb{Q}(\zeta_{q_1 m})/\mathbb{Q}(\zeta_m)}(\theta_{q_1,m}) \right|^{L_t/(q_1-1)}.\end{aligned} \tag{126}$$

Define

$$d_{m,q_1} \triangleq |1 - \zeta_m|^{q_1 - 1} \left| \mathbb{N}_{\mathbb{Q}(\zeta_{q_1 m})/\mathbb{Q}(\zeta_m)}(\theta_{q_1,m}) \right| \tag{127}$$

which is

$$d_{m,q_1} = |1 - \zeta_m|^{q_1 - 1} \left| \boldsymbol{y}_1' \cdots \boldsymbol{y}_{q_1 - 1}' \right| \tag{128}$$

where

$$[\boldsymbol{y}'_1,\ldots,\boldsymbol{y}'_{q_1-1}]^T = \begin{cases} G_{m,q_1}[1,-1]^T, & \text{when } q_1=3 \\ G_{m,q_1}[1,-2,1,0,\ldots,0]^T, & \text{when } q_1\geq 5 \end{cases}$$

and G_{m,q_1} is the $(q_1-1)\times(q_1-1)$ generating matrix of cyclotomic lattice $\Gamma_{q_1-1}(G_{m,q_1})$ over Λ_{ζ_m}: When $q_1=3$, we have $\boldsymbol{y}'_1=1-\zeta_{3m}$, $\boldsymbol{y}'_2=1-\zeta_3^l\zeta_{3m}$, where $l=\mathrm{mod}(m,3)$. When $q_1\geq 5$, we have

$$\boldsymbol{y}'_s=\sum_{v=1}^{q_1-1}\beta_v\left(\zeta_{q_1}^{l_s}\zeta_{q_1m}\right)^{v-1}$$

where $\beta_v=\alpha_{1+(v-1)N'}$, and $0\leq l_s\leq q_1$ such that $1+l_sm$ are coprime with q_1m for $s=1,2,\ldots,q_1-1$.

Therefore,

$$d_{\min}(\Gamma_{L_t}(G_{m,n}))\leq d_{m,q_1}^{L_t/(q_1-1)} \tag{129}$$

and

$$\frac{d_{\min}(\Gamma_{L_t}(G_{m,n}))}{|\det(G_{m,n})|\,|\det(\Lambda_{\zeta_m})|^{L_t/2}} \leq \frac{1}{|\det(G_{m,n})|}\left(\frac{d_{m,q_1}}{|\det(\Lambda_{\zeta_m})|^{(q_1-1)/2}}\right)^{L_t/(q_1-1)}. \tag{130}$$

For $q_1\geq 11$, we can also define another L_t-dimensional vector $\tilde{\boldsymbol{x}}=[\tilde{\boldsymbol{x}}_1,\ldots,\tilde{\boldsymbol{x}}_{L_t}]$ as $\tilde{\boldsymbol{x}}_v=(1-\zeta_m)\tilde{\alpha}_v$, $v=1,\ldots,L_t$, $\tilde{\alpha}_1=1$, $\tilde{\alpha}_{1+N'}=-2$, $\tilde{\alpha}_{1+2N'}=2$, $\tilde{\alpha}_{1+3N'}=-1$, and $\tilde{\alpha}_v=0$ for other v.

Let $\tilde{\boldsymbol{y}}=[\tilde{\boldsymbol{y}}_1,\ldots,\tilde{\boldsymbol{y}}_{L_t}]^T=G_{m,n}\tilde{\boldsymbol{x}}^T\in\Gamma_{L_t}(G_{m,n})$. Similar to the derivation of $\boldsymbol{y}$ above, we can get

$$d_{\min}(\Gamma_{L_t}(G_{m,n}))\leq|\tilde{\boldsymbol{y}}_1\cdots\tilde{\boldsymbol{y}}_{L_t}|=\tilde{d}_{m,q_1}^{L_t/(q_1-1)} \tag{131}$$

where

$$\begin{aligned}\tilde{d}_{m,q_1}&=|1-\zeta_m|^{q_1-1}\left|\tilde{\boldsymbol{y}}'_1\cdots\tilde{\boldsymbol{y}}'_{q_1-1}\right|,\\ [\tilde{\boldsymbol{y}}'_1,\ldots,\tilde{\boldsymbol{y}}'_{q_1-1}]^T&=G_{m,q_1}[1,-2,2,-1,0,\ldots,0]^T\end{aligned} \tag{132}$$

and G_{m,q_1} is the $(q_1-1)\times(q_1-1)$ generating matrix of cyclotomic lattice $\Gamma_{q_1-1}(G_{m,q_1})$ over Λ_{ζ_m} and

$$\tilde{\boldsymbol{y}}'_s=\sum_{v=1}^{q_1-1}\tilde{\beta}_v\left(\zeta_{q_1}^{l_s}\zeta_{q_1m}\right)^{v-1}$$

where $\tilde{\beta}_v=\tilde{\alpha}_{1+(v-1)N'}$, and $0\leq l_s\leq q_1$ such that $1+l_sm$ are coprime with q_1m for $s=1,2,\ldots,q_1-1$.

So, when $q_1\geq 11$

$$d_{\min}(\Gamma_{L_t}(G_{m,n}))\leq\min\left(d_{m,q_1}^{L_t/(q_1-1)},\tilde{d}_{m,q_1}^{L_t/(q_1-1)}\right). \tag{133}$$

Let

$$\hat{d}_{m,q_1}=\begin{cases} d_{m,q_1}, & \text{when } q_1<11 \\ \min\left\{d_{m,q_1},\tilde{d}_{m,q_1}\right\}, & \text{when } q_1\geq 11. \end{cases} \tag{134}$$

Combining (134), (133), and (130), we have

$$\frac{d_{\min}(\Gamma_{L_t}(G_{m,n}))}{|\det(G_{m,n})|\,|\det(\Lambda_{\zeta_m})|^{L_t/2}} \leq \frac{1}{|\det(G_{m,n})|}\left(\frac{\hat{d}_{m,q_1}}{|\det(\Lambda_{\zeta_m})|^{(q_1-1)/2}}\right)^{L_t/(q_1-1)}. \tag{135}$$

iii) Estimate $|\det(G_{m,n})|$

From Lemma 4 and (103) and (116) we have

$$G_{m,n}=A_{\mathcal{P}}\boxtimes_{w=1}^{k}\left[A_{q_w}^{\boxtimes i_w-1}\boxtimes B_{q_w}\right] \tag{136}$$

and $|\det(A_{\mathcal{P}})|=\mathcal{P}^{\mathcal{P}/2}$. Since

$$L_t=\frac{\phi(\mathcal{P}n)}{\phi(\mathcal{P})}=\mathcal{P}q_1^{i_w-1}(q_1-1)\cdots q_k^{i_k-1}(q_k-1) \tag{137}$$

$G_{\mathcal{P},n}$ is also a generating matrix of an L_t-dimensional cyclotomic lattice $\Gamma_{L_t}(G_{\mathcal{P},n})$ over $\Lambda_{\zeta_{\mathcal{P}}}$ and

$$G_{\mathcal{P},n}=A_{\mathcal{P}}\boxtimes_{w=1}^{k}\left[A_{q_w}^{\boxtimes i_w-1}\boxtimes B_{q_w}\right] \tag{138}$$

i.e.,

$$|\det(G_{\mathcal{P},n})|=|\det(G_{m,n})|. \tag{139}$$

Since $m=m_1\mathcal{P}\geq 5m_1$, it is not hard to check that

$$\frac{\hat{d}_{m,q_1}}{|\det(\Lambda_{\zeta_m})|^{(q_1-1)/2}}\leq\frac{\hat{d}_{\mathcal{P},q_1}}{|\det(\Lambda_{\zeta_{\mathcal{P}}})|^{(q_1-1)/2}} \tag{140}$$

where we get (141) at the bottom of the page, and

$$[\boldsymbol{y}'_1,\ldots,\boldsymbol{y}'_{q_1-1}]^T = \begin{cases} G_{\mathcal{P},q_1}[1,-1]^T, & \text{when } q_1=3 \\ G_{\mathcal{P},q_1}[1,-2,1,0,\ldots,0]^T, & \text{when } q_1\geq 5 \end{cases} \tag{142}$$

$$[\tilde{\boldsymbol{y}}'_1,\ldots,\tilde{\boldsymbol{y}}'_{q_1-1}]^T = G_{\mathcal{P},q_1}[1,-2,2,-1,0,\ldots,0]^T,\ \text{for } q_1\geq 11 \tag{143}$$

and $G_{\mathcal{P},q_1}$ is the generating matrix of q_1-1-dimensional cyclotomic lattice $\Gamma_{q_1-1}(G_{\mathcal{P},q_1})$ over $\Lambda_{\zeta_{\mathcal{P}}}$.

In fact, $|1-\zeta_m|=2\sin(\pi/m)$, $\det(\Lambda_{\zeta_m})=\sin(2\pi/m)$. Thus,

$$h_1(m)\triangleq\frac{|1-\zeta_m|}{\det(\Lambda_{\zeta_m})}=\frac{1}{\cos(\pi/m)} \tag{144}$$

is a decreasing function of m. By the definition of $\boldsymbol{y}'_1,\ldots,\boldsymbol{y}'_{q_1-1}$, and some numerical calculations, we find that

$$h_2(m)\triangleq\left|\boldsymbol{y}'_1\cdots\boldsymbol{y}'_{q_1-1}\right|$$

$$\hat{d}_{\mathcal{P},q_1}=\begin{cases} |1-\zeta_{\mathcal{P}}|^{q_1-1}\left|\boldsymbol{y}'_1\cdots\boldsymbol{y}'_{q_1-1}\right|, & \text{when } q_1<11 \\ \min\left\{|1-\zeta_{\mathcal{P}}|^{q_1-1}\left|\boldsymbol{y}'_1\cdots\boldsymbol{y}'_{q_1-1}\right|,|1-\zeta_{\mathcal{P}}|^{q_1-1}\left|\tilde{\boldsymbol{y}}'_1\cdots\tilde{\boldsymbol{y}}'_{q_1-1}\right|\right\}, & \text{when } q_1\geq 11 \end{cases} \tag{141}$$

is also a decreasing function of m for any given prime q_1. Then

$$\begin{aligned}\frac{\hat{d}_{m,q_1}}{|\det(\Lambda_{\zeta_m})|^{(q_1-1)/2}} &= |1-\zeta_m|^{(q_1-1)/2} h_1^{(q_1-1)/2}(m) h_2(m) \\ &\le |1-\zeta_m|^{(q_1-1)/2} h_1^{(q_1-1)/2}(\mathcal{P}) h_2(\mathcal{P}) \\ &\le |1-\zeta_{\mathcal{P}}|^{(q_1-1)/2} h_1^{(q_1-1)/2}(\mathcal{P}) h_2(\mathcal{P}) \\ &= \frac{\hat{d}_{\mathcal{P},q_1}}{|\det(\Lambda_{\zeta_{\mathcal{P}}})|^{(q_1-1)/2}}. \end{aligned} \tag{145}$$

From (135) to (142) we have

$$\begin{aligned}&\frac{d_{\min}(\Gamma_{L_t}(G_{m,n}))}{|\det(G_{m,n})|\,|\det(\Lambda_{\zeta_m})|^{L_t/2}} \\ &\quad\le \frac{1}{|\det(G_{\mathcal{P},n})|}\left(\frac{\hat{d}_{\mathcal{P},q_1}}{|\det(\Lambda_{\zeta_{\mathcal{P}}})|^{(q_1-1)/2}}\right)^{L_t/(q_1-1)}. \end{aligned} \tag{146}$$

iv) Prove inequality (104)

From (114) and (146), we can obtain (104) if we can show

$$\begin{aligned}&\frac{1}{|\det(G_{\mathcal{P},n})|^2}\left(\frac{\hat{d}^2_{\mathcal{P},q_1}}{|\det(\Lambda_{\zeta_{\mathcal{P}}})|^{q_1-1}}\right)^{L_t/(q_1-1)} \\ &\qquad\le \frac{1}{|\det(B_{L_t+1})|^2\,|\det(\Lambda_{\zeta_3})|^{L_t}}. \end{aligned} \tag{147}$$

Taking logarithms of both sides of (147), we have

$$\begin{aligned}&\log(|\det(G_{\mathcal{P},n})|^2) \\ &\quad\ge \log(|\det(B_{L_t+1})|^2) + L_t\left[\log(|\det(\Lambda_{\zeta_3})|)\right. \\ &\qquad\left. - \log(|\det(\Lambda_{\zeta_{\mathcal{P}}})|)\right] + \frac{2L_t}{(q_1-1)}\log(\hat{d}_{\mathcal{P},q_1}) \end{aligned} \tag{148}$$

i.e., we need to prove

$$\begin{aligned}&\log(M_0\mathcal{P}) + \sum_{w=1}^{k}\left(\frac{q_w-2}{q_w-1}\log(q_w)\right) \\ &\quad\ge \frac{L_t-1}{L_t}\log(L_t+1) + \log\left(\frac{\sin(2\pi/3)}{\sin(2\pi/\mathcal{P})}\right) \\ &\qquad + \frac{2}{q_1-1}\log(\hat{d}_{\mathcal{P},q_1}) \end{aligned} \tag{149}$$

due to

$$G_{\mathcal{P},n} = A_{\mathcal{P}} \boxtimes_{w=1}^{k} \left[A_{q_w}^{\boxtimes i_w - 1} \boxtimes B_{q_w}\right]$$

$$|\det(G_{\mathcal{P},n})|^2 = (M_0\mathcal{P})^{L_t}\prod_{w=1}^{k} q_w^{L_t\frac{q_w-2}{q_w-1}}$$

and $|\det(B_{L_t+1})| = (L_t+1)^{(L_t-1)/2}$, and

$$M_0 = \prod_{w=1}^{k} q_w^{i_w-1}.$$

Define the following function of k' integer variables:

$$\begin{aligned}\mathcal{F}(j_1,\ldots,j_{k'}) \triangleq\ &\log(\mathcal{P}M_0) + \sum_{w=1}^{k'}\left(\frac{j_w-2}{j_w-1}\log(j_w)\right) \\ &- \frac{L-1}{L}\log(L+1) \\ &- \log\left(\frac{\sin(2\pi/3)}{\sin(2\pi/\mathcal{P})}\right) - \frac{2}{j_1-1}\log(\hat{d}_{\mathcal{P},j_1}) \end{aligned} \tag{150}$$

where

$$L = \mathcal{P}M_0\prod_{w=1}^{k'}(j_w-1), \qquad 3 \le j_1 < \cdots < j_{k'}$$

are odd numbers, $\mathcal{P} \ge 5$ and $\mathcal{P} \nmid j_w$, and $j_w \nmid \mathcal{P}$, and $\hat{d}_{\mathcal{P},j_1}$ is from its definition (141).

Comparing (149) with (150), we can find that (149) can also be represented as

$$\mathcal{F}(j_1,\ldots,j_{k'}) \ge 0 \tag{151}$$

with $k' = k$, $j_w = q_w$, and $L = L_t$. In (149), it is an expression for primes p_l and q_w and is hard to handle. However, (150) or (151) is for any integers, which is easier to understand. Equation (151) can be numerically proved when

a) $\mathcal{P} = 7$ or $\mathcal{P} \ge 10$ or;
b) $j_1 = 3$ or;
c) $\mathcal{P} = 5$, and $k' = 1$ or;
d) $\mathcal{P} = 5$, and $k' = 2$, $(j_1-1)(j_2-1) < (23-1)(29-1)$.

So, when $L_t = L < 5\times(23-1)\times(29-1) = 3080$, (147) and therefore Theorem 4 is proved. For $L_t \ge 3080$, we need to re-estimate the value $d_{\min}(\Gamma_{L_t}(G_{m,n}))$, we omit the lengthy details. QED

C. Proof of Theorem 5

Before proving the theorem, we need the following lemma.

Lemma 5: For any $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{Z}[\zeta_{12}]$, if

$$\mathbb{N}_{\mathbb{Q}(\zeta_{12})/\mathbb{Q}(\zeta_4)}(\boldsymbol{x}) - (1+i)\mathbb{N}_{\mathbb{Q}(\zeta_{12})/\mathbb{Q}(\zeta_4)}(\boldsymbol{y}) = 0$$

then $\boldsymbol{x} = \boldsymbol{y} = 0$.

