

A Simple Construction of Nonvanishing Determinant Space-Time Block Codes Based on Cyclic Division Algebra

Xiaoyong Guo and Xiang-Gen Xia

Abstract—Cyclic division algebra (CDA) has recently become a major technique to construct nonvanishing determinant (NVD) space-time block codes. The CDA based construction method usually consists of two steps. The first step is to construct a degree- n cyclic extension over a base field and the second step is to find a non-norm algebraic integer in the base field. In this paper, we first propose a simple construction method for cyclic extensions and then propose an elementary condition for non-norm elements for QAM and HEX signal constellations. Design examples are shown for $n = 2$ to $n = 20$, where n is the number of transmit antennas, and it is shown that with our newly proposed construction, non-norm elements with smaller absolute values than the existing ones can be found.

I. INTRODUCTION

Space-time block codes (STBC) with nonvanishing determinant (NVD) have attracted much attention lately, see for example [1]–[14]. In particular, Elia et. al. [6] have shown that full rate STBC with NVD achieve the diversity-multiplexing tradeoff obtained by Zheng-Tse [15]. There are two major methods to construct full rate STBC with NVD. One is to use the multi-layer (threaded) structure, see for example [4], [9], [10], [13], [14] and the other is to use the cyclic division algebra (CDA) structure that was first used to construct full diversity STBC in [16], see for example [5]–[8], [11], [12]. This paper is only interested in the CDA approach.

In [5], Kiran and Rajan presented a general construction of CDA-based NVD STBC for a class of n : $n = 2^m, 2 \cdot 3^m, 3 \cdot 2^m$, and $n = q^k(q - 1)$, q is prime and $q = 3 \pmod{4}$, where n is the number of transmit antennas. In [6], Elia et. al. presented a more general construction of NVD STBC based on CDA for any n and all of them are for QAM signals (similar constructions were also obtained for HEX signals in $\mathbb{Z}[\mathbf{j}]$). In this paper, we propose a simple construction method, which is easy to implement on a computer. The CDA construction usually consists of two steps. The first step is to construct a degree- n cyclic extension over a base field and the second step is to find a non-norm algebraic integer in the base field. For the first step of the construction, we propose a simple construction method by using the Kronecker-Weber Theorem that implies that any cyclic extension \mathbb{K} over \mathbb{Q} is a subfield of some cyclotomic field. Then, \mathbf{i} or \mathbf{j} is properly added to

\mathbb{K} to make it a cyclic extension over $\mathbb{Q}(\mathbf{i})$ or $\mathbb{Q}(\mathbf{j})$. For the second step, based on Kiran and Rajan's sufficient condition for a non-norm element, we develop an elementary condition for non-norm elements that is easy to check.

This paper is organized as follows. In Section 2, we give a brief description of the CDA-based NVD STBC construction. In Section 3, we present a construction of cyclic extensions. In Section 4, we present an elementary condition for non-norm elements. In Section 5, we present some design examples and some comparison with the existing codes. Throughout this paper, we use \mathbb{Z} and \mathbb{Q} to denote integer ring and rational field, respectively, $\mathbf{i} = \sqrt{-1}$ and $\mathbf{j} = \exp(\frac{i2\pi}{3})$, and $\boldsymbol{\xi}$ can be either \mathbf{i} or \mathbf{j} .

II. STBC BASED ON CYCLIC DIVISION ALGEBRA

A cyclic algebra A over a number field \mathbb{F} is determined by

- 1) a degree- n cyclic extension \mathbb{L}/\mathbb{F} , i.e., Galois group $\text{Gal}(\mathbb{L}/\mathbb{F}) = \langle \sigma \rangle$ is cyclic;
- 2) a $\gamma \in \mathbb{F}^* \triangleq \mathbb{F} \setminus \{0\}$.

Every element in A can be represented by a matrix in the following form,

$$C = \begin{bmatrix} x_0 & \gamma\sigma(x_{n-1}) & \cdots & \gamma\sigma^{n-1}(x_1) \\ x_1 & \sigma(x_0) & \cdots & \gamma\sigma^{n-1}(x_2) \\ x_2 & \sigma(x_1) & \cdots & \gamma\sigma^{n-1}(x_3) \\ \vdots & \vdots & \ddots & \vdots \\ x_{n-2} & \sigma(x_{n-3}) & \cdots & \gamma\sigma^{n-1}(x_{n-1}) \\ x_{n-1} & \sigma(x_{n-2}) & \cdots & \sigma^{n-1}(x_0) \end{bmatrix}, \quad (1)$$

where $x_l \in \mathbb{L}, l = 0, 1, \dots, n - 1$. If $\gamma^l \notin N_{\mathbb{L}/\mathbb{F}}(\mathbb{L})$, i.e., $\gamma^l \neq \prod_{j=0}^{n-1} \sigma^j(x)$ for any $x \in \mathbb{L}, l = 1, 2, \dots, n - 1$, then the cyclic algebra A is a division algebra, i.e., every non-zero element in A has a multiplicative inverse. The above condition imposed on γ is called *norm condition*. A γ satisfying norm condition is said to be a *non-norm element* [6], [16], [17]. We always have $\det(C) \in \mathbb{F}$, a concise proof is given in [6]. And we also have that $\det(C) = 0$ if and only if $x_l = 0$ for all l , i.e., code $\{C\}$ has full diversity. If we choose $\mathbb{F} = \mathbb{Q}(\boldsymbol{\xi})$ and $x_l, l = 0, 1, \dots, n - 1$, to be algebraic integers in \mathbb{L} with $\prod_{l=0}^{n-1} x_l \neq 0$, in addition, we choose a $\gamma \in \mathbb{Z}[\boldsymbol{\xi}]$ which satisfies the norm condition, then $\det(C)$ is clearly a nonzero algebraic integer in $\mathbb{Q}(\boldsymbol{\xi})$, i.e., $\det(C) \in \mathbb{Z}[\boldsymbol{\xi}] \setminus \{0\}$. Therefore, we have $|\det(C)| \geq 1$. This division algebra property gives us a way to construct NVD STBC [5]. Let $e_l \in \mathcal{O}_{\mathbb{L}}, l =$

The authors are with the Department of Electrical and Computer Engineering, University of Delaware, Newark, DE 19716. Email: {guo, xxia}@ee.udel.edu. Their work was supported in part by the Air Force Office of Scientific Research (AFOSR) under Grant No. FA9550-05-1-0161, the National Science Foundation under Grant CCR-0325180.

$0, 1, \dots, n-1$, be a relative integer basis of $\mathbb{L}/\mathbb{Q}(\xi)$, where $\mathcal{O}_{\mathbb{L}}$ is the integer ring of the field \mathbb{L} , and let x_l in (1) be

$$x_l = \sum_{j=0}^{n-1} x_{l,j} e_j, \quad l = 0, 1, \dots, n-1, \quad (2)$$

for $x_{l,j} \in \mathcal{O}_{\mathbb{L}}$, then we can embed n^2 variables $\{x_{l,j}\}_{0 \leq l, j \leq n-1}$ into the code matrix C , and the resulting STBC is a rate- n (full rate) NVD code.

III. CONSTRUCTION OF CYCLIC EXTENSIONS OVER $\mathbb{Q}(\xi)$

We now present our simple construction method of degree- n cyclic extensions over $\mathbb{Q}(\xi)$ by first introducing a general theory and then a detailed implementation method.

A. Construction of Cyclic Extensions: Theory

We first construct a cyclic extension \mathbb{K}/\mathbb{Q} , then extend \mathbb{K} to make it a cyclic extension over $\mathbb{Q}(\xi)$. The following theorem about abelian field extension from the algebraic number theory is a guideline for the purpose of constructing a cyclic extension over \mathbb{Q} . An abelian field extension is a field extension for which the associated Galois group is abelian.

Theorem 1 (Kronecker-Weber [18]): Every abelian field extension over \mathbb{Q} is a subfield of some cyclotomic field.

Since a cyclic group is abelian, a cyclic extension over \mathbb{Q} is just a particular case of the abelian field extension over \mathbb{Q} . Therefore, according to the Kronecker-Weber Theorem, every cyclic extension over \mathbb{Q} is a subfield of some cyclotomic field. To construct a degree- n cyclic extension over \mathbb{Q} , first we need to choose a suitable cyclotomic field. Let ω_m denote the m -th root of unity. The degree of the cyclotomic field $\mathbb{E} = \mathbb{Q}(\omega_m)$ over \mathbb{Q} is $\phi(m)$, where ϕ is the Euler totient function [19], [20]. We choose \mathbb{E} such that there exists a subgroup \mathcal{G}_1 in $\text{Gal}(\mathbb{E}/\mathbb{Q})$ whose associated quotient group $\mathcal{G}_0 = \text{Gal}(\mathbb{E}/\mathbb{Q})/\mathcal{G}_1$ is an order- n cyclic group. Thus, according to the *fundamental theorem of Galois theory* (see [6], [21]), the fixed field \mathbb{K} of \mathcal{G}_1 is a cyclic extension over \mathbb{Q} , and $\text{Gal}(\mathbb{K}/\mathbb{Q}) \cong \mathcal{G}_0$. A necessary condition for such a cyclotomic field \mathbb{E} for constructing a degree n cyclic extension over \mathbb{Q} is that $\phi(m)$ must be a multiple of n . The details about the implementation will be explained later. Now we assume that we have already found a cyclic extension over \mathbb{Q} , how to get a cyclic extension over $\mathbb{Q}(\xi)$? The following theorem gives us a way to do so.

Theorem 2: Let $\mathbb{K} = \mathbb{Q}(\alpha)$, \mathbb{K}/\mathbb{Q} be a cyclic extension of degree n , $m_\alpha(x)$ be the minimal polynomial of α over \mathbb{Q} . Then $\mathbb{K}(\xi)/\mathbb{Q}(\xi)$ is a cyclic extension of degree n if and only if $m_\alpha(x)$ is irreducible over $\mathbb{Q}(\xi)$.

Proof: We have that $\mathbb{K}(\xi) = \mathbb{Q}(\alpha, \xi) = \mathbb{Q}(\xi, \alpha) = [\mathbb{Q}(\xi)](\alpha)$, α is the primitive element of $\mathbb{K}(\xi)/\mathbb{Q}(\xi)$. Since $\mathbb{K}(\xi)/\mathbb{Q}(\xi)$ is a cyclic extension of degree n , the minimal polynomial $\hat{m}_\alpha(x)$ of α over $\mathbb{Q}(\xi)$ has degree n . Suppose $m_\alpha(x)$ is reducible over $\mathbb{Q}(\xi)$, since $m_\alpha(\alpha) = 0$, there must be one prime factor $m_1(x)$ of $m_\alpha(x)$ such that $m_1(\alpha) = 0$. Then, $\deg(\hat{m}_\alpha(x)) \leq \deg(m_1(x)) < n$, which contradicts with the fact that $\deg \hat{m}_\alpha(x) = n$. Therefore, $m_\alpha(x)$ is irreducible and it is the minimal polynomial of α .

Conversely, since \mathbb{K}/\mathbb{Q} is a cyclic extension, the Galois group of $m_\alpha(x)$ is a cyclic group (the Galois group of a polynomial is defined as a permutation group of the roots) [21]. Because $m_\alpha(x)$ is an irreducible polynomial over $\mathbb{Q}(\xi)$, for the field extension

$$\mathbb{K}(\xi)/\mathbb{Q}(\xi) \cong \mathbb{Q}(\xi)[x]/(m_\alpha(x)), \quad (3)$$

the Galois group of $\mathbb{K}(\xi)/\mathbb{Q}(\xi)$ is isomorphic to the Galois group of $m_\alpha(x)$, which is cyclic. This leads to the conclusion that $\mathbb{K}(\xi)/\mathbb{Q}(\xi)$ is also a cyclic extension. ■

As a direct consequence of Theorem 2, we have the following corollary,

Corollary 1: Let $\mathbb{K} = \mathbb{Q}(\alpha)$ and \mathbb{K}/\mathbb{Q} be a degree n cyclic extension. Let $m_\alpha(x)$ be the minimal polynomial of α over \mathbb{Q} . If all the roots of $m_\alpha(x)$ in \mathbb{C} are real, then $\mathbb{K}(\xi)/\mathbb{Q}(\xi)$ is also a cyclic extension of degree n .

Proof: Since all the roots of $m_\alpha(x)$ are real, $m_\alpha(x)$ is also irreducible in $\mathbb{Q}(\xi)$. By Theorem 2, $\mathbb{K}(\xi)/\mathbb{Q}(\xi)$ is a cyclic extension of degree n . ■

Thus, a cyclic extension can be constructed in two steps: first we search for a cyclic extension \mathbb{K}/\mathbb{Q} , i.e., to identify a primitive element α and its associated minimal polynomial $m_\alpha(x)$; then we check whether $m_\alpha(x)$ is irreducible in $\mathbb{Q}(\xi)$, if this is true, then $\mathbb{K}(\xi)/\mathbb{Q}(\xi)$ is a desired cyclic extension, where the irreducibility holds automatically if all the roots of $m_\alpha(x)$ are real according to the above study. Existing cyclic extensions over $\mathbb{Q}(\xi)$ constructed in [2], [5], [6], [11], [12] can all be constructed in this way.

B. Construction of Cyclic Extensions: Implementation

We next explain our detailed implementation method of searching cyclic extensions over \mathbb{Q} . First we need an easy manipulating group G that is isomorphic to the Galois group $\text{Gal}(\mathbb{E}/\mathbb{Q})$, so that we can use a computer program to search for cyclotomic field \mathbb{E} whose Galois group $\text{Gal}(\mathbb{E}/\mathbb{Q})$ has an order- n cyclic quotient group. It is well known that the multiplicative group

$$G = \{k \mid 0 < k < m, \gcd(k, m) = 1\} \quad (4)$$

is isomorphic to the Galois group $\text{Gal}(\mathbb{E}/\mathbb{Q})$, where the multiplication defined as “modulo m ” multiplication. The isomorphism $\mathfrak{M} : \text{Gal}(\mathbb{E}/\mathbb{Q}) \mapsto G$ is defined by

$$\mathfrak{M}(g) = k, \quad g \in \text{Gal}(\mathbb{E}/\mathbb{Q}), \quad k \in G, \quad (5)$$

where g and k satisfies

$$g \left(\exp \left(\frac{\mathbf{i}2\pi}{m} \right) \right) = \exp \left(\frac{\mathbf{i}2k\pi}{m} \right). \quad (6)$$

In our implementation, we use G to represent the Galois group $\text{Gal}(\mathbb{E}/\mathbb{Q})$ since it is easier to manipulate. We search subgroups in G to find all the subgroups G_1 such that $G_0 = G/G_1$ are order- n cyclic groups. This can be done by our MATLAB program [22]. By the isomorphism between G and $\text{Gal}(\mathbb{E}/\mathbb{Q})$, we can get the corresponding subgroup \mathcal{G}_1 in the Galois group $\text{Gal}(\mathbb{E}/\mathbb{Q})$, and $\mathcal{G}_0 = \text{Gal}(\mathbb{E}/\mathbb{Q})/\mathcal{G}_1$ is an order- n cyclic group.