Proof: Since $\{1, \zeta_{12}\}$ is a basis of $\mathbb{Q}(\zeta_{12})$ over $\mathbb{Q}(\zeta_4)$, for any $\boldsymbol{x} \in \mathbb{Z}[\zeta_{12}]$, it can be expressed by $\boldsymbol{x} = \boldsymbol{x}_1 + \boldsymbol{x}_2\zeta_{12}$ with $\boldsymbol{x}_1, \boldsymbol{x}_2 \in \mathbb{Z}[\zeta_4]$. From the definition of relative algebraic norm, $\mathbb{N}_{\mathbb{Q}(\zeta_{12})/\mathbb{Q}(\zeta_4)}(\boldsymbol{x}) = \sigma_1(\boldsymbol{x})\sigma_2(\boldsymbol{x})$, where σ_1 and σ_2 are the embedding of $\mathbb{Q}(\zeta_{12})$ to $\mathbb{C}$ with $\sigma_1(\boldsymbol{z}) = \sigma_2(\boldsymbol{z}) = \boldsymbol{z}$ for any $\boldsymbol{z} \in \mathbb{Q}(\zeta_4)$ and $\sigma_1(\zeta_{12}) = \zeta_{12}$, $\sigma_2(\zeta_{12}) = \zeta_{12}^5$. Thus,

$$\mathbb{N}_{\mathbb{Q}(\zeta_{12})/\mathbb{Q}(\zeta_4)}(\boldsymbol{x}) = \sigma_1(\boldsymbol{x})\sigma_2(\boldsymbol{x}) = \boldsymbol{x}_1^2 - \boldsymbol{x}_1^2 + j\boldsymbol{x}_1\boldsymbol{x}_2. \tag{152}$$

Similarly, for any $\boldsymbol{y} \in \mathbb{Z}[\zeta_{12}]$ with $\boldsymbol{y} = \boldsymbol{y}_1 + \boldsymbol{y}_2\zeta_{12}$ and $\boldsymbol{y}_1, \boldsymbol{y}_2 \in \mathbb{Z}[\zeta_4]$, we have

$$\mathbb{N}_{\mathbb{Q}(\zeta_{12})/\mathbb{Q}(\zeta_4)}(\boldsymbol{y}) = \boldsymbol{y}_1^2 - \boldsymbol{y}_2^2 + j\boldsymbol{y}_1\boldsymbol{y}_2. \tag{153}$$

Since $(1+j)\mathbb{Z}[\zeta_4]$ is an ideal of ring $\mathbb{Z}[\zeta_4]$, for the above $\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{y}_1, \boldsymbol{y}_2$, there is an integer l_0 such that

$$\boldsymbol{x}_k = \sum_{l=1}^{l_0}\rho^{l-1}\boldsymbol{x}_{k,l} \quad\text{and}\quad \boldsymbol{y}_k = \sum_{l=1}^{l_0}\rho^{l-1}\boldsymbol{y}_{k,l} \tag{154}$$

where $\rho = 1+j$, and

$$\boldsymbol{x}_{k,l}, \boldsymbol{y}_{k,l} \in \{0, \exp(j2p\pi/4), p = 1,\ldots,4\}.$$

If $\mathbb{N}_{\mathbb{Q}(\zeta_{12})/\mathbb{Q}(\zeta_4)}(\boldsymbol{x}) - (1+j)\mathbb{N}_{\mathbb{Q}(\zeta_{12})/\mathbb{Q}(\zeta_4)}(\boldsymbol{y}) = 0$, from (152)–(154), we have

$$\begin{aligned}&\boldsymbol{x}_{1,1}^2 - \boldsymbol{x}_{2,1}^2 + j\boldsymbol{x}_{1,1}\boldsymbol{x}_{2,1} \\ &\quad= \rho\left(\boldsymbol{y}_1^2 - \boldsymbol{y}_2^2 + j\boldsymbol{y}_1\boldsymbol{y}_2\right) - \rho(\rho\bar{\boldsymbol{x}}_{1,1}^2 - \rho\bar{\boldsymbol{x}}_{2,1}^2 + j\rho\bar{\boldsymbol{x}}_{1,1}\bar{\boldsymbol{x}}_{2,1}) \\ &\qquad -2\rho(\boldsymbol{x}_{1,1}\bar{\boldsymbol{x}}_{1,1} - \boldsymbol{x}_{2,1}\bar{\boldsymbol{x}}_{2,1}) - j\rho(\boldsymbol{x}_{1,1}\bar{\boldsymbol{x}}_{2,1} + \boldsymbol{x}_{2,1}\bar{\boldsymbol{x}}_{1,1}) \end{aligned} \tag{155}$$

where

$$\bar{\boldsymbol{x}}_{k,1} = \sum_{l=2}^{l_0}\rho^{l-2}\boldsymbol{x}_{k,l} \in \mathbb{Z}[\zeta_4], \qquad k = 1,2.$$

Since the term on the right-hand side of (155) belongs to $\rho\mathbb{Z}[\zeta_4]$, the term on the left-hand side of (155) also belongs to $\rho\mathbb{Z}[\zeta_4]$, i.e.,

$$\boldsymbol{x}_{1,1}^2 - \boldsymbol{x}_{2,1}^2 + j\boldsymbol{x}_{1,1}\boldsymbol{x}_{2,1} \in \rho\mathbb{Z}[\zeta_4]. \tag{156}$$

Checking (156) with

$$\boldsymbol{x}_{1,1}, \boldsymbol{x}_{2,1} \in \{0, \exp(j2p\pi/4), p = 1, \ldots, 4\}$$

we find that (156) holds only when $\boldsymbol{x}_{1,1} = \boldsymbol{x}_{2,1} = 0$. In this case, (155) becomes

$$\boldsymbol{y}_1^2 - \boldsymbol{y}_1^2 + j\boldsymbol{y}_1\boldsymbol{y}_2 - \rho(\bar{\boldsymbol{x}}_{1,1}^2 - \bar{\boldsymbol{x}}_{2,1}^2 + j\bar{\boldsymbol{x}}_{1,1}\bar{\boldsymbol{x}}_{2,1}) = 0 \tag{157}$$

i.e.,

$$\begin{aligned}&\boldsymbol{y}_{1,1}^2 - \boldsymbol{y}_{2,1}^2 + j\boldsymbol{y}_{1,1}\boldsymbol{y}_{2,1}\\ &\quad= \rho\left(\bar{\boldsymbol{x}}_{1,1}^2 - \bar{\boldsymbol{x}}_{2,1}^2 + j\bar{\boldsymbol{x}}_{1,1}\bar{\boldsymbol{x}}_{2,1}\right) - \rho\left\{\rho(\bar{\boldsymbol{y}}_{1,1}^2 - \bar{\boldsymbol{y}}_{2,1}^2) + j\rho\bar{\boldsymbol{x}}_{1,1}\bar{\boldsymbol{x}}_{2,1}\right\}\\ &\qquad -2\rho(\boldsymbol{y}_{1,1}\bar{\boldsymbol{y}}_{1,1} - \boldsymbol{y}_{2,1}\bar{\boldsymbol{y}}_{2,1} + j\boldsymbol{y}_{1,1}\bar{\boldsymbol{y}}_{2,1} + j\boldsymbol{y}_{2,1}\bar{\boldsymbol{y}}_{1,1})\end{aligned} \tag{158}$$

where

$$\bar{\boldsymbol{y}}_{k,1} = \sum_{l=2}^{l_0} \rho^{l-2}\boldsymbol{y}_{k,l} \in \mathbb{Z}[\zeta_6], \qquad k = 1, 2.$$

Similar to the proof for $\boldsymbol{x}_{1,1}, \boldsymbol{x}_{2,1}$ in (156), we can get $\boldsymbol{y}_{1,1} = \boldsymbol{y}_{2,1} = 0$.

Similarly, we can prove that $\boldsymbol{x}_{1,2} = \boldsymbol{x}_{2,2} = 0$, and then $\boldsymbol{y}_{1,2} = \boldsymbol{y}_{2,2} = 0$, and so on. Finally, we can get $\boldsymbol{x} = \boldsymbol{y} = 0$. QED.

Now, we are ready to prove Theorem 5.

Let $\rho_0 = (1+i)^{1/2}$. We first prove that the diversity product $d_{\min}(G_{4,3}, \rho_0 G_{4,3})$ of two-layer cyclotomic space–time code $X(G_{4,3}, \rho_0 G_{4,3})$ is 1, i.e., $d_{\min}(G_{4,3}, \rho_0 G_{4,3}) = 1$, and then prove that $X(G_{4,3}, \rho_0 G_{4,3})$ is optimal.

For any nonzero two-layer cyclotomic space–time code $X \in X(G_{4,3}, \rho_0 G_{4,3})$, i.e.,

$$X = \begin{bmatrix} \boldsymbol{y}_1(1) & \rho_0\boldsymbol{y}_2(1) \\ \rho_0\boldsymbol{y}_2(2) & \boldsymbol{y}_1(2) \end{bmatrix} \tag{159}$$

where $[\boldsymbol{y}_1(1), \boldsymbol{y}_1(2)]^T, [\boldsymbol{y}_2(1), \boldsymbol{y}_2(2)]^T \in \Gamma_2(G_{4,3})$, from a result in algebraic number theory [37], [38], it is known that $\boldsymbol{y}_1(1)\boldsymbol{y}_1(2) \in \Lambda_{\zeta_4}$, $\boldsymbol{y}_2(1)\boldsymbol{y}_2(2) \in \Lambda_{\zeta_4}$. Furthermore

$$\rho_0^2\boldsymbol{y}_2(1)\boldsymbol{y}_2(2) = (1+j)\boldsymbol{y}_2(1)\boldsymbol{y}_2(2) \in \Lambda_{\zeta_4} \tag{160}$$

which means that the determinant value $\det(X)$ of X in (159) belongs to Λ_{ζ_4}, i.e., $\det(X) \in \Lambda_{\zeta_4}$. Therefore, either $\det(X) = 0$, or $|\det(X)| \geq 1$. We next show $|\det(X)| \geq 1$.

By the definition of cyclotomic lattice $\Gamma_2(G_{4,3})$ over Λ_{ζ_4}, we have

$$\begin{bmatrix} \boldsymbol{y}_1(1) \\ \boldsymbol{y}_1(2) \end{bmatrix} = \begin{bmatrix} \zeta_{12} & \zeta_{12}^2 \\ \zeta_{12}^5 & \zeta_{12}^{10} \end{bmatrix} \begin{bmatrix} \boldsymbol{x}_1 \\ \boldsymbol{x}_2 \end{bmatrix} \tag{161}$$

$$\begin{bmatrix} \boldsymbol{y}_2(1) \\ \boldsymbol{y}_2(2) \end{bmatrix} = \begin{bmatrix} \zeta_{12} & \zeta_{12}^2 \\ \zeta_{12}^5 & \zeta_{12}^{10} \end{bmatrix} \begin{bmatrix} \boldsymbol{y}_1 \\ \boldsymbol{y}_2 \end{bmatrix} \tag{162}$$

where $\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{y}_1, \boldsymbol{y}_2 \in \Lambda_{\zeta_4}$. It is easy to find that

$$\det(X) = \mathbb{N}_{\mathbb{Q}(\zeta_{12})/\mathbb{Q}(\zeta_4)}(\boldsymbol{x}) - (1+i)\mathbb{N}_{\mathbb{Q}(\zeta_{12})/\mathbb{Q}(\zeta_4)}(\boldsymbol{y})$$

where $\boldsymbol{x} = \boldsymbol{x}_1 + \zeta_{12}\boldsymbol{x}_2$, $\boldsymbol{y} = \boldsymbol{y}_1 + \zeta_{12}\boldsymbol{y}_2$.

From Lemma 5, we know that

$$\det(X) = \mathbb{N}_{\mathbb{Q}(\zeta_{12})/\mathbb{Q}(\zeta_4)}(\boldsymbol{x}) - (1+j)\mathbb{N}_{\mathbb{Q}(\zeta_{12})/\mathbb{Q}(\zeta_4)}(\boldsymbol{y}) \neq 0$$

except $\boldsymbol{x} = \boldsymbol{y} = 0$, i.e., codeword $X = 0$, which is also illustrated in Fig. 1. In Fig. 1, the product $\boldsymbol{y}_1(1)\boldsymbol{y}_1(2)$ of the first layer of X is marked by "$\cdot$, "and the product $\rho_0^2\boldsymbol{y}_2(1)\boldsymbol{y}_2(2)$ of the second layer of X is marked by "$\circ$." They do not overlape unless $\boldsymbol{x} = \boldsymbol{y} = 0$, i.e., $\boldsymbol{y}_1(1) = \boldsymbol{y}_1(2) = \boldsymbol{y}_2(1) = \boldsymbol{y}_2(2) = 0$.

This proves that the diversity product $d_{\min}(G_{4,3}, \rho_0 G_{4,3}) = 1$. Thus, we have

$$\frac{d_{\min}(G_{4,3}, \rho_0 G_{4,3})}{|\rho_0|^2 \left|\det(\Lambda_{\zeta_4})\det(G_{4,3})\right|^2} = \frac{1}{3\sqrt{2}} \tag{163}$$

since $|\det(\Lambda_{\zeta_4})| = 1$, $|\det(G_{4,3})| = \sqrt{3}$, and $|\rho_0|^2 = \sqrt{2}$.

We next prove that for any two-layer cyclotomic space–time code $X(\rho_1 G_{m_1,n_1}, \rho_2 G_{m_2,n_2})$, with diversity product $d_{\min}(\rho_1 G_{m_1,n_1}, \rho_2 G_{m_2,n_2})$, the following inequality holds:

$$\begin{aligned}&\frac{d_{\min}(\rho_1 G_{m_1,n_1}, \rho_2 G_{m_2,n_2})}{\left|\rho_1^2\rho_2^2 \det(\Lambda_{\zeta_{m_1}})\det(\Lambda_{\zeta_{m_2}})\det(G_{m_1,n_1})\det(G_{m_2,n_2})\right|}\\ &\qquad \leq \frac{d_{\min}(G_{4,3}, \rho_0 G_{4,3})}{|\rho_0|^2 \left|\det(\Lambda_{\zeta_4})\det(G_{4,3})\right|^2} = \frac{1}{3\sqrt{2}}\end{aligned} \tag{164}$$

which therefore proves that the code $X(G_{4,3}, \rho_0 G_{4,3})$ is optimal based on Lemma 2.

Without loss of generality, we may assume that one of ρ_1 and ρ_2 is 1, and the norm of the other is greater than or equal to 1 since a scaling factor does not affect the ratio at the left-hand side in (164). Since the symmetry of (m_1, n_1) and (m_2, n_2), we may also assume

$$\left|\det(\Lambda_{m_1})\right| \geq \left|\det(\Lambda_{m_2})\right|. \tag{165}$$

For $G_{m,n}$ to be a cyclotomic generating matrix, m has to be not less than 3. Thus, $m_1, m_2 \geq 3$. Under the assumption (165), for parameters m_1 and m_2 we have the following cases: $m_2 = 4$ and $m_1 = 4$; $m_2 = 3, 6$ and $m_1 = 3, 4, 5, 6$; $m_2 = 5$ and $m_1 = 4, 5$; $m_2 \geq 7$ and $m_1 \leq m_2$.

If $|\rho_1| \geq \rho_2 = 1$, then

$$d_{\min}(\rho_1 G_{m_1,n_1}, \rho_2 G_{m_2,n_2}) \leq d_{\min}(\Gamma_2(G_{m_2,n_2}))$$

and therefore,

$$\begin{aligned}&\frac{d_{\min}(\rho_1 G_{m_1,n_1}, \rho_2 G_{m_2,n_2})}{\left|\rho_1^2 \det(G_{m_1,n_1})\right| \left|\det(G_{m_2,n_2})\right| \left|\det(\Lambda_{\zeta_{m_1}})\right| \left|\det(\Lambda_{\zeta_{m_2}})\right|}\\ &\leq \frac{d_{\min}(\Gamma_2(G_{m_2,n_2}))}{|\rho_1^2| \left|\det(G_{m_1,n_1})\right| \left|\det(G_{m_2,n_2})\right| \left|\det(\Lambda_{\zeta_{m_1}})\right| \left|\det(\Lambda_{\zeta_{m_2}})\right|}\\ &\leq \frac{d_{\min}(\Gamma_2(G_{m_2,n_2}))}{\left|\det(G_{m_1,n_1})\right| \left|\det(G_{m_2,n_2})\right| \left|\det(\Lambda_{\zeta_{m_1}})\right| \left|\det(\Lambda_{\zeta_{m_2}})\right|}\\ &\leq \frac{d_{\min}(\Gamma_2(G_{m_2,n_2}))}{\left|\det(G_{m_1,n_1})\right| \left|\det(G_{m_2,n_2})\right| \left|\det(\Lambda_{\zeta_{m_2}})\right|^2}.\end{aligned} \tag{166}$$

If $|\rho_2| \geq \rho_1 = 1$, then

$$d_{\min}(\rho_1 G_{m_1,n_1}, \rho_2 G_{m_2,n_2}) \leq \left|\rho_2^2 d_{\min}(\Gamma_2(G_{m_2,n_2}))\right|$$

and therefore,

$$\begin{aligned}&\frac{d_{\min}(\rho_1 G_{m_1,n_1}, \rho_2 G_{m_2,n_2})}{|\rho_2^2| \left|\det(G_{m_1,n_1})\right| \left|\det(G_{m_2,n_2})\right| \left|\det(\Lambda_{\zeta_{m_1}})\right| \left|\det(\Lambda_{\zeta_{m_2}})\right|}\\ &\leq \frac{|\rho_2^2| d_{\min}(\Gamma_2(G_{m_2,n_2}))}{|\rho_2^2| \left|\det(G_{m_1,n_1})\right| \left|\det(G_{m_2,n_2})\right| \left|\det(\Lambda_{\zeta_{m_1}})\right| \left|\det(\Lambda_{\zeta_{m_2}})\right|}\\ &\leq \frac{d_{\min}(\Gamma_2(G_{m_2,n_2}))}{\left|\det(G_{m_1,n_1})\right| \left|\det(G_{m_2,n_2})\right| \left|\det(\Lambda_{\zeta_{m_2}})\right|^2}.\end{aligned} \tag{167}$$

From the above proof, one can see the left-hand side of (164) is always upper-bounded by

$$\frac{d_{\min}(\rho_1 G_{m_1,n_1}, \rho_2 G_{m_2,n_2})}{\left|\rho_1^2\rho_2^2 \det(\Lambda_{\zeta_{m_1}}) \det(\Lambda_{\zeta_{m_2}}) \det(G_{m_1,n_1}) \det(G_{m_2,n_2})\right|} \le \frac{d_{\min}(\Gamma_2(G_{m_i,n_i}))}{|\det(G_{m_1,n_1})|\,|\det(G_{m_2,n_2})|\,\left|\det(\Lambda_{\zeta_{m_1}})\right|\,\left|\det(\Lambda_{\zeta_{m_2}})\right|}, \quad \text{for } i = 1, 2. \tag{168}$$

In the above discussions, both G_{m_i,n_i} for $i = 1, 2$ have $L_t = 2$. Thus,

i) $|\det(G_{m,n})| = |\det(A_2)| = 2$, when $n = 2$ and m is an even number; or when $n = 4$ and m is an odd number;

ii) $|\det(G_{m,n})| = |\det(B_3)| = \sqrt{3}$, when $n = 3$ and $\gcd(m, n) = 1$; or when $n = 6$ and $\gcd(m, n) = 1$.