Now we have cyclotomic field \mathbb{E} , the Galois group $\text{Gal}(\mathbb{E}/\mathbb{Q})$, the subgroup \mathcal{G}_1 and the quotient group \mathcal{G}_0 . Next, we explain how to find the fixed field \mathbb{K} of \mathcal{G}_1 , or equivalently, find a primitive element α of \mathbb{K}/\mathbb{Q} and the corresponding minimal polynomial $m_\alpha(x)$. The following theorem gives a characterization of the primitive element α .

Theorem 3: Let \mathbb{E}/\mathbb{Q} be a degree- n Galois extension, \mathcal{G}_1 be a subgroup of $\text{Gal}(\mathbb{E}/\mathbb{Q})$, and the fixed field of \mathcal{G}_1 be \mathbb{K} . Then, α is a primitive element of the extension \mathbb{K}/\mathbb{Q} if and only if α satisfies the following two conditions:

- 1) α is invariant under the transforms of \mathcal{G}_1 , i.e., $g(\alpha) = \alpha$ for $\forall g \in \mathcal{G}_1$;
- 2) α is *fully variant* under the transforms of $\mathcal{G}_0 = \text{Gal}(\mathbb{K}/\mathbb{Q}) \cong \text{Gal}(\mathbb{E}/\mathbb{Q})/\mathcal{G}_1$, i.e., for any two different elements \hat{g}_1, \hat{g}_2 in \mathcal{G}_0 , $\hat{g}_1(\alpha) \neq \hat{g}_2(\alpha)$.

Proof: Since $\alpha \in \mathbb{K}$ and \mathbb{K} is the fixed field of \mathcal{G}_1 , for any $g \in \mathcal{G}_1$, we have $g(\alpha) = \alpha$. Let $m_\alpha(x)$ be the minimal polynomial of α . We know $[\mathbb{K} = \mathbb{Q}(\alpha) : \mathbb{Q}]$ equals to the degree of $m_\alpha(x)$. By the Galois theory, we also have $|\mathcal{G}_0| = [\mathbb{K} : \mathbb{Q}]$. Thus, $m_\alpha(x)$ has $|\mathcal{G}_0|$ numbers of roots. By the field theory, $R = \{\hat{g}(\alpha), \hat{g} \in \mathcal{G}_0\}$ is the full set of roots of $m_\alpha(x)$, so $|R| = |\mathcal{G}_0|$. Hence, we must have α fully variant under the transforms of \mathcal{G}_0 .

Next, we prove the converse part. By the first condition, we know $\alpha \in \mathbb{K}$. Since for any two different elements $\hat{g}_1, \hat{g}_2 \in \mathcal{G}_0$, $\hat{g}_1(\alpha) \neq \hat{g}_2(\alpha)$, the set $R = \{\hat{g}(\alpha), \hat{g} \in \mathcal{G}_0\}$ has $|\mathcal{G}_0|$ distinct elements. By the field theory, the minimal polynomial of α is

$$m_\alpha(x) = \prod_{\hat{g} \in \mathcal{G}_0} (x - \hat{g}(\alpha)), \quad (7)$$

and the degree of $m_\alpha(x)$ is $|\mathcal{G}_0|$. By the Galois theory, we know $|\mathcal{G}_0| = [\mathbb{K} : \mathbb{Q}]$. And we have $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ equals to the degree of $m_\alpha(x)$, i.e., $[\mathbb{Q}(\alpha) : \mathbb{Q}] = |\mathcal{G}_0|$, therefore $[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{K} : \mathbb{Q}]$. Since $\alpha \in \mathbb{K}$, $\mathbb{Q}(\alpha)$ is a subspace of \mathbb{K} . Since it has the same dimensionality as \mathbb{K} , we have $\mathbb{K} = \mathbb{Q}(\alpha)$ and therefore, α is a primitive element of \mathbb{K}/\mathbb{Q} . ■

In the following, we give a systematic method to find an α satisfying the two conditions given in the above theorem.

Corollary 2: Let \mathbb{K} and \mathcal{G}_1 be as mentioned above. Let $f(x)$ be

$$f(x) = \prod_{g \in \mathcal{G}_1} \left[x - g \left(\exp \left(\frac{i2\pi}{m} \right) \right) \right]. \quad (8)$$

Then, there exists an $x_0 \in \mathbb{Z}$ so that $f(x_0)$ is a primitive element for the extension \mathbb{K}/\mathbb{Q} .

Proof: Let $x_0 \in \mathbb{Q}$, for any $\tilde{g} \in \mathcal{G}_1 \subset \text{Gal}(\mathbb{E}/\mathbb{Q})$, we have $\tilde{g}(x_0) = x_0$, which is because \tilde{g} is an element in

$\text{Gal}(\mathbb{E}/\mathbb{Q})$ and it fixes the elements in \mathbb{Q} . Then

$$\begin{aligned} \tilde{g}(f(x_0)) &= \tilde{g} \left(\prod_{g \in \mathcal{G}_1} (x_0 - g(\exp(i2\pi/m))) \right) \\ &= \prod_{g \in \mathcal{G}_1} \tilde{g}(x_0 - g(\exp(i2\pi/m))) \\ &= \prod_{g \in \mathcal{G}_1} (\tilde{g}(x_0) - \tilde{g}g(\exp(i2\pi/m))) \\ &= \prod_{g \in \tilde{g}\mathcal{G}_1} (x_0 - g(\exp(i2\pi/m))) \\ &= \prod_{g \in \mathcal{G}_1} (x_0 - g(\exp(i2\pi/m))) = f(x_0). \end{aligned} \quad (9)$$

The last equality holds because for any group H and $h \in H$, we always have $hH = H$. So $\forall x_0 \in \mathbb{Q}$, $f(x_0)$ is invariant under the transform of any element in \mathcal{G}_1 , i.e., $f(x_0)$ satisfies the first condition in Theorem 3.