We now prove (164) in different cases in terms of values of m_2. When $3 \le m_2 \le 8$, for different m_2, we may need different estimation methods of the left-hand side of (164) and therefore they are listed into separate cases. When $m_2 \ge 9$, we may find a common estimation method of the left-hand side of (164) that is listed as the final case.

Case 1: $m_2 = 3, 4$, or 6: We consider this case in two subcases.

Subcase 1.1: $m_2 = 3, 4$ or 6 but $m_1 \ne 5$.

In this case, $m_1 \in \{3, 4, 6\}$. Let $\mathcal{S}_1$ and $\mathcal{S}_2$ be the following two sets in $\mathbb{C}$:

$$\mathcal{S}_1 = \{1, -1, j, -j\}$$
$$\mathcal{S}_2 = \left\{e^{\frac{j2k\pi}{6}}, \quad k = 1, 2, \ldots, 6\right\}.$$

It is not hard to check that for any $\boldsymbol{z} \in \mathcal{S}_1$, there is some $[\boldsymbol{y}(1), \boldsymbol{y}(2)]^T \in \Gamma_2(G_{4,n})$ such that $\boldsymbol{y}(1)\boldsymbol{y}(2) = \boldsymbol{z}$; and for any $\boldsymbol{z} \in \mathcal{S}_2$, there is some $[\boldsymbol{y}(1), \boldsymbol{y}(2)]^T \in \Gamma_2(G_{3,n})$ and some $[\boldsymbol{y}(1), \boldsymbol{y}(2)]^T \in \Gamma_2(G_{6,n})$ such that $\boldsymbol{y}(1)\boldsymbol{y}(2) = \boldsymbol{z}$.

Without loss of generality, we assume $|\rho_2| \ge \rho_1 = 1$, otherwise, the proof is similar due to the above similar forms of the above values of m_1 and m_2. In this case,

$$d_{\min}(\rho_1 G_{m_1,n_1}, \rho_2 G_{m_2,n_2}) \le \left|d_{\min}(\Gamma_2(G_{m_1,n_1}))\right|.$$

By the assumption (165) and $d_{\min}(\Gamma_2(G_{m_1,n_1})) \le 1$, when $|\rho_2| > 2^{1/4}$, the left-hand side of (164) is upper-bounded by

$$\frac{d_{\min}(\Gamma_2(G_{m_1,n_1}))}{|\rho_2|^2\,|\det(G_{m_1,n_1})|\,|\det(G_{m_2,n_2})|\,\left|\det(\Lambda_{\zeta_{m_2}})\right|^2} \le \frac{1}{3|\rho_2|^2} < \frac{1}{3\sqrt{2}} \tag{169}$$

which proves (164).

Next, we will prove the case of $1 \le |\rho_2| \le 2^{1/4}$.

Subcase 1.1.1: $m_1 \ne 4$, or $m_2 \ne 4$.

In this subcase, at least one of m_1 and m_2 is 3 or 6

$$d_{\min}(G_{m_1,n_1}, \rho_2 G_{m_2,n_2}) \le \min_{\boldsymbol{z}_1 \in \mathcal{S}_1', \boldsymbol{z}_2 \in \mathcal{S}_2'} \left|z_1 - \rho_2^2 z_2\right| \le \sqrt{1 + |\rho_2|^4 - 2|\rho_2|^2 \cos(\pi/6)} \tag{170}$$

where $\mathcal{S}_1'$ and $\mathcal{S}_2'$ are $\mathcal{S}_1$ or $\mathcal{S}_2$, and at least one of $\mathcal{S}_1'$ and $\mathcal{S}_2'$ is $\mathcal{S}_2$. From i) and ii), it is not hard to see that, since m_1, m_2 are $3, 4$, or 6, we have

$$\left|\det(G_{m_1,n_1}) \det(\Lambda_{\zeta_{m_1}})\right| \cdot \left|\det(G_{m_2,n_2}) \det(\Lambda_{\zeta_{m_2}})\right| \ge 3.$$

Thus, the left-hand side of (164) becomes

$$\frac{d_{\min}(G_{m_1,n_1}, \rho_2 G_{m_2,n_2})}{|\rho_2|^2\,|\det(G_{m_1,n_1})|\,|\det(G_{m_2,n_2})|\,\left|\det(\Lambda_{\zeta_{m_1}})\right|\,\left|\det(\Lambda_{\zeta_{m_2}})\right|} \le \frac{\sqrt{1 + |\rho_2|^4 - 2|\rho_2|^2 \cos(\pi/6)}}{3|\rho_2|^2} < \frac{1}{3\sqrt{2}} \tag{171}$$

where the last inequality is because

$$\frac{\sqrt{1 + x^2 - 2x\cos(\pi/6)}}{3x} \le \frac{1}{3\sqrt{2}}, \qquad \text{for } 1 \le x \le \sqrt{2} \tag{172}$$

which proves (164).

Subcase 1.1.2: $m_1 = 4$, and $m_2 = 4$.

In this subcase, by computer search, we find that for any $1 \le |\rho| \le 2^{1/4}$

$$\frac{d_{\min}(G_{4,3}, \rho G_{4,3})}{3|\rho|^2} \le \frac{d_{\min}(G_{4,3}, \sqrt{1+i} G_{4,3})}{3\sqrt{2}} = \frac{1}{3\sqrt{2}}.$$

Subcase 1.2: $m_2 = 6$ or $m_2 = 3$, and $m_1 = 5$.

In this case, $n_1 = 3, 4$ or 6.

Subcase 1.2.1: $m_2 = 6$ or $m_2 = 3$, $m_1 = 5$, $n_1 = 6$.

In this subcase, choose $[\boldsymbol{x}_1, \boldsymbol{x}_2] = [1, -1]$

$$d_{\min}(\Gamma_2(G_{m_1,n_1})) \le |\boldsymbol{y}_1 \boldsymbol{y}_2| \le 0.3820$$

where $[\boldsymbol{y}_1, \boldsymbol{y}_2]^T = G_{5,6}[\boldsymbol{x}_1, \boldsymbol{x}_2]^T$, and

$$G_{5,6} = \begin{bmatrix} 1 & 1 \\ \zeta_3 & \zeta_3^2 \end{bmatrix} \begin{bmatrix} \zeta_{30} & \\ & \zeta_{30}^2 \end{bmatrix}.$$

From (168), $\left|\det(G_{m_1,n_1})\right| \ge \sqrt{3}$ and $\left|\det(G_{m_2,n_2})\right| \ge \sqrt{3}$ in i) and ii), the left-hand side of (164) is upper-bounded by

$$\frac{d_{\min}(\Gamma_2(G_{m_1,n_1}))}{|\det(G_{m_1,n_1})|\,|\det(G_{m_2,n_2})|\,\left|\det(\Lambda_{\zeta_{m_1}})\right|\,\left|\det(\Lambda_{\zeta_{m_2}})\right|} \le \frac{0.3820}{3 \times |\det(\Lambda_{\zeta_5})|\,\left|\det(\Lambda_{\zeta_{m_2}})\right|} \le \frac{1}{3\sqrt{2}}$$

which proves (164).

Subcase 1.2.2: $m_2 = 6$ or $m_2 = 3$, $m_1 = 5$, $n_1 = 4$.

In this subcase, choose $[\boldsymbol{x}_1, \boldsymbol{x}_2] = [1, -1]$

$$d_{\min}(\Gamma_2(G_{m_1,n_1})) \le |\boldsymbol{y}_1 \boldsymbol{y}_2| = 0.6180$$

where $[\boldsymbol{y}_1, \boldsymbol{y}_2]^T = G_{5,4}[\boldsymbol{x}_1, \boldsymbol{x}_2]^T$, with

$$G_{5,4} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} \zeta_{20} & \\ & \zeta_{20}^2 \end{bmatrix}. \tag{173}$$

By using i) and ii), we have $|\det(G_{m_2,n_2}) \det(\Lambda_{\zeta_{m_2}})| = \sqrt{3}$. From (168) and i), the left-hand side of (164) is upper-bounded by

$$\frac{d_{\min}(\Gamma_2(G_{m_1,n_1}))}{|\det(G_{m_1,n_1})|\,|\det(G_{m_2,n_2})|\,\left|\det(\Lambda_{\zeta_{m_1}})\right|\,\left|\det(\Lambda_{\zeta_{m_2}})\right|} \le \frac{d_{\min}(\Gamma_2(G_{m_1,n_1}))}{2\sqrt{3} \times |\det(\Lambda_{\zeta_5})|} \le 0.1876 < \frac{1}{3\sqrt{2}} \tag{174}$$

which proves (164).

Subcase 1.2.3: $m_2 = 6$ *or* $m_2 = 3$, $m_1 = 5$, $n_1 = 3$.

By using i) and ii), we have $|\det(G_{m_2,n_2})\det(\Lambda_{\zeta_{m_2}})| = \sqrt{3}$. In this subcase, choose $[\boldsymbol{x}_1, \boldsymbol{x}_2] = [-(1+2\zeta_5), 2+\zeta_5]$

$$d_{\min}\left(\Gamma_2\left(G_{m_1,n_1}\right)\right) \le |\boldsymbol{y}_1\boldsymbol{y}_2| = 0.5982$$

where

$$G_{5,3} = \begin{bmatrix} 1 & 1 \\ \zeta_3 & \zeta_3^2 \end{bmatrix} \begin{bmatrix} \zeta_{15} & \\ & \zeta_{15}^2 \end{bmatrix}. \tag{175}$$

Without loss of generality, we assume $|\rho_2| \ge \rho_1 = 1$.

When $|\rho_2| > 1.1^{1/2}$,

$$\begin{aligned} &d_{\min}(\rho_1 G_{m_1,n_1}, \rho_2 G_{m_2,n_2}) \\ &\quad \le_{\min}\left(\Gamma_2\left(G_{m_1,n_1}\right)\right) \le |\boldsymbol{y}_1\boldsymbol{y}_2| = 0.5982. \\ &\frac{d_{\min}(\rho_1 G_{m_1,n_1}, \rho_2 G_{m_2,n_2})}{\left|\rho_1^2\rho_2^2 \det(\Lambda_{\zeta_{m_1}})\det(\Lambda_{\zeta_{m_2}})\det(G_{m_1,n_1})\det(G_{m_2,n_2})\right|} \\ &\quad \le \frac{0.5982}{|\rho_2|^2\left|\det(\Lambda_{\zeta_{m_2}})\det(\Lambda_{\zeta_5})\det(G_{m_2,n_2})\det(G_{5,3})\right|} \\ &\quad = \frac{0.5982}{1.1 \times 3\sin(2\pi/5)} < \frac{1}{3\sqrt{2}}. \end{aligned} \tag{176}$$

When $1 \le |\rho_2| \le 1.1^{1/2}$, similar to Subcase 1.1

$$d_{\min}(G_{m_1,n_1}, \rho_2 G_{m_2,n_2}) \le \min_{\boldsymbol{z}_1 \in \mathcal{S}_1', \boldsymbol{z}_2 \in \mathcal{S}_2'} \left|z_1 - \rho_2^2 z_2\right| \le 0.4$$

where $\mathcal{S}_1'$ and $\mathcal{S}_2'$ are $\mathcal{S}_1$ or $\mathcal{S}_2$, and $\mathcal{S}_2$ is the same as the one in Subcase 1.1 but $\mathcal{S}_1$ is taken from the set of all products of components $[\boldsymbol{y}(1), \boldsymbol{y}(2)]$ on the lattice $\Gamma_2\left(G_{5,3}\right)$ as

$$\mathcal{S}_1 = \{\boldsymbol{y}_1(k)\boldsymbol{y}_2(k), \quad k = 1, 2, \ldots, 6\}$$

where

$$\begin{aligned} [\boldsymbol{y}_1(k), \boldsymbol{y}_2(k)]^T &= G_{5,3}[\boldsymbol{x}_1(k), \boldsymbol{x}_2(k)]^T \\ [\boldsymbol{x}_1(1), \boldsymbol{x}_2(1)] &= [-2+\zeta_5, -2] \\ [\boldsymbol{x}_1(2), \boldsymbol{x}_2(2)] &= [-1-2\zeta_5, 2+\zeta_5] \\ [\boldsymbol{x}_1(3), \boldsymbol{x}_2(3)] &= [-1, -\zeta_5] \\ [\boldsymbol{x}_1(4), \boldsymbol{x}_2(4)] &= [-1, 1] \\ [\boldsymbol{x}_1(5), \boldsymbol{x}_2(5)] &= [-2\zeta_5, 1-2\zeta_5] \\ [\boldsymbol{x}_1(6), \boldsymbol{x}_2(6)] &= [-\zeta_5, \zeta_5]. \end{aligned}$$

Thus,

$$\begin{aligned} &\frac{d_{\min}(G_{m_1,n_1}, \rho_2 G_{m_2,n_2})}{\left|\rho_2^2 \det(\Lambda_{\zeta_{m_1}})\det(\Lambda_{\zeta_{m_2}})\det(G_{m_1,n_1})\det(G_{m_2,n_2})\right|} \\ &\quad \le \frac{0.4}{|\rho_2|^2\left|\det(\Lambda_{\zeta_{m_2}})\det(\Lambda_{\zeta_5})\det(G_{m_2,n_2})\det(G_{5,3})\right|} \\ &\quad \le \frac{0.4}{3\sin(2\pi/5)} < \frac{1}{3\sqrt{2}} \end{aligned} \tag{177}$$

which proves (164).

Case 2: $m_2 = 5$*:* In this case, $n_2 = 3, 4$, or 6.

Subcase 2.1: $m_2 = 5$, $n_2 = 3$ *or* $n_2 = 6$.

Subcase 2.1.1: $m_2 = 5$, $n_2 = 6$.

In this subcase, similar to Subcase 1.2.1, we have

$$d_{\min}\left(\Gamma_2\left(G_{m_2,n_2}\right)\right) \le 0.3820$$

and from (166) and (167), the left-hand side of (164) is upper-bounded by

$$\begin{aligned} &\frac{d_{\min}\left(\Gamma_2\left(G_{m_2,n_2}\right)\right)}{\left|\det\left(G_{m_1,n_1}\right)\right|\left|\det\left(G_{m_2,n_2}\right)\right|\left|\det\left(\Lambda_{\zeta_{m_2}}\right)\right|^2} \\ &\qquad \le \frac{0.3820}{3 \times \left|\det\left(\Lambda_{\zeta_5}\right)\right|^2} = 0.1408 \le \frac{1}{3\sqrt{2}} \end{aligned} \tag{178}$$

which proves (164).

Subcase 2.1.2: $m_2 = 5$, $n_2 = 3$.

This subcase can be proved similarly to Subcase 1.2.3.

Subcase 2.2: $m_2 = 5$, $n_2 = 4$.

In this subcase, similarly to Subcase 1.2.2, we have

$$d_{\min}\left(\Gamma_2\left(G_{m_2,n_2}\right)\right) \le 0.6180.$$

By assumption (165), we have $m_1 = 4$ or 5. By i), we have $|\det(G_{5,4})| = 2$.

Subcase 2.2.1: $m_2 = 5$, $n_2 = 4$; $m_1 = 4$.

In this subcase, by i) and ii), we have

$$\left|\det\left(G_{m_1,n_1}\right)\det\left(\Lambda_{\zeta_{m_1}}\right)\right| \ge \sqrt{3}.$$

From (168), the left-hand side of (164) is upper-bounded by

$$\begin{aligned} &\frac{d_{\min}\left(\Gamma_2\left(G_{m_2,n_2}\right)\right)}{\left|\det\left(G_{m_1,n_1}\right)\right|\left|\det\left(G_{m_2,n_2}\right)\right|\left|\det\left(\Lambda_{\zeta_{m_1}}\right)\right|\left|\det\left(\Lambda_{\zeta_{m_2}}\right)\right|} \\ &\quad \le \frac{d_{\min}\left(\Gamma_2\left(G_{m_2,n_2}\right)\right)}{2\sqrt{3} \times \left|\det\left(\Lambda_{\zeta_5}\right)\right|} \\ &\quad \le 0.1876 < \frac{1}{3\sqrt{2}} \end{aligned} \tag{179}$$

which proves (164).

Subcase 2.2.2: $m_2 = 5$, $n_2 = 4$; $m_1 = 5$, $n_1 = 3$ *or* $n_1 = 6$.

In this subcase

$$d_{\min}\left(\Gamma_2\left(G_{m_1,n_1}\right)\right) \le 0.5982$$

and $|\det(G_{5,4})| = 2$. From (168), the left-hand side of (164) is upper-bounded by

$$\begin{aligned} &\frac{d_{\min}\left(\Gamma_2\left(G_{m_1,n_1}\right)\right)}{\left|\det\left(G_{m_1,n_1}\right)\right|\left|\det\left(G_{m_2,n_2}\right)\right|\left|\det\left(\Lambda_{\zeta_{m_1}}\right)\right|\left|\det\left(\Lambda_{\zeta_{m_2}}\right)\right|} \\ &\qquad \le \frac{d_{\min}\left(\Gamma_2\left(G_{m_1,n_1}\right)\right)}{2\sqrt{3} \times \left|\det\left(\Lambda_{\zeta_5}\right)\right|^2} \le 0.1909 < \frac{1}{3\sqrt{2}} \end{aligned} \tag{180}$$

which proves (164).

Subcase 2.2.3: $m_2 = 5$, $n_2 = 4$; $m_1 = 5$, $n_1 = 4$.

By (168), the left-hand side of (164) is upper-bounded by

$$\begin{aligned} &\frac{d_{\min}(\Gamma_2(G_{m_2,n_2}))}{|\det(G_{m_1,n_1})|\,|\det(G_{m_2,n_2})|\,\left|\det(\Lambda_{\zeta_{m_1}})\right|\left|\det(\Lambda_{\zeta_{m_2}})\right|} \\ &\quad = \frac{d_{\min}(\Gamma_2(G_{5,4}))}{|\det(G_{5,4})|^2|\det(\Lambda_{\zeta_5})|^2} \le \frac{0.6180}{4\sin^2(2\pi/5)} < \frac{1}{3\sqrt{2}} \end{aligned} \tag{181}$$

which proves (164).

Case 3: $m_2 = 7$*:* In this case, $n_2 = 3, 4$, or 6.

Subcase 3.1: $m_2 = 7$, $n_2 = 4$.

In this subcase, let $\boldsymbol{x} = 1 - \zeta_7$

$$[\boldsymbol{y}_1, \boldsymbol{y}_2]^T = G_{7,4}[\boldsymbol{x}, -\boldsymbol{x}]^T \in \Gamma_2(G_{7,4})$$

$|\det(G_{7,4})| = 2$, where

$$G_{7,4} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} \zeta_{28} & \\ & \zeta_{28}^2 \end{bmatrix}. \tag{182}$$

It is easy to calculate that

$$\begin{aligned} |\boldsymbol{x}| &= 2\sin(\pi/7) \\ |\boldsymbol{y}_1| &= |\boldsymbol{x}||1-\zeta_{28}| = 2|\boldsymbol{x}|\sin(\pi/28) \\ |\boldsymbol{y}_2| &= |\boldsymbol{x}||1+\zeta_{28}| \le 2|\boldsymbol{x}| \\ |\det(\Lambda_{\zeta_7})| &= \sin(2\pi/7) = 2\sin(\pi/7)\cos(\pi/7). \end{aligned}$$

Thus,

$$\begin{aligned} d_{\min}(\Gamma_2(G_{7,4})) &\le |\boldsymbol{y}_1\boldsymbol{y}_2| \le 4|\boldsymbol{x}|^2\sin(\pi/28) \\ &= 16\sin^2(\pi/7)\sin(\pi/28). \end{aligned}$$

By (166) and (167) and $|\det(G_{m_1,n_1})| \ge \sqrt{3}$ in i) and ii), the left-hand side of (164) is upper-bounded by

$$\begin{aligned} &\frac{d_{\min}(\Gamma_2(G_{7,4}))}{|\det(G_{m_1,n_1})|\,|\det(G_{7,4})|\,|\det(\Lambda_{\zeta_7})|^2} \\ &\le \frac{16\sin^2(\pi/7)\sin(\pi/28)}{3\times 4\sin^2(\pi/7)\cos^2(\pi/7)} \\ &= \frac{4\sin(\pi/28)}{3\cos^2(\pi/7)} = 0.1839 < \frac{1}{3\sqrt{2}} \end{aligned} \tag{183}$$

which proves (164).

Subcase 3.2: $m_2 = 7$, $n_2 = 3$ *or* $n_2 = 6$.

In this subcase, choose $[\boldsymbol{x}_1\boldsymbol{x}_2] = [1, \zeta_7]$, $[\boldsymbol{y}_1, \boldsymbol{y}_2]^T = G_{7,n_2}[\boldsymbol{x}_1, \boldsymbol{x}_2]^2$, where

$$\begin{aligned} G_{7,3} &= \begin{bmatrix} 1 & 1 \\ \zeta_3 & \zeta_3^2 \end{bmatrix} \begin{bmatrix} \zeta_{21} & \\ & \zeta_{21}^2 \end{bmatrix} \\ G_{7,6} &= \begin{bmatrix} 1 & 1 \\ \zeta_3 & \zeta_3^2 \end{bmatrix} \begin{bmatrix} \zeta_{42} & \\ & \zeta_{42}^2 \end{bmatrix}. \end{aligned} \tag{184}$$

It is easy to check that

$$d_{\min}(\Gamma_2(G_{m_1,n_1})) \le |\boldsymbol{y}_1\boldsymbol{y}_2| \le 0.2470.$$

Since

$$\begin{aligned} |\det(G_{m_1,n_1})| &\ge \sqrt{3} \\ |\det(G_{7,3})| &= \sqrt{3} \\ |\det(\Lambda_{m_1,n_1})| &\ge |\det(\Lambda_{m_2,n_2})| = \sin(2\pi/7) \end{aligned}$$

and (168), the left-hand side of (164) is upper-bounded by

$$\begin{aligned} &\frac{d_{\min}(\Gamma_2(G_{m_1,n_1}))}{\left|\det(G_{7,3})\det(\Lambda_{\zeta_{m_1}})\right|\,|\det(G_{7,3})|\,|\det(\Lambda_{\zeta_7})|} \\ &\le \frac{0.2470}{3\sin^2(2\pi/7)} < \frac{1}{3\sqrt{2}}, \end{aligned} \tag{185}$$

which proves (164).

Case 4: $m_2 = 8$: In this case, $n_2 = 3$, or $n_2 = 2$.

Subcase 4.1: $m_2 = 8$, $n_2 = 3$.

In this subcase, let $\boldsymbol{x} = 1 - \zeta_8$

$$[\boldsymbol{y}_1, \boldsymbol{y}_2]^T = G_{8,3}[\boldsymbol{x}, -\boldsymbol{x}]^T \in \Gamma_2(G_{8,3})$$

$|\det(G_{8,3})| = \sqrt{3}$, where

$$G_{8,3} = \begin{bmatrix} 1 & 1 \\ \zeta_3^2 & \zeta_3^4 \end{bmatrix} \begin{bmatrix} \zeta_{24} & \\ & \zeta_{24}^2 \end{bmatrix}. \tag{186}$$

It is easy to calculate that

$$\begin{aligned} |\boldsymbol{x}| &= 2\sin(\pi/8) \\ |\boldsymbol{y}_1| &= |\boldsymbol{x}||1-\zeta_{24}| = 2|\boldsymbol{x}|\sin(\pi/24) \\ |\boldsymbol{y}_2| &= |\boldsymbol{x}||1-\zeta_3^2\zeta_{24}| \\ |\boldsymbol{y}_1\boldsymbol{y}_2| &= 0.2426 \end{aligned}$$

and

$$|\det(\Lambda_{\zeta_8})| = \sin(2\pi/8).$$

By the assumption

$$|\det(\Lambda_{m_1})| \ge |\det(\Lambda_{\zeta_8})|$$

in (165), (168), the left-hand side of (164) is upper-bounded by

$$\begin{aligned} &\frac{d_{\min}(\Gamma_2(G_{8,3}))}{\left|\det(G_{m_1,n_1})\det(\Lambda_{\zeta_{m_1}})\right|\,|\det(G_{8,3})|\,|\det(\Lambda_{\zeta_8})|} \\ &\le \frac{0.2426}{3\sin^2(2\pi/8)} < \frac{1}{3\sqrt{2}} \end{aligned} \tag{187}$$

which proves (164).

Subcase 4.2: $m_2 = 8$, $n_2 = 2$.

In this subcase, let $\boldsymbol{x} = 1 - \zeta_8$,

$$[\boldsymbol{y}_1, \boldsymbol{y}_2]^T = G_{8,2}[\boldsymbol{x}, -\boldsymbol{x}]^T \in \Gamma_2(G_{8,2})$$

$|\det(G_{8,2})| = 2$, where

$$G_{8,2} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} \zeta_{16} & \\ & \zeta_{16}^2 \end{bmatrix}. \tag{188}$$

It is easy to calculate that

$$\begin{aligned} |\boldsymbol{x}| &= 2\sin(\pi/8) \\ |\boldsymbol{y}_1| &= |\boldsymbol{x}||1-\zeta_{16}| \\ |\boldsymbol{y}_2| &= |\boldsymbol{x}||1+\zeta_{16}| \\ d_{\min}(\Gamma_2(G_{8,2})) &\le |\boldsymbol{y}_1\boldsymbol{y}_2| = 0.4483 \end{aligned}$$

and

$$|\det(\Lambda_{\zeta_8})| = \sin(2\pi/8).$$

Since the assumption

$$\left|\det(\Lambda_{\zeta_{m_1}})\right| \ge \left|\det(\Lambda_{\zeta_{m_8}})\right|$$

in (165), m_1 has to be an integer in the range $3 \le m_1 \le 8$.

Subcase 4.2.1: $m_2 = 8$, $n_2 = 2$; $m_1 = 3, 4,$ *or* 6.

In these subcase

$$|\det(G_{m_1,n_1})|\,|\det(\Lambda_{\zeta_{m_1}})| \ge \sqrt{3}.$$

By (168), the left-hand side of (164) is upper-bounded by

$$\begin{aligned} &\frac{d_{\min}(\Gamma_2(G_{8,2}))}{|\det(G_{m_1,n_1})\det(\Lambda_{m_1})|\,|\det(G_{8,2})|\,|\det(\Lambda_{\zeta_8})|} \\ &\le \frac{0.4483}{2\sqrt{3}\sin(2\pi/8)} < \frac{1}{3\sqrt{2}} \end{aligned} \tag{189}$$

which proves (164).

Subcase 4.2.2: $m_2 = 8$, $n_2 = 2$; $m_1 = 5$, $n_1 = 4$.

In this subcase

$$|\det(G_{m_1,n_1})| = |\det(G_{5,4})| = 2$$

$|\det(\Lambda_{\zeta_{m_1}})| = \sin(2\pi/5)$. By (168), the left-hand side of (164) is upper-bounded by

$$\frac{d_{\min}(\Gamma_2(G_{8,2}))}{|\det(G_{m_1,n_1})\det(\Lambda_{\zeta_{m_1}})|\,|\det(G_{8,2})|\,|\det(\Lambda_{\zeta_8})|} \le \frac{0.4483}{4\sin(2\pi/5)\sin(2\pi/8)} < \frac{1}{3\sqrt{2}} \quad (190)$$

which proves (164).

Subcase 4.2.3: $m_2 = 8$, $n_2 = 2$; $m_1 = 5$, $n_1 = 3$, *or* $n_1 = 6$.

In this subcase, we have

$$d_{\min}(\Gamma_2(G_{m_2,n_2})) = d_{\min}(\Gamma_2(G_{8,2})) \le 0.4483.$$

By (168), the left-hand side of (164) is upper-bounded by

$$\frac{d_{\min}(\Gamma_2(G_{8,2}))}{|\det(G_{5,n_1})\det(\Lambda_5)|\,|\det(G_{8,2})|\,|\det(\Lambda_{\zeta_8})|} \le \frac{0.4483}{2\sqrt{3}\sin(2\pi/5)\sin(2\pi/8)} \le \frac{1}{3\sqrt{2}} \quad (191)$$

which proves (164).

Subcase 4.2.4: $m_2 = 8$, $n_2 = 2$; $m_1 = 7$, $n_1 = 4$.

In this subcase, from Subcase 3.1, we have

$$d_{\min}(\Gamma_2(G_{m_1,n_1})) = d_{\min}(\Gamma_2(G_{7,4})) \le 16\sin^2(\pi/7)\sin(\pi/28) = 0.3372.$$

Similarly to Subcase 4.2.3, the left-hand side of (164) is upper-bounded by

$$\frac{d_{\min}(\Gamma_2(G_{7,4}))}{|\det(G_{7,4})\det(\Lambda_7)|\,|\det(G_{8,2})|\,|\det(\Lambda_{\zeta_8})|} \le \frac{0.3372}{4\sin(2\pi/7)\sin(2\pi/8)} < \frac{1}{3\sqrt{2}} \quad (192)$$

which proves (164).

Subcase 4.2.5: $m_2 = 8$, $n_2 = 2$; $m_1 = 7$, $n_1 = 3$.

In this subcase, from Subcase 3.2, we have

$$d_{\min}(\Gamma_2(G_{m_1,n_1})) = d_{\min}(\Gamma_2(G_{7,3})) \le 0.2470.$$

Similarly to Subcase 4.2.3, the left-hand side of (164) is upper-bounded by

$$\frac{d_{\min}(\Gamma_2(G_{7,3}))}{|\det(G_{7,3})\det(\Lambda_7)|\,|\det(G_{8,2})|\,|\det(\Lambda_{\zeta_8})|} \le \frac{0.2470}{2\sqrt{3}\sin(2\pi/7)\sin(2\pi/8)} < \frac{1}{3\sqrt{2}} \quad (193)$$

which proves (164).

Subcase 4.2.6: $m_2 = 8$, $n_2 = 2$; $m_1 = 8$, $n_1 = 3$.

This subcase is the same as Subcase 4.1.

Subcase 4.2.7: $m_2 = 8$, $n_2 = 2$; $m_1 = 8$, $n_1 = 2$.

In this subcase, $G_{m_1,n_1} = G_{m_2,n_2} = G_{8,2}$ and we may assume $|\rho_2| \ge \rho_1 = 1$, otherwise, the proof is the same. Thus,

$$d_{\min}(G_{8,2}, \rho_2 G_{8,2}) \le d_{\min}(\Gamma_2(G_{m_1,n_1})) = d_{\min}(\Gamma_2(G_{8,2})) \le 0.4483.$$

When $|\rho_2| > 1.08$, the left hand side of (164) becomes

$$\frac{d_{\min}(G_{8,2}, \rho_2 G_{8,3})}{|\rho_2^2|\,|\det(G_{8,2})|\,|\det(G_{8,2})|\,|\det(\Lambda_{\zeta_8})|^2} \le \frac{0.4483}{1.08^2 \times 4\sin^2(2\pi/8)} < \frac{1}{3\sqrt{2}} \quad (194)$$

which proves (164).