Similarly, let $x \in \mathbb{Q}$ and $\hat{g} \in \mathcal{G}_0$, we have

$$\begin{aligned} \hat{g}(f(x)) &= \prod_{g \in \mathcal{G}_1} (x - \hat{g}g(\exp(i2\pi/m))) \\ &= \prod_{g \in \hat{g}\mathcal{G}_1} (x - g(\exp(i2\pi/m))), \end{aligned} \quad (10)$$

which is because, when \hat{g} runs through \mathcal{G}_0 , $\hat{g}\mathcal{G}_1$ runs through all the cosets of \mathcal{G}_1 in $\text{Gal}(\mathbb{E}/\mathbb{Q})$. Polynomials $\hat{g}(f(x))$ for different $\hat{g} \in \mathcal{G}_0$ are different, since otherwise $m_0(x) = \prod_{\hat{g} \in \mathcal{G}_0} \hat{g}(f(x))$ is reducible. So $\{\hat{g}(f(x)), \hat{g} \in \mathcal{G}_0, x \in \mathbb{Q}\}$ contains $|\mathcal{G}_0|$ numbers of different polynomials. We use $\{p_1(x), \dots, p_k(x)\}$ to denote these polynomials, where $k = |\mathcal{G}_0|$. We want $f(x_0)$ to be *fully variant* under the transforms of \mathcal{G}_0 , i.e., $\{p_1(x_0), \dots, p_k(x_0)\}$ are k different numbers. Note that for k different polynomials $\{p_1(x), \dots, p_k(x)\}$, we can always find a number x_0 in \mathbb{Z} so that $\{p_1(x_0), \dots, p_k(x_0)\}$ are k different numbers, i.e., $f(x_0)$ is *fully variant* under the transforms of \mathcal{G}_0 . Thus, we can choose such an $f(x_0)$ as a primitive element α of \mathbb{K}/\mathbb{Q} . ■

Another method that often works is to choose α from the coefficients of $f(x)$, since by Eq. (9) all the coefficients are invariant under the transforms of \mathcal{G}_1 . From these coefficients, we choose one that is *fully variant* under the transforms of \mathcal{G}_0 . The minimal polynomial of α can be obtained by (7). Since \mathbb{Q} is the fixed field of \mathcal{G}_0 , any rational number is invariant under the transforms of \mathcal{G}_0 . Thus, we only need to consider those non-rational coefficients. There must be at least one of the coefficients of $f(x)$ that is not a rational number, otherwise $f(x)$ is a proper factor of $m_0(x)$ in \mathbb{Q} , which then contradicts with the fact that $m_0(x)$ is irreducible in \mathbb{Q} . The coefficients of $f(x)$ are algebraic integers with relatively smaller absolute values. Thus, in our implementation, we first check whether there is a coefficient of $f(x)$ that is fully variant under \mathcal{G}_0 . If this fails, we choose an $x_0 \in \mathbb{Z}$ so that $f(x_0)$ is fully variant under the transforms of \mathcal{G}_0 , which can be done by simply searching integers in \mathbb{Z} .

IV. AN ELEMENTARY CONDITION FOR NON-NORM ELEMENTS γ

In this section, we present an elementary condition for a non-norm element γ of the Galois extension $\mathbb{K}(\xi)/\mathbb{Q}(\xi)$. We first introduce the following theorem by Kiran and Rajan.

Theorem 4 (Kiran and Rajan [5]): Let \mathbb{L} be a degree- n Galois extension of a number field \mathbb{F} . Let \mathfrak{p} be a prime ideal in $\mathcal{O}_{\mathbb{F}}$. Let prime ideal $\mathfrak{P} \in \mathcal{O}_{\mathbb{L}}$ be one of the factors of $\mathfrak{p}\mathcal{O}_{\mathbb{L}}$ in $\mathcal{O}_{\mathbb{L}}$ and the inertial degree of \mathfrak{P} over \mathbb{F} be $f(\mathfrak{P}/\mathfrak{p}) = f$. If γ is any element of $\mathfrak{p} \setminus \mathfrak{p}^2$, then $\gamma^j \notin N_{\mathbb{L}/\mathbb{F}}(\mathbb{L})$ for any $j = 1, 2, \dots, f-1$.

Let $\mathbb{F} = \mathbb{Q}(\xi)$. We know that $\mathcal{O}_{\mathbb{Q}(\xi)} = \mathbb{Z}[\xi]$ is a principal ideal domain for $\xi = \mathbf{i}$ or $\xi = \mathbf{j}$. Thus, every prime ideal in $\mathbb{Z}[\xi]$ can be written as $\langle p \rangle$ for some prime p in $\mathbb{Z}[\xi]$. Let $\langle p \rangle$ be a prime ideal in $\mathbb{Z}[\xi]$ and $\langle p \rangle$ be inert in \mathbb{L} , i.e., $p\mathcal{O}_{\mathbb{L}} = \mathfrak{P}$ is a prime ideal, then $f = f(\mathfrak{P}/\langle p \rangle) = n$. Since $p \in \langle p \rangle \setminus \langle p \rangle^2$, according to Theorem 4, $p^j \notin N_{\mathbb{L}/\mathbb{Q}(\xi)}(\mathbb{L})$, $j = 1, 2, \dots, n-1$, namely, p is a non-norm element in $\mathbb{L}/\mathbb{Q}(\xi)$. This leads to the following lemma, which is used in the proof of Theorem 5.

Lemma 1: Let \mathbb{L} be a degree- n Galois extension of the field $\mathbb{Q}(\xi)$ and let p be a prime in $\mathbb{Z}[\xi]$. If $p\mathcal{O}_{\mathbb{L}}$ is a prime ideal in $\mathcal{O}_{\mathbb{L}}$, then $p^j \notin N_{\mathbb{L}/\mathbb{Q}(\xi)}(\mathbb{L})$, $j = 1, 2, \dots, n-1$, i.e., p is a non-norm element.

Based on the above theorem and lemma, we can prove the following theorem [23].

Theorem 5: Let $\mathbb{K} = \mathbb{Q}(\alpha)$ and \mathbb{K}/\mathbb{Q} be a degree- n Galois extension. Let $m_{\alpha}(x)$ be the minimal polynomial of α and remain irreducible in $\mathbb{Q}(\xi)$. Let p be a prime in \mathbb{Z} and $p\mathcal{O}_{\mathbb{K}}$ remain prime in $\mathcal{O}_{\mathbb{K}}$. Then

- 1) if p is also a prime in $\mathbb{Z}[\xi]$ and n is odd, then $p^j \notin N_{\mathbb{K}(\xi)/\mathbb{Q}(\xi)}(\mathbb{K}(\xi))$, $j = 1, 2, \dots, n-1$, i.e., p is a non-norm element in $\mathbb{K}(\xi)/\mathbb{Q}(\xi)$;
- 2) if p is not a prime in $\mathbb{Z}[\xi]$, then $p = p_o p_o^*$ for some prime p_o in $\mathbb{Z}[\xi]$, and $p_o^j \notin N_{\mathbb{K}(\xi)/\mathbb{Q}(\xi)}(\mathbb{K}(\xi))$, $j = 1, 2, \dots, n-1$, i.e., p_o is a non-norm element in $\mathbb{K}(\xi)/\mathbb{Q}(\xi)$.

In order to use Theorem 5 to find a non-norm element γ , we have to check whether a prime number p is inert in \mathbb{K} , i.e., whether $p\mathcal{O}_{\mathbb{K}}$ remains prime. The following theorem is the *prime ideal factorization theorem* [24], which tells us the relationship between the factorization of $p\mathcal{O}_{\mathbb{L}}$ and the factorization of $m_{\alpha}(x)$ over the finite field $\mathcal{O}_{\mathbb{F}}/\mathfrak{p}$, where $\mathbb{L} = \mathbb{F}(\alpha)$ and \mathfrak{p} is a prime ideal in $\mathcal{O}_{\mathbb{F}}$.