When $1 \le |\rho_2| \le 1.08$, let $\mathcal{S} = \{[\boldsymbol{y}_1, \boldsymbol{y}_2]^T\}$ be a subset of $\Gamma_2(G_{8,2})$ with

$$[\boldsymbol{y}_1, \boldsymbol{y}_2]^T = G_{8,2}[\boldsymbol{x}_1, \boldsymbol{x}_2]^T, \quad \text{with } \boldsymbol{x}_1, \boldsymbol{x}_2 \in \{-2, -1, 0, 1, 2\}$$

One can check that for $[\boldsymbol{y}_1, \boldsymbol{y}_2]^T, [\boldsymbol{y}_1', \boldsymbol{y}_2']^T \in \mathcal{S}$ with $[\boldsymbol{y}_1, \boldsymbol{y}_2] \ne [0,0]$ or $[\boldsymbol{y}_1', \boldsymbol{y}_2'] \ne [0,0]$, we have $|\boldsymbol{y}_1\boldsymbol{y}_2 - \rho_2\boldsymbol{y}_1'\boldsymbol{y}_2'| \le 0.25$. This means $d_{\min}(G_{8,2}, \rho_2 G_{8,2}) \le 0.25$. Therefore, the left-hand side of (164) becomes

$$\frac{d_{\min}(G_{8,2}, \rho_2 G_{8,3})}{|\rho_2^2|\,|\det(G_{8,2})|\,|\det(G_{8,2})|\,|\det(\Lambda_{\zeta_8})|^2} \le \frac{0.25}{4\sin^2(2\pi/8)} < \frac{1}{3\sqrt{2}} \quad (195)$$

which proves (164).

Case 5: $m_2 \ge 9$: In this case $n_2 = 2, 3, 4$, or 6.

Subcase 5.1: $m_2 \ge 9$, *but* $m_2 \ne 10$, $n_2 = 4$ *or* $n_2 = 2$.

Let $\boldsymbol{x} = 1 - \zeta_{m_2}$

$$[\boldsymbol{y}_1, \boldsymbol{y}_2]^T = G_{m_2,n_2}[\boldsymbol{x}, -\boldsymbol{x}]^T \in \Gamma_2(G_{m_2,n_2})$$

where

$$G_{m_2,n_2} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} \zeta_{k_1 m_2} & \\ & \zeta_{k_1 m_2}^2 \end{bmatrix} \quad (196)$$

and $k_1 = 2$ when m_2 is an even number; $k_1 = 4$ when m_2 is an odd number. It is easy to calculate that

$$|\boldsymbol{x}| = 2\sin(\pi/m_2)$$
$$|\boldsymbol{y}_1| = |\boldsymbol{x}||1 - \zeta_{k_1 m_2}| = 2|\boldsymbol{x}|\sin(\pi/(k_1 m_2))$$
$$|\boldsymbol{y}_2| = |\boldsymbol{x}||1 + \zeta_{k_1 m_2}| \le 2|\boldsymbol{x}|.$$

Thus,

$$d_{\min}(\Gamma_2(G_{m_2,n_2})) \le |\boldsymbol{y}_1\boldsymbol{y}_2| \le 4|\boldsymbol{x}|^2\sin(\pi/(k_1 m_2)) = 16\sin^2(\pi/m_2)\sin(\pi/(k_1 m_2)). \quad (197)$$

Therefore, when $m_2 > 9$ and $m_2 \ne 10$

$$\frac{d_{\min}(\Gamma_2(G_{m_2,n_2}))}{|\det(G_{m_1,n_1})|\,|\det(G_{m_2,n_2})|\,|\det(\Lambda_{\zeta_{m_2}})|^2} \le \frac{16\sin^2(\pi/m_2)\sin(\pi/(k_1 m_2))}{3 \times 4\sin^2(\pi/m_2)\cos^2(\pi/m_2)} = \frac{4\sin(\pi/(k_1 m_2))}{3\cos^2(\pi/m_2)} < \frac{1}{3\sqrt{2}} \quad (198)$$

which proves (164).

Subcase 5.2: $m_2 \geq 9$, $n_2 = 3$ *or* $n_2 = 6$.

In this subcase, 3 is not a factor of m_2, and, therefore, $m_2 \geq 10$. Let

$$\boldsymbol{x} = 1 - \zeta_{m_2},\ [\boldsymbol{y}_1, \boldsymbol{y}_2]^T = G_{m_2,3}[\boldsymbol{x}, \boldsymbol{x}]^T$$

where

$$G_{m_2,3} = \begin{bmatrix} 1 & 1 \\ \zeta_3^k & \zeta_3^{2k} \end{bmatrix} \begin{bmatrix} \zeta_{3m_2} & \\ & \zeta_{3m_2}^2 \end{bmatrix}. \tag{199}$$

$$\boldsymbol{y}_1 = \boldsymbol{x}(1 - \zeta_{3m_2}),\ \boldsymbol{y}_2 = \boldsymbol{x}(1 - \zeta_3^k \zeta_{3m})$$

$$d_{\min}\left(\Gamma_2(G_{m_2,n_2})\right) \leq |\boldsymbol{y}_1 \boldsymbol{y}_2| < 2|\boldsymbol{x}|^2 |1 - \zeta_{3m_2}|.$$

From (166) and (167), the left-hand side of (164) is upper-bounded by

$$\begin{aligned} &\frac{d_{\min}(\Gamma_2(G_{m_2,n_2}))}{|\det(G_{m_1,n_1})|\,|\det(G_{m_2,n_2})|\,\left|\det(\Lambda_{\zeta_{m_2}})\right|^2} \\ &\leq \frac{2|\boldsymbol{x}|^2|1-\zeta_{3m_2}|}{|\det(G_{m_1,3})|\,|\det(G_{m_2,3})|\,\left|\det(\Lambda_{\zeta_{m_2}})\right|^2} \\ &= \frac{2|\boldsymbol{x}|^2|1-\zeta_{3m_2}|}{3\sin^2(2\pi/m_2)} \leq 0.1541 < \frac{1}{3\sqrt{2}} \end{aligned}$$

which proves (164).

Subcase 5.3: $m_2 = 10$, $n_2 = 2$.

In this subcase, we prove this theorem under two different situations: $m_1 = 10$ and $m_1 \leq 9$. Note that when $m_2 = 10$, we have $n_2 \neq 4$ since $L_t = 2$.

Subcase 5.3.1: $m_2 = 10$, $n_2 = 2$, $m_1 = 10$, $n_1 = 2$

In this subcase, from i) we have

$$|\det(G_{m_1,n_1})| = |\det(G_{m_2,n_2})| = 2.$$

Since (197) does not require a specific condition on m_2 and n_2, it applies here too. Thus, from (197) we have

$$\begin{aligned} d_{\min}\left(\Gamma_2(G_{m_2,n_2})\right) &\leq |\boldsymbol{y}_1 \boldsymbol{y}_2| \leq 4|\boldsymbol{x}|^2 \sin\left(\pi/(k_1 m_2)\right) \\ &= 16\sin^2(\pi/10)\sin(\pi/20). \end{aligned} \tag{200}$$

Therefore,

$$\begin{aligned} &\frac{d_{\min}\left(\Gamma_2(G_{m_2,n_2})\right)}{|\det(G_{m_1,n_1})|\,|\det(G_{m_2,n_2})|\,\left|\det\left(\Lambda_{\zeta_{m_2}}\right)\right|^2} \\ &\leq \frac{16\sin^2(\pi/m_2)\sin\left(\pi/(k_1 m_2)\right)}{4\times 4\sin^2(\pi/m_2)\cos^2(\pi/m_2)} \\ &= \frac{\sin(\pi/20)}{\cos^2(\pi/10)} < \frac{1}{3\sqrt{2}} \end{aligned} \tag{201}$$

which proves (164).

Subcase 5.3.2: $m_2 = 10$, $n_2 = 2$, $m_1 \leq 9$.

In this subcase $m_1 \leq 9$

$$\begin{aligned} &|\det(G_{m_1,n_1})| \geq \sqrt{3} \\ &|\det(G_{m_2,n_2})| = |\det(G_{10,2})| = 2. \end{aligned}$$

Therefore, from (200) we have

$$\begin{aligned} &\frac{d_{\min}\left(\Gamma_2(G_{m_2,n_2})\right)}{|\det(G_{m_1,n_1})|\,|\det(G_{m_2,n_2})|\,\left|\det\left(\Lambda_{\zeta_{m_2}}\right)\right|\,\left|\det\left(\Lambda_{\zeta_{m_1}}\right)\right|} \\ &\leq \frac{16\sin^2(\pi/10)\sin(\pi/20)}{2\sqrt{3}\sin(2\pi/9)\sin(2\pi/10)} \\ &< \frac{1}{3\sqrt{2}} \end{aligned} \tag{202}$$

which proves (164). QED.

D. Proof of Theorem 6

Before proving the theorem, we need the following lemma.

Lemma 6: For any $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{Z}[\zeta_{18}]$ (or $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{Z}[\zeta_9]$), if $\mathbb{N}_{\mathbb{Q}(\zeta_{18})/\mathbb{Q}(\zeta_6)}(\boldsymbol{x}) - 2\mathbb{N}_{\mathbb{Q}(\zeta_{18})/\mathbb{Q}(\zeta_6)}(\boldsymbol{y}) = 0$ (or $\mathbb{N}_{\mathbb{Q}(\zeta_9)/\mathbb{Q}(\zeta_3)}(\boldsymbol{x}) = 2\mathbb{N}_{\mathbb{Q}(\zeta_9)/\mathbb{Q}(\zeta_3)}(\boldsymbol{y}) = 0$), then $\boldsymbol{x} = \boldsymbol{y} = 0$.

Proof: The proof of this lemma is similar to the proof of Lemma 5. We only prove the case for $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{Z}[\zeta_{18}]$ and the case for $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{Z}[\zeta_9]$ can be proved similarly.

Since $\{1, \zeta_{18}, \zeta_{18}^2\}$ is a basis of $\mathbb{Q}(\zeta_{18})$ over $\mathbb{Q}(\zeta_6)$, and $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{Z}(\zeta_{18})$ can be written as $\boldsymbol{x} = \boldsymbol{x}_1 + \boldsymbol{x}_2\zeta_{18} + \boldsymbol{x}_3\zeta_{18}^2$ and $\boldsymbol{y} = \boldsymbol{y}_1 + \boldsymbol{y}_2\zeta_{18} + \boldsymbol{y}_3\zeta_{18}^2$, with $\boldsymbol{x}_k, \boldsymbol{y}_k \in \mathbb{Z}[\zeta_6]$, $k = 1, 2, 3$. In the meantime

$$\mathbb{N}_{\mathbb{Q}(\zeta_{18})/\mathbb{Q}(\zeta_6)}(\boldsymbol{x}) = \prod_{k=1}^{3}\sigma_k(\boldsymbol{x}),\ \mathbb{N}_{\mathbb{Q}(\zeta_{18})/\mathbb{Q}(\zeta_6)}(\boldsymbol{y}) = \prod_{k=1}^{3}\sigma_k(\boldsymbol{y})$$

where σ_k, $k = 1, 2, 3$, are the three embeddings of $\mathbb{Q}(\zeta_{18})$ to $\mathbb{C}$ such that $\mathbb{Q}(\zeta_6)$ is fixed with σ_k and $\sigma_k(\zeta_{18}) = \zeta_3^{k-1}\zeta_{18}$. Therefore,

$$\begin{aligned} \mathbb{N}_{\mathbb{Q}(\zeta_{18})/\mathbb{Q}(\zeta_6)}(\boldsymbol{x}) &= \boldsymbol{x}_1^3 + \boldsymbol{x}_2^3\zeta_{18}^3 + \boldsymbol{x}_3^3\zeta_{18}^6 + 3\boldsymbol{x}_1\boldsymbol{x}_2\boldsymbol{x}_3(\zeta_3 + \zeta_3^2)\zeta_{18}^3 \\ &= \boldsymbol{x}_1^3 + \boldsymbol{x}_2^3\zeta_6 + \boldsymbol{x}_3^3\zeta_3 - 3\boldsymbol{x}_1\boldsymbol{x}_2\boldsymbol{x}_3\zeta_6 \in \mathbb{Z}[\zeta_6] \end{aligned} \tag{203}$$

$$\mathbb{N}_{\mathbb{Q}(\zeta_{18})/\mathbb{Q}(\zeta_6)}(\boldsymbol{y}) = \boldsymbol{y}_1^3 + \boldsymbol{y}_2^3\zeta_6 + \boldsymbol{y}_3^3\zeta_3 - 3\boldsymbol{y}_1\boldsymbol{y}_2\boldsymbol{y}_3\zeta_6 \in \mathbb{Z}[\zeta_6]. \tag{204}$$

Since $2\mathbb{Z}[\zeta_6]$ is an ideal of ring $\mathbb{Z}[\zeta_6]$, for the above $\boldsymbol{x}_k, \boldsymbol{y}_k \in \mathbb{Z}[\zeta_6]$, $k = 1, 2, 3$, there exists an integer l_0 such that

$$\boldsymbol{x}_k = \sum_{l=1}^{l_0} 2^{l-1}\boldsymbol{x}_{k,l}, \quad \boldsymbol{y}_k = \sum_{l=1}^{l_0} 2^{l-1}\boldsymbol{y}_{k,l} \tag{205}$$

where

$$\begin{aligned} \boldsymbol{x}_{k,l}, \boldsymbol{y}_{k,l} \in \{0, \exp(i2p\pi/6), \sqrt{3}\exp(i\pi/6)\exp(i2p\pi/6), \\ p = 1, \ldots, 6\} \end{aligned}$$

$k = 1, 2, 3$; $l = 1, \ldots, l_0$. Thus,

$$\begin{aligned} &\mathbb{N}_{\mathbb{Q}(\zeta_{18})/\mathbb{Q}(\zeta_6)}(\boldsymbol{x}) \\ &= \boldsymbol{x}_{1,1}^3 + \boldsymbol{x}_{2,1}^3\zeta_6 + \boldsymbol{x}_{3,1}^3\zeta_3 - 3\boldsymbol{x}_{1,1}\boldsymbol{x}_{2,1}\boldsymbol{x}_{3,1}\zeta_6 \\ &+ 8(\bar{\boldsymbol{x}}_{1,1}^3 + \bar{\boldsymbol{x}}_{2,1}^3\zeta_6 + \bar{\boldsymbol{x}}_{3,1}^3\zeta_3 - 3\bar{\boldsymbol{x}}_{1,1}\bar{\boldsymbol{x}}_{2,1}\bar{\boldsymbol{x}}_{3,1}) \\ &+ 6(\boldsymbol{x}_{1,1}^2\bar{\boldsymbol{x}}_{1,1} + \boldsymbol{x}_{2,1}^2\bar{\boldsymbol{x}}_{2,1}\zeta_6 + \boldsymbol{x}_{3,1}^2\bar{\boldsymbol{x}}_{3,1}\zeta_3 \\ &- \boldsymbol{x}_{1,1}\boldsymbol{x}_{2,1}\bar{\boldsymbol{x}}_{3,1} - \boldsymbol{x}_{1,1}\bar{\boldsymbol{x}}_{2,1}\boldsymbol{x}_{3,1} - \bar{\boldsymbol{x}}_{1,1}\boldsymbol{x}_{2,1}\boldsymbol{x}_{3,1}) \\ &- 12(\boldsymbol{x}_{1,1}\bar{\boldsymbol{x}}_{2,1}\bar{\boldsymbol{x}}_{3,1} + \bar{\boldsymbol{x}}_{1,1}\boldsymbol{x}_{2,1}\bar{\boldsymbol{x}}_{3,1} + \bar{\boldsymbol{x}}_{1,1}\bar{\boldsymbol{x}}_{2,1}\boldsymbol{x}_{3,1}) \end{aligned} \tag{206}$$

where $\bar{\boldsymbol{x}}_{k,1} = \sum_{l=2}^{l_0} 2^{l-2}\boldsymbol{x}_{k,l} \in \mathbb{Z}[\zeta_6]$.

When $\mathbb{N}_{\mathbb{Q}(\zeta_{18})/\mathbb{Q}(\zeta_6)}(\boldsymbol{x}) = 2\mathbb{N}_{\mathbb{Q}(\zeta_{18})/\mathbb{Q}(\zeta_6)}(\boldsymbol{y})$, from (204) and (206), we have

$$\begin{aligned} &\boldsymbol{x}_{1,1}^3 + \boldsymbol{x}_{2,1}^3\zeta_6 + \boldsymbol{x}_{3,1}^3\zeta_3 - 3\boldsymbol{x}_{1,1}\boldsymbol{x}_{2,1}\boldsymbol{x}_{3,1}\zeta_6 \\ &= 2\mathbb{N}_{\mathbb{Q}(\zeta_{18})/\mathbb{Q}(\zeta_6)}(\boldsymbol{y}) \\ &- 8(\bar{\boldsymbol{x}}_{1,1}^3 + \bar{\boldsymbol{x}}_{2,1}^3\zeta_6 + \bar{\boldsymbol{x}}_{3,1}^3\zeta_3 - 3\bar{\boldsymbol{x}}_{1,1}\bar{\boldsymbol{x}}_{2,1}\boldsymbol{x}_{3,1}) \\ &- 6(\boldsymbol{x}_{1,1}^2\bar{\boldsymbol{x}}_{1,1} + \boldsymbol{x}_{2,1}^2\bar{\boldsymbol{x}}_{2,1}\zeta_6 + \boldsymbol{x}_{3,1}^2\bar{\boldsymbol{x}}_{3,1}\zeta_3 - \boldsymbol{x}_{1,1}\boldsymbol{x}_{2,1}\bar{\boldsymbol{x}}_{3,1} \\ &- \boldsymbol{x}_{1,1}\bar{\boldsymbol{x}}_{2,1}\boldsymbol{x}_{3,1} - \bar{\boldsymbol{x}}_{1,1}\boldsymbol{x}_{2,1}\boldsymbol{x}_{3,1}) \\ &+ 12(\boldsymbol{x}_{1,1}\bar{\boldsymbol{x}}_{2,1}\bar{\boldsymbol{x}}_{3,1} + \bar{\boldsymbol{x}}_{1,1}\boldsymbol{x}_{2,1}\bar{\boldsymbol{x}}_{3,1} + \bar{\boldsymbol{x}}_{1,1}\bar{\boldsymbol{x}}_{2,1}\boldsymbol{x}_{3,1}). \end{aligned} \tag{207}$$

Since $\mathbb{N}_{\mathbb{Q}(\zeta_{18})/\mathbb{Q}(\zeta_6)}(\boldsymbol{y}) \in \mathbb{Z}[\zeta_6]$, the right-hand side of (207) belongs to $2\mathbb{Z}[\zeta_6]$. Thus,

$$\boldsymbol{x}_{1,1}^3 + \boldsymbol{x}_{2,1}^3\zeta_6 + \boldsymbol{x}_{3,1}^3\zeta_3 - 3\boldsymbol{x}_{1,1}\boldsymbol{x}_2\boldsymbol{x}_{3,1}\zeta_6 \in 2\mathbb{Z}[\zeta_6]. \quad (208)$$

From (205), we know that

$$\boldsymbol{x}_{1,1}, \boldsymbol{x}_{2,1}, \boldsymbol{x}_{3,1} \in \{0, \exp(i2p\pi/6), \sqrt{3}\exp(i\pi/6)\exp(i2p\pi/6), p = 1, \ldots, 6\} = \mathcal{S}. \quad (209)$$

Checking (208) with $\boldsymbol{x}_{1,1}, \boldsymbol{x}_{2,1}, \boldsymbol{x}_{3,1} \in \mathcal{S}$, we can find that (208) holds only when $\boldsymbol{x}_{1,1} = \boldsymbol{x}_{2,1} = \boldsymbol{x}_{3,1} = 0$. Then, in this case $\boldsymbol{x} = 2\bar{\boldsymbol{x}}_1$, where $\bar{\boldsymbol{x}}_1 = \bar{\boldsymbol{x}}_{1,1} + \bar{\boldsymbol{x}}_{2,1}\zeta_{18} + \bar{\boldsymbol{x}}_{3,1}\zeta_{18}^2$, and

$$\begin{aligned} 2\mathbb{N}_{\mathbb{Q}(\zeta_{18})/\mathbb{Q}(\zeta_6)}(\boldsymbol{y}) &= \mathbb{N}_{\mathbb{Q}(\zeta_{18})/\mathbb{Q}(\zeta_6)}(\boldsymbol{x}) \\ &= 8\mathbb{N}_{\mathbb{Q}(\zeta_{18})/\mathbb{Q}(\zeta_6)}(\bar{\boldsymbol{x}}_1) \end{aligned} \quad (210)$$

i.e.,

$$\mathbb{N}_{\mathbb{Q}(\zeta_{18})/\mathbb{Q}(\zeta_6)}(\boldsymbol{y}) = 4\mathbb{N}_{\mathbb{Q}(\zeta_{18})/\mathbb{Q}(\zeta_6)}(\bar{\boldsymbol{x}}_1). \quad (211)$$

Similarly, we can show $\boldsymbol{y}_{1,1} = \boldsymbol{y}_{2,1} = \boldsymbol{y}_{3,1} = 0$, and then $\boldsymbol{x}_{1,2} = \boldsymbol{x}_{2,2} = \boldsymbol{x}_{3,2} = 0$, and so on. Finally, we have $\boldsymbol{x} = \boldsymbol{y} = 0$. QED.

Now, we are ready to prove Theorem 6.

The basic idea to prove this theorem is similar to the one to prove Theorem 5. By the definition of cyclotomic lattice $\Gamma_3(G_{6,3})$, for any two

$$[\boldsymbol{y}_i(1), \boldsymbol{y}_i(2), \boldsymbol{y}_i(3)]^T \in \Gamma_3(G_{6,3}), \qquad \text{for } i = 1, 2$$

there are $\boldsymbol{x} = \boldsymbol{x}_1 + \boldsymbol{x}_2\zeta_{18} + \boldsymbol{x}_3\zeta_{18}^2$, $\boldsymbol{y} = \boldsymbol{y}_1 + \boldsymbol{y}_2\zeta_{18} + \boldsymbol{y}_3\zeta_{18}^2$, with $\boldsymbol{x}_k, \boldsymbol{y}_k \in \mathbb{Z}[\zeta_6]$, such that $\boldsymbol{y}_1(k) = \sigma_k(\boldsymbol{x})$, $\boldsymbol{y}_2(k) = \sigma_k(\boldsymbol{y})$, where σ_k, $k = 1, 2, 3$, are the three embeddings of $\mathbb{Q}(\zeta_{18})$ to $\mathbb{C}$ and fix $\mathbb{Q}(\zeta_6)$, and $\sigma_k(\zeta_{18}) = \zeta_{18}^k$. From a result in algebraic number theory [37], [38], it is known that the product $\boldsymbol{y}_i(1)\boldsymbol{y}_i(2)\boldsymbol{y}_i(3) \in \Lambda_{\zeta_3}$. Then, we have

$$\boldsymbol{y}_1(1)\boldsymbol{y}_1(2)\boldsymbol{y}_1(3) - 2\boldsymbol{y}_2(1)\boldsymbol{y}_2(2)\boldsymbol{y}_2(3) \in \Lambda_{\zeta_3}.$$

By the definition of relative norm, we have

$$\mathbb{N}_{\mathbb{Q}(\zeta_{18})/\mathbb{Q}(\zeta_6)}(\boldsymbol{x}) = \boldsymbol{y}_1(1)\boldsymbol{y}_1(2)\boldsymbol{y}_1(3)$$

and

$$\mathbb{N}_{\mathbb{Q}(\zeta_{18})/\mathbb{Q}(\zeta_6)}(\boldsymbol{y}) = \boldsymbol{y}_2(1)\boldsymbol{y}_2(2)\boldsymbol{y}_2(3).$$

From Lemma 6, we have

$$\begin{aligned} &|\boldsymbol{y}_1(1)\boldsymbol{y}_1(2)\boldsymbol{y}_1(3) - 2\boldsymbol{y}_2(1)\boldsymbol{y}_2(2)\boldsymbol{y}_2(3)| \\ &\quad = \left|\mathbb{N}_{\mathbb{Q}(\zeta_{18})/\mathbb{Q}(\zeta_6)}(\boldsymbol{x}) - 2\mathbb{N}_{\mathbb{Q}(\zeta_{18})/\mathbb{Q}(\zeta_6)}(\boldsymbol{y})\right| \geq 1 \end{aligned}$$

unless $\boldsymbol{x} = \boldsymbol{y} = 0$, i.e., the codeword $X\left(G_{6,3}, 2^{1/3}G_{6,3}\right) = 0$. This proves that the diversity product of $X(G_{6,3}, 2^{1/3}G_{6,3})$ is 1, i.e., $d_{\min}(G_{6,3}, 2^{1/3}G_{6,3}) = 1$.

Since the two-layer cyclotomic space–time code $X\left(G_{6,3}, 2^{1/3}G_{6,3}\right)$ has the following property:

$$\frac{d_{\min}(G_{6,3}, 2^{1/3}G_{6,3})}{\left|2\det(G_{6,3})^2\det(\Lambda_{\zeta_3})^3\right|} = \frac{4}{3^4\sqrt{3}} \quad (212)$$

based on Lemma 2, to prove the optimality of the code $X\left(G_{6,3}, 2^{1/3}G_{6,3}\right)$ we need to prove that any two-layer cyclotomic space–time code $X(\rho_1 G_{m_1,n_1}, \rho_2 G_{m_2,n_2})$ of three transmitters satisfies (213) (at the bottom of the page).

Without loss of generality, we assume one of ρ_1 and ρ_2 is 1 and the absolute value of the other is not less than 1 and

$$\left|\det\left(\Lambda_{\zeta_{m_2}}\right)\right| \leq \left|\det\left(\Lambda_{\zeta_{m_1}}\right)\right|. \quad (214)$$

If $|\rho_1| \geq \rho_2 = 1$, then

$$d_{\min}\left(\rho_1 G_{m_1,n_1}, \rho_2 G_{m_2,n_2}\right) \leq \left|\det\left(\Gamma_2(G_{m_2,n_2})\right)\right|$$

and we have (215), at the bottom of the page. If $|\rho_2| \geq \rho_1 = 1$, then, $d_{\min}\left(\rho_1 G_{m_1,n_1}, \rho_2 G_{m_2,n_2}\right) \leq \left|\rho_2^3 \det\left(\Gamma_2(G_{m_2,n_2})\right)\right|$ and we get (216) at the bottom of the next page.

When $\frac{\phi(mn)}{\phi(m)} = 3 = L_t$, it is not hard to see that $3|m$ and $n = 3$ or $n = 6$, and

$$|\det(G_{m,3})| = |\det(A_3)| = 3^{3/2} \quad (217)$$

for all the generating matrix $G_{m,3}$ of the three-dimensional cyclotomic lattice $\Gamma_3(G_{m,3})$. Thus, $3|m_1$ and $3|m_2$ for three transmit antenna and the two-layer cyclotomic space–time code

$$\frac{d_{\min}(\rho_1 G_{m_1,n_1}, \rho_2 G_{m_2,n_2})}{\left|\rho_1^3\rho_2^3 \det\left(\Lambda_{\zeta_{m_1}}\right)^{3/2} \det\left(\Lambda_{\zeta_{m_2}}\right)^{3/2} \det\left(G_{m_1,n_1}\right)\det\left(G_{m_2,n_2}\right)\right|} \leq \frac{4}{3^4\sqrt{3}}. \quad (213)$$

$$\begin{aligned} &\frac{d_{\min}(\rho_1 G_{m_1,n_1}, \rho_2 G_{m_2,n_2})}{|\rho_1^3 \det\left(G_{m_1,n_1}\right)|\,|\det(G_{m_2,n_2})|\left|\det\left(\Lambda_{\zeta_{m_1}}\right)^{3/2}\right|\left|\det\left(\Lambda_{\zeta_{m_2}}\right)^{3/2}\right|} \\ &\quad \leq \frac{d_{\min}(\Gamma_2(G_{m_2,n_2}))}{|\rho_1^3 \det(\rho_1 G_{m_1,n_1})|\,|\det(G_{m_2,n_2})|\,|\det(\Lambda_{\zeta_{m_2}})^{3/2}|\,|\det(\Lambda_{\zeta_{m_1}})^{3/2}|} \\ &\quad \leq \frac{d_{\min}\left(\Gamma_2(G_{m_2,n_2})\right)}{|\det\left(G_{m_1,n_1}\right)|\,|\det\left(G_{m_2,n_2}\right)|\left|\det\left(\Lambda_{\zeta_{m_1}}\right)^{3/2}\right|\left|\det\left(\Lambda_{\zeta_{m_2}}\right)^{3/2}\right|} \\ &\quad \leq \frac{d_{\min}\left(\Gamma_2(G_{m_2,n_2})\right)}{|\det\left(G_{m_1,n_1}\right)|\,|\det(G_{m_2,n_2})|\left|\det\left(\Lambda_{\zeta_{m_2}}\right)^{3}\right|}. \end{aligned} \quad (215)$$

$X(\rho_1 G_{m_1,m_2}, \rho_2 G_{m_2,n_2})$. We next prove this theorem in two cases in terms of m_2.

Case 1: $m_2 > 6$: In this case, $m_2 \geq 9$. We only consider the case $n_2 = 3$ and the case $n_2 = 6$ is similar. Let $\boldsymbol{x} = 1 - \zeta_{m_2}$, $[\boldsymbol{y}_1, \boldsymbol{y}_2, \boldsymbol{y}_3]^T = G_{m_2,3}[\boldsymbol{x}, \boldsymbol{x}, \boldsymbol{x}]^T$, where

$$G_{m_2,3} = \begin{bmatrix} 1 & 1 & 1 \\ \zeta_3 & \zeta_3^2 & \zeta_3^3 \\ \zeta_3^2 & \zeta_3^4 & \zeta_3^6 \end{bmatrix} \begin{bmatrix} \zeta_{3m_2} & & \\ & \zeta_{3m_2}^2 & \\ & & \zeta_{3m_2}^3 \end{bmatrix}. \quad (218)$$

Clearly, $d_{\min}(\Gamma_3(G_{m_2,n_2})) \leq |\boldsymbol{y}_1\boldsymbol{y}_2\boldsymbol{y}_3|$.

Define

$$f(m) \triangleq \frac{|\boldsymbol{y}_1\boldsymbol{y}_2\boldsymbol{y}_3|}{|\sin(2\pi/m)|^3}, \qquad \text{for } m \geq 9. \quad (219)$$

It is not hard to check that $f(m)$ is a decreasing function of m, and $f(9) = 0.5639$. From (215) and (216), the left-hand side of (213) is upper-bounded by

$$\begin{aligned} &\frac{|\boldsymbol{y}_1\boldsymbol{y}_2\boldsymbol{y}_3|}{|\det(G_{m_1,n_1})|\,|\det(G_{m_2,n_2})|\left|\det\left(\Lambda_{\zeta_{m_2}}\right)\right|^3} \\ &\quad \leq \frac{f(m)}{|\det(G_{m_1,n_1})|\,|\det(G_{m_2,n_2})|} \\ &\quad = \frac{f(m_2)}{3^3} \leq \frac{f(9)}{3^3} \leq \frac{4}{3^4\sqrt{3}}. \end{aligned} \quad (220)$$

Case 2: $m_2 = 3$ or $m_2 = 6$: In this case, by the assumption (214), $m_1 = 3$ or $m_1 = 6$. Thus, we may assume that $|\rho_2| \geq \rho_1 = 1$, otherwise the proof is similar. When $|\rho_2| > 2^{1/3}$, we get (221) at the bottom of the page, which proves (213).

Consider the case when $1 \leq |\rho_2| \leq 2^{1/3}$. Let

$$\mathcal{S} = \{\exp(jk\pi/3), \sqrt{3}\exp(j\pi/6)\exp(jk\pi/3), 3\exp(jk\pi/3), k = 1, \ldots, 6\}.$$

From Fig. 2, $\mathcal{S}$ is a subset of the set of points marked by "$\cdot$" and thus, for any point $\boldsymbol{z} \in \mathcal{S}$, there exist $[\boldsymbol{y}_1, \boldsymbol{y}_2, \boldsymbol{y}_3]^T \in \Gamma_3(G_{3,3})$ and $[\boldsymbol{y}_1', \boldsymbol{y}_2', \boldsymbol{y}_3']^T \in \Gamma_3(G_{6,3})$ such that $\boldsymbol{y}_1\boldsymbol{y}_2\boldsymbol{y}_3 = \boldsymbol{y}_1'\boldsymbol{y}_2'\boldsymbol{y}_3' = \boldsymbol{z}$. Therefore, we have

$$d_{\min}(G_{m_1,3}, \rho_2 G_{m_2,3}) \leq \min_{\boldsymbol{z},\boldsymbol{z}' \in \mathcal{S}} \left|\boldsymbol{z} - \rho_2^3 \boldsymbol{z}'\right| \triangleq \mu_{\rho_2}.$$

Because of the symmetry structure of $\mathcal{S}$, to consider μ_{ρ_2} we only need to consider ρ_2 of the form $\rho_2 = |\rho_2|\exp(i\theta)$, where $0 \leq \theta \leq \pi/6$. Let $\boldsymbol{z}_1 = 1$, $\boldsymbol{z}_2 = \sqrt{3}\exp(j\pi/6)$, $\boldsymbol{z}_3 = \exp(j\pi/3)$, $\boldsymbol{z}_4 = 3\exp(j\pi/3)$, $\boldsymbol{z}_1' = \rho_2^3\boldsymbol{z}_1$, and $\boldsymbol{z}_2' = \rho_2^3\boldsymbol{z}_2$. Then,

$$\mu_{\rho_2} \leq \min\{|\boldsymbol{z}_1 - \boldsymbol{z}_1'|, |\boldsymbol{z}_2 - \boldsymbol{z}_1'|, |\boldsymbol{z}_3 - \boldsymbol{z}_1'|, |\boldsymbol{z}_4 - \boldsymbol{z}_2'|\}$$

i.e.,

$$\begin{aligned} \mu_{\rho_2}^2 \leq \min\{&1 + |\rho_2|^6 - 2|\rho_2|^3\cos(\theta), \\ &3 + |\rho_2|^6 - 2\sqrt{3}|\rho_2|^3\cos(\pi/6 - \theta), \\ &1 + |\rho_2|^6 - 2|\rho_2|^3\cos(\pi/6 - \theta), \\ &9 + 3|\rho_2|^6 - 6\sqrt{3}|\rho_2|^3\cos(\pi/6 - \theta)\}. \end{aligned} \quad (222)$$