Theorem 6 (Prime Ideal Factorization Theorem): Let \mathbb{L}/\mathbb{F} be a number field extension, and $\mathbb{L} = \mathbb{F}(\alpha)$, $\alpha \in \mathcal{O}_{\mathbb{L}}$. Let $m_{\alpha}(x)$ denote the minimal polynomial of α over \mathbb{F} . Suppose that \mathfrak{p} is a prime ideal in $\mathcal{O}_{\mathbb{F}}$ and the characteristic of the finite field $\mathcal{O}_{\mathbb{F}}/\mathfrak{p}$ is p , which can not divide $|\mathcal{O}_{\mathbb{L}}/\mathcal{O}_{\mathbb{F}}[\alpha]|$. If $m_{\alpha}(x)$ can be factorized over the finite field $\mathcal{O}_{\mathbb{F}}/\mathfrak{p}$ as follows,

$$m_{\alpha}(x) = \prod_{j=1}^g m_j^{e_j}(x), \quad (11)$$

where $m_j(x)$ are distinct irreducible polynomials over $\mathcal{O}_{\mathbb{F}}/\mathfrak{p}$, then

$$\mathfrak{p}\mathcal{O}_{\mathbb{L}} = \prod_{j=1}^g \mathfrak{p}_j^{e_j}, \quad (12)$$

where $\mathfrak{p}_j = \langle \mathfrak{p}, m_j(\alpha) \rangle$.

If we only consider the case when $\mathbb{F} = \mathbb{Q}$, as a consequence of the *prime ideal factorization theorem*, we have the following corollary.

Corollary 3: Let $\mathbb{K} = \mathbb{Q}(\alpha)$, $\alpha \in \mathcal{O}_{\mathbb{K}}$, \mathbb{K}/\mathbb{Q} be a degree- n Galois extension. Let $m_{\alpha}(x)$ be the minimal polynomial of α over \mathbb{Q} . Let p be a prime number in \mathbb{Z} , which can not divide $\text{disc}(m_{\alpha}(x))$. If $m_{\alpha}(x)$ is irreducible over the finite field $\mathbb{Z}/\langle p \rangle$, then $p\mathcal{O}_{\mathbb{K}}$ is a prime ideal in $\mathcal{O}_{\mathbb{K}}$.

In the above corollary, $\text{disc}(m_{\alpha}(x))$ is the discriminant of the minimal polynomial $m_{\alpha}(x)$ [25]. Write $m_{\alpha}(x) = \prod (x - r_i)$, then $\text{disc}(m_{\alpha}(x))$ is defined as

$$\text{disc}(m_{\alpha}(x)) = \prod_{i < j} (r_i - r_j)^2. \quad (13)$$

Proof: From the algebraic number theory, we know $|\mathcal{O}_{\mathbb{K}}/\mathcal{O}_{\mathbb{Q}}[\alpha]|^2 = |\text{disc}(m_{\alpha}(x))/\text{disc}(\mathbb{K})|$ [26], where $\text{disc}(\mathbb{K})$ is the discriminant of field \mathbb{K} . If p is not a factor of $\text{disc}(m_{\alpha}(x))$, then p cannot divide $|\mathcal{O}_{\mathbb{K}}/\mathcal{O}_{\mathbb{Q}}[\alpha]|$. By Theorem 6, since $m_{\alpha}(x)$ is irreducible over the finite field $\mathbb{Z}/\langle p \rangle$, $p\mathcal{O}_{\mathbb{K}}$ is also reducible, i.e., $p\mathcal{O}_{\mathbb{K}}$ remains prime in $\mathcal{O}_{\mathbb{K}}$. ■

By combining Corollary 3 and Theorem 5, we immediately have the following theorem on sufficient conditions for a non-norm element, which is more elementary and easier to understand than the existing ones.

Theorem 7: Let $\mathbb{K} = \mathbb{Q}(\alpha)$, $\alpha \in \mathcal{O}_{\mathbb{K}}$, \mathbb{K}/\mathbb{Q} be a degree- n Galois extension. Let $m_{\alpha}(x)$ be the minimal polynomial of α and it remains irreducible in $\mathbb{Q}(\xi)$. Let p be a prime in \mathbb{Z} , which cannot divide $\text{disc}(m_{\alpha}(x))$. If $m_{\alpha}(x)$ is irreducible over $\mathbb{Z}/\langle p \rangle$, then

- 1) if p is also a prime in $\mathbb{Z}[\xi]$ and n is odd, then $p^j \notin N_{\mathbb{K}(\xi)/\mathbb{Q}(\xi)}(\mathbb{K}(\xi))$, $j = 1, 2, \dots, n-1$, i.e., p is a non-norm element in $\mathbb{K}(\xi)/\mathbb{Q}(\xi)$;
- 2) if p is not a prime in $\mathbb{Z}[\xi]$, then $p = p_o p_o^*$ for some prime p_o in $\mathbb{Z}[\xi]$, and $p_o^j \notin N_{\mathbb{K}(\xi)/\mathbb{Q}(\xi)}(\mathbb{K}(\xi))$, $j = 1, 2, \dots, n-1$, i.e., p_o is a non-norm element in $\mathbb{K}(\xi)/\mathbb{Q}(\xi)$.

V. DESIGN EXAMPLES AND COMPARISON WITH EXISTING CODE

In Table I, we list some design examples of cyclic extensions over \mathbb{Q} . The primitive elements and their conjugates are listed in the third column. The corresponding minimal polynomials are listed in Table II. It can be easily checked (in MATLAB we can use MAPLE function *irreduc*) that all the minimal polynomials are irreducible over $\mathbb{Q}(\mathbf{i})$, so all these cyclic extensions over \mathbb{Q} can be extended to be a cyclic extensions over $\mathbb{Q}(\mathbf{i})$ by just adding \mathbf{i} to the field.

We next apply Theorem 7 to prove that the γ 's listed in Table I are non-norm elements of $\mathbb{K}(\mathbf{i})/\mathbb{Q}(\mathbf{i})$. For the cases $n = 2, 3, 4, 5, 6, 7, 9, 10, 11, 12, 13, 14, 15, 17, 18, 19, 20$, the discriminants of the minimal polynomials as listed in Table II are all odd numbers, which cannot be divided by 2. We check whether $m_{\alpha}(x)$ can be factorized over the finite field $\mathbb{Z}/\langle 2 \rangle$. It turns out that in all these cases $m_{\alpha}(x)$ are irreducible over $\mathbb{Z}/\langle 2 \rangle$. In addition, all these minimal polynomials are irreducible over $\mathbb{Q}(\mathbf{i})$. Since $2 = (1 + \mathbf{i})(1 - \mathbf{i})$ in $\mathbb{Q}(\mathbf{i})$, by using Theorem 7, we conclude that $\gamma = 1 + \mathbf{i}$ satisfies the norm condition for all these cases.

For the cases $n = 8, 16$, the discriminants of the minimal polynomials $m_\alpha(x)$ are coprime with 5, and $m_\alpha(x)$ are irreducible over the finite field $\mathbb{Z}/\langle 5 \rangle$ (note that they are reducible over $\mathbb{Z}/\langle 2 \rangle$), and $m_\alpha(x)$ are also irreducible over $\mathbb{Q}(\mathbf{i})$. Since $5 = (2 + \mathbf{i})(2 - \mathbf{i})$, by Theorem 7, $\gamma = 2 + \mathbf{i}$ is a non-norm element for these two cases.