Thus, it is not hard to find that $\mu_{\rho_2} \leq |\rho_2|^3/2$. Therefore, we have (223) at the bottom of the page, which proves (213). QED

$$\begin{aligned} &\frac{d_{\min}(\rho_1 G_{m_1,m_2}, \rho_2 G_{m_2,n_2})}{|\rho_2^3|\,|\det(G_{m_1,n_1})|\,|\det(G_{m_2,n_2})|\left|\det\left(\Lambda_{\zeta_{m_1}}\right)^{3/2}\right|\left|\det\left(\Lambda_{\zeta_{m_2}}\right)^{3/2}\right|} \\ &\quad \leq \frac{|\rho_2^3| d_{\min}(\Gamma_2(G_{m_2,n_2}))}{|\rho_2^3|\,|\det(G_{m_1,n_1})|\,|\det(G_{m_2,n_2})|\left|\det\left(\Lambda_{\zeta_{m_1}}\right)^{3/2}\right|\left|\det\left(\Lambda_{\zeta_{m_2}}\right)^{3/2}\right|} \\ &\quad \leq \frac{d_{\min}(\Gamma_2(G_{m_2,n_2}))}{|\det(G_{m_1,n_1})|\,|\det(G_{m_2,n_2})|\left|\det\left(\Lambda_{\zeta_{m_2}}\right)^3\right|}. \end{aligned} \quad (216)$$

$$\begin{aligned} &\frac{d_{\min}(\rho_1 G_{m_1,n_1}, \rho_2 G_{m_2,n_2})}{|\rho_2^3|\,|\det(G_{m_1,n_1})|\,|\det(G_{m_2,n_2})|\left|\det\left(\Lambda_{\zeta_{m_1}}\right)^{3/2}\right|\left|\det\left(\Lambda_{\zeta_{m_2}}\right)^{3/2}\right|} \\ &\quad < \frac{1}{2\,|\det(G_{m_1,n_1})|\,|\det(G_{m_2,n_2})|\left|\det\left(\Lambda_{\zeta_{m_2}}\right)^3\right|} \\ &\quad \leq \frac{1}{2 \times 3^3 \sin^3(2\pi/3)} = \frac{4}{3^4\sqrt{3}} \end{aligned} \quad (221)$$

$$\begin{aligned} &\frac{d_{\min}(\rho_1 G_{m_1,n_1}, \rho_2 G_{m_2,n_2})}{|\rho_2^3|\,|\det(G_{m_1,n_1})|\,|\det(G_{m_2,n_2})|\left|\det\left(\Lambda_{\zeta_{m_1}}\right)^{3/2}\right|\left|\det\left(\Lambda_{\zeta_{m_2}}\right)^{3/2}\right|} \\ &\quad \leq \frac{\mu_{\rho_2}}{|\rho_2|^3 3^3 \times \left(\sqrt{3}/2\right)^3} \leq \frac{4}{3^4\sqrt{3}}, \end{aligned} \quad (223)$$

E. Proof of Theorem 8

We only consider

$$X(G_{6,3}, 2^{1/3}G_{6,3}, 4^{1/3}G_{6,3})$$

and $X(G_{3,3}, 2^{1/3}G_{3,3}, 4^{1/3}G_{3,3})$ is similar. The code

$$X = X(G_{6,3}, \gamma G_{6,3}, \gamma^2 G_{6,3})$$

is expressed as

$$X = \begin{bmatrix} \boldsymbol{y}_1(1) & \gamma\boldsymbol{y}_2(1) & \gamma^2\boldsymbol{y}_3(1) \\ \gamma^2\boldsymbol{y}_3(2) & \boldsymbol{y}_1(2) & \gamma\boldsymbol{y}_2(2) \\ \gamma\boldsymbol{y}_2(3) & \gamma^2\boldsymbol{y}_3(3) & \boldsymbol{y}_1(3) \end{bmatrix} \tag{224}$$

where $\boldsymbol{y}_1(k) = \sigma_k(\boldsymbol{x})$, $\boldsymbol{y}_2(k) = \sigma_k(\boldsymbol{y})$, $\boldsymbol{y}_3(k) = \sigma_k(\boldsymbol{z})$, $\gamma = 2^{1/3}$, σ_k, $k = 1, 2, 3$, are the three embeedings of $\mathbb{Q}(\zeta_{18})$ to $\mathbb{C}$ that are fixed on $\mathbb{Q}(\zeta_6)$ and $\sigma_k(\zeta_{18}) = \zeta_{18}^{k-1}$, and

$$\boldsymbol{x} = \sum_{k=1}^{3} \boldsymbol{x}_k \zeta_{18}^{k-1}, \quad \boldsymbol{y} = \sum_{k=1}^{3} \boldsymbol{y}_k \zeta_{18}^{k-1}, \quad \boldsymbol{z} = \sum_{k=1}^{3} \boldsymbol{z}_k \zeta_{18}^{k-1}$$

with $\boldsymbol{x}_k, \boldsymbol{y}_k, \boldsymbol{z}_k \in \mathbb{Z}[\zeta_6]$.

We first prove $\det(X) \in \mathbb{Z}[\zeta_6]$. It is not hard to see that

$$\begin{aligned} \det(X) = &\boldsymbol{y}_1(1)\boldsymbol{y}_1(2)\boldsymbol{y}_1(3) + 2\boldsymbol{y}_2(1)\boldsymbol{y}_2(2)\boldsymbol{y}_2(3) \\ &+ 4\boldsymbol{y}_3(1)\boldsymbol{y}_3(2)\boldsymbol{y}_3(3) \\ &- 2(\boldsymbol{y}_1(1)\boldsymbol{y}_2(2)\boldsymbol{y}_3(3) + \boldsymbol{y}_2(1)\boldsymbol{y}_3(2)\boldsymbol{y}_1(3) \\ &+ \boldsymbol{y}_3(1)\boldsymbol{y}_1(2)\boldsymbol{y}_2(3)). \end{aligned} \tag{225}$$

Since

$$\begin{aligned} \boldsymbol{y}_1(1)\boldsymbol{y}_1(2)\boldsymbol{y}_1(3) &= \mathbb{N}_{\mathbb{Q}(\zeta_{18})/\mathbb{Q}(\zeta_6)}(\boldsymbol{x}) \in \mathbb{Z}[\zeta_6] \\ \boldsymbol{y}_2(1)\boldsymbol{y}_2(2)\boldsymbol{y}_2(3) &= \mathbb{N}_{\mathbb{Q}(\zeta_{18})/\mathbb{Q}(\zeta_6)}(\boldsymbol{y}) \in \mathbb{Z}[\zeta_6] \end{aligned}$$

and

$$\boldsymbol{y}_3(1)\boldsymbol{y}_3(2)\boldsymbol{y}_3(3) = \mathbb{N}_{\mathbb{Q}(\zeta_{18})/\mathbb{Q}(\zeta_6)}(\boldsymbol{z}) \in \mathbb{Z}[\zeta_6]$$

what we need to do is to prove

$$\boldsymbol{y}_1(1)\boldsymbol{y}_2(2)\boldsymbol{y}_3(3) + \boldsymbol{y}_2(1)\boldsymbol{y}_3(2)\boldsymbol{y}_1(3) + \boldsymbol{y}_3(1)\boldsymbol{y}_1(2)\boldsymbol{y}_2(3) \in \mathbb{Z}[\zeta_6].$$

By the definitions of $\boldsymbol{y}_1(k)$, $\boldsymbol{y}_2(k)$, and $\boldsymbol{y}_3(k)$, $k = 1, 2, 3$, $\boldsymbol{y}_1(1)\boldsymbol{y}_2(2)\boldsymbol{y}_3(3) + \boldsymbol{y}_2(1)\boldsymbol{y}_3(2)\boldsymbol{y}_1(3) + \boldsymbol{y}_3(1)\boldsymbol{y}_1(2)\boldsymbol{y}_2(3)$ in (225) can be rewritten as

$$\begin{aligned} &\boldsymbol{y}_1(1)\boldsymbol{y}_2(2)\boldsymbol{y}_3(3) + \boldsymbol{y}_2(1)\boldsymbol{y}_3(2)\boldsymbol{y}_1(3) + \boldsymbol{y}_3(1)\boldsymbol{y}_1(2)\boldsymbol{y}_2(3) \\ &= \sum_{l_1,l_2,l_3 \in \{1,2,3\}} \zeta_{18}^{l_1+l_2+l_3-3} \boldsymbol{x}_{l_1}\boldsymbol{y}_{l_2}\boldsymbol{z}_{l_3}\left(\zeta_3^{l_2+2l_3} + \zeta_3^{l_3+2l_1} + \zeta_3^{l_1+2l_2}\right). \end{aligned} \tag{226}$$

When $l_1 + l_2 + l_3$ can be divided by 3

$$\zeta_{18}^{l_1+l_2+l_3-3} \boldsymbol{x}_{l_1}\boldsymbol{y}_{l_2}\boldsymbol{z}_{l_3}\left(\zeta_3^{l_2+2l_3} + \zeta_3^{l_3+2l_1} + \zeta_3^{l_1+2l_2}\right) \in \mathbb{Z}[\zeta_6].$$

We next prove that a term in the summation in the right-hand side of (226) when its indices $3 \nmid (l_1 + l_2 + l_3)$ is 0.

It is not hard to see that $(l_1, l_2, l_3) \in \mathcal{S}$, when $l_1 + l_2 + l_3$ can not be divided by 3, where $\mathcal{S}$ is the set of triplets shown in (227) at the bottom of the page. One can easily see that

$$\zeta_3^{l_2+2l_3} + \zeta_3^{l_3+2l_1} + \zeta_3^{l_1+2l_2} = 1 + \zeta_3 + \zeta_3^2 = 0$$

when $(l_1, l_2, l_3) \in \mathcal{S}$. Thus, we have proved that

$$\boldsymbol{y}_1(1)\boldsymbol{y}_2(2)\boldsymbol{y}_3(3) + \boldsymbol{y}_2(1)\boldsymbol{y}_3(2)\boldsymbol{y}_1(3) + \boldsymbol{y}_3(1)\boldsymbol{y}_1(2)\boldsymbol{y}_2(3) \in \mathbb{Z}[\zeta_6],$$

i.e., $\det(X) \in \mathbb{Z}[\zeta_6]$.

To show that its diversity product is 1, we only need to show that $\det(X) \neq 0$ when $X \neq 0$. Similarly to the proof of Lemma 6, for a given X, i.e., $\boldsymbol{y}_1(k) = \sigma_k(\boldsymbol{x})$, $\boldsymbol{y}_2(k) = \sigma_k(\boldsymbol{y})$, $\boldsymbol{y}_3(k) = \sigma_k(\boldsymbol{z})$, $k = 1, 2, 3$, there exists an integer l_0 such that

$$\begin{aligned} \boldsymbol{x} = \boldsymbol{x}_1 + \boldsymbol{x}_2\zeta_{18} + \boldsymbol{x}_3\zeta_{18}^2, \quad \boldsymbol{y} = \boldsymbol{y}_1 + \boldsymbol{y}_2\zeta_{18} + \boldsymbol{y}_3\zeta_{18}^2 \\ \boldsymbol{z} = \boldsymbol{z}_1 + \boldsymbol{z}_2\zeta_{18} + \boldsymbol{z}_3\zeta_{18}^2 \end{aligned} \tag{228}$$

with

$$\boldsymbol{x}_k = \sum_{l=1}^{l_0} \boldsymbol{x}_{k,l} 2^{l-1}, \ \boldsymbol{y}_k = \sum_{l=1}^{l_0} \boldsymbol{y}_{k,l} 2^{l-1}, \ \boldsymbol{z}_k = \sum_{l=1}^{l_0} \boldsymbol{z}_{k,l} 2^{l-1}, \tag{229}$$

where

$$\boldsymbol{x}_{k,l}, \boldsymbol{y}_{k,l}, \boldsymbol{z}_{k,l} \in \{0, \exp(i2p\pi/6), \sqrt{3}\zeta_{12}\exp(i2p\pi/6), p = 1, \ldots, 6\}, \qquad k = 1, 2, 3. \tag{230}$$

From (225), $\det(X)$ can be rewritten as follows:

$$\begin{aligned} \det(X) = &\boldsymbol{y}_1(1)\boldsymbol{y}_1(2)\boldsymbol{y}_1(3) + 2\boldsymbol{y}_2(1)\boldsymbol{y}_2(2)\boldsymbol{y}_2(3) \\ &+ 4\boldsymbol{y}_3(1)\boldsymbol{y}_3(2)\boldsymbol{y}_3(3) \\ &- 2(\boldsymbol{y}_1(1)\boldsymbol{y}_2(2)\boldsymbol{y}_3(3) + \boldsymbol{y}_2(1)\boldsymbol{y}_3(2)\boldsymbol{y}_1(3) \\ &+ \boldsymbol{y}_3(1)\boldsymbol{y}_1(2)\boldsymbol{y}_2(3)) \end{aligned} \tag{231}$$

with

$$\begin{aligned} \boldsymbol{y}_1(k) = \sigma_k(\boldsymbol{x}) = &\sum_{l=1}^{l_0} \boldsymbol{x}_{1,l} 2^{l-1} + \zeta_{18}\zeta_3^{k-1} \sum_{l=1}^{l_0} \boldsymbol{x}_{2,l} 2^{l-1} \\ &+ \zeta_{18}^2\zeta_3^{2(k-1)} \sum_{l=1}^{l_0} \boldsymbol{x}_{3,l} 2^{l-1} \end{aligned} \tag{232}$$

$$\mathcal{S} = \left\{ \begin{matrix} (1,2,1), & (1,2,2), & (1,3,1), & (2,3,2), & (2,3,3), & (3,3,1), \\ (1,1,2), & (2,1,2), & (1,1,3), & (2,2,3), & (3,2,3), & (1,3,3), \\ (2,1,1), & (2,2,1), & (3,1,1), & (3,2,2), & (3,3,2), & (3,1,3) \end{matrix} \right\}. \tag{227}$$

$$\boldsymbol{y}_2(k)=\sigma_k(\boldsymbol{y})=\sum_{l=1}^{l_0}\boldsymbol{y}_{1,l}2^{l-1}+\zeta_{18}\zeta_3^{k-1}\sum_{l=1}^{l_0}\boldsymbol{y}_{2,l}2^{l-1}+\zeta_{18}^2\zeta_3^{2(k-1)}\sum_{l=1}^{l_0}\boldsymbol{y}_{3,l}2^{l-1} \quad (233)$$

$$\boldsymbol{y}_3(k)=\sigma_k(\boldsymbol{z})=\sum_{l=1}^{l_0}\boldsymbol{z}_{1,l}2^{l-1}+\zeta_{18}\zeta_3^{k-1}\sum_{l=1}^{l_0}\boldsymbol{z}_{2,l}2^{l-1}+\zeta_{18}^2\zeta_3^{2(k-1)}\sum_{l=1}^{l_0}\boldsymbol{z}_{3,l}2^{l-1}. \quad (234)$$

When $\det(X)=0$

$$\begin{aligned}&\boldsymbol{y}_1(1)\boldsymbol{y}_1(2)\boldsymbol{y}_1(3)+2\boldsymbol{y}_2(1)\boldsymbol{y}_2(2)\boldsymbol{y}_2(3)\\&+4\boldsymbol{y}_3(1)\boldsymbol{y}_3(2)\boldsymbol{y}_3(3)\\&-2(\boldsymbol{y}_1(1)\boldsymbol{y}_2(2)\boldsymbol{y}_3(3)+\boldsymbol{y}_2(1)\boldsymbol{y}_3(2)\boldsymbol{y}_1(3)\\&+\boldsymbol{y}_3(1)\boldsymbol{y}_1(2)\boldsymbol{y}_2(3))=0. \quad (235)\end{aligned}$$