In the case of HEX constellations, we need to find non-norm elements in $\mathbb{Q}(\mathbf{j})$. By a similar procedure, we can prove that $\gamma = 2 + \mathbf{j}$ is a non-norm element for $n = 3, 4, 5, 7, 8, 9, 13, 14, 16, 17, 18, 19, 20$; $\gamma = 3 + \mathbf{j}$ is a non-norm element for $n = 10, 11, 12, 15$. But for $n = 2, 6$, the minimal polynomial $m_\alpha(x)$ is reducible in $\mathbb{Q}(\mathbf{j})$, so we can not extend the field to a cyclic extension field of $\mathbb{Q}(\mathbf{j})$. A proper choice for $n = 2$ is to choose the cyclic field with primitive element $\alpha = -\frac{1}{2} + \mathbf{i}\frac{\sqrt{7}}{2}$ and the corresponding minimal polynomial is $m_\alpha = x^2 + x + 2$. For $n = 6$, we can choose primitive element $\alpha = -\cos(\frac{2\pi}{7}) - \mathbf{i}\sin(\frac{2\pi}{7})$ and the corresponding minimal polynomial is $m_\alpha = x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$. For these two cases, the γ can be chosen to be $2 + \mathbf{j}$.

Next, we show an example to compare the normalized diversity product between the code we constructed and the code constructed in [6] for QAM signals. The normalized diversity product is defined as

$$\zeta(\mathcal{C}) = \frac{\delta(\mathcal{C}_\infty)}{E^n}, \quad (14)$$

where $\delta(\mathcal{C}_\infty)$ is the *minimum determinant* as defined in [2], [8] and E is the total energy of the generator matrices of all layers.

Consider $n = 3$ and let $e = [e_0, e_1, e_2]$ be the relative integer basis. The code matrix C in (1) can be written as

$$C = \text{diag}[Ax_0] + \text{diag}[Bx_1]S_1 + \text{diag}[Cx_2]S_2, \quad (15)$$

where

$$x_l = [x_{l,0}, x_{l,1}, x_{l,2}]^T, \quad l = 0, 1, 2,$$

$$A = \begin{bmatrix} e \\ \sigma(e) \\ \sigma^2(e) \end{bmatrix}, \quad B = \begin{bmatrix} e \\ \sigma(e) \\ \gamma\sigma^2(e) \end{bmatrix}, \quad C = \begin{bmatrix} e \\ \gamma\sigma(e) \\ \gamma\sigma^2(e) \end{bmatrix},$$

$$S_1 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \quad S_2 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

We call A, B, C the generator matrices of the code matrix. The generator matrices of the 3×3 code constructed in [6] are

$$A = \begin{bmatrix} 1 & 2 \cos\left(\frac{2\pi}{7}\right) & 2 \cos\left(\frac{4\pi}{7}\right) \\ 1 & 2 \cos\left(\frac{4\pi}{7}\right) & 2 \cos\left(\frac{8\pi}{7}\right) \\ 1 & 2 \cos\left(\frac{8\pi}{7}\right) & 2 \cos\left(\frac{2\pi}{7}\right) \end{bmatrix}, \quad (16)$$

$$B = \begin{bmatrix} 1 & 2 \cos\left(\frac{2\pi}{7}\right) & 2 \cos\left(\frac{4\pi}{7}\right) \\ 1 & 2 \cos\left(\frac{4\pi}{7}\right) & 2 \cos\left(\frac{8\pi}{7}\right) \\ \gamma & 2\gamma \cos\left(\frac{8\pi}{7}\right) & 2\gamma \cos\left(\frac{2\pi}{7}\right) \end{bmatrix}, \quad (17)$$

$$C = \begin{bmatrix} 1 & 2 \cos\left(\frac{2\pi}{7}\right) & 2 \cos\left(\frac{4\pi}{7}\right) \\ \gamma & 2\gamma \cos\left(\frac{4\pi}{7}\right) & 2\gamma \cos\left(\frac{8\pi}{7}\right) \\ \gamma & 2\gamma \cos\left(\frac{8\pi}{7}\right) & 2\gamma \cos\left(\frac{2\pi}{7}\right) \end{bmatrix}, \quad (18)$$

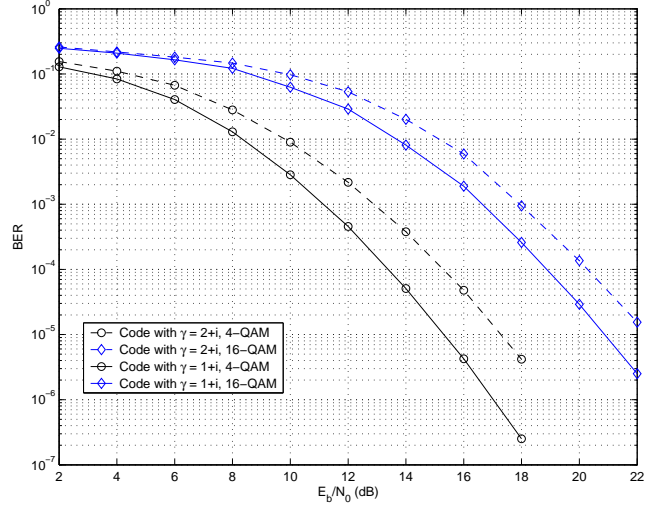


Fig. 1. Comparison of the codes with $\gamma = 2 + \mathbf{i}$ and $\gamma = 1 + \mathbf{i}$

where $\gamma = 2 + \mathbf{i}$, the total energy of the generator matrices of all three layers is 103.1957, and the minimum determinant $\delta(\mathcal{C}_\infty) = 1$. Thus, the normalized diversity product is $\frac{1}{103.1957^3}$.

The generator matrices of the code constructed using our method are of the same form as the previous one, except $\gamma = 1 + \mathbf{i}$. The total energy of the generator matrices of all three layers is 55.0489 and the minimum determinant $\delta(\mathcal{C}_\infty) = 1$. Thus, the normalized diversity product is $\frac{1}{55.0489^3}$. We can see that by using our new γ , the normalized diversity product is much larger. The reason for this is that the new γ has smaller absolute values than the γ presented in [6] does. The simulation results in Fig. 1 show that for 4-QAM and 16-QAM constellations, the performance of the code with $\gamma = 1 + \mathbf{i}$ is about 2 dB and 1.5 dB better than that of the code with $\gamma = 2 + \mathbf{i}$, respectively.

VI. CONCLUSION

In this paper, we proposed a simple construction method of CDA-based NVD STBC for both QAM and HEX constellations. For the first step, we start from a cyclotomic field and then find a cyclic subfield. Because there exists an isomorphism between the Galois group and a simple multiplicative group, the searching procedure is easy to implement on a computer. For the second step, we presented an elementary condition for non-norm elements that is easy to check.

REFERENCES

- [1] 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*, Illinois, USA, Oct. 1-3 2003.
- [2] J.-C. Belfiore, G. Rekaya, and E. Viterbo, "The Golden code: a 2×2 full-rate space-time code with nonvanishing determinants," *IEEE Trans. Info. Theory*, vol. 51, no. 4, pp. 1432-1436, Apr. 2005.
- [3] P. Dayal and M. K. Varanasi, "An optimal two transmit antenna space-time code and its stacked extensions," *IEEE Trans. Info. Theory*, vol. 51, no. 12, pp. 4348-4355, Dec. 2005.
- [4] G. Wang and X.-G. Xia, "On optimal multi-layer cyclotomic space-time code designs," *IEEE Trans. Info. Theory*, vol. 51, no. 3, pp. 1102-1135, Mar. 2005.