Combining (231)–(235), we have

$$\begin{aligned}&\boldsymbol{x}^3{}_{1,1}+\boldsymbol{x}_{2,1}^3\zeta_6+\boldsymbol{x}_{3,1}^3\zeta_3-3\boldsymbol{x}_{1,1}\boldsymbol{x}_{2,1}\boldsymbol{x}_{3,1}\zeta_6\\&=2(\boldsymbol{y}_1(1)\boldsymbol{y}_2(2)\boldsymbol{y}_3(3)+\boldsymbol{y}_2(1)\boldsymbol{y}_3(2)\boldsymbol{y}_1(3)\\&\quad+\boldsymbol{y}_3(1)\boldsymbol{y}_1(2)\boldsymbol{y}_2(3))-2\boldsymbol{y}_2(1)\boldsymbol{y}_2(2)\boldsymbol{y}_2(3)\\&\quad-4\boldsymbol{y}_3(1)\boldsymbol{y}_3(2)\boldsymbol{y}_3(3)\\&\quad-8(\bar{\boldsymbol{x}}_{1,1}^3+\bar{\boldsymbol{x}}_{2,1}^3\zeta_6+\bar{\boldsymbol{x}}_{3,1}^3\zeta_3-3\bar{\boldsymbol{x}}_{1,1}\bar{\boldsymbol{x}}_{2,1}\bar{\boldsymbol{x}}_{3,1})\\&\quad-6(\boldsymbol{x}_{1,1}^2\bar{\boldsymbol{x}}_{1,1}+\boldsymbol{x}_{2,1}^2\bar{\boldsymbol{x}}_{2,1}\zeta_6+\boldsymbol{x}_{3,1}^2\bar{\boldsymbol{x}}_{3,1}\zeta_3-\boldsymbol{x}_{1,1}\boldsymbol{x}_{2,1}\bar{\boldsymbol{x}}_{3,1}\\&\quad-\boldsymbol{x}_{1,1}\bar{\boldsymbol{x}}_{2,1}\boldsymbol{x}_{3,1}-\bar{\boldsymbol{x}}_{1,1}\boldsymbol{x}_{2,1}\boldsymbol{x}_{3,1})\\&\quad+12(\boldsymbol{x}_{1,1}\bar{\boldsymbol{x}}_{2,1}\bar{\boldsymbol{x}}_{3,1}+\bar{\boldsymbol{x}}_{1,1}\boldsymbol{x}_{2,1}\bar{\boldsymbol{x}}_{3,1}+\bar{\boldsymbol{x}}_{1,1}\bar{\boldsymbol{x}}_{2,1}\boldsymbol{x}_{3,1}) \quad (236)\end{aligned}$$

where

$$\bar{\boldsymbol{x}}_{i,1}=\sum_{l=2}^{l_0}2^{l-2}\boldsymbol{x}_{i,l}\in\mathbb{Z}[\zeta_6],\qquad i=1,2,3.$$

By the definition of $\boldsymbol{y}_2(k)$ and $\boldsymbol{y}_3(k)$, $k=1,2,3$, we have

$$\begin{aligned}\boldsymbol{y}_2(1)\boldsymbol{y}_2(2)\boldsymbol{y}_2(3)&=\mathbb{N}_{\mathbb{Q}(\zeta_{18})/\mathbb{Q}(\zeta_6)}(\boldsymbol{y})\in\mathbb{Z}[\zeta_6]\\\boldsymbol{y}_3(1)\boldsymbol{y}_3(2)\boldsymbol{y}_3(3)&=\mathbb{N}_{\mathbb{Q}(\zeta_{18})/\mathbb{Q}(\zeta_6)}(\boldsymbol{z})\in\mathbb{Z}[\zeta_6].\end{aligned}$$

And from the previous proof we know that

$$\boldsymbol{y}_1(1)\boldsymbol{y}_2(2)\boldsymbol{y}_3(3)+\boldsymbol{y}_2(1)\boldsymbol{y}_3(2)\boldsymbol{y}_1(3)+\boldsymbol{y}_3(1)\boldsymbol{y}_1(2)\boldsymbol{y}_2(3)\in\mathbb{Z}[\zeta_6]$$

so the term on the right-hand side of (236) belongs to $2\mathbb{Z}[\zeta_6]$. Thus, the term on the left-hand side of (236) also belongs to $2\mathbb{Z}[\zeta_6]$, i.e.,

$$\boldsymbol{x}_{1,1}^3+\boldsymbol{x}_{2,1}^3\zeta_6+\boldsymbol{x}_{3,1}^3\zeta_3-3\boldsymbol{x}_{1,1}\boldsymbol{x}_2\boldsymbol{x}_{3,1}\zeta_6\in2\mathbb{Z}[\zeta_6]. \quad (237)$$

Similarly to the proof in (208), we can obtain $\boldsymbol{x}_{1,1}=\boldsymbol{x}_{2,1}=\boldsymbol{x}_{3,1}=0$. Then $\boldsymbol{x}=2\bar{\boldsymbol{x}}_1$, where

$$\bar{\boldsymbol{x}}_1=\sum_{l=2}^{l_0}2^{l-2}\boldsymbol{x}_{1,l}+\zeta_{18}\sum_{l=2}^{l_0}2^{l-2}\boldsymbol{x}_{2,l}+\zeta_{18}^2\sum_{l=2}^{l_0}2^{l-2}\boldsymbol{x}_{3,l}.$$

Thus, $\boldsymbol{y}_1(1)=2\boldsymbol{y}_{1,1}(1)=2\sigma_1(\bar{\boldsymbol{x}}_{1,1})$, $\boldsymbol{y}_1(2)=2\boldsymbol{y}_{1,1}(2)=2\sigma_2(\bar{\boldsymbol{x}}_{1,1})$, $\boldsymbol{y}_1(3)=2\boldsymbol{y}_{1,1}(3)=2\sigma_3(\bar{\boldsymbol{x}}_{1,1})$. Then, (235) becomes

$$\begin{aligned}&\boldsymbol{y}_2(1)\boldsymbol{y}_2(2)\boldsymbol{y}_2(3)+2\boldsymbol{y}_3(1)\boldsymbol{y}_3(2)\boldsymbol{y}_3(3)\\&+4\boldsymbol{y}_{1,1}(1)\boldsymbol{y}_{1,1}(2)\boldsymbol{y}_{1,1}(3)\\&-2(\boldsymbol{y}_{1,1}(1)\boldsymbol{y}_2(2)\boldsymbol{y}_3(3)+\boldsymbol{y}_2(1)\boldsymbol{y}_3(2)\boldsymbol{y}_{1,1}(3)\\&+\boldsymbol{y}_3(1)\boldsymbol{y}_{1,1}(2)\boldsymbol{y}_2(3))=0. \quad (238)\end{aligned}$$

Similarly, we can prove $\boldsymbol{y}_{1,1}=\boldsymbol{y}_{2,1}=\boldsymbol{y}_{3,1}=0$, and $\boldsymbol{z}_{1,1}=\boldsymbol{z}_{2,1}=\boldsymbol{z}_{3,1}=0$, $\boldsymbol{x}_{1,2}=\boldsymbol{y}_{1,2}=\boldsymbol{z}_{1,2}=0$, and so on. Finally, we can prove $\boldsymbol{x}=\boldsymbol{y}=\boldsymbol{z}=0$, i.e, $X=0$.

The above proved result is also illustrated in Fig. 2. In Fig. 2, the product $\boldsymbol{y}_1(1)\boldsymbol{y}_1(2)\boldsymbol{y}_1(3)$ of the first layer of X is marked by "$\cdot$," the product $\gamma^3\boldsymbol{y}_2(1)\boldsymbol{y}_2(2)\boldsymbol{y}_2(3)$ of the second layer of X is marked by "$\circ$," and the product $\gamma^6\boldsymbol{y}_3(1)\boldsymbol{y}_3(2)\boldsymbol{y}_3(3)$ of the third layer of X is marked by "$\square$." They do not overlape unless $\boldsymbol{x}=\boldsymbol{y}=\boldsymbol{z}=0$, i.e., $\boldsymbol{y}_i(k)=0$ for $1\le i,k\le3$, or $X=0$.

QED

ACKNOWLEDGMENT

The authors would like to thank Huiyong Liao and Haiquan Wang for their helpful discussions and for finding an error in the original optimality proof of Theorem 5. Huiyong Liao and Haiquan Wang have also independently found the optimal full rate (two-layer) code for two transmit antennas presented in Theorem 5. The authors would also like to thank the reviewers for their useful comments and suggestions, in particular one of the reviewers provided a proof of Lemma 5 in a different version that provides the full diversity property of the code and also diversity product of the code to be 1.

REFERENCES

[1] K. Boulle and J.-C Belfiore, "Modulation schemes designed for the Rayleigh fading channel," in *Proc. 26th Conf. Information Sciences and Systems (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. Inf. Theory*, vol. 43, no. 3, 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. Inf. Theory*, vol. 44, no. 4, pp. 1453–1467, Jul. 1998.

[4] M. O. Damen, K. A. Meraim, and J.-C. Belfiore, "Diagonal algebraic space-time block codes," *IEEE Trans. Inf. Theory*, vol. 48, no. 3, pp. 628–636, Mar. 2002.

[5] M. O. Damen, A. Tewfik, and J.-C. Belfiore, "A construction of a space-time code based on number theory," *IEEE Trans. Inf. Theory*, vol. 48, no. 3, pp. 753–760, Mar. 2002.

[6] B. A. Sethuraman, B. S. Rajan, and V. Shashidhar, "Full-diversity, high rate space-time block codes from division algebras," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2596–2616, Oct. 2003.

[7] M. O. Damen and N. C. Beaulieu, "On two high-rate algebraic space–time codes," *IEEE Trans. Inform. Theory*, vol. 49, no. 4, pp. 1059–1063, Apr. 2003.

[8] H. El Gamal and M. O. Damen, "Universal space–time coding," *IEEE Trans. Inf. Theory*, vol. 49, no. 5, pp. 1097–1119, May 2003.

[9] M. O. Damen, H. El Gamal, and N. C. Beaulieu, "Systematic construction of full diversity algebraic constellations," *IEEE Trans. Inf. Theory*, vol. 49, no. 12, pp. 3344–3349, Dec, 2003.

[10] S. Galliou and J. C. Belfiore, "A new family of full rate, fully diversity space-time codes based on Galois theory," in *Proc. IEEE Int. Symp. Information Theory*, Lausanne, Switzerland, Jun/Jul. 2002, p. 419.

[11] A. Medles and D. T. M. Slock, "Linear space-time coding at full rate and full diversity," in *Proc. IEEE Int. Symp. Information Theory*, Lausanne, Switzerland, Jun./Jul. 2002, p. 221.
[12] M. O. Damen, H. El Gamal, and N. C. Beaulieu, "Linear threaded algebraic space-time constellations," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2372–2388, Oct. 2003.
[13] X. Ma and G. B. Giannakis, "Full-diversity full rate complex-field space-time coding," *IEEE Trans. Signal Process.*, vol. 51, no. 11, pp. 2917–2930, Nov. 2003.
[14] G. Wang, H. Liao, H. Wang, and X.-G. Xia, "Systematic and optimal cyclotomic lattices and diagonal space-time block code designs," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3348–3360, Dec. 2004.
[15] G. J. Foschini, "Layered space-time architecture for wireless communication in a fading environment when using multiple antennas," *AT&T Bell Labs. Tech. J.*, vol. 1, no. 2, pp. 41–59, 1996.
[16] H. El Gamal and A. R. Hammons Jr., "A new approach to layered space-time code and signal processing," *IEEE Trans. Inf. Theory*, vol. 47, no. 6, pp. 2335–2367, Sep. 2001.
[17] B. Hassibi and B. M. Hochwald, "High-rate codes that are linear in space and time," *IEEE Trans. Inf. Theory*, vol. 48, no. 6, pp. 1473–1484, Jun. 2002.
[18] S. Sandhu and A. J. Paulraj, "Space-time blocks: A capacity perspective," *IEEE Commun. Lett.*, vol. 4, pp. 384–386, Dec. 2000.
[19] R. W. Heath and A. J. Paulraj, "Linear dispersion codes for MIMO systems based on frame theory," *IEEE Trans. Signal Process.*, vol. 50, no. 10, pp. 2429–2441, Oct. 2002.
[20] 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," in *Proc. IEEE Vehicular Technology Conf.*, Apr. 1996, pp. 136–140.
[21] V. Tarokh, N. Seshadri, and A. R. Calderbank, "Space-time codes for high data rate wireless communication: Performance criterion and code construction," *IEEE Trans. Inf. Theory*, vol. 44, no. 2, pp. 744–765, Mar. 1998.
[22] S. Alamouti, "A simple transmit diversity technique for wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 16, no. 8, pp. 1451–1458, Oct. 1998.
[23] V. Tarokh, H. Jafarkhani, and A. R. Calderbank, "Space-time block codes from orthogonal designs," *IEEE Trans. Inf. Theory*, vol. 45, no. 5, pp. 1456–1467, Jul. 1999.
[24] G. Ganesan and P. Stoica, "Space-time block codes: A maximum SNR," *IEEE Trans. Inf. Theory*, vol. 47, no. 4, pp. 1650–1656, May 2001.
[25] O. Tirkkonen and A. Hottinen, "Square-matrix embeddable space-time block codes for complex signal constellations," *IEEE. Trans. Inf. Theory*, vol. 48, no. 2, pp. 384–395, Feb. 2002.
[26] W. Su and X.-G. Xia, "On space-time block codes from complex orthogonal designs," *Wireless Personal Commun.* , vol. 25, no. 1, pp. 1–26, Apr. 2003.
[27] X.-B. Liang and X.-G. Xia, "On the nonexistence of rate-one generalized complex orthogonal designs," *IEEE Trans. Inf. Theory*, vol. 49, no. 11, pp. 2984–2989, Nov. 2003.
[28] H. Wang and X.-G. Xia, "Upper bounds of rates of complex orthogonal designs," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2788–2796, Oct. 2003.
[29] W. H. Mow, "Maximum likelihood sequence estimation from the lattice viewpoint," *IEEE Trans. Inf. Theory*, vol. 40, no. 5, pp. 1591–1600, Sep. 1994. See also M. Phil. thesis, Dept. Inf. Eng., the Chinese Univ. Hong Kong, Jun. 1991.
[30] ——, "Universal lattice decoding: Principle and recent advances," *Wireless Commun. Mobile Comput.*, vol. 3, pp. 553–569, Aug. 2003.
[31] E. Viterbo and E. Biglieri, "A universal lattice decoder," in *GRETSI 14-ème Colloque*, Juan-les-Pins, France, Sep. 1993, pp. 611–614.
[32] E. Viterbo and J. Boutros, "A universal lattice code decoder for fading channel," *IEEE Trans. Inf. Theory*, vol. 45, no. 5, pp. 1639–1642, Jul. 1999.
[33] M. O. Damen, K. Abed-Meraim, and J. C. Belfiore, "Generalized sphere decoder for asymmetrical space-time communication architecture," *IEE Electron. Lett.*, vol. 36, p. 166, Jan. 2000.
[34] M. O. Damen, A. Chkeif, and J. C. Belfiore, "Lattice code decoder for space-time codes," *IEEE Commun. Lett.*, vol. 4, no. 5, pp. 161–163, May 2000.
[35] H. Vikalo and B. Hassibi, "Maximum-likelihood sequence detection of multiple antenna systems over dispersive channels via sphere decoding," *EURASIP J. Appl. Signal Process.*, vol. 2002, no. 5, pp. 525–531, 2002.
[36] ——, "The expected complexity of sphere decoding, Part I: Theory and Part II: Applications," *IEEE Trans. Signal Process.*, submitted for publication.
[37] S. Lang, *Algebraic Number Fields*. New York: Springer-Verlag, 1986.
[38] D. A. Marcus, *Number Fields*. New York: Springer-Verlag, 1977.
[39] P. Morandi, *Field and Galois Theory*. New York: Springer-Verlag, 1996.
[40] I. Stewart and D. Tall, *Algebraic Number Theory and Fermat's Last Theorem*, 3rd ed. Natick, MA: A K Peters, 2002.
[41] R. A. Mollin, *Algebraic Number Theory*. Boca Raton, FL: Chapman & Hall/CRC, 1999.
[42] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, 3rd ed. New York: Springer-Verlag, 1998.
[43] H. Yao and G. W. Wornell, "Achieving the full MIMO diversity-multiplexing frontier with the rotation-based space-time codes," in *Proc. Allerton Conf. Communication, Control, and Computing*, Monticello, IL, Oct. 2003.
[44] P. Dayal and M. K. Varanasi, "An optimal two transmit antenna space time code and its stacked extensions," in *Proc. Asilomar Conf. Signals, Systems and Computers*, Monterey, CA, Nov. 2003.
[45] J.-C. Belfiore, G. Rekaya, and E. Viterbo, "The Golden code: a 2×2 full-rate space-time code with nonvanishing determinant," *IEEE Trans. Inf. Theory*, submitted for publication. See Also *Proc. IEEE Int. Symp. Information Theory*, Chicago, IL, Jun./Jul. 2004, p. 308.
[46] F. Oggier, G. Rekaya, J.-C. Belfiore, and E. Viterbo, "Perfect space time block codes," *IEEE Trans. Inf. Theory*, submitted for publication.
[47] T. Kiran and B. S. Rajan, "STBC-schemes with nonvanishing determinant for certain number of transmit antennas," *IEEE Trans. Inf. Theory*, submitted for publication.
[48] P. Elia, K. R. Kumar, S. A. Pawar, P. V. Kumar, and H.-f. Lu, "Explicit minimum-delay space-time codes achieving the diversity-multiplexing gain tradeoff," preprint, Sep. 2004.