TABLE I
CYCLOTOMIC FIELDS \mathbb{E} , PRIMITIVE ELEMENTS α AND THEIR
CONJUGATES, AND NON-NORM ELEMENTS γ

n	\mathbb{E}	$\{e_1 = \alpha, e_2, \dots, e_n\}$	γ
2	$\mathbb{Q}(\omega_3)$	$2 \cos(2m\pi/3), m = [1, 2]$	$1 + i$
3	$\mathbb{Q}(\omega_7)$	$2 \cos(2m\pi/7), m = [1, 2, 3]$	$1 + i$
4	$\mathbb{Q}(\omega_5)$	$\exp(i2m\pi/5), m = [1, 2, 4, 3]$	$1 + i$
5	$\mathbb{Q}(\omega_{11})$	$2 \cos(2m\pi/11), m = [1, 2, 4, 3, 5]$	$1 + i$
6	$\mathbb{Q}(\omega_9)$	$\exp(i2m\pi/9), m = [1, 2, 4, 8, 7, 5]$	$1 + i$
7	$\mathbb{Q}(\omega_{29})$	$2 \cos(2m_1\pi/29) + 2 \cos(2m_2\pi/29)$ $m_1 = [1, 2, 4, 8, 13, 3, 6],$ $m_2 = [12, 5, 10, 9, 11, 7, 14]$	$1 + i$
8	$\mathbb{Q}(\omega_{17})$	$2 \cos(2m\pi/17), m = [1, 3, 8, 7, 4, 5, 2, 6]$	$2 + i$
9	$\mathbb{Q}(\omega_{19})$	$2 \cos(2m\pi/19),$ $m = [1, 2, 4, 8, 3, 6, 7, 5, 9]$	$1 + i$
10	$\mathbb{Q}(\omega_{11})$	$\exp(i2m\pi/11),$ $m = [1, 2, 4, 8, 5, 10, 9, 7, 3, 6]$	$1 + i$
11	$\mathbb{Q}(\omega_{23})$	$2 \cos(2m\pi/23),$ $m = [1, 2, 4, 8, 7, 9, 5, 10, 3, 6, 11]$	$1 + i$
12	$\mathbb{Q}(\omega_{13})$	$\exp(i2m\pi/13),$ $m = [1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7]$	$1 + i$
13	$\mathbb{Q}(\omega_{53})$	$2 \cos(2m_1\pi/53) + 2 \cos(2m_2\pi/53)$ $m_1 = [1, 2, 4, 8, 16, 21, 11, 22, 9,$ $18, 17, 19, 15],$ $m_2 = [23, 7, 14, 25, 3, 6, 12, 24, 5,$ $10, 20, 13, 26]$	$1 + i$
14	$\mathbb{Q}(\omega_{29})$	$2 \cos(2m\pi/29)$ $m = [1, 2, 4, 8, 13, 3, 6, 12, 5,$ $10, 9, 11, 7, 14]$	$1 + i$
15	$\mathbb{Q}(\omega_{61})$	$2 \cos(2m_1\pi/61) + 2 \cos(2m_2\pi/61)$ $m_1 = [1, 2, 4, 8, 7, 14, 3, 5, 10, 20,$ $13, 19, 9, 15, 25]$ $m_2 = [11, 22, 17, 27, 16, 29, 28, 6, 12, 24,$ $21, 26, 23, 18, 30]$	$1 + i$
16	$\mathbb{Q}(\omega_{17})$	$\exp(i2m\pi/17),$ $m = [1, 3, 9, 10, 13, 5, 15, 11,$ $16, 14, 8, 7, 4, 12, 2, 6]$	$2 + i$
17	$\mathbb{Q}(\omega_{103})$	$2 \cos(2m_1\pi/103) + 2 \cos(2m_2\pi/103)$ $+ 2 \cos(2m_3\pi/103)$ $m_1 = [1, 2, 4, 8, 15, 30, 21, 17, 19, 3,$ $6, 12, 5, 10, 7, 14, 23]$ $m_2 = [46, 9, 18, 36, 16, 32, 39, 25, 34, 35,$ $27, 24, 45, 13, 26, 28]$ $m_3 = [47, 11, 38, 22, 29, 33, 20, 44, 48, 49,$ $40, 31, 42, 50, 43, 51, 41]$	$1 + i$
18	$\mathbb{Q}(\omega_{19})$	$\exp(i2m\pi/19)$ $m = [1, 2, 4, 8, 16, 13, 7, 14,$ $9, 18, 17, 15, 11, 3, 6, 12, 5, 10]$	$1 + i$
19	$\mathbb{Q}(\omega_{191})$	$2 \cos(2m_1\pi/191) + 2 \cos(2m_2\pi/191)$ $+ 2 \cos(2m_3\pi/191) + 2 \cos(2m_4\pi/191)$ $+ 2 \cos(2m_5\pi/191)$ $m_1 = [1, 2, 4, 8, 16, 32, 13, 9, 18, 36, 17,$ $11, 22, 3, 6, 12, 19, 38, 41]$ $m_2 = [7, 14, 5, 10, 20, 33, 64, 26, 52,$ $45, 57, 34, 37, 21, 42, 15, 23, 46, 71]$ $m_3 = [39, 27, 28, 56, 25, 40, 66, 31, 62,$ $61, 69, 47, 68, 44, 43, 29, 24, 48, 76]$ $m_4 = [49, 78, 35, 70, 51, 50, 80, 59, 65, 67,$ $72, 53, 85, 55, 81, 84, 30, 60, 92]$ $m_5 = [82, 93, 54, 83, 79, 89, 91, 63, 73, 87,$ $90, 77, 94, 74, 88, 86, 58, 75, 95]$	$1 + i$
20	$\mathbb{Q}(\omega_{25})$	$\cos(2m\pi/25)$ $m = [1, 2, 4, 8, 16, 7, 14, 3, 6, 12, 24,$ $23, 21, 17, 9, 18, 11, 22, 19, 13]$	$1 + i$

- [5] T. Kiran and B. S. Rajan, "STBC-scheme with nonvanishing determinant for certain number of transmit antennas," *IEEE Trans. Info. Theory*, vol. 51, no. 8, pp. 2984–2992, Aug. 2005.
- [6] P. Elia, K. R. Kumar, S. A. Pawar, P. V. Kumar, and H.-F. Lu, "Explicit space-time codes achieving the diversity-multiplexing gain tradeoff," *IEEE Trans. Info. Theory*, vol. 52, no. 9, pp. 3869–3884, Sept. 2006.
- [7] G. Rekaya, J.-C. Belfiore, and E. Viterbo, "Algebraic $3 \times 3, 4 \times 4, 6 \times 6$ space-time codes with non-vanishing determinants," in *Proc. IEEE Int. Symp. Information Theory and its Applications*, Parma, Italy, Oct. 10-13 2004, pp. 325–329.
- [8] F. Oggier, G. Rekaya, J.-C. Belfiore, and E. Viterbo, "Perfect space time block codes," *IEEE Trans. Info. Theory*, vol. 52, no. 9, pp. 3885–3902, Sept. 2006.
- [9] J.-K. Zhang, G. Wang, and K. M. Wong, "Optimal norm form integer space-time codes for two antenna mimo systems," in *Proc. IEEE Int. Conf. Acoustic, Speech and Signal Processing*, Philadelphia, Mar. 18-23 2005.
- [10] G. Wang, J.-K. Zhang, Y. Zhang, and K. M. Wong, "Space-time code designs with non-vanishing determinant for three, four and six transmitter antennas," in *Proc. IEEE Int. Conf. Acoustic, Speech and Signal Processing*, Philadelphia, Mar. 18-23 2005.
- [11] P. Elia, B. A. Sethuraman, and P. V. Kumar, "Perfect space-time codes with minimum and non-minimum delay for any number of antennas," *arXiv:cs.IT/0512023 v1*, Dec. 2005.
- [12] P. V. Kumar, "Achieving the D-MG and DMD tradeoffs of MIMO fading channels," in *Proc. Information Theory and Application Workshop*, San Diego, Feb. 6-10 2006.
- [13] H. Liao, H. Wang, and X.-G. Xia, "Some designs and normalized diversity product upper bounds for lattice based diagonal and full rate space-time block codes," *preprint*, 2004.
- [14] H. Liao and X.-G. Xia, "Some designs of full rate space-time codes with non-vanishing determinant," *preprint*, Mar. 2006.
- [15] L. Zheng and D. Tse, "Diversity and multiplexing: A fundamental trade-off in multiple-antenna channels," *IEEE Trans. Info. Theory*, vol. 49, no. 5, pp. 1073–1096, Mar. 2003.
- [16] B. A. Sethuraman, B. S. Rajan, and V. Shashidhar, "Full-diversity, high-rate space-time block codes from division algebras," *IEEE Trans. Info. Theory*, vol. 49, no. 10, pp. 2596–2616, Oct. 2003.
- [17] J. H. M. Wedderburn, "A type of primitive algebra," *Trans. American Math. Soc.*, vol. 15, no. 2, pp. 162–166, Apr. 1914.
- [18] S. Lang, *Algebraic Number Theory*, 2nd ed., ser. Graduate Texts in Mathematics 110. New York: Springer-Verlag, 1994.
- [19] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., ser. Graduate Texts in Mathematics. New York: Springer-Verlag, 1990, vol. 83.
- [20] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*. New York: Dover, 1964.
- [21] J. J. Rotman, *Galois Theory*, 4th ed., ser. Graduate Texts in Mathematics. Springer-Verlag, 1999, vol. 148.
- [22] X. Guo, "A matlab search program," <http://www.ee.udel.edu/~guo/paper/codes.html>.
- [23] X. Guo and X.-G. Xia, "An elementary condition for non-norm elements," *preprint*, Dec. 2006.
- [24] W. Stein, *A Brief Introduction to Classical and Adelic Algebraic Number Theory*. Lecture Notes, 2004.
- [25] H. Cohen, *Resultants and Discriminants*. New York: Springer-Verlag, 1993.
- [26] D. A. Marcus, *Number Fields*. New York: Springer-Verlag, Jan. 1995.
- [27] J.-C. Belfiore and G. Rekaya, "Quaternionic lattices for space-time coding," in *Proc. IEEE Information Theory Workshop, Paris*, Mar. 31 - Apr. 4 2003, pp. 267–270.
- [28] P. Dayal and M. K. Varanasi, "An algebraic family of complex lattices for fading channels with application to space-time codes," *IEEE Trans. Info. Theory*, vol. 51, no. 12, pp. 4184–4202, Dec. 2005.
- [29] J. H. M. Wedderburn, "On division algebra," *Trans. American Math. Soc.*, vol. 22, no. 2, pp. 129–135, Apr. 1921.

TABLE II
THE MINIMAL POLYNOMIALS AND THEIR DISCRIMINANTS ASSOCIATED
WITH TABLE I

n	$m_\alpha(x)$	$\text{disc}(m_\alpha(x))$
2	$x^2 + x + 1$	-3
3	$x^3 + x^2 - 2x - 1$	49
4	$x^4 + x^3 + x^2 + x + 1$	125
5	$x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$	11^4
6	$x^6 + x^3 + 1$	-3^9
7	$x^7 + x^6 - 12x^5 - 7x^4$ $+28x^3 + 14x^2 - 9x + 1$	$17^2 \cdot 29^6$
8	$x^8 + x^7 - 7x^6 - 6x^5$ $+15x^4 + 10x^3 - 10x^2 - 4x + 1$	17^7
9	$x^9 + x^8 - 8x^7 - 7x^6 + 21x^5$ $+15x^4 - 20x^3 - 10x^2 + 5x + 1$	19^8
10	$x^{10} + x^9 + x^8 + x^7 + x^6 + x^5$ $+x^4 + x^3 + x^2 + x + 1$	-11^9
11	$x^{11} + x^{10} - 10x^9 - 9x^8$ $+36x^7 + 28x^6 - 56x^5 - 35x^4$ $+35x^3 + 15x^2 - 6x - 1$	23^{10}
12	$x^{12} + x^{11} + x^{10} + x^9 + x^8$ $+x^7 + x^6 + x^5 + x^4 + x^3$ $+x^2 + x + 1$	11^{13}
13	$x^{13} + x^{12} - 24x^{11} - 19x^{10}$ $+190x^9 + 116x^8 - 601x^7 - 246x^6$ $+738x^5 + 215x^4 - 291x^3$ $-68x^2 + 10x + 1$	$23^4 \cdot 53^{12}$ $\cdot 83^2 \cdot 317^2 \cdot 719^2$
14	$x^{14} + x^{13} - 13x^{12} - 12x^{11} + 66x^{10}$ $+55x^9 - 165x^8 - 120x^7 + 210x^6$ $+126x^5 - 126x^4 - 56x^3$ $+28x^2 + 7x - 1$	23^9
15	$x^{15} + x^{14} - 28x^{13} - 23x^{12}$ $+276x^{11} + 182x^{10} - 1193x^9$ $-592x^8 + 2307x^7 + 956x^6 - 1721x^5$ $-908x^4 + 316x^3 + 262x^2 + 42x + 1$	$11^{14} \cdot 61^{14} \cdot 599^2$
16	$x^{16} - x^{15} + x^{14} - x^{13} + x^{12} - x^{11}$ $+x^{10} - x^9 + x^8 - x^7 + x^6$ $-x^5 + x^4 - x^3 + x^2 - x + 1$	17^{15}
17	$x^{17} + x^{16} - 48x^{15} - 105x^{14} + 763x^{13}$ $+2579x^{12} - 3653x^{11} - 23311x^{10}$ $-11031x^9 + 74838x^8 + 107759x^7$ $-50288x^6 - 198615x^5 - 102976x^4$ $+58507x^3 + 75722x^2$ $+25763x + 2837$	$47^4 \cdot 103^{16}$ $\cdot 149^4 \cdot 983^2$ $\cdot 2677^2 \cdot 5413^2$
18	$x^{18} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13}$ $+x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7$ $+x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$	-19^{17}
19	$x^{19} + x^{18} - 90x^{17} - 57x^{16} + 3044x^{15}$ $+1124x^{14} - 51184x^{13} - 4822x^{12}$ $+474003x^{11} - 90110x^{10} - 2465084x^9$ $+1153239x^8 + 6854098x^7$ $-5023125x^6 - 8711114x^5$ $+8950277x^4 + 2600136x^3$ $-5125792x^2 + 1553447x - 117649$	$7^{52} \cdot 109^2 \cdot 191^{18}$ $\cdot 383^2 \cdot 389^2$ $\cdot 421^2 \cdot 431^2$ $\cdot 491^2 \cdot 1567^2$ $\cdot 9161^2 \cdot 6883^2$ $\cdot 1801^2$
20	$x^{20} + x^{15} + x^{10} + x^5 + 1$	5^{35}